IBM Security QRadar
Version 7.3.0

Guide d'utilisation

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 241.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.3.0 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

© Copyright IBM France 2016. Tous droits réservés.

© Copyright IBM Corporation 2012, 2017.

Table des matières

Avis aux lecteurs canadiens ix

A propos de ce guide xi

Chapitre 1. Nouveautés pour les utilisateurs de QRadar version 7.3.0 1

Chapitre 2. A propos de QRadar SIEM 3
Fonctions de votre produit Security Intelligence 3
Navigateurs Web pris en charge 4
Activation du mode document et du mode navigateur dans Internet Explorer 5
Connexion à IBM Security QRadar 5
Interface de programme d'application RESTful 6
Onglets d'interface utilisateur 7
Onglet Tableau de bord 7
Onglet Infractions 7
Onglet Activité du journal 8
Onglet Activité réseau 8
Onglet Actifs 8
Onglet Rapports 8
IBM Security QRadar Risk Manager 9
Onglet Admin 9
Procédures communes de QRadar 10
Affichage des messages 10
Tri de résultats 12
Actualisation et mise en pause de l'interface utilisateur 12
Analyse des adresses IP 13
Etude des noms d'utilisateurs 15
Heure système 15
Mise à jour des préférences utilisateur 15
Accès à l'aide en ligne 16
Redimensionnement des colonnes 16
Taille de page 17

Chapitre 3. Gestion du tableau de bord 19
Tableaux de bord par défaut 19
Tableaux de bord personnalisés 19
Personnalisation de votre tableau de bord 20
Recherche de flux 20
Infractions 21
Activité du journal 21
Rapports les plus récents 23
Récapitulatif système 23
Tableau de bord Surveillance des risques 23
Surveillance de la conformité aux règles 24
Surveillance des modifications de risques 26
Eléments de Gestion des vulnérabilités 27
Notification de système 27
Centre de documentation de menaces Internet 28
Création d'un tableau de bord personnalisé 29
Utilisation du tableau de bord pour analyser l'activité réseau ou de journal 29
Configuration des graphiques 30
Suppression d'éléments de tableau de bord 32
Détachement d'un élément de tableau de bord 32
Renommage d'un tableau de bord 32

© Copyright IBM Corp. 2012, 2017

Suppression d'un tableau de bord . . . 33
Gestion des notifications système . . . 33
Ajout d'éléments de tableau de bord basés sur des recherches à la liste Ajouter des articles . . . 33

Chapitre 4. Gestion des infractions . . . 35
Définition des priorités des infractions . . . 35
Chaînage des infractions . . . 36
Indexation des infractions . . . 36
Considérations sur l'indexation des infractions . . . 36
Exemple : Détection de l'apparition d'un logiciel malveillant à l'aide de la signature MD5 . . . 37
Conservation des infractions . . . 38
Protection des infractions . . . 38
Annulation de la protection des infractions . . . 39
Etude des infractions . . . 39
Sélection d'une infraction à examiner . . . 41
Examen d'une infraction à l'aide des informations récapitulatives . . . 42
Analyse d'événements . . . 47
Examen des flux . . . 48
Actions de gestion des infractions . . . 49
Ajout de remarques . . . 49
Masquage des infractions . . . 50
Affichage des infractions masquées . . . 50
Fermeture des infractions . . . 50
Exportation d'infractions . . . 51
Affectation d'infractions aux utilisateurs . . . 52
Envoi de notifications par e-mail . . . 53
Marquage d'une infraction pour suivi . . . 54

Chapitre 5. Étude de l'activité du journal . . . 55
Présentation de l'onglet Activité du journal . . . 55
Barre d'outils de l'onglet Activité du journal . . . 55
Options de menu contextuel . . . 60
Barre d'état . . . 61
Surveillance de l'activité du journal . . . 61
Affichage des événements de diffusion en flux . . . 61
Affichage des événements normalisés . . . 62
Affichage des événements bruts . . . 65
Affichage d'événements groupés . . . 67
Affichage des détails des événements . . . 72
Barre d'outils des détails d'événements . . . 76
Affichage des infractions associées . . . 77
Modification de mappage d'événement . . . 77
Réglage des faux positifs . . . 79
Données PCAP . . . 79
Affichage de la colonne de données PCAP . . . 80
Affichage des informations PCAP . . . 81
Téléchargement du fichier PCAP sur votre système de bureau . . . 81
Exportation d'événements . . . 82

Chapitre 6. Surveillance de l'activité réseau . . . 85
Présentation de l'onglet Activité réseau . . . 85
Barre d'outils de l'onglet Activité réseau . . . 85
Options du menu contextuel . . . 88
Barre d'état . . . 89
Enregistrements des dépassements . . . 89
Surveillance de l'activité réseau . . . 89
Affichage des flux en continu . . . 90
Affichage des flux normalisés . . . 90
Affichage des flux regroupés . . . 94
Détails de flux . . . 97

Barre d'outils des détails de flux . . . 101
Réglage des faux positifs . . . 101
Exportation de flux . . . 102

Chapitre 7. Gestion des actifs . . . 103
Sources des données d'actif . . . 104
Flux des données d'actifs entrantes . . . 106
Mises à jour des données d'actifs . . . 107
Règles d'exclusion de rapprochement d'actifs . . . 108
Exemple : règles d'exclusion d'actifs ajustées pour exclure des adresses IP de la liste noire . . . 109
Fusion d'actifs . . . 110
Identification des écarts de croissance d'actifs . . . 111
Notifications système indiquant des écarts de croissance d'actifs . . . 112
Exemple : comment les erreurs de configuration pour extensions de source de journal peuvent causer des écarts de croissance d'actifs . . . 112
Traitement des problèmes des profils d'actifs qui dépassent le seuil de taille normale . . . 113
De nouvelles données d'actifs sont ajoutées aux listes noires d'actifs . . . 114
Listes noires et listes blanches d'actifs . . . 114
Listes noires d'actifs . . . 115
Liste blanches d'actifs. . . . 115
Profils d'actifs . . . 116
Vulnérabilités . . . 117
Présentation de l'onglet Actifs . . . 117
Affichage d'un profil d'actif. . . . 118
Ajout ou édition d'un profil d'actif . . . 120
Recherche de profils d'actifs . . . 124
Sauvegarde des critères de recherche d'un actif . . . 125
Groupes de recherche d'actifs . . . 126
Affichage des groupes de recherche . . . 126
Création d'un groupe de recherche . . . 127
Edition d'un groupe de recherche. . . . 127
Copie d'une recherche sauvegardée vers un autre groupe. . . . 128
Suppression d'un groupe ou d'une recherche sauvegardée dans un groupe . . . 128
Tâches de gestion des profils d'actif . . . 128
Suppression des actifs . . . 129
Importation de profils d'actif . . . 129
Exportation des actifs. . . . 130
Recherche de vulnérabilités pour l'actif . . . 130

Chapitre 8. Gestion des graphiques . . . 135
Gestion des graphiques . . . 135
Présentation des graphiques de série temporelle . . . 136
Légendes des graphiques . . . 137
Configuration des graphiques . . . 138

Chapitre 9. Recherches . . . 141
Recherches d'événement et de flux . . . 141
Création d'une recherche personnalisée . . . 141
Création d'une présentation de colonne personnalisée . . . 147
Suppression d'une présentation de colonne personnalisée . . . 147
Sauvegarde des critères de recherche . . . 148
Recherche planifiée . . . 149
Options de recherches avancées . . . 150
Exemples de chaînes de recherche AQL . . . 152
Options de recherche du filtrage rapide . . . 156
Recherches d'infractions . . . 159
Recherche d'infractions dans les pages Mes Infractions et Toutes les infractions . . . 159
Recherche d'infractions dans la page Par adresse IP source . . . 167
Recherche d'infractions dans la page Par adresse IP de destination . . . 168
Recherche d'infractions dans la page Par réseau . . . 170

Sauvegarde de critères de recherche sur l'onglet **Infractions** . . . 171
Recherche d'infractions indexées sur une propriété personnalisée . . . 172
Recherche rapide des indicateurs de compromis avec la recherche flexible . . . 173
Suppression des critères de recherche . . . 174
Utilisation d'une sous-recherche pour affiner les résultats de recherche . . . 175
Gestion des résultats de recherche . . . 176
Annulation d'une recherche . . . 176
Suppression d'une recherche . . . 176
Gestion des groupes de recherche . . . 177
Affichage des groupes de recherche . . . 177
Création d'un groupe de recherche . . . 178
Edition d'un groupe de recherche. . . . 178
Copie d'une recherche sauvegardée vers un autre groupe. . . . 179
Suppression d'un groupe ou d'une recherche sauvegardée dans un groupe . . . 179
Exemple de recherche : Rapports quotidiens sur les employés . . . 179

Chapitre 10. Propriétés d'événementet de flux personnalisés . . . 181
Autorisations obligatoires . . . 181
Types de propriétés personnalisées . . . 181
Création d'une propriété personnalisée basée sur une expression régulière . . . 182
Création d'une propriété personnalisée basée sur le calcul . . . 185
Modification d'une propriété personnalisée . . . 187
Copie d'une propriété personnalisée. . . . 189
Suppression d'une propriété personnalisée . . . 189

Chapitre 11. Règles . . . 191
Règles personnalisées. . . . 192
Création d'une règle personnalisée . . . 194
Configuration d'un événement ou d'un flux en tant que faux positif . . . 199
Règles de détection des anomalies . . . 199
Création d'une règle de détection des anomalies. . . . 201
Configuration d'une réponse à la règle pour ajouter des données à une collecte de données de référence . . . 206
Edition d'éléments structurants . . . 208

Chapitre 12. Corrélation d'historique . . . 209
Présentation de la corrélation d'historique . . . 210
Création d'un profil de corrélation d'historique . . . 211
Affichage des informations relatives aux exécutions de corrélation d'historique . . . 212

Chapitre 13. Intégration de IBM X-Force . . . 215
Centre d'informations sur les menaces Internet - Widget du tableau de bord . . . 215
Application IBM Security Threat Content . . . 216
Activation des règles X-Force dans IBM Security QRadar . . . 216
Catégories d'adresses IP et d'URL . . . 217
Recherche d'informations sur les adresses IP et les URL dans X-Force Exchange . . . 217
Création d'une règle de catégorisation pour surveiller l'accès à certains types de site Web . . . 218
Facteur de fiabilité et réputation de l'adresse IP . . . 219
Réglage des faux positifs à l'aide de la définition du facteur de fiabilité . . . 219
Recherche de données dans IBM X-Force Exchange avec des critères de recherche avancés . . . 220

Chapitre 14. Gestion de rapports . . . 223
Présentation de rapport . . . 224
Types de graphique . . . 224
Barre d'outils de l'onglet Rapport. . . . 226
Types de graphique . . . 228
Création de rapports personnalisés . . . 229
Edition d'un rapport . . . 233
Affichage de rapports générés . . . 234
Suppression du contenu généré . . . 235
Génération manuelle d'un rapport . . . 235

Duplication d'un rapport 235
Partage d'un rapport 236
Personnalisation de rapports 236
Groupe de rapports 237
Création d'un groupe de rapports 237
Modification d'un groupe 238
Partage des groupes de rapports 238
Affectation d'un rapport à un groupe 239
Copie d'un rapport vers un autre groupe 240
Suppression d'un rapport 240

Remarques 241
Marques 243
Dispositions relatives à la documentation du produit 243
Déclaration IBM de confidentialité en ligne 244

Glossaire 245
A 245
C 245
D 246
E 246
F 246
G 247
H 247
I. 247
J. 247
L 247
M 248
N 248
O 249
P 249
R 249
S 250
T 251
V 251

Index 253

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

© Copyright IBM Corp. 2012, 2017

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de ce guide

Le guide d'utilisation d'IBM® Security QRadar fournit des informations sur la gestion d'IBM Security QRadar SIEM, notamment sur les onglets Tableau de bord, Infractions, Activité du journal, Activité réseau, Actifs et Rapports.

Utilisateurs concernés

Ce guide est destiné à tous les utilisateurs QRadar SIEM chargés de l'étude et de la gestion de la sécurité réseau. Il suppose que vous avez accès à QRadar SIEM et que vous maîtrisez votre réseau d'entreprise et les technologies réseau.

Documentation technique

Pour obtenir davantage de documentation technique, de notes technique et de notes sur l'édition, voir Accessing IBM Security QRadar Documentation (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Contacter le service clients

Pour contacter le service clients, voir Support and Download Technical Note (en anglais) (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Déclaration de pratiques de sécurité recommandées

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention par la détection et la réponse aux accès non autorisés depuis l'intérieur ou l'extérieur de votre entreprise. L'accès incorrect peut engendrer la modification, la destruction, le détournement la mauvaise utilisation des informations ou peut engendrer l'endommagement ou la mauvaise utilisation des systèmes, en particulier pour l'utilisation dans les attaques ou autres. Aucun système informatique ou produit ne doit être considéré comme entièrement sécurisé et aucun produit unique, service ou aucune mesure de sécurité ne peut être entièrement efficace dans la prévention d'une utilisation ou d'un accès incorrect. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produit ou services pour optimiser leur efficacité. IBM NE GARANTIT EN AUCUN CAS L'IMMUNITE DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITE DE VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLEGAL DE L'UNE DES PARTIES.

Remarque/Commentaire :

L'utilisation de ce programme peut impliquer différents lois ou réglementations, concernant notamment la confidentialité, la protection des données, l'emploi, ainsi que les communications électroniques et le stockage. IBM Security QRadar peut être utilisé uniquement de façon réglementaire. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à s'y conformer. Le détenteur de licence déclare qu'il détiendra ou qu'il a obtenu les agréments, les autorisations ou les licences nécessaires pour une utilisation réglementaire d'IBM Security QRadar.

© Copyright IBM Corp. 2012, 2017

Chapitre 1. Nouveautés pour les utilisateurs de QRadar version 7.3.0

IBM Security QRadar version 7.3.0 offre de nouvelles fonctionnalités aux utilisateurs des environnements à service partagé.

Les utilisateurs titulaires peuvent créer des propriétés personnalisées

Vous pouvez créer des propriétés personnalisées pour extraire ou calculer des informations importantes à partir des contenus de flux ou d'événement sans l'aide de votre administrateur de fournisseur de services de sécurité gérés (MSSP). Cette fonctionnalité vous permet de rechercher, d'afficher et de signaler des informations présentes dans les journaux et que QRadar ne normalise et n'affiche généralement pas.

Votre administrateur MSSP peut choisir d'optimiser des propriétés personnalisées fréquemment utilisées dans les règles et les rapports.

En savoir plus sur la création de propriétés d'événements et de flux personnalisées...

Les utilisateurs titulaires peuvent créer des collectes de données de référence

QRadar version 7.2.8 vous permet de consulter les données de référence créées par l'administrateur MSSP. Désormais, dans version 7.3.0, vous pouvez créer et gérer vous-même vos collectes de données de référence sans l'aide de l'administrateur MSSP.

Cette fonctionnalité permet de mettre à jour les listes de données auxquelles vous vous référez souvent, telles que des listes d'adresses IP ou de noms d'utilisateur, et d'utiliser ces données dans les recherches, les filtres, les conditions de test des règles et les réponses des règles de QRadar. Par exemple, un ensemble de références contenant une liste d'adresses URL interdites peut être utilisée pour empêcher les employés de consulter certains sites Web.

Pour que vous puissiez gérer les données de référence, l'administrateur MSSP doit donner à votre compte le rôle utilisateur **Administration déléguée** > **Gérer les données de référence**.

Pour en savoir plus sur la création et la gestion des collectes de données de référence, voir le manuel *IBM Security QRadar Administration Guide*.

© Copyright IBM Corp. 2012, 2017

Chapitre 2. A propos de QRadar SIEM

QRadar SIEM est une plateforme de gestion de la sécurité des réseaux offrant la prise en charge de la géolocalisation et de la conformité grâce à la combinaison de la connaissance de réseau de flux, de la corrélation des événements de sécurité et de l'évaluation de la vulnérabilité des actifs.

Clé de licence par défaut

Une clé de licence par défaut vous donne accès à l'interface utilisateur pour une durée de cinq semaines. Lorsque vous vous connectez à QRadar SIEM, une fenêtre affiche la date à laquelle la clé de licence temporaire expire. Pour plus d'informations sur l'installation d'une clé de licence, voir *IBM Security QRadar Administration Guide*.

Certificats et exceptions de sécurité

Si vous utilisez le navigateur Web Mozilla Firefox, vous devez ajouter une exception à Mozilla Firefox pour pouvoir vous connecter à QRadar SIEM. Pour plus d'informations, voir la documentation de votre navigateur Web Mozilla Firefox.

Si vous utilisez le navigateur Web Microsoft Internet Explorer, un message de certificat de sécurité de site Web s'affiche lorsque vous accédez au système QRadar SIEM. Vous devez sélectionner l'option **Poursuivre sur ce site Web** pour vous connecter à QRadar SIEM.

Accès à l'application Web

Lorsque vous utilisez QRadar SIEM, utilisez les options de navigation disponibles dans l'interface utilisateur de QRadar SIEM au lieu du bouton **Retour** de votre navigateur.

Fonctions de votre produit Security Intelligence

La documentation du produit de IBM Security QRadar décrit des fonctionnalités, notamment les infractions, les flux, les actifs et la corrélation d'historique, qui ne pas toujours disponibles dans les produits QRadar. Selon le produit que vous utilisez, certaines des fonctionnalités décrites peuvent ne pas être disponibles dans votre déploiement. Passez en revue les fonctions de chaque produit pour trouver les informations dont vous avez besoin.

IBM Security QRadar SIEM inclut la gamme complète de fonctions de renseignement de sécurité pour les déploiements sur site. QRadar SIEM consolide les données d'événement de source de journal à partir des noeuds finaux et des applications d'unité qui sont répartis au sein de votre réseau, puis il effectue une normalisation immédiate et des activités de corrélation sur les données brutes afin de distinguer les menaces réelles des faux positifs.

Utilisez IBM QRadar on Cloud pour collecter, analyser, archiver et stocker de gros volumes de données des journaux d'événements réseau et sécurité dans un environnement hébergé. Analysez vos données afin de permettre une visibilité des

© Copyright IBM Corp. 2012, 2017

menaces en cours de développement, et respectez les exigences de conformité en termes de surveillance et de génération de rapports, tout en réduisant votre coût total de possession.

Utilisez IBM QRadar Log Manager pour collecter, analyser, archiver et stocker de gros volumes de données des journaux d'événements réseau et sécurité. QRadar Log Manager analyse les données pour fournir une visibilité des menaces en cours de développement, et il peut vous aider à répondre aux exigences de conformité en termes de surveillance et de génération de rapports.

Si vous avez besoin d'aide, consultez le tableau suivant, qui répertorie les fonctions des produits :

Tableau 1. Comparaison des fonctions de QRadar

Fonctions	**QRadar SIEM**	**IBM QRadar on Cloud**	**IBM QRadar Log Manager**
Prend en charge les déploiements hébergés	Non	Oui	Non
Tableaux de bords personnalisables	Oui	Oui	Oui
Moteur de règles personnalisé	Oui	Oui	Oui
Gestion des événement réseau et des événements de sécurité	Oui	Oui	Oui
Gestion des hôte et des journaux d'application	Oui	Oui	Oui
Alertes basées sur les seuils	Oui	Oui	Oui
Modèles de conformité	Oui	Oui	Oui
Archivage des données	Oui	Oui	Oui
intégration de flux de réputation IP IBM Security X-Force Threat Intelligence	Oui	Oui	Oui
Déploiements autonomes WinCollect	Oui	Oui	Oui
Déploiements gérés par WinCollect	Oui	Non	Oui
Intégration de QRadar Vulnerability Manager	Oui	Non	Oui
Surveillance de l'activité réseau	Oui	Non	Non
Profilage d'actif	Oui	Oui	Non [1]
Gestion des infractions	Oui	Oui	Non
Capture et analyse du flux réseau	Oui	Non	Non
Corrélation d'historique	Oui	Oui	Non
Intégration de QRadar Risk Manager	Oui	Non	Non
Intégration de QRadar Incident Forensics	Oui	Non	Non
[1] QRadar Log Manager effectue un suivi des données d'actif uniquement si QRadar Vulnerability Manager est installé.			

Navigateurs Web pris en charge

Pour que les fonctions des produits IBM Security QRadar fonctionnent correctement, vous devez utiliser un navigateur Web pris en charge.

Lorsque vous accédez au système QRadar, vous êtes invité à entrer un nom d'utilisateur et un mot de passe. Les noms d'utilisateur et mot de passe doivent être configurés à l'avance par l'administrateur.

Le tableau ci-après répertorie les versions de navigateurs web pris en charge.

Tableau 2. Navigateurs Web pris en charge par les produits QRadar

Navigateur Web	**Versions prises en charge**
Mozilla Firefox	45.2 Extended Support Release
Microsoft Internet Explorer 64 bits avec le mode Microsoft Edge activé.	11.0
Google Chrome	54 et 55

Activation du mode document et du mode navigateur dans Internet Explorer

Si vous utilisez Microsoft Internet Explorer pour accéder aux produits IBM Security QRadar, vous devez activer les modes navigateur et document.

Procédure

1. Dans votre navigateur Web Internet Explorer, appuyez sur F12 pour ouvrir la fenêtre des outils de développement.
2. Cliquez sur **Mode navigateur** et sélectionnez la version de votre navigateur Web.
3. Cliquez sur **Document Mode** et sélectionnez **Internet Explorer standards** pour votre version d'Internet Explorer.

Connexion à IBM Security QRadar

IBM Security QRadar est une application Web. QRadar utilise les informations de connexion par défaut pour l'URL, le nom d'utilisateur et le mot de passe.

Utilisez les informations du tableau suivant lorsque vous vous connectez à votre console IBM Security QRadar.

Tableau 3. Informations de connexion par défaut de QRadar

Informations de connexion	**Par défaut**
URL	https://<Adresse IP>, où <Adresse IP> correspond à l'adresse IP de la console QRadar. Pour vous connecter à QRadar dans un environnement IPv6 ou mixte, placez l'adresse IP entre crochets : `https://[<adresse IP>]`
Nom d'utilisateur	admin
Mot de passe	Mot de passe attribué à QRadar lors du processus d'installation.
Clé de licence	Une clé de licence par défaut vous donne accès à l'interface utilisateur pour une durée de cinq semaines.

Interface de programme d'application RESTful

Utilisez l'interface de programme d'application (API) REST (Representational State Transfer) pour créer des requêtes HTTPS et intégrer IBM Security QRadar à d'autres solutions.

Accès et droits d'accès de rôle utilisateur

Vous devez posséder des droits associés au rôle d'administrateur dans QRadar pour accéder et utiliser les API RESTful. Pour plus d'informations sur la gestion des droits associés au rôle d'administrateur, voir le *IBM Security QRadar Administration Guide*.

Accès à l'interface utilisateur de la documentation technique de l'API REST

L'interface utilisateur de l'API fournit des descriptions et des fonctions pour les interfaces d'API REST suivantes :

Tableau 4. Interfaces d'API REST

API REST	Description
`/api/ariel`	Interroge les bases de données, les recherches, les ID de recherche et les résultats de recherche.
`/api/asset_model`	Renvoie une liste de tous les actifs du modèle. Vous pouvez également afficher une liste de toutes les recherches sauvegardées et de tous les types de propriétés d'actifs disponibles et mettre à jour un actif.
`/api/auth`	Déconnecte et invalide la session en cours.
`/api/help`	Renvoie une liste des fonctions de l'API.
`/api/siem`	Renvoie une liste de toutes les infractions.
`/api/qvm`	Renvoie et gère les données IBM Security QRadar Vulnerability Manager.
`/api/reference_data`	Affiche et gère les collectes de données de référence.
`/api/qvm`	Extrait les actifs, les vulnérabilités, les réseaux, les services ouverts et les filtres. Vous pouvez également créer ou mettre à jour des tickets de rattrapage.
`/api/scanner`	Affiche, crée ou démarre une analyse distante associée à un profil d'analyse.

L'interface de la documentation technique de l'API REST fournit une infrastructure que vous pouvez utiliser pour collecter le code requis pour implémenter des fonctions QRadar dans d'autres produits.

1. Entrez l'adresse URL suivante dans votre navigateur Web pour accéder à l'interface de la documentation technique : `https://`*`AdresseIPconsole`*`/api_doc`.
2. Cliquez sur l'en-tête de l'API auquel vous souhaitez accéder, par exemple **/ariel**.
3. Cliquez sur la sous en-tête du point de terminaison auquel vous souhaitez accéder, par exemple **/databases**.
4. Cliquez sur la sous en-tête Experimental ou Provisional.

Remarque :

Les points de terminaison de l'API sont annotés en tant que *experimental* ou *stable*.

Experimental
Indique que le point de terminaison de l'API est susceptible de ne pas être entièrement testé et qu'il risque d'être modifié ou supprimé sans préavis à l'avenir.

Stable Indique que le point de terminaison de l'API est entièrement testé et pris en charge.

5. Cliquez sur **Try it out** pour recevoir des réponses HTTPS correctement formatées.
6. Examinez et collectez les informations que vous avez besoin d'implémenter dans votre solution tierce.

Forum d'API et exemples de code QRadar

Le forum d'API fournit des informations supplémentaires sur l'API REST, ainsi que des réponses aux questions fréquentes et des exemples de codes annotés que vous pouvez utiliser dans un environnement test. Pour plus d'informations, voir le forum d'API (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca).

Onglets d'interface utilisateur

La fonctionnalité se compose de différents onglets. L'onglet **Tableau de bord** s'affiche lorsque vous vous connectez.

Vous pouvez facilement naviguer sur les onglets pour localiser les données ou les fonctionnalités requises.

Onglet Tableau de bord

L'onglet **Tableau de bord** est l'onglet par défaut qui s'affiche lorsque vous vous connectez.

L'onglet **Tableau de bord** fournit un environnement d'espace de travail prenant en charge plusieurs tableaux de bord sur lesquels vous pouvez afficher vos vues de sécurité des réseaux, d'activité ou de données collectées par QRadar. Cinq tableaux de bord par défaut sont disponibles. Chaque tableau de bord contient des éléments qui fournissent un récapitulatif et des informations détaillées concernant les infractions qui surviennent sur votre réseau. Vous pouvez également créer un tableau de bord personnalisé pour vous permettre de vous concentrer sur les responsabilités de vos opérations de sécurité et de réseau. Pour en savoir plus sur l'utilisation de l'onglet Tableau de bord, consultez la section Gestion des tableaux de bord.

Onglet Infractions

L'onglet **Infractions** vous permet d'afficher les infractions qui se produisent sur votre réseau, que vous pouvez localiser à l'aide des diverses options de navigation ou grâce aux recherches avancées.

L'onglet **Infractions** vous permet d'étudier une infraction afin de déterminer la cause première d'un problème. Vous pouvez également résoudre le problème.

Pour plus d'informations sur l'onglet **Infractions** voir Gestion des infractions.

Onglet Activité du journal

L'onglet **Activité du journal** vous permet d'étudier les journaux d'événements envoyés à QRadar en temps réel, d'effectuer des recherches avancées et d'afficher l'activité du journal à l'aide de graphiques de séries temporelles configurables.

L'onglet **Activité du journal** vous permet d'effectuer des études approfondies sur les données d'événements.

Pour plus d'informations, voir Etude de l'activité du journal.

Onglet Activité réseau

L'onglet **Activité réseau** vous permet d'étudier les flux envoyés en temps réel, d'effectuer des recherches efficaces et d'afficher l'activité réseau à l'aide des graphiques de série temporelle configurables.

Un flux est une session de communication entre deux hôtes. L'affichage des informations sur le flux vous permet de déterminer comment le trafic est communiqué, ce qui est communiqué (si l'option de capture de contenu est activée) et qui effectue la communication. Les données de flux contiennent également les détails tels que les protocoles, les valeurs ASN, les valeurs IFIndex et les priorités.

Pour plus d'informations, voir Surveillance de l'activité réseau.

Onglet Actifs

QRadar détecte automatiquement les actifs, serveurs et hôtes fonctionnant sur votre réseau.

La détection automatique repose sur des données de flux passifs et des données de vulnérabilité, permettant à QRadar de générer un profil d'actif.

Les profils d'actif fournissent des informations sur chaque actif connu de votre réseau, y compris les informations d'identité, le cas échéant, ainsi que les services s'exécutant sur chaque actif. Ces données de profil sont utilisées à des fins de comparaison, ce qui permet de réduire le nombre de faux positifs.

Par exemple, une attaque tente d'utiliser un service spécifique qui s'exécute sur un actif spécifique. Dans ce cas, QRadar peut déterminer si l'actif est vulnérable à cette attaque en comparant l'attaque au profil d'actif. L'onglet **Actifs** vous permet d'afficher les actifs étudiés ou de rechercher des actifs spécifiques afin d'afficher leurs profils.

Onglet Rapports

L'onglet **Rapports** vous permet de créer, distribuer et gérer des rapports pour toutes les données au sein de QRadar.

La fonction Rapports vous permet de créer des rapports personnalisés pour une utilisation de fonctionnement et d'exécution. Afin de créer un rapport, vous pouvez combiner les informations (telles que celles de sécurité ou de réseau) au sein d'un seul rapport. Vous pouvez également utiliser les modèles de rapport préinstallés fournis avec QRadar.

L'onglet **Rapports** vous permet d'apposer une marque à vos rapports avec des logos personnalisés. Cette personnalisation est intéressante pour la distribution de rapports auprès d'audiences différentes.

Pour plus d'informations sur les rapports, voir Gestion des rapports.

IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager est un dispositif installé séparément permettant de contrôler les configurations des périphériques, de simuler les changements apportés à votre environnement réseau et de classer les risques et les vulnérabilités par ordre de priorité sur votre réseau.

IBM Security QRadar Risk Manager utilise les données collectées par les données de configuration provenant des dispositifs de réseau et de sécurité, tels que les pare-feux, les routeurs, les commutateurs ou les systèmes de prévention contre les intrusions (IPS), les flux de vulnérabilité et les sources de sécurité du fournisseur. Ces données sont utilisées pour identifier les risques associés à la sécurité, à la stratégie et à la conformité au sein de votre infrastructure de sécurité réseau et la probabilité de ces risques exploités.

Remarque : Pour plus d'informations sur IBM Security QRadar Risk Manager, contactez votre représentant commercial.

Onglet Admin

Les administrateurs utilisent l'onglet Admin pour configurer et gérer les utilisateurs, les systèmes, les réseaux, les plug-ins, ainsi que les composants. Les utilisateurs dotés de privilèges d'administration peuvent accéder à l'onglet **Admin**.

Les outils d'administration auxquels les administrateurs peuvent avoir accès dans l'onglet **Admin** sont décrits dans Table 1.

Tableau 5. Outils de gestion d'administration disponibles dans QRadar

Outil d'administration	Description
Configuration du système	Options de configuration du système et de gestion d'utilisateur.
Sources de données	Options de configuration des sources de journal, des sources de flux et de vulnérabilité.
Configuration de réseaux distants et de services	Configuration de réseaux distants et de groupes de services.
Editeur de déploiement	Gestion des composants individuels de votre déploiement QRadar.

Toutes les mises à jour de configuration effectuées dans l'onglet **Admin** sont enregistrées dans une zone de transfert. Lorsque tous les changements sont complets, vous pouvez déployer les mises à jour de configuration pour l'hôte géré dans votre déploiement.

Procédures communes de QRadar

Plusieurs commandes de l'interface utilisateur QRadar sont communes à la plupart des onglets de l'interface.

Ces procédures communes sont décrites dans les sections ci-après.

Affichage des messages

Le menu **Messages**, qui se trouve dans le coin supérieur droit de l'interface utilisateur, permet d'accéder à une fenêtre dans laquelle vous pouvez lire et gérer vos notifications système.

Avant de commencer

Pour afficher les notifications système dans la fenêtre **Messages**, l'administrateur doit créer une règle basée sur chaque type de message de notification et cocher la case **Envoyer une notification** dans **Assistant de règles personnalisées**.

Pourquoi et quand exécuter cette tâche

Le menu **Messages** indique le nombre de notifications système non lues présentes dans votre système. Cet indicateur incrémente le nombre jusqu'à la fermeture des notifications système. Pour chaque notification système, la fenêtre **Messages** fournit un récapitulatif et l'horodatage déterminant le moment auquel la notification système a été créée. Vous pouvez placer le pointeur de la souris sur une notification pour afficher davantage de détails. Les fonctions de la fenêtre **Messages** vous permettent de gérer les notifications système.

Les notifications système sont également disponibles dans l'onglet **Tableau de bord** et sur une fenêtre en incrustation facultative qui peut être affichée dans le coin inférieur gauche de l'interface utilisateur. Les actions que vous effectuez dans la fenêtre **Messages** sont étendues à l'onglet **Tableau de bord** et à la fenêtre en incrustation. Par exemple, si vous fermez une notification système à partir de la fenêtre **Messages**, la notification système est supprimée de tous les écrans de notification système.

Pour plus d'informations sur les notifications système dans l'onglet Tableau de bord, voir Elément Notifications système.

La fenêtre **Messages** propose les fonctions suivantes :

Tableau 6. Fonctions disponibles dans la fenêtre Messages

Fonction	Description
Tout	Cliquez sur **Tout** pour afficher toutes les notifications système. Cette option est définie par défaut. Par conséquent, cliquez sur **Tout** uniquement si vous avez sélectionné une autre option et que vous souhaitez afficher à nouveau toutes les notifications système.
Etat de santé	Cliquez sur **Etat de santé** pour afficher uniquement les notifications système possédant un niveau de gravité Health.

Tableau 6. Fonctions disponibles dans la fenêtre Messages (suite)

Fonction	Description
Erreurs	Cliquez sur **Erreurs** pour afficher uniquement les notifications système possédant un niveau de gravité Error.
Avertissements	Cliquez sur **Avertissements** pour afficher uniquement les notifications système possédant un niveau de gravité Warning.
Information	Cliquez sur **Information** pour afficher uniquement les notifications système possédant un niveau de gravité Information.
Ignorer tout	Cliquez sur **Ignorer tout** pour fermer toutes les notifications système de votre système. Si vous avez filtré la liste des notifications système à l'aide des icônes **Etat de santé**, **Erreurs**, **Avertissements** ou **Information**, le texte de l'icône **Afficher tout** est remplacé par l'une des options suivantes : • **Ignorer toutes les erreurs** • **Ignorer tous les états de santé** • **Ignorer tous les avertissements** • **Ignorer tous les avertissements** • **Ignorer toutes les informations**
Afficher tout	Cliquez sur **Afficher tout** pour afficher les événements de notification système dans l'onglet **Activité du journal**. Si vous avez filtré la liste des notifications système à l'aide des icônes **Etat de santé**, **Erreurs**, **Avertissements** ou **Information**, le texte de l'icône **Afficher tout** est remplacé par l'une des options suivantes : • **Afficher toutes les erreurs** • **Afficher tous les états de santé** • **Afficher tous les avertissements** • **Afficher toutes les informations**
Ignorer	Cliquez sur l'icône **Ignorer** en regard d'une notification système pour fermer la notification système à partir de votre système.

Procédure

1. Connectez-vous à QRadar.
2. Dans le coin supérieur droit de l'interface utilisateur, cliquez sur **Messages**.
3. Dans la fenêtre **Messages**, affichez les détails de notification système.
4. Facultatif. Pour affiner la liste des notifications système, cliquez sur l'une des options suivantes :
   - **Erreurs**
   - **Avertissements**
   - **Information**
5. Facultatif. Pour fermer les notifications système, choisissez l'une des options suivantes :

Option	Description
Ignorer tout	Cliquez ici pour fermer toutes les notifications système.
Ignorer	Cliquez sur l'icône **Ignorer** en regard de la notification système que vous souhaitez fermer.

6. Facultatif. Pour afficher les détails de la notification système, placez le pointeur de la souris sur la notification système.

Tri de résultats

Vous pouvez trier les résultats des tables en cliquant sur un en-tête de colonne. Une flèche au dessus de la colonne indique l'ordre du tri.

Procédure

1. Connectez-vous à QRadar.
2. Cliquez une fois sur l'en-tête de colonne pour trier la table dans l'ordre décroissant ; cliquez deux fois pour trier la table dans l'ordre croissant.

Actualisation et mise en pause de l'interface utilisateur

Vous pouvez actualiser manuellement, mettre en pause et lire les données affichées sur les onglets.

Onglet Tableau de bord
L'onglet **Tableau de bord** s'actualise automatiquement toutes les 60 secondes. Le minuteur, situé dans l'angle supérieur droit de l'interface, indique le temps restant avant l'actualisation automatique de l'onglet.

Cliquez sur la barre de titre de n'importe que élément de tableau de bord pour mettre automatiquement en pause la durée avant d'actualisation. Le minuteur clignote en rouge pour indiquer que l'affichage en cours est en pause.

Onglets Activité du journal et Activité réseau
Les onglets **Activité du journal** et **Activité réseau** s'actualisent automatiquement toutes les 60 secondes si vous affichez l'onglet en mode Dernier intervalle (actualisation automatique).

Lorsque vous visualisez l'onglet **Activité du journal** ou **Activité réseau** en mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), vous pouvez utiliser l'icône **Pause** pour mettre en pause l'affichage actuel.

Onglet Infractions
L'onglet **Infractions** doit être actualisé manuellement. Le minuteur, situé dans l'angle supérieur droit de l'interface, indique le temps écoulé depuis la dernière actualisation des données. Le minuteur clignote en rouge lorsqu'il est en pause.

Procédure

1. Connectez-vous à QRadar.
2. Cliquez sur l'onglet que vous voulez afficher.
3. Sélectionnez l'une des options suivantes :

Option	Description
Actualiser	Cliquez sur **Actualiser**, dans le coin droit de l'onglet, pour actualiser celui-ci.
Pause	Cliquez sur cette option pour mettre en pause l'affichage de l'onglet.
Play	Cette option permet de redémarrer le minuteur après sa mise en pause.

Analyse des adresses IP

Il existe plusieurs méthodes permettant d'analyser les informations sur les adresses IP des onglets Tableau de bord, Activité du journal et Activité réseau.

Procédure

1. Connectez-vous à QRadar.
2. Cliquez sur l'onglet que vous voulez afficher.
3. Placez le pointeur de votre souris sur une adresse IP pour visualiser l'emplacement de l'adresse IP.
4. Cliquez avec le bouton droit de la souris sur l'adresse IP ou sur le nom de l'actif et sélectionnez l'une des options suivantes :

Tableau 7. Informations sur les adresses IP

Option	Description
Naviguer > **Afficher par réseau**	Affiche les réseaux associés à l'adresse IP sélectionnée.
Naviguer > **Afficher le récapitulatif de la source**	Affiche les infractions associées à l'adresse IP source sélectionnée.
Naviguer > **Afficher le récapitulatif de la destination**	Affiche les infractions associées à l'adresse IP de destination sélectionnée.
Information > **Recherche DNS**	Recherche les entrées DNS basées sur l'adresse IP
Information > **Recherche WHOIS**	Recherche le propriétaire enregistré d'une adresse IP distante. Le serveur WHOIS par défaut est whois.arin.net.
Information > **Analyse du port**	Effectue une analyse Network Mapper (NMAP) de l'adresse IP sélectionnée. Cette option est disponible uniquement si NMAP est installé sur votre système. Pour plus d'informations sur l'installation de NMAP, consultez la documentation de votre vendeur.

Tableau 7. Informations sur les adresses IP (suite)

Option	Description
Information > **Profil d'actif**	Affiche les informations relatives au profil de l'actif. Cette option s'affiche si IBM Security QRadar Vulnerability Manager a été acheté et mis sous licence. Pour plus d'informations, voir *IBM Security QRadar Vulnerability Manager - Guide d'utilisation*. Cette option de menu est uniquement disponible si QRadar a acquis les données de profil activement via une analyse ou passivement via des sources de flux. Pour plus d'informations, voir *IBM Security QRadar Administration Guide*.
Information > **Recherche d'événements**	Recherche les événements associés à cette adresse IP.
Information > **Recherche de flux**	Recherche les flux associés à cette adresse IP.
Information > **Rechercher des connexions**	Recherche les connexions associées à cette adresse IP. Cette option s'affiche uniquement si vous avez acheté et mis IBM Security QRadar Risk Manager sous licence et connecté QRadar et le dispositif IBM Security QRadar Risk Manager. Pour plus d'informations, voir *IBM Security QRadar Risk Manager - Guide d'utilisation*.
Information > **Switch Port Lookup**	Détermine le port de commutation sur un périphérique Cisco IOS lié à cette adresse IP. Cette option s'applique uniquement aux commutateurs reconnus à l'aide de l'option de **reconnaissance d'unités** sur l'onglet **Risques**. **Remarque :** Cette option de menu n'est pas disponible dans QRadar Log Manager
Information > **Afficher la topologie**	Affiche l'onglet **Risques**, qui décrit la topologie de couche 3 de votre réseau. Cette option est disponible si vous avez acheté et mis IBM Security QRadar Risk Manager sous licence et connecté QRadar et le dispositif IBM Security QRadar Risk Manager.
Exécuter une analyse de vulnérabilité	Sélectionnez l'option **Exécuter une analyse de vulnérabilité** pour exécuter une analyse d'IBM Security QRadar Vulnerability Manager sur cette adresse IP. Cette option s'affiche uniquement si IBM Security QRadar Vulnerability Manager a été acheté et mis sous licence. Pour plus d'informations, voir *IBM Security QRadar Vulnerability Manager - Guide d'utilisation*.

Etude des noms d'utilisateurs

Vous pouvez cliquer avec le bouton droit de la souris sur le nom d'utilisateur pour accéder à plusieurs options de menu. Utilisez ces options pour afficher plus d'informations sur le nom d'utilisateur ou l'adresse IP.

Pour pouvoir étudier les noms d'utilisateurs, vous devez avoir acheté et mis IBM Security QRadar Vulnerability Manager sous licence. Pour plus d'informations, voir le *IBM Security QRadar Vulnerability Manager - Guide d'utilisation*.

Vous pouvez sélectionner les options de menu suivantes en faisant un clic droit sur le nom d'utilisateur.

Tableau 8. Options de menu pour étudier le nom d'utilisateur

Option	Description
Afficher les actifs	Affiche les actifs en cours qui sont associés au nom d'utilisateur sélectionné.
Afficher l'historique de l'utilisateur	Affiche tous les actifs associés au nom d'utilisateur sélectionné au cours des dernières 24 heures.
Afficher les événements	Affiche les événements associés au nom d'utilisateur sélectionné. Pour plus d'informations sur la fenêtre Liste d'événements, voir Surveillance de l'activité du journal.

Pour plus d'informations sur la personnalisation du menu contextuel, voir le manuel *IBM Security QRadar Administration Guide* de votre produit.

Heure système

Le coin droit de l'interface utilisateur QRadar affiche l'heure système, qui correspond à l'heure de la console.

L'heure de la console synchronise les systèmes QRadar lors du déploiement de QRadar. L'heure de la console est utilisée pour déterminer l'heure de réception des événements à partir d'autres dispositifs pour une corrélation correcte de la synchronisation de l'heure.

Dans un déploiement réparti, la console peut se trouver dans un fuseau horaire différent de celui de votre ordinateur de bureau.

Lorsque vous appliquez des filtres et des recherches basés sur le temps aux onglets **Activité du journal** et **Activité réseau**, vous devez utiliser l'heure système de la console pour spécifier un intervalle.

Lorsque vous appliquez des filtres et des recherches basés sur le temps à l'onglet **Activité du journal**, vous devez utiliser l'heure système de la console pour spécifier un intervalle.

Mise à jour des préférences utilisateur

Vous pouvez définir vos préférences utilisateur (environnement local, par exemple) dans l'interface utilisateur IBM Security QRadar SIEM principale.

Procédure

1. Pour accéder à vos informations utilisateur, cliquez sur **Préférences**.
2. Mettez à jour vos préférences.

Option	Description
Nom d'utilisateur	Affiche votre nom d'utilisateur. Vous ne pouvez pas éditer cette zone.
Mot de passe	Les mots de passe utilisateur QRadar sont stockés sous forme de chaîne SHA-256 cryptée. Le mot de passe doit répondre aux critères suivants : • Doit contenir au minimum 6 caractères • Doit contenir au maximum 255 caractères • Contient au moins un caractère spécial • Contient un caractère en majuscules
Mot de passe (confirmation)	Confirmation du mot de passe
Adresse e-mail	L'adresse e-mail doit répondre aux conditions suivantes : • Doit contenir au minimum 10 caractères • Doit contenir au maximum 255 caractères
Environnement local	QRadar est disponible dans les langues suivantes : anglais, chinois simplifié, chinois traditionnel, japonais, coréen, français, allemand, italien, espagnol, russe et portugais (brésilien). Si vous choisissez une langue différente, l'interface utilisateur s'affiche en anglais. D'autres conventions culturelles associées, comme le type de caractère, le classement, le format de date et heure, l'unité monétaire sont utilisées.
Activer les notifications en incrustation	Sélectionnez cette case si vous souhaitez activer les notifications système contextuelles à afficher sur votre interface utilisateur.

Accès à l'aide en ligne

Vous pouvez accéder à l'aide en ligne de QRadar via l'interface utilisateur QRadar principale.

Pour avoir accès à l'aide en ligne, cliquez sur **Aide** > **Menu de l'aide**.

Redimensionnement des colonnes

Vous pouvez redimensionner les colonnes sur plusieurs onglets dans QRadar.

Placez le pointeur de votre souris sur la ligne qui sépare les colonnes et glissez le bord de la colonne vers le nouvel emplacement. Vous pouvez également redimensionner les colonnes en cliquant deux fois sur la ligne qui sépare les colonnes pour redimensionner automatiquement la colonne sur la largeur de la zone la plus grande.

Remarque : Le redimensionnement des colonnes ne fonctionne pas dans les navigateurs Web Microsoft Internet Explorer, Version 7.0 lorsque les onglets affichent des enregistrements en mode de diffusion en flux.

Taille de page

Les utilisateurs dotés de privilèges d'administration peuvent configurer le nombre maximal de résultats s'affichant dans les tableaux sur plusieurs onglets de QRadar.

Chapitre 3. Gestion du tableau de bord

L'onglet **Tableau de bord** correspond à la vue par défaut lorsque vous vous connectez.

Il fournit un environnement d'espace de travail qui prend en charge plusieurs tableaux de bord sur lesquels vous pouvez afficher vos vues de sécurité des réseaux, d'activité ou de données collectées.

Les tableaux de bord vous permettent d'organiser vos éléments de tableaux de bord en vues fonctionnelles vous permettant de vous concentrer sur des zones spécifiques de votre réseau.

Utilisez l'onglet Tableau de bord pour surveiller le comportement de vos événements de sécurité.

Vous pouvez personnaliser votre tableau de bord. Le contenu affiché dans l'onglet **Tableau de bord** représente un utilisateur spécifique. Les changements effectués dans une session affectent uniquement votre système.

Tableaux de bord par défaut

Le tableau de bord par défaut permet de personnaliser vos éléments en vues fonctionnelles. Ces vues fonctionnelles concernent des zones spécifiques de votre réseau.

L'onglet **Tableau de bord** fournit cinq tableaux de bord par défaut axés sur la sécurité, l'activité réseau, l'activité des applications, la surveillance du système et la conformité.

Chaque tableau de bord affiche un ensemble par défaut d'éléments de tableau de bord. Les éléments du tableau de bord agissent comme un point de départ pour accéder à des données plus détaillées. Le tableau suivant définit les tableaux de bord par défaut.

Tableaux de bord personnalisés

Vous pouvez personnaliser vos tableaux de bord. Le contenu affiché dans l'onglet **Tableau de bord** représente un utilisateur spécifique. Les changements effectués dans une session QRadar affectent votre système uniquement.

Pour personnaliser votre onglet **Tableau de bord**, vous pouvez effectuer les tâches suivantes :

- Créer des tableaux de bord personnalisés adaptés à vos responsabilités. Le nombre maximal est de 255 tableaux de bord par utilisateur ; toutefois, des problèmes de performance peuvent se produire si vous créez plus de 10 tableaux de bord.
- Ajouter et supprimer des éléments de tableau de bord à partir des tableaux de bord personnalisés ou par défaut.
- Déplacer et positionner des éléments selon vos besoins. Lorsque vous positionnez des éléments, chaque élément est automatiquement redimensionné selon les proportions du tableau de bord.

© Copyright IBM Corp. 2012, 2017

- Ajouter des éléments de tableau de bord personnalisés qui reposent sur n'importe quelles données.

Par exemple, vous pouvez ajouter un élément de tableau de bord qui fournit un graphique de séries temporelles ou un graphique à barres qui représente les 10 activités réseau principales.

Pour créer des éléments personnalisés, vous pouvez créer des recherches sauvegardées sur les onglets **Activité du journal** ou **Activité réseau** et choisir comment vous souhaitez que les résultats soient représentés dans votre tableau de bord. Chaque tableau de bord affiche les données actualisées en temps réel. Les graphiques de séries temporelles sur le tableau de bord sont actualisés toutes les 5 minutes.

Personnalisation de votre tableau de bord

Vous pouvez ajouter plusieurs éléments de tableau de bord à vos tableaux de bord par défaut ou personnalisés.

Vous pouvez personnaliser vos tableaux de bord pour afficher et organiser les éléments de tableau de bord qui répondent aux exigences de sécurité de votre réseau.

Il existe 5 tableaux de bord par défaut, auxquels vous pouvez accéder à partir de la zone de liste **Afficher le tableau de bord** sur l'onglet **Tableau de bord**. Si vous avez précédemment consulté un tableau de bord avant de retourner à l'onglet **Tableau de bord**, le dernier tableau de bord consulté s'affiche.

Recherche de flux

Vous pouvez personnaliser un élément de tableau de bord qui repose des critères de recherche enregistrés à partir de l'onglet **Activité réseau**.

Des éléments de recherche de flux figurent dans le menu **Ajouter un article** > **Activité réseau** > **Recherches de flux**. Le nom de l'élément de recherche de flux correspond au nom des critères de recherche enregistrés sur lequel l'élément est basé.

Les critères de recherche enregistrés par défaut sont disponibles et préconfigurés pour afficher les éléments de recherche de flux dans votre menu d'onglet **Tableau de bord**. Vous pouvez ajouter des éléments de tableau de bord de recherche de flux supplémentaires dans votre menu d'onglet **Tableau de bord**. Pour plus d'informations, voir Ajout d'éléments de tableau de bord basés sur des recherches à la liste Ajouter des articles.

Sur un élément de tableau de bord de recherche de flux, les résultats de recherche affichent des données actualisées en temps réel sur un graphique. Les types de graphiques pris en charge sont des séries temporelles, des tableaux, des graphiques circulaires et des graphiques à barres. Le type de graphique par défaut est le graphique à barres. Ces graphiques sont configurables. Pour plus d'informations sur la configuration des graphiques, voir Configuration des graphiques.

Les graphiques de série temporelle sont interactifs. En utilisant des graphiques de série temporelle, vous pouvez agrandir et analyser un calendrier pour étudier l'activité réseau.

Infractions

Vous pouvez ajouter plusieurs éléments liés à l'infraction dans votre tableau de bord.

Remarque : Les infractions masquées ou fermées ne sont pas incluses dans les valeurs affichées dans l'onglet **Tableau de bord**. Pour plus d'informations sur les événements masqués ou fermés, voir Gestion des infractions.

Le tableau suivant décrit les éléments d'infraction :

Tableau 9. Eléments d'infraction

Eléments de tableau de bord	Description
Infractions les plus récentes	Les cinq infractions les plus récentes sont identifiées par une barre d'amplitude pour vous signifier leur importance. Pointez votre souris sur le nom de l'infraction pour afficher des informations détaillées sur l'adresse IP.
Infractions les plus graves	Les cinq infractions les plus graves sont identifiées par une barre d'amplitude pour vous signifier leur importance. Pointez votre souris sur le nom de l'infraction pour afficher des informations détaillées sur l'adresse IP.
Mes Infractions	L'élément **Mes Infractions** affiche les cinq infractions les plus récentes qui vous sont affectées. Les infractions sont identifiées par une barre d'amplitude pour vous informer de leur importance. Pointez votre souris sur l'adresse IP pour afficher des informations détaillées sur cette dernière.
Principales sources	L'élément **Principales sources** affiche les principales sources d'infraction. Chaque source est identifiée par une barre d'amplitude pour vous informer de son importance. Pointez votre souris sur l'adresse IP pour afficher des informations détaillées sur cette dernière.
Destinations locales principales	L'élément **Destinations locales principales** affiche les principales destinations locales. Chaque destination est identifiée par une barre d'amplitude pour vous informer de son importance. Pointez votre souris sur l'adresse IP pour afficher des informations détaillées sur cette dernière.
Catégories	L'élément **Types de catégories principaux** affiche les cinq principales catégories associées au plus grand nombre d'infractions.

Activité du journal

Les éléments de tableau de bord **Activité du journal** vous permettent de surveiller et d'étudier des événements en temps réel.

Remarque : Les événements masqués ou fermés ne sont pas inclus dans les valeurs affichées dans l'onglet **Tableau de bord**.

Tableau 10. Eléments de l'activité du journal

Elément de tableau de bord	Description
Recherches d'événements	Vous pouvez afficher un élément de tableau de bord personnalisé qui est basé sur des critères de recherche enregistrés à partir de l'onglet Activité du journal. Des éléments de recherche d'événements figurent dans le menu **Ajouter un article** > **Activité réseau** > **Recherches d'événements**. Le nom de l'élément de recherche d'événements correspond au nom des critères de recherche enregistrés sur lequel l'élément est basé. QRadar inclut les critères de recherche enregistrés par défaut qui sont préconfigurés pour afficher les éléments de recherche d'événements dans votre menu d'onglet **Tableau de bord**. Vous pouvez ajouter d'autres éléments de tableau de bord de recherche d'événements dans votre menu d'onglet **Tableau de bord**. Pour plus d'informations, voir Ajout d'éléments de tableau basés sur la recherche à la liste Ajout d'éléments. Sur un élément du tableau de bord, **Activité du journal**, les résultats de recherche affichent des données de dernière minute en temps réel sur un graphique. Les types de graphiques pris en charge sont la série temporelle, le tableau, le graphique circulaire et la barre. Le type de graphique par défaut est le graphique à barres. Ces graphiques sont configurables. Les graphiques de série temporelle sont interactifs. Vous pouvez agrandir et parcourir un calendrier linéaire pour étudier l'activité du journal.
Evénements par gravité	L'élément de tableau de bord **Evénements par gravité** affiche le nombre d'événements actifs regroupés par ordre de gravité. Cet élément vous permettra de voir le nombre d'événements reçus par le niveau de gravité qui a été attribué. La gravité indique le niveau de menace créé par une source d'infraction par rapport à la préparation de la destination à l'attaque. La plage de gravité est de 0 (faible) à 10 (élevé). Les types de graphiques pris en charge sont le tableau, le graphique circulaire et le graphique à barres.

Tableau 10. Eléments de l'activité du journal (suite)

Elément de tableau de bord	Description
Principales sources de journal	L'élément de tableau de bord **Principales sources de journal** affiche les 5 principales sources de journal ayant envoyé des événements à QRadar au cours des 5 dernières minutes. Le nombre d'événements envoyés à partir de la source de journal spécifiée est indiqué dans le graphique circulaire. Cet élément vous permet de visualiser des changements potentiels dans le comportement, par exemple, si une source du journal pare-feu qui n'est généralement pas dans la liste des 10 principales sources contribue actuellement à un grand pourcentage du comptage de message global, vous devriez étudier cette occurrence. Les types de graphiques pris en charge sont le tableau, le graphique circulaire et le graphique à barres.

Rapports les plus récents

L'élément de tableau de bord **Rapports les plus récents** affiche les premiers rapports récemment générés.

L'affichage fournit le titre du rapport, l'heure et la date auxquelles il a été généré ainsi que son format.

Récapitulatif système

L'élément de tableau de bord **Récapitulatif du système** fournit un récapitulatif de haut niveau de l'activité au cours des dernières 24 heures.

Dans la rubrique récapitulative, vous pouvez afficher les informations suivantes :

- **Flux en cours par seconde** - Indique le débit par seconde.
- **Flux (dernières 24 heures)** - Indique le nombre total de flux actifs observés au cours des dernières 24 heures.
- **Evénements en cours par seconde** - Indique le débit d'événements par seconde.
- **Nouveaux événements (dernières 24 heures)** - Indique le nombre total de nouveaux événements reçus au cours des dernières 24 heures.
- **Infractions mises à jour (dernières 24 heures)** - Indique le nombre total d'infractions qui ont été créées ou modifiées avec de nouvelles preuves au cours des dernières 24 heures.
- **Taux de réduction des données** - Indique le rapport de réduction de données en fonction du total d'événements détectés et du nombre d'infractions modifiées au cours des dernières 24 heures.

Tableau de bord Surveillance des risques

Vous pouvez utiliser le tableau de bord **Surveillance des risques** pour surveiller les risques des règles et les modifications apportées à ces risques pour les actifs, les règles et les groupes de règles.

Par défaut, le tableau de bord **Surveillance des risques** affiche les éléments **Risque** et **Modification du risque** qui surveillent le score de risque des règles des actifs dans les groupes de règles Vulnérabilité élevée, Vulnérabilité moyenne et Vulnérabilité élevée, ainsi que les taux de conformité et les modifications d'historique dans le groupe de règles CIS.

Les éléments du tableau de bord Surveillance des risques n'affichent aucun résultat si IBM Security QRadar Risk Manager n'est pas sous licence. Pour plus d'informations, voir le guide d'utilisation de QRadar Risk Manager.

Pour afficher le tableau de bord **Surveillance des risques** par défaut, sélectionnez **Afficher le tableau de bord** > **Surveillance des risques** sur l'onglet **Tableau de bord**.

Tâches associées:

«Surveillance de la conformité aux règles»
Vous pouvez créer un élément de tableau de bord indiquant les pourcentages de conformité aux règles et le score de risque des règles pour des actifs, des règles et des groupes de règles sélectionnés.

«Surveillance des modifications de risques», à la page 26
Vous pouvez créer un élément de tableau de bord pour indiquer une modification du risque des règles pour des actifs, des règles et des groupes de règles sélectionnés, de façon quotidienne, hebdomadaire ou mensuelle.

Surveillance de la conformité aux règles

Vous pouvez créer un élément de tableau de bord indiquant les pourcentages de conformité aux règles et le score de risque des règles pour des actifs, des règles et des groupes de règles sélectionnés.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Dans la barre d'outils, cliquez sur **Nouveau tableau de bord**.
3. Entrez un nom et une description pour votre tableau de bord Conformité des règles.
4. Cliquez sur **OK**.
5. Dans la barre d'outils, sélectionnez **Ajouter un article** > **Gestionnaire de risques** > **Risque**.

   Les éléments du tableau de bord **Gestionnaire de risques** s'affichent uniquement lorsque IBM Security QRadar Risk Manager est sous licence.
6. Dans l'en-tête du nouvel élément de tableau de bord, cliquez sur l'icône jaune **Paramètres**.
7. Utilisez les listes **Type de graphique**, **Afficher les meilleurs** et **Tri** pour configurer le graphique.
8. Dans la liste **Groupe**, sélectionnez le groupe que vous souhaitez surveiller. Pour plus d'informations, reportez-vous à l'étape 9 du tableau.

   Lorsque vous sélectionnez l'option **Actif**, un lien vers la page **Risques** > **Gestion des règles** > **Par actif** apparaît au base de l'élément du tableau de bord **Risque**. La page **Par actif** affiche plus d'informations détaillées sur tous les résultats renvoyés pour le **Groupe des règles** sélectionné. Pour plus d'informations sur un actif spécifique, sélectionnez **Tableau** dans la liste **Type de graphique** et cliquez sur le lien dans la colonne **Actif** pour afficher les détails de l'actif dans la page **Par actif**.

Lorsque vous sélectionnez l'option **Règle**, un lien vers la page **Risques** > **Gestion des règles** > **Par règle** apparaît au bas de l'élément du tableau de bord **Risque**. La page **Par règle** affiche des informations détaillées sur tous les résultats renvoyés pour le **Groupe de règles**. Pour plus d'informations sur une règle, sélectionnez **Tableau** dans la liste **Type de graphique** et cliquez sur le lien de la colonne **Règle** pour afficher les détails concernant la règle dans la page **Par règle**.

9. Dans la liste **Graphique**, sélectionnez le type de graphique que vous souhaitez utiliser. Pour plus d'informations, voir le tableau suivant :

Groupe	Pourcentage d'actifs transmis	Pourcentage de règles transmises	Pourcentage de groupes de règles transmis	Score de risque des règles
Tous	Renvoie le pourcentage moyen d'actifs transmis parmi les actifs, les règles et le groupe de règles.	Renvoie le pourcentage moyen de vérifications de règles transmises parmi les actifs, les règles et le groupe de règles.	Renvoie le pourcentage moyen de groupes de règles transmis parmi les actifs, les règles et le groupe de règles.	Renvoie le score moyen de risque des règles parmi tous les actifs, les règles et le groupe de règles.
Actif	Indique si un actif a réussi le test de conformité (100%=réussite, 0%=échec). Utilisez ce paramètre pour montrer quels actifs associés à un groupe de règles réussissent le test de conformité.	Renvoie le pourcentage de vérifications de règles ayant réussi pour un actif. Utilisez ce paramètre pour afficher le pourcentage de vérifications de règles ayant réussi pour chaque actif associé au Groupe de règles.	Renvoie le pourcentage de sous-groupes de règles associés à l'actif ayant réussi le test de conformité.	Renvoie la somme de toutes les valeurs de coefficients d'importance pour les questions de règles associées à chaque actif. Utilisez ce paramètre pour afficher le risque des règles de chaque actif associé à un groupe de règle sélectionné.
Règle	Indique si tous les actifs associés à chaque règle dans un groupe de règles réussissent le test de conformité. Utilisez ce paramètre pour surveiller si tous les actifs associés à chaque règle d'un groupe de règles réussissent ou non le test de conformité.	Renvoie le pourcentage des vérifications de règles réussissant le test de conformité par règle dans le groupe de règles. Utilisez ce paramètre pour surveiller combien de vérifications de règles échouent par règle.	Renvoie le pourcentage de sous-groupes de règles dont la règle fait partie, réussissant le test de conformité.	Renvoie les valeurs du coefficient d'importance pour chaque question de règle dans le groupe Règles. Utilisez ce paramètre pour afficher le coefficient d'importance de chaque règle dans un groupe de règles.

Groupe	Pourcentage d'actifs transmis	Pourcentage de règles transmises	Pourcentage de groupes de règles transmis	Score de risque des règles
Groupe de règles	Renvoie le pourcentage d'actifs réussissant le test de conformité pour le groupe de règles sélectionné dans son ensemble.	Renvoie le pourcentage de vérifications de règles réussissant le test de conformité par règle pour le groupe de règles dans son ensemble.	Renvoie le pourcentage de sous-groupes de règles appartenant au groupe de règles, réussissant le test de conformité.	Renvoie la somme de toutes les valeurs de coefficients d'importance de toutes les questions de règles du groupe de règles.

10. Dans la liste **Groupe de règles**, sélectionnez les groupes de règles que vous souhaitez surveiller.
11. Cliquez sur **Sauvegarder**.

Surveillance des modifications de risques

Vous pouvez créer un élément de tableau de bord pour indiquer une modification du risque des règles pour des actifs, des règles et des groupes de règles sélectionnés, de façon quotidienne, hebdomadaire ou mensuelle.

Pourquoi et quand exécuter cette tâche

Utilisez cet élément de tableau de bord pour comparer les modifications des valeurs de Score de risque des règles, Vérification de règle et Règles pour un groupe de règles dans le temps.

L'élément de tableau de bord **Modification du risque** utilise des flèches pour indiquer les risques de règles ayant augmenté, diminué ou stagné pour les valeurs sélectionnées, au cours d'une période choisie :

- Le nombre situé en dessous de la flèche rouge indique les valeurs dont le risque a augmenté.
- Le nombre situé en dessous des flèches grises indique les valeurs présentant un risque identique.
- Le nombre situé en dessous de la flèche verte indique les valeurs dont le risque a diminué.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Dans la barre d'outils, cliquez sur **Nouveau tableau de bord**.
3. Entrez un nom et une description pour votre tableau de bord Conformité aux règles historique.
4. Cliquez sur **OK**.
5. Sur la barre d'outils, sélectionnez **Ajouter un article** > **Gestionnaire de risques** > **Modification du risque**.

   Les éléments du tableau de bord **Gestionnaire de risques** s'affichent uniquement lorsque IBM Security QRadar Risk Manager est sous licence.
6. Dans l'en-tête du nouvel élément de tableau de bord, cliquez sur l'icône jaune **Paramètres**.

7. Dans la liste **Groupe de règles**, sélectionnez les groupes de règles que vous souhaitez surveiller.
8. Sélectionnez une option dans la liste **Valeur à comparer** :
   - Si vous souhaitez afficher les modifications cumulées par facteur d'importance pour toutes les questions de règles des groupes de règles sélectionnés, sélectionnez **Score de risque des règles**.
   - Si vous souhaitez voir combien de vérifications de règles ont été modifiées dans les groupes de règles sélectionnés, sélectionnez **Vérifications de règle**.
   - Si vous souhaitez voir combien de règles ont été modifiées dans les groupes de règles sélectionnés, sélectionnez **Règles**.
9. Sélectionnez la période de modification des risques que vous souhaitez surveiller dans la liste **Intervalle delta** :
   - Si vous souhaitez comparer les modifications des risques entre aujourd'hui 12h00 et hier, sélectionnez **Jour**.
   - Si vous souhaitez comparer les modifications des risques entre lundi 12h00 de cette semaine et la semaine dernière, sélectionnez **Semaine**.
   - Si vous souhaitez comparer les modifications des risques entre le premier jour du mois à 12h00 et le mois antérieur, sélectionnez **Mois**.
10. Cliquez sur **Sauvegarder**.

Eléments de Gestion des vulnérabilités

Les éléments de tableau de bord Gestion des vulnérabilités s'affichent uniquement si vous achetez et mettez sous licence IBM Security QRadar Vulnerability Manager.

Pour plus d'informations, voir le *IBM Security QRadar Vulnerability Manager - Guide d'utilisation*.

Vous pouvez afficher un élément de tableau de bord personnalisé en fonction des critères de recherche sauvegardés à partir de l'onglet **Vulnérabilités**. Les éléments de recherche sont répertoriés dans le menu **Ajouter un article** > **Gestion des vulnérabilités** > **Recherche de vulnérabilités**. Le nom de l'élément de recherche correspond au nom des critères de recherche sauvegardés sur lesquels l'élément est basé.

QRadar inclut les critères de recherche enregistrés par défaut qui sont préconfigurés pour afficher les éléments de recherche dans votre menu d'**onglet Tableau de bord**. Vous pouvez ajouter d'autres éléments de tableau de bord de recherche dans le menu de votre onglet **Tableau de bord**.

Les types de graphiques pris en charge sont le diagramme à barres, le graphique circulaire et le tableau. Par défaut, le diagramme à barres est utilisé. Ces graphiques sont configurables.

Notification de système

L'élément de tableau de bord Notification système affiche des notifications d'événements reçues par votre système.

Pour que les notifications s'affichent dans l'élément de tableau de bord **Notification système**, l'administrateur doit créer une règle basée sur chaque type de message de notification et sélectionner la case **Envoyer une notification** dans l'assistant de règles personnalisées.

Pour plus d'informations sur la configuration des notifications d'événement et la création de règles d'événements, voir *IBM Security QRadar Administration Guide*.

Sur l'élément de tableau de bord **Notifications système**, vous pouvez afficher les informations suivantes :

- **Indicateur** - Affiche un symbole pour indiquer le niveau de gravité de la notification. Pointez vers le symbole pour afficher plus de détails sur le niveau de gravité.
  - Icône **Etat de santé**
  - Icône **Information** (?)
  - Icône **Erreur** (X)
  - Icône **Avertissement** (!)
- **Créé** - Indique la durée qui s'est écoulée depuis la création de la notification.
- **Description** - Indique les informations sur la notification.
- **Ignorer l'icône (x)** - Permet de fermer une notification du système.

Vous pouvez pointer votre souris sur la notification pour afficher plus de détails :

- **IP hôte** - Indique l'adresse IP de l'hôte qui a créé la notification.
- **Gravité** - Indique le niveau de gravité de l'incident qui a créé cette notification.
- **Catégorie de niveau inférieur** - Indique la catégorie associée à l'incident qui a généré cette notification. Par exemple : Interruption du service.
- **Contenu** - Indique le contenu qui est associé à l'incident qui a généré cette notification.
- **Créé** - Indique la durée qui s'est écoulée depuis la création de la notification.

Lorsque vous ajoutez l'élément de tableau de bord **Notifications système**, les notifications de système peuvent également s'afficher comme des notifications contextuelles dans l'interface utilisateur QRadar. Ces notifications contextuelles sont affichées sur le coin droit inférieur de l'interface utilisateur, quel que soit l'onglet sélectionné.

Les notifications contextuelles ne sont disponibles que pour les utilisateurs ayant des droits d'administration et sont activées par défaut. Pour désactiver les notifications contextuelles, sélectionnez **Préférences utilisateur** et décochez la case **Activer les notifications en incrustation**.

Dans la fenêtre contextuelle Notifications système, le nombre de notifications dans la file d'attente est mis en évidence. Par exemple, si (1 à 12) est affiché dans l'en-tête, la notification en cours indique de 1 sur 12 notifications à afficher.

La fenêtre contextuelle Notification système offre les options suivantes :

- **Icône Suivant (>)** - Affiche le message de notification suivant. Par exemple, si le message de notification actuel est de 3 sur 6, cliquez sur l'icône pour afficher 4 sur 6.
- **Icône Fermer (X)** - Ferme la fenêtre contextuelle de cette notification.
- **(détails)** - Affiche des informations supplémentaires concernant cette notification de système.

Centre de documentation de menaces Internet

L'élément de tableau de bord du centre de documentation de menaces Internet est un flux RSS intégré qui vous fournit des mises à jour des recommandations sur les

questions de sécurité, des évaluations de menaces quotidiennes, des informations en matière de sécurité et des référentiels de menace.

Le diagramme Niveau de menace en cours indique le niveau de la menace actuelle et fournit un lien vers la page Current Internet Threat Level du site Web IBM Internet Security Systems.

Les recommandations en cours sont répertoriées dans l'élément de tableau de bord. Pour voir un récapitulatif de la recommandation, cliquez sur la **Flèche** à côté de la recommandation. La recommandation se déploie pour afficher un récapitulatif. Cliquez à nouveau sur la **Flèche** pour masquer le récapitulatif.

Pour étudier l'intégralité de la recommandation, cliquez sur le lien associé. Le site Web IBM Internet Security Systems s'ouvre dans une autre fenêtre du navigateur et affiche les détails de l'intégralité de la recommandation.

Création d'un tableau de bord personnalisé

Vous pouvez créer un tableau de bord personnalisé pour afficher un groupe d'éléments de tableau de bord répondant à une exigence spécifique.

Pourquoi et quand exécuter cette tâche

Une fois le tableau de bord personnalisé créé, il apparaît dans l'onglet **Tableau de bord** et est répertorié dans la zone de liste **Afficher le tableau de bord**. Un nouveau tableau de bord personnalisé est vide par défaut. Par conséquent, vous devez y ajouter des éléments.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Cliquez sur l'icône **Nouveau tableau de bord**.
3. Dans la zone **Nom**, entrez un nom unique pour le tableau de bord. La longueur maximale est de 65 caractères.
4. Dans la zone **Description**, entrez la description du tableau de bord. La longueur maximale est de 255 caractères. Cette description s'affiche dans l'infobulle du nom du tableau de bord dans la zone de liste **Afficher le tableau de bord**.
5. Cliquez sur **OK**.

Utilisation du tableau de bord pour analyser l'activité réseau ou de journal

Les éléments de tableau de bord basés sur la recherche fournissent un lien vers les onglets **Activité du journal** ou **Activité réseau**.

Pourquoi et quand exécuter cette tâche

Pour analyser les flux à partir d'un élément de tableau de bord **Activité du journal** :

1. Cliquez sur le lien **Afficher dans Activité du journal**. L'onglet **Activité du journal** s'affiche et présente les résultats et deux graphiques correspondant aux paramètres de votre élément de tableau de bord.

Pour analyser les flux à partir d'un élément de tableau de bord **Activité réseau** :

1. Cliquez sur le lien **Afficher dans Activité réseau**. L'onglet Activité réseau s'affiche et présente les résultats et deux graphiques correspondant aux paramètres de votre élément de tableau de bord.

L'onglet **Activité réseau** s'affiche et présente les résultats et deux graphiques correspondant aux paramètres de votre élément de tableau de bord. Les types de graphique affichés sur l'onglet **Activité du journal** ou **Activité réseau** dépendent du graphique qui est configuré dans l'élément de tableau de bord :

Type de graphique	Description
A barres, circulaire et en tableau	L'onglet **Activité du journal** ou **Activité réseau** affiche un graphique à barres, un graphique circulaire et un tableau contenant les détails de flux.
Séries temporelles	L'onglet **Activité du journal** ou **Activité réseau** affiche des graphiques en fonction des critères suivants : 1. Si votre intervalle est inférieur ou égal à 1 heure, un graphique de série temporelle, un graphique à barres et une table avec les détails d'événement ou de flux sont affichés. 2. Si votre intervalle est supérieur à 1 heure, un graphique de série temporelle s'affiche et vous êtes invité à cliquer sur Mettre à jour les détails. Cette action démarre la recherche qui remplit les détails d'événement ou de flux et génère le graphique à barres. Une fois la recherche terminée, le graphique à barres et le tableau avec les détails d'événement ou de flux sont affichés.

Configuration des graphiques

Vous pouvez configurer des éléments de tableau de bord **Activité du journal**, **Activité réseau** et **Connexions**, si applicable, pour spécifier le type de graphique et le nombre d'objets de données à afficher.

Pourquoi et quand exécuter cette tâche

Tableau 11. Configuration de graphiques. Options de paramètres.

Option	Description
Valeur vers graphique	Dans la zone de liste, sélectionnez le type d'objet que vous voulez représenter sur le graphique. Les options comprennent tous les paramètres d'événements ou de flux normalisés et personnalisés inclus dans vos paramètres de recherche.

Tableau 11. Configuration de graphiques (suite). Options de paramètres.

Option	Description
Type de graphique	Dans la zone de liste, sélectionnez le type de graphique que vous souhaitez afficher. Ces options incluent : 1. **Graphique à barres** - Affiche les données dans un diagramme à barres. Cette option est uniquement disponible pour les événements ou flux regroupés. 2. **Graphique à secteurs** - Affiche les données dans un graphique circulaire. Cette option est uniquement disponible pour les événements ou flux regroupés. 3. **Table** - Affiche les données dans un tableau. Cette option est uniquement disponible pour les événements ou flux regroupés. 4. **Série temporelle** - Affiche un graphique à courbes interactif qui représente les enregistrements mis en correspondance selon un intervalle de temps spécifié.
Afficher les meilleurs	Dans la zone de liste, sélectionnez le nombre d'objets que vous voulez afficher dans le graphique. Ces options incluent **5** et **10**. La valeur par défaut est **10**.
Capture des données de séries temporelles	Cochez cette case pour activer la capture de série temporelle. Lorsque vous sélectionnez cette option, la fonction de graphique comment à accumuler des données pour les graphiques de série temporelle. Cette option est désactivée par défaut.
Intervalle	Dans la zone de liste, sélectionnez l'intervalle de temps que vous souhaitez afficher.

Les configurations personnalisées de vos graphiques sont conservées de telle sorte qu'ils s'affichent selon la configuration à chaque fois que vous accédez à l'onglet **Tableau de bord**.

Les données sont cumulées de sorte que lorsque vous exécutez une recherche sauvegardée de série temporelle, il existe une mémoire cache des données d'événements ou de flux disponibles pour afficher les données relatives à la période précédente. Les paramètres accumulés sont indiqués par un astérisque (*) dans la zone de liste **Valeur vers graphique**. Si vous sélectionnez une valeur pour un graphique qui n'est pas cumulée (sans astérisque), les données de série temporelle ne sont pas disponibles.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Dans la zone de liste **Afficher le tableau de bord**, sélectionnez le tableau de bord qui contient l'élément que vous souhaitez personnaliser.
3. Sur l'en-tête de l'élément du tableau de bord que vous souhaitez configurer, cliquez sur l'icône **Paramètres**.
4. Configurez les paramètres de graphique.

Suppression d'éléments de tableau de bord

Vous pouvez supprimer des éléments d'un tableau de bord et y ajouter les éléments à nouveau à tout moment.

Pourquoi et quand exécuter cette tâche

Lorsque vous supprimez un élément du tableau de bord, il n'est pas supprimé complètement.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Dans la zone de liste **Afficher le tableau de bord**, sélectionnez le tableau de bord à partir duquel vous souhaitez supprimer un élément.
3. Sur l'en-tête de l'élément de tableau de bord, cliquez sur l'icône [x] rouge pour supprimer l'élément du tableau de bord.

Détachement d'un élément de tableau de bord

Vous pouvez détacher un élément de votre tableau de bord et l'afficher dans une nouvelle fenêtre de votre système de bureau.

Pourquoi et quand exécuter cette tâche

Lorsque vous détachez un élément de tableau de bord, l'élément de tableau de bord d'origine reste dans l'onglet **Tableau de bord**, mais une fenêtre détachée avec un doublon d'élément de tableau de bord reste ouverte et s'actualise lors d'intervalles planifiés. Si vous fermez l'application QRadar, la fenêtre détachée reste ouverte pour la surveillance et continue de s'actualiser jusqu'à ce que vous la fermiez manuellement ou que vous arrêtiez votre système informatique.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Dans la zone de liste **Afficher le tableau de bord**, sélectionnez le tableau de bord à partir duquel vous souhaitez détacher un élément.
3. Dans l'en-tête de l'élément de tableau de bord, cliquez sur l'icône verte pour détacher l'élément de tableau de bord et l'ouvrir dans une autre fenêtre.

Renommage d'un tableau de bord

Vous pouvez renommer un tableau de bord et mettre à jour la description.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Dans la zone de liste **Afficher le tableau de bord**, sélectionnez le tableau de bord que vous souhaitez éditer.
3. Dans la barre d'outils, cliquez sur l'icône **Renommer le tableau de bord**.
4. Dans la zone **Nom**, entrez un nouveau nom pour le tableau de bord. La longueur maximale est de 65 caractères.
5. Dans la zone **Description**, saisissez une nouvelle description du tableau de bord. La longueur maximale est de 255 caractères.
6. Cliquez sur **OK**.

Suppression d'un tableau de bord

Vous pouvez supprimer un tableau de bord.

Pourquoi et quand exécuter cette tâche

Une fois qu'un tableau de bord est supprimé, l'onglet **Tableau de bord** s'actualise et le premier tableau de bord répertorié dans la zone de liste **Afficher le tableau de bord** apparaît. Le tableau de bord que vous avez supprimé n'apparaît plus dans la zone de liste **Afficher le tableau de bord**.

Procédure

1. Cliquez sur l'onglet **Tableau de bord**.
2. Dans la zone de liste **Afficher le tableau de bord**, sélectionnez le tableau de bord que vous souhaitez supprimer.
3. Dans la barre d'outils, cliquez sur **Supprimer le tableau de bord**.
4. Cliquez sur **Oui**.

Gestion des notifications système

Vous pouvez indiquer le nombre de notifications que vous souhaitez afficher sur votre élément de tableau de bord **Notification système** et fermer les notifications système une fois que vous les avez lues.

Avant de commencer

Assurez-vous que l'élément de tableau de bord **Notification système** a été ajouté à votre tableau de bord.

Procédure

1. Dans l'en-tête de l'élément de tableau de bord Notification système, cliquez sur l'icône **Paramètres**.
2. Dans la zone de liste **Afficher**, sélectionnez le nombre de notifications système que vous souhaitez afficher.
   - Les options sont les suivantes : **5**, **10** (valeur par défaut), **20**, **50** et **Tout**.
   - Pour afficher toutes les notifications système connectées dans les dernières 24 heures, cliquez sur **Tout**.
3. Pour fermer une notification système, cliquez sur l'icône **Supprimer**.

Ajout d'éléments de tableau de bord basés sur des recherches à la liste Ajouter des articles

Vous pouvez ajouter des éléments de tableau de bord basés sur des recherches à votre menu **Ajouter des articles**.

Avant de commencer

Pour ajouter un élément de tableau de bord de recherche de flux et d'événement au menu **Ajouter un article** de l'onglet **Tableau de bord**, vous devez accéder à l'onglet **Activité du journal** ou **Activité réseau** pour créer des critères de recherche permettant de définir l'affichage des résultats de la recherche sur l'onglet **Tableau de bord**. Les critères de recherche doivent également préciser que les résultats sont regroupés sur un paramètre.

Procédure

1. Choisissez l'un des éléments suivants :
   - Pour ajouter un élément de tableau de bord de recherche de flux, cliquez sur l'onglet **Activité réseau**.
   - Pour ajouter un élément de tableau de bord de recherche d'événement, cliquez sur l'onglet **Activité du journal**.
2. Dans la zone de liste **Rechercher**, sélectionnez l'une des options suivantes :
   - Pour créer une recherche, sélectionnez **Nouvelle recherche**.
   - Pour éditer une recherche sauvegardée, sélectionnez **Editer la recherche**.
3. Configurez ou éditez vos paramètres de recherche, si nécessaire.
   - Dans le volet Editer la recherche, sélectionnez l'option **Inclure dans mon tableau de bord**.
   - Dans le volet Définition de colonne, sélectionnez une colonne et cliquez sur l'icône **Ajouter une colonne** pour déplacer la colonne vers la liste **Grouper par**.
4. Cliquez sur **Filtrer**. Les résultats de la recherche s'affichent.
5. Cliquez sur **Sauvegarder les critères**. Voir Enregistrement de critères de recherche dans l'onglet Infraction
6. Cliquez sur **OK**.
7. Vérifiez que vos critères de recherche sauvegardés ont correctement ajouté l'élément de tableau de bord de recherche de flux ou d'événement à la liste **Ajouter des articles**.
   a. Cliquez sur l'onglet **Tableau de bord**.
   b. Sélectionnez une des options suivantes :
   a. Pour contrôler un élément de recherche d'événement, sélectionnez **Ajouter un article** > **Activité du journal** > **Recherches d'événements** > **Ajouter un article**.
   b. Pour contrôler un élément de recherche de flux, sélectionnez **Ajouter un article** > **Activité réseau** > **Recherches de flux**. L'élément de tableau de bord s'affiche dans la liste et utilise le même nom que vos critères de recherche sauvegardés.

Chapitre 4. Gestion des infractions

IBM Security QRadar réduit des milliards d'événements et de flux en un nombre gérable d'infractions à résoudre, qui sont classées en fonction de leur impact sur l'activité commerciale. Utilisez l'onglet **Infractions** pour accéder facilement à toutes les données dont vous avez besoin pour comprendre les menaces même les plus complexes.

En apportant un contexte immédiat à l'infraction, QRadar vous permet d'identifier rapidement quelles infractions sont les plus importantes et de commencer un examen pour trouver la source de l'attaque de sécurité ou de la violation de règle suspectée.

Restriction : Vous ne pouvez pas gérer des infractions dans IBM QRadar Log Manager. Pour plus d'informations sur les différences entre IBM Security QRadar SIEM et IBM QRadar Log Manager, voir «Fonctions de votre produit Security Intelligence», à la page 3.

Définition des priorités des infractions

L'indice de magnitude d'une infraction est une mesure de l'importance de l'infraction dans votre environnement. IBM Security QRadar utilise l'indice de magnitude pour affecter des priorités aux infractions et vous aider à déterminer quelles infractions doivent être examinées en premier.

L'*indice de magnitude* d'une infraction est calculée en fonction de la pertinence, de la gravité et de la crédibilité.

- La *pertinence* détermine l'impact de l'infraction sur votre réseau. Par exemple, si un port est ouvert, la pertinence est élevée.
- La *crédibilité* indique l'intégrité de l'infraction telle que déterminée par l'indice de crédibilité configuré dans la source de journal. La crédibilité s'accroît lorsque plusieurs sources signalent le même événement.
- La *gravité* indique le niveau de menace que représente une source par rapport au degré de préparation de la destination face à l'attaque.

QRadar utilise des algorithmes complexes pour calculer l'indice de magnitude et cet indice est réévalué à des intervalles planifiés et lorsque de nouveaux événements sont ajoutés à l'infraction. Les informations suivantes sont prises en compte lors du calcul de la magnitude de l'infraction :

- nombre d'événements et de flux associés à l'infraction
- nombre de sources de journal
- âge de l'infraction
- poids de l'objet réseau associé à l'infraction
- catégories, gravité, pertinence et crédibilité des événements et des flux qui contribuent à l'infraction
- évaluation des menaces et vulnérabilités des hôtes impliqués dans l'infraction

L'indice de magnitude d'une infraction est différent de l'indice de magnitude d'un événement. Vous pouvez influencer la magnitude d'une infraction en réglant la

© Copyright IBM Corp. 2012, 2017

magnitude d'événement dans les actions de règle mais vous ne pouvez pas ignorer les algorithmes de QRadar pour définir la magnitude de l'infraction vous-même.

Chaînage des infractions

IBM Security QRadar enchaîne les infractions pour réduire le nombre d'infractions à réviser et ainsi réduire les temps d'examen et de résolution de la menace.

Le chaînage des infractions vous aide à trouver la cause première d'un problème en connectant plusieurs symptômes ensemble et en les affichant comme une même infraction. En comprenant comment une infraction a évolué, vous pouvez voir certaines choses que vous n'auriez pas vues autrement lors de votre analyse. Certains événements qui ne seraient pas nécessaire d'examiner individuellement peuvent soudainement offrir un intérêt lorsqu'ils sont corrélés à d'autres événements pour former un modèle.

Le chaînage des infractions est basé sur la zone d'indexation de l'infraction spécifiée sur la règle. Par exemple, si votre règle est configurée pour utiliser l'adresse IP source comme zone d'indexation de l'infraction, une seule infraction est associée à cette adresse IP source tant que l'infraction est active.

Vous pouvez identifier une infraction chaînée en recherchant `précédé de` dans la zone **Description** de la page **Récapitulatif d'infraction**. Dans l'exemple suivant, QRadar a combiné tous les événements qui ont déclenché une infraction pour chacune des trois règles, et il a ajouté les noms de règles à la **Description** :

```
Exploit Followed By Suspicious Host Activity - Chained
preceded by Local UDP Scanner Detected
preceded by XForce Communication to a known Bot Command and Control
```

Indexation des infractions

L'indexation des infractions permet de regrouper des événements ou des flux de différentes règles indexées sur la même propriété sous une même infraction.

Par exemple, une infraction ayant une seule adresse IP source et plusieurs adresses IP de destination indique que la menace comporte un seul attaquant et plusieurs victimes. Si vous indexez ce type d'infraction par adresse IP source, tous les événements et tous les flux qui proviennent de la même adresse IP sont ajoutés à la même infraction. IBM Security QRadar utilise le paramètre d'indexation des infractions pour déterminer quelles infractions doivent être chaînées ensemble.

Vous pouvez configurer des règles pour indexer une infraction sur la base de n'importe quelle information. QRadar inclut un ensemble de zones normalisées prédéfinies que vous pouvez utiliser pour indexer vos infractions. Si la zone sur laquelle vous souhaitez indexer n'est pas inclue dans les zones normalisées, créez une propriété d'événement ou de flux personnalisée pour extraire les données du contenu et les utiliser comme zone d'indexation des infractions dans votre règle. La propriété personnalisée sur laquelle vous indexez peut être basée sur une expression régulière ou sur un calcul.

Considérations sur l'indexation des infractions

Il est important de comprendre dans quelle mesure l'indexation des infractions affecte votre déploiement IBM Security QRadar.

Performances du système

Assurez-vous d'optimiser et d'activer toutes les propriétés personnalisées utilisées pour l'indexation des infractions. L'utilisation de propriétés non optimisées peut avoir un impact négatif sur les performances.

Lorsque vous créez une règle, vous ne pouvez pas sélectionner des propriétés non optimisées dans la zone **Indexer l'infraction en fonction de**. Cependant, si une règle existante est indexée sur une propriété personnalisée et si la propriété personnalisée est ensuite désoptimisée, la propriété reste disponible dans la liste d'index de l'infraction. Ne désoptimisez pas les propriétés personnalisées utilisées dans les règles.

Action associée à la règle et réponse

Lorsque la valeur de propriété indexée est nulle, aucune offense n'est créée, même si vous cochez la case **Vérifier que l'élément événement détecté fait partie d'une infraction** dans l'action associée à la règle. Par exemple, si une règle est configurée pour créer une infraction indexée par nom d'hôte, mais le nom d'hôte est vide dans l'événement, aucune infraction n'est créée, même si toutes les conditions des tests de règles sont remplies.

Lorsque le limiteur de réponse utilise une propriété personnalisée, si celle-ci est nulle, la limite est appliquée à la valeur nulle. Par exemple, si la réponse est **E-mail**, et si le limiteur indique **Ne pas répondre plus de 1 fois chaque 1 heure par propriété personnalisée**, si la règle se déclenche une seconde fois avec une propriété nulle dans l'heure qui suit, aucun e-mail n'est envoyé.

Lorsque vous indexez à l'aide d'une propriété personnalisée, les propriétés que vous pouvez utiliser dans l'index de règles et dans la zone Limiteur de réponse dépend du type de règle que vous créez. Une règle d'événement accepte les propriétés d'événements personnalisées dans les zones de l'index de règle et du limiteur de réponses, alors qu'une règle de flux accepte uniquement les propriétés de flux personnalisées. Une règle commune accepte soit les propriétés d'événements soit les propriétés de flux personnalisées dans les zones de l'index de règle et du limiteur de réponses.

Vous ne pouvez pas utiliser des propriétés personnalisées pour indexer une infraction créée par un événement attribué.

Exemple : Détection de l'apparition d'un logiciel malveillant à l'aide de la signature MD5

En tant qu'analyste de la sécurité du réseau d'une grande entreprise, vous utilisez QRadar pour détecter l'apparition d'un logiciel malveillant. Vous définissez les critères correspondants comme une menace qui se produit sur 10 hôtes durant 4 heures. Vous souhaitez utiliser la signature MD5 comme base de la détection de cette menace.

Vous configurez IBM Security QRadar pour évaluer les journaux entrants afin de déterminer si une menace existe puis regroupez toutes les règles déclenchées contenant la même signature MD5 comme une même infraction.

1. Créez une propriété personnalisée basée sur une expression régulière pour extraire la signature MD5 des journaux. Vérifiez que la propriété personnalisée est optimisée et activée.

2. Créez une règle et configurez-la pour créer une infraction qui utilise la propriété personnalisée de la signature MD5 comme zone d'indexation de l'infraction. Lorsque la règle se déclenche, une infraction est créée. Toutes les règles déclenchées ayant la même signature MD5 sont regroupées sous une même infraction.
3. Vous pouvez lancer une recherche par type d'infraction pour trouver les infractions qui sont indexées par la propriété personnalisée de la signature MD5.

Conservation des infractions

L'état d'une infraction détermine pendant combien de temps IBM Security QRadar conserve l'infraction dans le système. La période de conservation des infraction détermine pendant combien de temps les infractions inactives et fermées sont conservées avant d'être supprimées de la console QRadar.

Infractions actives
Lorsqu'une règle déclenche une infraction, l'infraction est active. Dans cet état, QRadar attend d'évaluer les nouveaux événements ou flux par rapport au test de la règle d'infraction. Lorsque de nouveaux éléments sont évalués, l'horloge de l'infraction est réinitialisée pour conserver l'infraction active pendant 30 minutes supplémentaires.

Infractions à l'état de veille
Une infraction passe à l'état de veille lorsque aucun nouvel événements ou flux n'est ajouté à l'infraction pendant un intervalle de 30 minutes, ou si QRadar n'a traité aucun événement pendant 4 heures. Une infraction reste à l'état de veille pendant 5 jours. Si un événement est ajouté alors qu'une infraction se trouve à l'état de veille, le compteur de 5 jours est réinitialisé.

Infractions inactives
Une infraction devient inactive après une période de 5 jours passée à l'état de veille. Dans un état inactif, les nouveaux événements qui déclenchent le test de la règle d'infraction ne contribuent pas à l'infraction inactive. Ils sont ajoutés à une nouvelle infraction.

Les infractions inactives sont supprimées lorsque la période de conservation des infractions est écoulée.

Infractions fermées
Les infractions fermées sont supprimées lorsque la période de conservation des infractions est écoulée. Si de nouveaux événements se produisent pour une infraction fermée, une nouvelle infraction est créée.

Si vous incluez des infractions fermées dans une recherche, et si l'infraction n'a pas été supprimée de la console QRadar, l'infraction s'affiche dans les résultats de la recherche.

La période de conservation des infractions par défaut est de 30 jours. Lorsque la période de conservation d'une infraction expire, les infractions fermées et inactives sont supprimées du système. Les infractions qui ne sont pas inactives ou fermées sont conservées indéfiniment. Vous pouvez protéger une infraction pour éviter qu'elle soit supprimée lors de l'expiration de la période de conservation.

Protection des infractions

Vous pourriez disposer d'infractions que vous souhaitez conserver, quelle que soit la durée de conservation. Vous pouvez protéger des infractions pour les empêcher d'être supprimées de QRadar après l'écoulement de la période de conservation.

Pourquoi et quand exécuter cette tâche

Par défaut, les infractions sont conservées pendant trente jours. Pour en savoir plus sur la personnalisation de la période de conservation des infractions, voir le manuel *IBM Security QRadar Administration Guide*.

Procédure

1. Cliquez sur l'onglet **Infractions** puis sur **Toutes les infractions**.
2. Sélectionnez l'une des options suivantes :
   - Sélectionnez l'infraction que vous souhaitez protéger, puis sélectionnez **Protéger** dans la liste **Actions**.
   - Dans la zone de liste **Actions**, sélectionnez **Protéger les infractions répertoriées**.
3. Cliquez sur **OK**.

Résultats

L'infraction est protégée et elle ne sera pas supprimée de QRadar. Dans la fenêtre Infraction, l'infraction protégée est identifiée par un icône **Protégé** dans la colonne Indicateurs.

Annulation de la protection des infractions

Vous pouvez annuler la protection des infractions auparavant protégées contre la suppression une fois la durée de conservation des infractions écoulée.

Pourquoi et quand exécuter cette tâche

Pour énumérer uniquement les infractions protégées, vous pouvez effectuer une recherche qui filtre uniquement les infractions protégées. Si vous décochez la case **Protégé** et vous assurez que toutes les autres options sont sélectionnées dans la liste **Exclure** du volet Paramètres de recherche, seules les infractions protégées s'affichent.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Cliquez sur **Toutes les infractions**.
3. Facultatif : Effectuez une recherche qui affiche uniquement les infractions protégées.
4. Sélectionnez une des options suivantes :
   - Sélectionnez l'infraction que vous ne voulez plus protéger, puis sélectionnez **Déprotéger** dans la zone de liste Actions.
   - Dans la zone de liste **Actions**, sélectionnez **Déprotéger les infractions répertoriées**.
5. Cliquez sur **OK**.

Etude des infractions

IBM Security QRadar utilise des règles pour surveiller les événements et les flux de votre réseau afin de détecter les menaces de sécurité. Lorsque les événements et les flux correspondent aux critères de test définis dans les règles, une infraction est créée pour montrer qu'une attaque de sécurité ou qu'une violation de règle est

suspectée. Cependant, savoir qu'une infraction s'est produite n'est que la première étape. Vous devrez ensuite examiner comment elle s'est produite, où elle s'est produite et qui est à son origine.

Le fenêtre Récapitulatif d'infraction vous aide à commencer votre examen de l'infraction en fournissant un contexte pour aider à comprendre ce qui s'est passé et pour déterminer comment isoler et résoudre le problème.

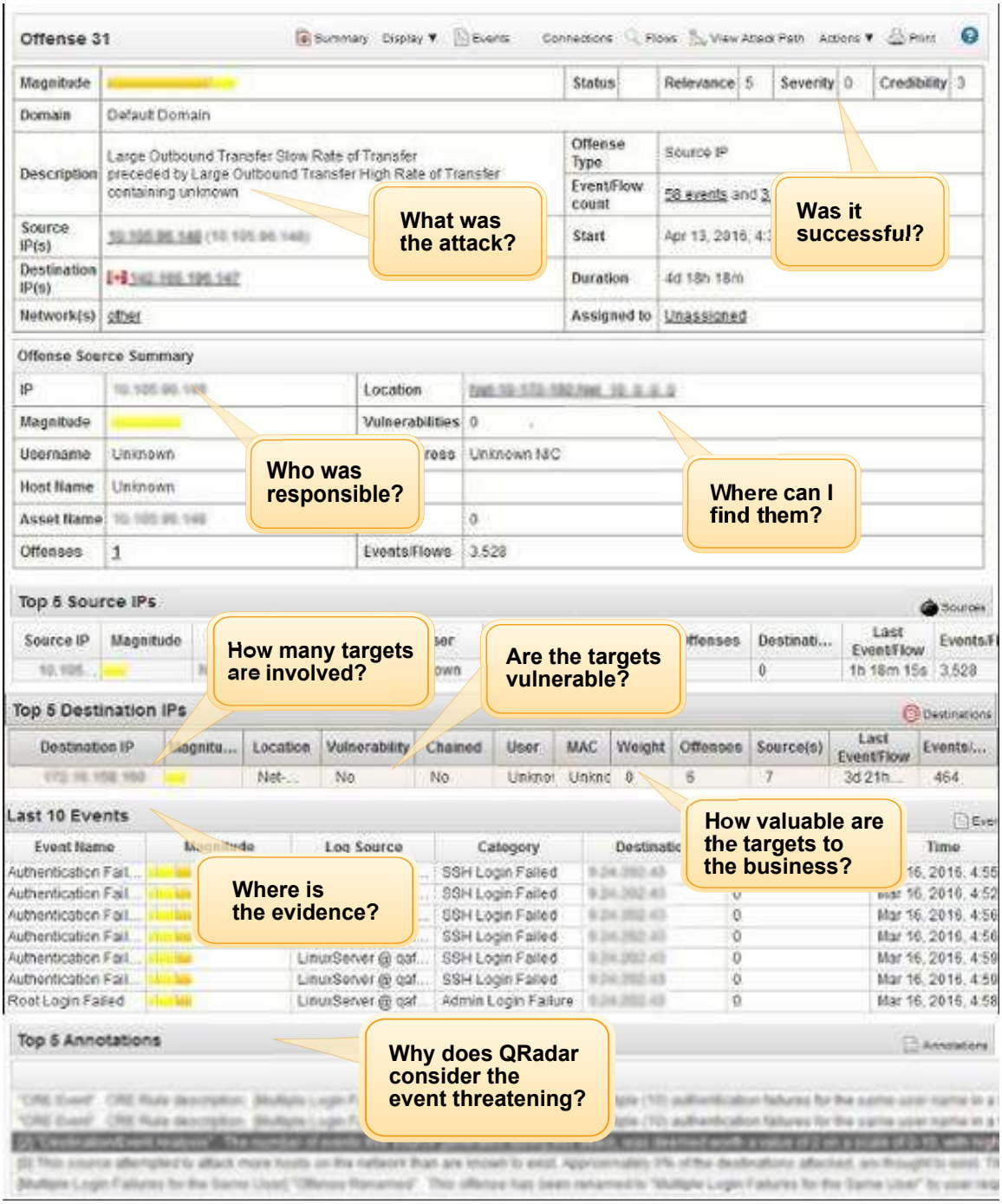

Figure 1. Vue récapitulative de l'infraction

QRadar n'utilise pas les droits d'utilisateurs des périphériques pour déterminer les infractions que chaque utilisateur peut afficher. Tous les utilisateurs ayant accès au réseau peuvent afficher toutes les infractions, quelle que soit la source de journal ou la source de flux associée à l'infraction. Pour en savoir plus sur la limitation de l'accès réseau, voir la documentation sur les profils de sécurité dans le *IBM Security QRadar Administration Guide*.

Sélection d'une infraction à examiner

L'onglet **Infraction** affiche les attaques de sécurité suspectée et les violations de sécurité qui se produisent sur votre réseau. Les infractions sont énumérées d'abord en fonction de la plus grande ampleur. Examinez d'abord les infractions apparaissant en tête de liste.

Pourquoi et quand exécuter cette tâche

Utilisez les options de navigation de gauche pour afficher les infractions sous différentes perspectives. Par exemple, sélectionnez **Par adresse IP source** ou **Par adresse IP de destination** pour afficher des informations sur les attaquants répétés, les adresses IP qui génèrent un grand nombre d'attaques ou sur les systèmes faisant l'objet d'attaques continues. Vous pouvez affiner la liste des infractions en sélectionnant la période durant laquelle vous souhaitez afficher les infractions ou en modifiant les paramètres de recherche.

Vous pouvez également rechercher des infractions basées sur divers critères. Pour plus d'informations sur la recherche d'infractions, voir «Recherches d'infractions», à la page 159.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Sur le menu de navigation, sélectionnez la catégorie d'infraction que vous souhaitez afficher.
3. Facultatif : Suivant la catégorie sélectionnée, les options de filtrage suivantes peuvent être sélectionnées :
   a. Dans la liste **Afficher les infractions**, sélectionnez une option pour filtrer la liste des infractions durant une période de temps déterminée.
   b. Dans le panneau **Paramètres de recherche actuels**, cliquez sur les liens **Effacer le filtre** pour affiner la liste des infractions.
4. Pour afficher toutes les infractions globales qui se produisent sur votre réseau, cliquez sur **Toutes les infractions**.
5. Pour afficher toutes les infractions qui vous sont affectées, cliquez sur **Mes infractions**.
6. Pour afficher les infractions groupées sur la catégorie de niveau supérieur, cliquez sur **Par catégorie**.
   a. Pour afficher les groupes de catégories de niveau inférieur liés à une catégorie particulière de niveau supérieur, cliquez sur la flèche située en regard du nom de la catégorie de niveau supérieur.
   b. Pour afficher une liste des infractions liées à une catégorie de niveau inférieur, cliquez deux fois sur la catégorie de niveau inférieur.

      Les zones de comptage telles que **Nombre d'événements/de flux** et **Nombre de sources** ne tiennent pas compte des droits d'accès au réseau de l'utilisateur.

7. Pour afficher les infractions par adresse IP source, cliquez sur **Par adresse IP source**. La liste des infractions affiche uniquement les adresses IP source comportant des infractions actives.
   a. Cliquez deux fois sur le groupe **Adresse IP source** que vous souhaitez afficher.
   b. Pour afficher une liste des adresses IP de destination locales liées à l'adresse IP source, cliquez sur **Destinations** sur la barre d'outils de la page Source.
   c. Pour afficher une liste d'infractions associées à cette adresse IP source, cliquez sur **Infractions** sur la barre d'outils de la page Source.
8. Pour afficher les infractions par adresse IP de destination, cliquez sur **Par adresse IP de destination**.
   a. Cliquez deux fois sur le groupe d'adresse **Adresse IP source** que vous souhaitez afficher.
   b. Pour afficher une liste des infractions associées à l'adresse IP de destination, cliquez sur **Infractions** sur la barre d'outils de la page Destination.
   c. Pour afficher une liste des adresses IP source associées à l'adresse IP de destination, cliquez sur **Sources** sur la barre d'outils de la page Destination.
9. Pour afficher les infractions par réseau, sélectionnez **Par réseau**.
   a. Cliquez deux fois sur le **Réseau** que vous souhaitez afficher.
   b. Pour afficher une liste d'adresses IP source associées à ce réseau, cliquez sur **Sources** sur la barre d'outils de la page Réseau.
   c. Pour afficher une liste d'adresses IP de destination associées à ce réseau, cliquez sur **Destinations** sur la barre d'outils de la page Réseau.
   d. Pour afficher une liste d'infractions associées à ce réseau, cliquez sur **Infractions** sur la barre d'outils de la page Réseau.
10. Cliquez deux fois sur l'infraction pour afficher des informations supplémentaires.

Que faire ensuite

Utilisez les informations du récapitulatif et des détails de l'infraction pour examiner l'infraction et entreprendre les actions nécessaires.

Examen d'une infraction à l'aide des informations récapitulatives

La fenêtre Récapitulatif d'infraction fournit les informations dont vous avez besoin pour commencer à examiner une infraction dans IBM Security QRadar. Les informations qui sont le plus importantes pour vous lors de votre examen sont différentes suivant le type d'infraction que vous examinez.

Pour vous aider à examiner une infraction, la partie inférieure de la page **Récapitulatif de l'infraction** regroupe des informations sur les principaux facteurs de l'infraction et affiche uniquement les informations les plus récentes ou les plus importantes dans cette catégorie. Plusieurs zones affichent des informations supplémentaires lorsque vous les survolez avec la souris. Certaines zones offrent des options de menu supplémentaires que vous pouvez afficher en cliquant sur le bouton droit de la souris .

Procédure

1. Cliquez sur l'onglet **Infractions** et cliquez deux fois sur l'infraction que vous souhaitez examiner. La fenêtre **Récapitulatif de l'infraction** s'ouvre.
2. Pour connaître le niveau d'importance que QRadar a affecté à l'infraction, reportez-vous à la première ligne de données.

   Détails de l'indice de magnitude :

Paramètre	Description
Magnitude	Indique l'importance relative de l'infraction. Cette valeur est calculée à partir de l'indice de pertinence, de gravité et de crédibilité.
Etat	Survolez l'icône d'état pour afficher l'état. QRadar n'affiche pas d'icône d'état lorsqu'une infraction est active.
Pertinence	Indique l'importance de la destination. QRadar détermine la pertinence en fonction du poids que l'administrateur a assigné aux réseaux et aux actifs.
Gravité	Indique la menace que représente une attaque en fonction du niveau de préparation de la destination face à l'attaque.
Crédibilité	Indique l'intégrité de l'infraction, qui est déterminée par l'indice de crédibilité configuré dans la source de journal. La crédibilité s'accroît lorsque plusieurs sources signalent le même événement. Les administrateurs QRadar configurent l'indice de crédibilité des sources de journal.

3. Consultez les informations figurant dans la partie supérieure de la fenêtre **Récapitulatif de l'infraction** pour en savoir plus sur le type d'attaque et sur la période durant laquelle l'attaque s'est produite.

   Détails des informations sur l'infraction :

Paramètre	Description
Description	Montre la cause de l'infraction. Les infractions en chaîne affichent la mention **Précédé de** qui indique que l'infraction a évolué à mesure que de nouveaux événements et flux ont été ajoutés à l'infraction.
Type d'infraction	Le type d'infraction est déterminé par la règle qui a créé l'infraction. Le type d'infraction détermine le type d'information qui s'affiche dans le panneau Récapitulatif des sources des infractions.
Nombre d'événements/de flux	Pour afficher la liste des événements ayant contribué à l'infraction, cliquez sur les liens **Evénement** ou **Flux**. Si le nombre de flux affiche **Non applicable**, il est possible que l'infraction ait une date de début antérieure à la date que vous avez mis à niveau dans IBM Security QRadar version 7.1 (MR1). Les flux ne peuvent pas être comptés mais vous pouvez cliquer sur le lien **Non applicable** pour examiner les flux.

Paramètre	Description
Adresse(s) IP source	Désigne le périphérique qui tente de violer la sécurité d'un composant sur votre réseau. Les infractions de type **Adresse IP source** sont toujours issues d'une seule adresse IP source. Les infractions appartenant aux autres types peuvent avoir plus d'une adresse IP source. Pour afficher des informations supplémentaires sur l'adresse IP source, survolez l'adresse ou utilisez les actions du bouton droit et du bouton gauche de la souris.
Adresse(s) IP de destination	Désigne le périphérique réseau à laquelle l'adresse IP source a tenté d'accéder. Si l'infraction ne comporte qu'une destination, l'adresse IP s'affiche. Si l'infraction comporte plusieurs destinations, le nombre d'adresse IP locales ou distantes ciblées s'affiche. Pour obtenir des informations supplémentaires, survolez l'adresse ou utilisez les actions du bouton droit et du bouton gauche de la souris.
Démarrer	Indique la date et l'heure à laquelle le premier événement ou flux s'est produit pour l'infraction.
Durée	Spécifie la durée écoulée depuis la création du premier événement ou flux associé à l'infraction.
Réseau(x)	Indique les réseaux locaux des adresses IP de destination locales qui ont été ciblées. QRadar prend en compte tous les réseaux spécifiés dans la hiérarchie du réseau comme locaux. Le système n'associe pas les réseaux distants à une infraction, même s'ils sont spécifiés comme réseau distant ou comme un service distant sur l'onglet **Admin**.

4. Dans la fenêtre **Récapitulatif des sources des infractions**, consultez les informations sur la source de l'infraction.

   Les informations qui s'affichent dans la fenêtre **Récapitulatif des sources des infractions** dépendent de la zone **Type d'infraction**.

   Détails des informations récapitulatives sur l'infraction :

Paramètre	Description
Chaîné	Indique si l'adresse IP de destination est intégrée à une chaîne. Une adresse IP en chaîne est associés à d'autres infractions. Par exemple, une adresse IP de destination peut devenir l'adresse IP source pour une autre infraction. Si l'adresse IP de destination est intégrée à une chaîne, cliquez sur **Oui** pour afficher les infractions mises en chaînes.
Adresse(s) IP de destination	Désigne le périphérique réseau à laquelle l'adresse IP source a tenté d'accéder. Si l'infraction ne comporte qu'une destination, l'adresse IP s'affiche. Si l'infraction compte plusieurs destinations, cette zone affiche le nombre d'adresses IP locales ou distantes ciblées. Pour obtenir des informations supplémentaires, survolez l'adresse ou utilisez les actions du bouton droit et du bouton gauche de la souris.
Emplacement	Indique l'emplacement réseau de l'adresse IP source ou de destination. Si l'emplacement est local, cliquez sur le lien pour afficher les réseaux.

Paramètre	Description
Magnitude	Indique l'importance relative de l'adresse IP source ou l'adresse IP de destination. La barre de l'ampleur fournit une représentation visuelle de la valeur du risque CVSS de l'actif associé à l'adresse IP. Survolez la barre de magnitude avec votre souris pour afficher la magnitude calculée.
Gravité	Indique la gravité de l'événement ou d'une infraction. La gravité indique le niveau de menace que constitue une infraction par rapport au degré de préparation de l'adresse IP de destination face à l'attaque. Cette valeur est directement associée à la catégorie d'événement qui correspond à l'infraction. Par exemple, une attaque par saturation (DoS) présente une gravité de 10, ce qui indique une occurrence grave.
Adresse(s) IP source	Désigne le périphérique qui a tenté de violer la sécurité d'un composant sur votre réseau. Les infractions de type **Adresse IP source** sont toujours issues d'une seule adresse IP source. Les infractions appartenant aux autres types peuvent avoir plus d'une adresse IP source. Pour afficher des informations supplémentaires sur l'adresse IP source, survolez l'adresse ou utilisez les actions du bouton droit et du bouton gauche de la souris.
Nom d'utilisateur	Spécifie le nom de l'utilisateur associé à l'événement ou au flux ayant créé l'infraction. Survolez le nom d'utilisateur avec votre souris pour afficher les informations les plus récentes dans la base de données du modèle d'actif pour l'utilisateur. Les événements qui n'incluent pas de nom d'utilisateur dans le contenu ou les événements générés par le systèmes qui appartiennent à un ordinateur local ou à un compte système affichent la mention Non applicable.
Vulnérabilités	Indique le nombre de vulnérabilités identifiées qui sont associées à l'adresse IP source ou de destination. Cette valeur inclut également le nombre de vulnérabilités actives et passives.

Lorsque vous affichez les informations récapitulatives des infractions de l'historique, les zones de données **Dernier connu** ne sont pas remplies.

5. Dans la partie inférieure de la fenêtre Récapitulatif de l'infraction, consultez les informations supplémentaires sur les principaux contributeurs à l'infraction, notamment les remarques et les annotations qui sont collectées au sujet de l'infraction. Pour afficher toutes les informations collectées par QRadar dans une catégorie, cliquez sur les liens situés sur la partie de droite de l'en-tête de catégorie.

En savoir plus sur les informations présentées dans les détails de l'infraction :

Catégorie des détails de l'infraction	Description
5 dernières remarques	Utilisez les remarques pour effectuer le suivi des informations importantes qui ont été collectées lors le l'examen de l'infraction. Vous pouvez ajouter une remarque au sujet d'une infraction, mais vous ne pouvez pas éditer ni supprimer les remarques.
Résultats de la recherche	
5 principales IP source	Affiche les 5 adresses IP principales possédant la magnitude la plus élevée, autrement dit, d'où provient l'attaque ou la violation de sécurité suspectée. Les infractions ayant une seule adresse IP source affichent une seule entrée dans la table.
5 principales IP de destination	Affiche les 5 principales adresses IP locales ayant la magnitude la plus élevée, ce qui peut indiquer la destination de l'attaque. Les infractions ciblant moins de 5 adresses IP locales affichent un nombre d'entrée inférieur dans la table. La colonne **Chaînée** indique si l'adresse IP de destination est l'adresse IP source d'une autre infraction. La mention **Oui** dans cette colonne indique qu'un attaquant contrôle le système avec cette adresse IP et qu'il l'utilise pour attaquer d'autres systèmes. Le colonne **Magnitude** affiche le score CVSS (Common Vulnerability Scoring System) agrégé, s'il existe. Si aucun score CVSS n'est disponible, la colonne affiche la magnitude supérieure de toutes les infractions dont fait partie l'adresse IP. Lorsque vous survolez l'adresse IP de destination avec la souris, la **Magnitude de destination** affiche le score CVSS. Si aucun score CVSS n'est disponible, un zéro s'affiche.
5 principales sources de journal	Affiche les sources de journal qui contribuent à l'infraction avec le plus grand nombre d'événements. Le moteur Custom Rule Engine (CRE) crée un événement et l'ajoute à l'infraction lorsque le critère de test spécifié dans la règle personnalisée correspond à l'événement entrant. Lorsqu'une source de journal affiche **Custom Rule Engine** dans la zone **Description**, cela indique que QRadar a créé les événements depuis cette source de journal. Le **Total des événements** affiche la somme de tous les événements reçus de cette source de journal pendant que l'infraction était active.
5 principaux utilisateurs	Les événements doivent inclure des informations utilisateurs pour que QRadar puisse renseigner cette table.
5 principales catégories	Affiche les catégories de niveau inférieur possédant le plus grand nombre d'événements ayant contribué à l'infraction. Le **Nombre de destinations locales** affiche le nombre d'adresses IP de destination locales affectées par des infractions avec des événements dans la catégorie. Lorsque toutes les adresses IP de destination sont distantes, cette zone affiche 0.
10 derniers événements	Affiche des informations sur les 10 derniers événements ayant contribué à l'infraction.

Catégorie des détails de l'infraction	Description
10 derniers flux	Affiche des informations sur les 10 derniers flux ayant contribué à l'infraction. La colonne **Nombre total d'octets** affiche la somme des octets transférés dans les deux directions.
Annotations	Les annotations permettent de savoir pourquoi QRadar considère que l'événement ou le trafic observé constitue une menace. QRadar peut ajouter des annotations lorsqu'il ajoute des événements ou des flux à une infraction. L'annotation la plus ancienne affiche les informations ajoutées par QRadar lors de la création de l'infraction. Les utilisateurs ne peuvent pas ajouter, éditer ni supprimer les annotations.

6. Si vous avez installé IBM Security QRadar Risk Manager, cliquez sur **Visualisation du chemin d'attaque** pour voir quels actifs de votre réseau communiquent afin de permettre à une infraction de se déplacer dans le réseau.

Analyse d'événements

Un événement est un enregistrement d'une source de journal, par exemple un périphérique pare-feu ou un routeur, qui décrit une action sur un réseau ou un hôte. Les événements associés à une infraction apportent la preuve qu'une activité suspecte se produit sur votre réseau. L'examen des données d'événement vous permet de comprendre les détails de l'infraction et de définir les meilleurs actions à effectuer pour isoler et réduire la menace.

Pourquoi et quand exécuter cette tâche

Certains événements sont créés sur la base d'un événement brut entrant tandis que d'autres sont créés par le moteur QRadar Custom Rule Engine (CRE). Les événements qui sont créés par QRadar n'ont pas de contenu car ils ne sont pas basés sur des événements bruts.

Procédure

1. Dans la fenêtre Récapitulatif d'infraction, cliquez sur **Evénements**.

   La fenêtre **Liste d'événements** affiche tous les événements associés à l'infraction.
2. Spécifiez les options **Heure de début**, **Heure de fin** et **Afficher** pour afficher les événements qui se sont produits durant un intervalle de temps spécifique.
3. Cliquez sur l'en-tête de la colonne Evénement pour trier la liste des événements.
4. Dans la liste des événements, cliquez avec le bouton droit de la souris sur le nom d'événement pour appliquer les options de filtre rapide afin de réduire le nombre d'événements à réviser.

   Vous pouvez également appliquer des filtres rapides à d'autres colonnes de la liste d'événements.
5. Cliquez deux fois sur un événement pour afficher ses détails.

   Les fenêtres **Informations sur l'événement** et **Informations sur la source et la destination** montrent uniquement les informations qui sont connues sur l'événement. Suivant le type d'événement, certaines zones peuvent être vides.

Détails des zones Heure de la fenêtre Informations sur l'événement :

Zone	Description
Heure de début	Heure à laquelle QRadar a reçu l'événement brut de la source de journal.
Heure de stockage	Heure à laquelle QRadar a stocké l'événement normalisé.
Heure de la source de journal	Heure enregistrée dans l'événement brut de la source de journal.

6. Dans la zone **Informations de contenu**, révisez les informations de l'événement brut que QRadar n'a pas normalisé.

   Les informations qui ne sont pas normalisées n'apparaissent pas dans l'interface QRadar, mais elles peuvent être utiles pour votre examen.

Que faire ensuite

Pour en savoir plus sur l'utilisation de QRadar pour réviser les données d'événement, voir «Surveillance de l'activité du journal», à la page 61 et Chapitre 9, «Recherches», à la page 141.

Examen des flux

IBM Security QRadar corrèle les flux dans une infraction lorsqu'il identifie des activités suspectes dans les communications réseau. L'analyse des flux offre une visibilité de la couche 7 ou de la couche application, pour les applications telles que les navigateurs Web, NFS, SNMP, Telnet et FTP. Un flux peut fournir des informations sur les adresses IP, les ports, les applications, les statistiques de trafic et le contenu des paquets issus du trafic non chiffré.

Par défaut, QRadar tente d'extraire les zones normalisées et de personnaliser les propriétés de flux des 64 premiers octets de données de flux mais les administrateurs peuvent augmenter la longueur de capture de contenu pour collecter plus de données. Pour plus d'informations, voir le manuel *IBM Security QRadar Administration Guide*.

Procédure

1. Dans la fenêtre Récapitulatif d'infraction, cliquez sur **Flux** dans le menu supérieur droit.

   La fenêtre Liste de flux affiche tous les flux associés à l'infraction.
2. Spécifiez les options **Heure de début**, **Heure de fin** et **Afficher** pour afficher les flux qui se sont produits durant un intervalle de temps spécifique.
3. Cliquez sur l'en-tête de la colonne Flux pour trier la liste des flux.
4. Dans la liste des flux, cliquez avec le bouton droit de la souris sur le nom du flux pour appliquer les options de filtre rapide afin de réduire le nombre de flux à réviser.

   Vous pouvez également appliquer des filtres rapides à d'autres colonnes de la liste de flux.
5. Cliquez deux fois sur un flux pour réviser ses détails.

   En savoir plus sur les détails des flux :

Zone	Description
Description de l'événement	Lorsque l'application n'est pas identifiée dans le contenu, QRadar utilise la fonction de décodage intégrée pour identifier l'application et affiche `Application détectée avec décodage basé sur état` dans la **Description de l'événement**.
Contenu source et **Contenu de destination**	Affiche la taille du contenu. Lorsque la taille dépasse 64 octets, le contenu peut contenir des informations supplémentaires qui ne s'affichent pas dans l'interface QRadar.
Correspondance partielle avec les règles personnalisées	Affiche les règles pour lesquelles la valeur de seuil n'a pas été atteinte, mais dont les autres éléments correspondent.
Direction du flux	Spécifie la direction du flux, où `L` indique un réseau local et `R` un réseau distant.

Que faire ensuite

Pour en savoir plus sur l'utilisation de QRadar pour réviser les données de flux, voir Chapitre 6, «Surveillance de l'activité réseau», à la page 85 et «Recherches d'événement et de flux», à la page 141.

Actions de gestion des infractions

IBM Security QRadar offre la possibilité d'agir sur les infractions pendant les opérations d'investigation. Pour vous aider à suivre les infractions qui font l'objet d'une action, QRadar ajoute une icône dans la colonne **Indicateurs** lorsque vous affectez une infraction à un utilisateur, ou encore lorsque vous protégez ou masquez une infraction, ajoutez des remarques ou marquez l'infraction pour suivi.

Pour effectuer la même action sur plusieurs infractions, maintenez la touche Ctrl enfoncée pendant que vous sélectionnez chaque infraction. Pour afficher les détails d'infraction sur une nouvelle page, maintenez la touche Ctrl enfoncée lorsque vous cliquez deux fois sur une infraction.

Ajout de remarques

Ajoutez des remarques à une infraction afin de suivre les informations qui sont collectées au cours d'une investigation. Les remarques ne doivent pas dépasser 2000 caractères.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Sélectionnez l'infraction à laquelle vous souhaitez ajouter la remarque. Pour ajouter la même remarque à plusieurs infractions, appuyez sur la touche Ctrl et sélectionnez chaque infraction.
3. Dans la liste **Actions**, sélectionnez **Ajouter une remarque**.
4. Saisissez la remarque que vous souhaitez inclure pour cette infraction.
5. Cliquez sur **Ajouter une remarque**.

Résultats

La remarque s'affiche dans le volet 5 dernières remarques de la fenêtre Récapitulatif d'infraction. Une icône **Remarques** s'affiche dans la colonne Indicateurs de la liste des infractions.

Pour afficher une remarque, déplacez votre souris sur l'indicateur des remarques dans la colonne **Indicateurs** de la liste **Infraction**.

Masquage des infractions

Masquez une infraction afin d'empêcher son affichage dans la liste des infractions. Une fois l'infraction masquée, elle n'est plus affichée dans aucune liste de l'onglet **Infractions**, y compris la liste **Toutes les infractions**. Toutefois, si vous effectuez une recherche qui inclut les infractions masquées, l'infraction figure dans les résultats de la recherche.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Sélectionnez l'infraction que vous souhaitez masquer. Pour masquer plusieurs infractions, maintenez la touche Ctrl enfoncée pendant que vous sélectionnez chaque infraction.
3. Dans la zone de liste **Actions**, sélectionnez **Masquer**.
4. Cliquez sur **OK**.

Affichage des infractions masquées

Par défaut, la liste des infractions sous l'onglet **Infractions** est filtrée afin d'exclure les infractions masquées. Pour afficher les infractions masquées, effacez le filtre sous l'onglet **Infractions** ou effectuez une recherche qui inclue les infractions masquées. Lorsque vous incluez les infractions masquées dans la liste des infractions, l'icône **Masqué** figure dans la colonne **Indicateurs** de ces infractions.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Pour effacer le filtre dans la liste des infractions, cliquez sur **Effacer le filtre** en regard du paramètre de recherche **Exclure Infractions masquées**.
3. Pour créer une nouvelle recherche qui inclut les infractions masquées, procédez comme suit :
   a. Dans la zone de liste **Rechercher**, sélectionnez **Nouvelle recherche**.
   b. Dans la fenêtre Paramètres de recherche, désélectionnez la case **Infractions masquées** dans la liste d'options **Exclure**.
   c. Cliquez sur **Rechercher**.
4. Pour retirer l'indicateur de masquage d'une infraction, procédez comme suit :
   a. Sélectionnez l'infraction pour laquelle vous souhaitez retirer l'indicateur de masquage. Pour sélectionner plusieurs infractions, maintenez la touche Ctrl enfoncée pendant que vous sélectionnez chaque infraction.
   b. Dans la zone de liste **Actions**, sélectionnez **Afficher**.

   L'indicateur de masquage est retiré et l'infraction apparaît dans la liste des infractions sans que vous ayez à effacer le filtre **Exclure Infractions masquées**.

Fermeture des infractions

Fermez une infraction afin de pouvoir la retirer complètement de votre système.

Pourquoi et quand exécuter cette tâche

La période de conservation des infractions par défaut est de 30 jours. Lorsque la période de conservation d'une infraction expire, les infractions fermées sont supprimées du système. Vous pouvez protéger une infraction pour éviter qu'elle soit supprimée lors de l'expiration de la période de conservation.

Les infractions fermées ne sont plus affichées dans aucune liste de l'onglet **Infractions**, y compris la liste **Toutes les infractions**. Lorsque vous incluez des infractions fermées dans une recherche, si une infraction est toujours en période de conservation, elle figure dans les résultats de recherche. Si de nouveaux événements se produisent pour une infraction fermée, une nouvelle infraction est créée.

Lorsque vous fermez des infractions, vous devez sélectionner un motif de fermeture. Si vous disposez du droit **Gérer la fermeture des infractions**, vous pouvez ajouter des motifs de fermeture personnalisés. Pour plus d'informations sur les autorisations de rôles, voir *IBM Security QRadar Administration Guide*.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Sélectionnez l'infraction que vous souhaitez fermer. Pour fermer plusieurs infractions, maintenez la touche Ctrl enfoncée pendant que vous sélectionnez chaque infraction.
3. Dans la liste **Actions**, sélectionnez **Fermer**.
4. Dans la liste **Motif de la fermeture**, indiquez un motif de fermeture.

   Pour ajouter un motif de fermeture, cliquez sur l'icône en regard de **Motif de la fermeture** afin d'ouvrir la boîte de dialogue Motifs de la fermeture de l'infraction personnalisée.
5. Facultatif : Dans la zone **Remarques**, entrez une note pour fournir des informations supplémentaires.

   La zone **Remarques** affiche la note saisie pour la fermeture de l'infraction précédente. Les remarques ne doivent pas dépasser 2000 caractères.
6. Cliquez sur **OK**.

Résultats

Après avoir fermé les infractions, les nombres affichés dans le volet Par catégorie de l'onglet **Infractions** peuvent nécessiter plusieurs minutes pour prendre en compte les infractions fermées.

Exportation d'infractions

Exportez des infractions lorsque vous voulez réutiliser des données ou lorsque vous voulez stocker les données en externe. Par exemple, vous pouvez utiliser les données d'infraction pour créer des rapports dans une application tierce. Vous pouvez également exporter des infractions comme stratégie secondaire de conservation à long terme. Le service clients peut vous demander d'exporter des infractions à des fins d'identification et de résolution des problèmes.

Vous pouvez exporter des infractions au format XML (Extensible Markup Language) ou CSV (Comma-Separated Values). Le fichier XML ou CSV obtenu

contient les paramètres spécifiés dans le volet Définition de colonne des paramètres de recherche. La durée nécessaire à l'exportation des données dépend du nombre de paramètres spécifiés.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Sélectionnez les infractions que vous souhaitez exporter. Pour sélectionnez plusieurs infractions, maintenez la touche Ctrl enfoncée pendant que vous sélectionnez chaque infraction.
3. Sélectionnez l'une des options suivantes :
   - Pour exporter les infractions au format XML, sélectionnez **Actions** > **Exporter au format XML**.
   - Pour exporter les infractions au format CSV, sélectionnez **Actions** > **Exporter au format CSV**.
4. Sélectionnez l'une des options suivantes :
   - Si vous souhaitez ouvrir le fichier pour une consultation immédiate, sélectionnez l'option **Ouvrir avec** et sélectionnez une application dans la liste.
   - Pour sauvegarder le fichier, sélectionnez **Sauvegarder**.
5. Cliquez sur **OK**.

   Le fichier, `<date>-data_export.xml.zip`, est sauvegardé dans le dossier de téléchargement par défaut sur votre ordinateur.

Affectation d'infractions aux utilisateurs

Par défaut, toutes les nouvelles infractions ne pas affectées. Vous pouvez affecter une infraction à un utilisateur IBM Security QRadar à des fins d'investigation.

Pourquoi et quand exécuter cette tâche

Lorsque vous affectez une infraction à un utilisateur, celle-ci s'affiche sur la page Mes Infractions appartenant à cet utilisateur. Vous devez disposer du droit **Affecter des infractions à des utilisateurs** pour affecter des infractions aux utilisateurs. Pour plus d'informations sur les autorisations de rôles, voir *IBM Security QRadar Administration Guide*.

Vous pouvez affecter des infractions aux utilisateurs depuis l'onglet **Infractions** ou les pages Récapitulatif d'infraction. Cette procédure fournit des instructions concernant l'affectation des infractions depuis l'onglet **Infractions**.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Sélectionnez l'infraction que vous souhaitez affecter. Pour affecter plusieurs infractions, maintenez la touche Ctrl enfoncée pendant que vous sélectionnez chaque infraction.
3. Dans la liste **Actions**, sélectionnez **Affecter**.
4. Dans la liste **Affecter à un utilisateur**, sélectionnez l'utilisateur auquel vous souhaitez affecter cette infraction.

   Remarque : La liste **Affecter à un utilisateur** comporte uniquement les utilisateurs qui disposent de privilèges leur permettant d'afficher l'onglet **Infractions**. Les paramètres de profil de sécurité pour l'utilisateur sont également pris en compte.
5. Cliquez sur **Sauvegarder**.

Résultats

L'infraction est affectée à l'utilisateur sélectionné. L'icône **Utilisateur** s'affiche dans la colonne d'indicateur de l'onglet **Infractions** pour indiquer que l'infraction a été affectée. L'utilisateur désigné peut consulter cette infraction sur la page Mes Infractions.

Envoi de notifications par e-mail

Partagez des informations récapitulatives sur une infraction avec une autre personne par l'envoi d'un e-mail.

Le corps de l'e-mail contient les informations suivantes, si disponibles :

- Adresse IP source
- Nom d'utilisateur source, nom d'hôte ou nom de l'actif.
- Nombre total des sources
- Les cinq principales sources par amplitude
- Réseaux sources
- Adresse IP de destination
- Nom d'utilisateur de destination, nom d'hôte ou nom de l'actif.
- Nombre total de destinations
- Les cinq principales destinations par amplitude
- Réseaux de destination
- Nombre total des événements
- Les règles qui ont causé le déclenchement de l'infraction ou de la règle d'événement
- Description complète de l'infraction ou de la règle d'événement
- ID de l'infraction
- Les cinq principales catégories
- Heure de début de l'infraction ou heure de l'événement généré
- Les cinq principales annotations
- Lien vers l'infraction dans l'interface utilisateur
- Contribution aux règles CRE

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Sélectionnez l'infraction pour laquelle vous souhaitez envoyer une notification par e-mail
3. Dans la zone de liste **Actions**, sélectionnez **E-mail**.
4. Configurez les paramètres suivants :

Option	Description
Paramètre	Description
A	Entrez l'adresse e-mail de l'utilisateur que vous souhaitez notifier si un changement se produit dans l'infraction sélectionnée. Séparez chaque adresse e-mail par une virgule.
De	Saisissez l'adresse e-mail d'origine. La valeur par défaut est root@localhost.com.

Option	Description
Objet de l'e-mail	Entrez l'objet de l'e-mail. La valeur par défaut est **ID de l'infraction**.
Message de l'e-mail	Saisissez le message standard de votre choix qui accompagnera la notification par e-mail.

5. Cliquez sur **Envoyer**.

Marquage d'une infraction pour suivi

Marquez une infraction pour suivi lorsque vous voulez en vue d'une investigation supplémentaire.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Recherchez l'infraction que vous souhaitez marquer pour suivi.
3. Cliquez deux fois sur l'infraction.
4. Dans la liste **Actions**, sélectionnez **Suivre**.

Résultats

L'infraction affiche maintenant l'icône de suivi dans la colonne **Indicateurs**. Pour trier la liste des infractions afin que les infractions marquées figurent en haut de la liste, cliquez sur l'en-tête de colonne **Indicateurs**.

Chapitre 5. Étude de l'activité du journal

Vous pouvez surveiller et étudier les événements en temps réel ou effectuer des recherches avancées.

A l'aide de l'onglet **Activité du journal**, vous pouvez surveiller et étudier l'activité du journal (événements) en temps réel ou effectuer des recherches avancées.

Présentation de l'onglet Activité du journal

Un événement est un enregistrement d'une source de journal, par exemple un périphérique pare-feu ou un routeur, qui décrit une action sur un réseau ou un hôte.

L'onglet **Activité du journal** spécifie les événements qui sont associés aux infractions.

Vous devez avoir l'autorisation d'afficher l'onglet **Activité du journal**.

Barre d'outils de l'onglet Activité du journal

Vous pouvez accéder à plusieurs onglets à partir de la barre d'outils Activité du journal

A l'aide de la barre d'outils, vous pouvez accéder aux options suivantes :

Tableau 12. Options de la barre d'outils Activité du journal

Option	Description
Recherche	Cliquez sur **Rechercher** pour effectuer des recherches avancées sur les événements. Les options incluent : • **Nouvelle recherche** - Sélectionnez cette option pour créer une nouvelle recherche d'événement. • **Editer la recherche** - Sélectionnez cette option pour sélectionner et modifier une recherche d'événement. • **Gérer les résultats de la recherche** - Sélectionnez cette option pour afficher et gérer les résultats de la recherche.
Recherches rapides	Dans cette zone de liste, vous pouvez exécuter des recherches précédemment enregistrées. Les options ne sont affichées dans la zone de liste **Recherches rapides** que lorsque vous avez enregistré un critère de recherche qui indique l'option **Inclure dans mes recherches rapides**.
Ajouter un filtre	Cliquez sur **Ajouter un filtre** pour ajouter un filtre aux résultats de recherche actuelle.
Sauvegarder les critères	Cliquez sur **Sauvegarder les critères** pour sauvegarder les critères de la recherche actuelle.

© Copyright IBM Corp. 2012, 2017

Tableau 12. Options de la barre d'outils Activité du journal (suite)

Option	Description
Sauvegarder les résultats	Cliquez sur **Sauvegarder les résultats** pour sauvegarder les résultats de la recherche actuelle. Cette option ne s'affiche qu'après la fin d'une recherche. Cette option est désactivée en mode de diffusion en flux.
Annuler	Cliquez sur **Annuler** pour annuler une recherche en cours. Cette option est désactivée en mode de diffusion en flux.
Faux positif	Cliquez sur **Faux positif** pour ouvrir la fenêtre Ajustement des faux positifs, qui vous permet de désactiver les flux connus en tant que faux positifs pour les empêcher de créer des infractions. Cette option est désactivée en mode de diffusion en flux. Pour plus d'informations sur le réglage des faux positifs, voir Réglage des faux positifs.

Tableau 12. Options de la barre d'outils Activité du journal (suite)

Option	Description
Règles	L'option Règles n'est disponible que si vous disposez de l'autorisation d'afficher les règles. Cliquez sur **Règles** pour configurer les règles d'événements personnalisés. Les options incluent : • **Règles** - Sélectionnez cette option pour afficher ou créer une règle. Si vous ne disposez que de l'autorisation d'afficher les règles, la page de synthèse de l'assistant Règles s'affiche. Si vous avez l'autorisation de maintenir des règles personnalisées, l'assistant Règles s'affiche et vous pouvez modifier la règle. Afin d'activer les options de la règle de détection des anomalies (Ajouter une règle de seuil, Ajouter une règle de comportement et Ajouter une règle d'anomalie), vous devez sauvegarder le critère de recherche agrégé parce que le critère de recherche sauvegardé indique les paramètres requis. **Remarque :** Les options de la règle de détection des anomalies ne sont visibles que si vous avez l'autorisation **Activité du journal** > **Gestion de règles personnalisées**. • **Ajouter une règle de seuil** - Sélectionnez cette option pour créer une règle de seuil. Une règle de seuil teste le trafic d'événement de l'activité qui dépasse un seuil configuré. Les seuils peuvent reposer sur toutes les données collectées par QRadar. Par exemple, si vous créez une règle de seuil indiquant que le nombre de clients pouvant se connecter au serveur ne doit pas dépasser 220 clients entre 08h00 et 17h00, les règles génèrent une alerte lorsque le 221ème client tente de se connecter. Lorsque vous sélectionnez l'option **Ajouter une règle de seuil**, l'assistant Règles s'affiche, prérempli avec les options appropriées pour la création d'une règle de seuil.

Tableau 12. Options de la barre d'outils Activité du journal (suite)

Option	Description
Règles (suite)	• **Ajouter une règle de comportement** - Sélectionnez cette option pour créer une règle comportementale. Une règle comportementale teste le trafic d'événement pour une activité anormale, telle que l'existence d'un trafic nouveau ou inconnu, qui correspond à un trafic qui cesse soudainement ou un changement de pourcentage de la durée où un objet est actif. Par exemple, vous pouvez créer une règle comportementale pour comparer le volume moyen du trafic pour les 5 dernières minutes par rapport au volume moyen du trafic au cours de la dernière heure. S'il existe un changement de plus de 40 %, la règle génère une réponse. Lorsque vous sélectionnez l'option **Ajouter une règle de comportement**, l'assistant Règles s'affiche, prérempli avec les options appropriées pour la création d'une règle comportementale. • **Ajouter une règle d'anomalie** - Sélectionnez cette option pour créer une règle d'anomalie. Une règle d'anomalie teste le trafic d'événement pour une activité anormale, telle que l'existence d'un trafic nouveau ou inconnu, qui correspond à un trafic qui cesse soudainement ou un changement de pourcentage de la durée où un objet est actif. Par exemple, si une zone de votre réseau qui ne communique jamais avec l'Asie commence à communiquer avec des hôtes dans ce pays, une règle d'anomalie génère une alerte. Lorsque vous sélectionnez l'option **Ajouter une règle d'anomalie**, l'assistant Règles s'affiche, prérempli avec les options appropriées pour la création d'une règle d'anomalie.

Tableau 12. Options de la barre d'outils Activité du journal (suite)

Option	Description
Actions	Cliquez sur **Actions** pour effectuer les actions suivantes : • **Afficher tout** - Sélectionnez cette option pour supprimer tous les filtres sur les critères de recherche et afficher tous les événements non filtrés. • **Imprimer** - Sélectionnez cette option pour imprimer les événements affichés sur la page. • **Exporter au format XML** > **Colonnes visibles** - Sélectionnez cette option pour n'exporter que les colonnes visibles dans l'onglet Activité du journal. Il s'agit de l'option recommandée. Voir Exportation des événements. • **Exporter au format XML** > **Exportation complète (toutes les colonnes)** - Sélectionnez cette option pour exporter tous les paramètres d'événement. Une exportation complète peut prendre un certain temps pour s'achever. Voir Exportation des événements. • **Exporter au format CSV** > **Colonnes visibles** - Sélectionnez cette option pour n'exporter que les colonnes qui sont visibles dans l'onglet Activité du journal. Il s'agit de l'option recommandée. Voir Exportation des événements. • **Exporter au format CSV** > **Exportation complète (toutes les colonnes)** - Sélectionnez cette option pour exporter tous les paramètres d'événement. Une exportation complète peut prendre un certain temps pour s'achever. Voir Exportation des événements. • **Supprimer** - Sélectionnez cette option pour supprimer un résultat de recherche. Voir Gestion des résultats de recherche de flux et d'événement. • **Envoyer une notification** - Sélectionnez cette option pour indiquer que vous souhaitez recevoir une notification par e-mail à la fin des recherches sélectionnées. Cette option n'est activée que pour les recherches en cours. **Remarque :** Les options **Imprimer**, **Exporter au format XML** et **Exporter au format CSV** sont désactivées en mode de diffusion en flux et lors de l'affichage des résultats de recherche partielle.

Tableau 12. Options de la barre d'outils Activité du journal (suite)

Option	Description
Barre d'outils de recherche	**Recherche avancée** Sélectionnez **Recherche avancée** dans la zone de liste pour entrer une chaîne de recherche AQL (Ariel Query Language) pour spécifier les zones que vous souhaitez renvoyer. **Filtrage rapide** Sélectionnez Filtrage rapide dans la zone de liste pour rechercher des contenus à l'aide de mots ou de phrases simples.
Afficher	La vue par défaut sous l'onglet **Activité du journal** est un flux des événements en temps réel. La liste **Vue** contient des options qui permettent d'afficher également des événements au cours de plages de temps spécifiques. Après avoir choisi une plage de temps spécifique dans la liste **Vue**, vous pouvez modifier la plage de temps affichée en changeant les valeurs de date et d'heure dans les zones **Heure de début** et **Heure de fin**.

Options de menu contextuel

Sur l'onglet **Activité du journal**, vous pouvez cliquer avec le bouton droit de votre souris sur un événement pour accéder à plus d'informations de filtre d'événement.

Les options du menu contextuel sont :

Tableau 13. Options de menu contextuel

Option	Description
Filtrer sur	Sélectionnez cette option pour filtrer d'après l'événement sélectionné, en fonction du paramètre sélectionné dans cet événement.
Faux positif	Sélectionnez cette option pour ouvrir la fenêtre Faux positif, qui vous permet de désactiver les événements connus en tant que faux positifs pour les empêcher de créer des infractions. Cette option est désactivée en mode de diffusion en flux. Voir Réglage des faux positifs.
Options supplémentaires :	Sélectionnez cette option pour examiner une adresse IP ou un nom d'utilisateur. Pour plus d'informations sur l'étude d'une adresse IP, voir Etude des adresses IP. Pour plus d'informations sur l'étude d'un nom d'utilisateur, voir Etude des noms d'utilisateur. **Remarque :** Cette option n'est pas affichée en mode de diffusion en flux.
Filtrage rapide	Filtrage des éléments qui correspondent, ou qui ne correspondent pas, à la sélection.

Barre d'état

Lors de la diffusion d'événements, la barre d'état affiche la moyenne des résultats reçus par seconde.

Il s'agit du nombre de résultats que la console a reçu avec succès de la part des processeurs d'événement. Si ce nombre est supérieur à 40 résultats par seconde, seulement 40 résultats s'affichent. Le reste est mémorisé dans la mémoire tampon. Pour afficher plus d'informations d'état, déplacez le pointeur de votre souris sur la barre d'état.

Lorsque les événements ne sont pas en cours de diffusion, la barre d'état affiche le nombre de résultats de recherche en cours d'affichage sur l'onglet ainsi que le temps nécessaire au traitement des résultats de recherche.

Surveillance de l'activité du journal

Par défaut, l'onglet **Activité du journal** affiche les événements en mode diffusion en flux, ce qui vous permet d'afficher les événements en temps réel.

Pour plus d'informations sur la diffusion en mode continu, voir, Affichage des événements de diffusion en continu . Vous pouvez indiquer une plage de temps différente pour filtrer les événements à l'aide de la zone de liste **Vue**.

Si vous avez précédemment configuré des critères de recherche sauvegardés par défaut, les résultats de cette recherche sont automatiquement affichés lorsque vous accédez à l'onglet **Activité du journal**. Pour plus d'informations sur la sauvegarde des critères de recherche, voir Sauvegarde des critères de recherche d'événements et de flux .

Affichage des événements de diffusion en flux

Le mode de diffusion en flux vous permet d'afficher les données d'événements entrantes dans votre système. Ce mode vous donne une vue en temps réel de votre activité actuelle en affichant les 50 derniers événements.

Pourquoi et quand exécuter cette tâche

Si vous appliquez des filtres sur l'onglet **Activité du journal** ou dans vos critères de recherche avant d'activer le mode de diffusion en flux, les filtres sont maintenus dans le mode de diffusion en flux. Toutefois, le mode de diffusion en flux ne supporte pas les recherches qui incluent des événements groupés. Si vous activez le mode de diffusion en flux sur les événements groupés ou les critères de recherche groupés, l'onglet **Activité du journal** affiche les événements normalisés. Voir Affichage des événements normalisés.

Pour sélectionner un événement afin d'afficher les détails ou d'effectuer une action, vous devez mettre en pause le mode de diffusion en flux avant de cliquer deux fois sur un événement. Lorsque la diffusion en flux est suspendue, les 1 000 derniers événements s'affichent.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.

2. Dans la zone de liste **Vue**, sélectionnez **Temps réel (diffusion en flux)**. Pour plus d'informations sur les options de la barre d'outils, voir la table 4-1. Pour plus d'informations sur les paramètres affichés en mode de diffusion en flux, voir la table 4-7.
3. Facultatif. Suspendez ou lisez les événements en mode de diffusion en flux. Choisissez l'une des options suivantes :
   - Pour sélectionner un enregistrement d'événement, cliquez sur l'icône **Pause** pour suspendre la diffusion en flux.
   - Pour redémarrer le mode de diffusion en flux, cliquez sur l'icône **Play**.

Affichage des événements normalisés

Les événements sont collectés au format brut, puis normalisés pour l'affichage sur l'onglet **Activité du journal**.

Pourquoi et quand exécuter cette tâche

La normalisation implique l'analyse syntaxique des données d'événements bruts et la préparation des données pour afficher des informations lisibles sur l'onglet. Lorsque les événements sont normalisés, le système normalise également leur nom. Par conséquent, le nom qui s'affiche sur l'onglet **Activité du journal** peut ne pas correspondre au nom qui s'affiche dans l'événement.

Remarque : Si vous avez sélectionné un délai à afficher, un graphique de série temporelle s'affiche. Pour plus d'informations sur l'utilisation des graphiques de série temporelle, voir Présentation des graphiques de série temporelle.

L'onglet **Activité du journal** affiche les paramètres suivants lorsque vous affichez les événements normalisés :

Tableau 14. Onglet Activité du journal - Paramètres par défaut (normalisés)

Paramètre	Description
Filtres en cours	Le haut du tableau affiche les détails des filtres appliqués aux résultats de recherche. Pour effacer ces valeurs de filtre, cliquez sur **Effacer le filtre**. **Remarque :** Ce paramètre s'affiche uniquement après avoir appliqué un filtre.
Afficher	Dans cette zone de liste, vous pouvez sélectionner l'intervalle selon lequel vous souhaitez filtrer.

Tableau 14. Onglet Activité du journal - Paramètres par défaut (normalisés) (suite)

Paramètre	Description
Statistiques en cours	Lorsque vous n'êtes pas en mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), les statistiques en cours ci-après s'affichent : **Remarque :** Cliquez sur la flèche à côté de **Statistiques en cours** pour afficher ou masquer les statistiques. • **Résultats totaux** - Indique le nombre total de résultats correspondant à vos critères de recherche. • **Fichiers de données recherchés** - Indique le nombre total de fichiers de données recherchés au cours de l'intervalle de temps spécifié. • **Fichiers de données compressés recherchés** - Indique le nombre total de fichiers de données compressés recherchés dans l'intervalle de temps spécifié. • **Nombre de fichiers d'index** - Indique le nombre total de fichiers d'indexation recherchés au cours de l'intervalle de temps spécifié. • **Durée** - Indique la durée de la recherche. **Remarque :** Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service client pour identifier et résoudre les événements, vous pouvez être invité à fournir des informations statistiques en cours.
Graphiques	Affiche les graphiques configurables qui représentent les enregistrements correspondant à l'intervalle de temps et l'option de regroupement. Cliquez sur **Masquer les graphiques** si vous voulez supprimer les graphiques de votre affichage. Les graphiques s'affichent uniquement après avoir sélectionné un délai de type Dernier intervalle (actualisation automatique) au minimum et une option de regroupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir Gestion des graphiques. **Remarque :** Si vous utilisez Mozilla Firefox en tant que navigateur et qu'une extension de navigateur de blocage de publicité est installée, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez supprimer l'extension de navigateur de blocage de publicité. Pour plus d'informations, voir la documentation de votre navigateur.

Tableau 14. Onglet Activité du journal - Paramètres par défaut (normalisés) (suite)

Paramètre	Description
Icône Infractions	Cliquez sur cette icône pour afficher les détails de l'infraction associée à cet événement. Pour plus d'informations, voir Gestion des graphiques. **Remarque :** Selon votre produit, cette icône peut ne pas être disponible. Vous devez avoir IBM Security QRadar SIEM.
Heure de début	Indique l'heure du premier événement, tel que rapporté à QRadar par la source du journal.
Nom d'événement	Indique le nom normalisé de l'événement.
Source de journal	Indique la source du journal qui a généré cet événement. S'il existe plusieurs sources de journal associées à cet événement, cette zone indique le terme Multiple et le nombre de sources du journal.
Nombre d'événements	Indique le nombre total d'événements regroupés dans cet événement normalisé. Les événements sont regroupés lorsque plusieurs événements du même type pour la même adresse IP source et de destination sont identifiés dans une courte période.
Heure	Indique la date et l'heure auxquelles QRadar a reçu l'événement.
Catégorie de niveau inférieur	Indique la catégorie de bas niveau associée à cet événement. Pour plus d'informations sur les catégories d'événements, voir *IBM Security QRadar Administration Guide*.
IP source	Indique l'adresse IP source de l'événement.
Port source	Indique le port source de l'événement.
IP de destination	Indique l'adresse IP de destination de l'événement.
Port de destination	Indique le port de destination de l'événement.
Nom d'utilisateur	Indique le nom d'utilisateur associé à cet événement. Les noms d'utilisateur sont souvent disponibles dans les événements associés à l'authentification. Pour tous les autres types d'événements où le nom d'utilisateur n'est pas disponible, cette zone indique N/A.
Magnitude	Indique l'ampleur de cet événement. Les variables comprennent la crédibilité, la pertinence et la gravité. Placez le pointeur de votre souris sur la barre d'ampleur pour afficher les valeurs et l'ampleur calculée.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Dans la zone de liste **Affichage**, sélectionnez **Par défaut (normalisé)**.
3. Dans la zone de liste **Vue**, sélectionnez le délai que vous souhaitez afficher.
4. Cliquez sur l'icône **Pause** pour mettre en pause la diffusion en flux.
5. Cliquez deux fois sur l'événement que vous souhaitez afficher de façon plus détaillée. Pour plus d'informations, voir Détails d'événement.

Affichage des événements bruts

Vous pouvez afficher des données d'événements bruts. Il s'agit des données d'événements non analysées à partir de la source de journal.

Pourquoi et quand exécuter cette tâche

Lorsque vous affichez les données d'événements bruts, l'onglet **Activité du journal** fournit les paramètres suivants pour chaque événement.

Tableau 15. Paramètres d'événements bruts

Paramètre	Description
Filtres en cours	Le haut du tableau affiche les détails des filtres appliqués aux résultats de recherche. Pour effacer ces valeurs de filtre, cliquez sur **Effacer le filtre**. **Remarque :** Ce paramètre s'affiche uniquement après avoir appliqué un filtre.
Afficher	Dans cette zone de liste, vous pouvez sélectionner l'intervalle selon lequel vous souhaitez filtrer.

Tableau 15. Paramètres d'événements bruts (suite)

Paramètre	Description
Statistiques en cours	Lorsque vous n'êtes pas en mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), les statistiques en cours ci-après s'affichent : **Remarque :** Cliquez sur la flèche à côté de **Statistiques en cours** pour afficher ou masquer les statistiques • **Résultats totaux** - Indique le nombre total de résultats correspondant à vos critères de recherche. • **Fichiers de données recherchés** - Indique le nombre total de fichiers de données recherchés au cours de l'intervalle de temps spécifié. • **Fichiers de données compressés recherchés** - Indique le nombre total de fichiers de données compressés recherchés dans l'intervalle de temps spécifié. • **Nombre de fichiers d'index** - Indique le nombre total de fichiers d'indexation recherchés au cours de l'intervalle de temps spécifié. • **Durée** - Indique la durée de la recherche. **Remarque :** Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service client pour identifier et résoudre les problèmes des événements, vous pouvez être invité à fournir des informations statistiques en cours.
Graphiques	Affiche les graphiques configurables qui représentent les enregistrements correspondant à l'intervalle de temps et l'option de regroupement. Cliquez sur **Masquer les graphiques** si vous voulez supprimer les graphiques de votre affichage. Les graphiques s'affichent uniquement après avoir sélectionné un délai de type Dernier intervalle (actualisation automatique) au minimum et une option de regroupement à afficher. **Remarque :** Si vous utilisez Mozilla Firefox en tant que navigateur et qu'une extension de navigateur de blocage de publicité est installée, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez supprimer l'extension de navigateur de blocage de publicité. Pour plus d'informations, voir la documentation de votre navigateur.
Icône Infractions	Cliquez sur cette icône pour afficher les détails de l'infraction associée à cet événement.

Tableau 15. Paramètres d'événements bruts (suite)

Paramètre	Description
Heure de début	Indique l'heure du premier événement, tel que rapporté à QRadar par la source du journal.
Source de journal	Indique la source du journal qui a généré cet événement. S'il existe plusieurs sources de journal associées à cet événement, cette zone indique le terme Multiple et le nombre de sources du journal.
Contenu	Indique les informations de contenu d'événement original au format UTF-8.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Dans la zone de liste **Affichage**, sélectionnez **Evénements bruts**.
3. Dans la zone de liste **Vue**, sélectionnez le délai que vous souhaitez afficher.
4. Cliquez deux fois sur l'événement que vous souhaitez afficher de façon plus détaillée. Voir Détails d'événement.

Affichage d'événements groupés

Grâce à l'onglet **Activité du journal**, vous pouvez afficher les événements groupés selon différentes options. Dans la zone de liste **Afficher**, vous pouvez sélectionner le paramètre par lequel vous souhaitez grouper les événements.

Pourquoi et quand exécuter cette tâche

La zone de liste Afficher ne s'affiche pas en mode de diffusion en flux car ce mode ne prend pas en charge les événements regroupés. Si vous entrez le mode de diffusion en flux à l'aide de critères de recherche non groupés, cette option s'affiche.

La zone de liste Afficher fournit les options suivantes :

Tableau 16. Options des événements regroupés

Option de groupe	Description
Catégorie de niveau inférieur	Affiche une liste résumée des événements groupés en fonction de la catégorie de bas niveau de l'événement. Pour plus d'informations sur les catégories, voir *IBM Security QRadar Administration Guide*.
Nom d'événement	Affiche une liste résumée des événements groupés par le nom normalisé de l'événement.
IP de destination	Affiche une liste résumée des événements groupés par l'adresse IP de destination de l'événement.
Port de destination	Affiche une liste résumée des événements groupés par l'adresse du port de destination de l'événement.

Tableau 16. Options des événements regroupés (suite)

Option de groupe	Description
IP source	Affiche une liste résumée des événements groupés par l'adresse IP source de l'événement.
Règle personnalisée	Affiche une liste résumée des événements regroupés par la règle personnalisée associée.
Nom d'utilisateur	Affiche une liste résumée des événements regroupés par le nom d'utilisateur associé à l'événement.
Source de journal	Affiche une liste résumée des événements regroupés par les sources de journal ayant envoyé l'événement à QRadar.
Catégorie de niveau supérieur	Affiche une liste résumée des événements regroupés par la catégorie de haut niveau de l'événement.
Réseau	Affiche une liste résumée des événements regroupés par le réseau associé à l'événement.
Port source	Affiche une liste résumée des événements regroupés par l'adresse source du port de l'événement.

Après avoir sélectionné une option dans la zone de liste **Afficher**, l'agencement de colonne des données dépend de l'option de groupe choisie. Chaque ligne dans la table d'événements représente un groupe d'événements. L'onglet **Activité du journal** fournit les informations suivantes pour chaque groupe d'événements

Tableau 17. Paramètres des événements regroupés

Paramètre	Description
Groupement par	Indique le paramètre sur lequel la recherche est regroupée.
Filtres en cours	Le haut du tableau affiche les détails du filtre appliqué aux résultats de la recherche. Pour effacer ces valeurs de filtre, cliquez sur **Effacer le filtre**.
Afficher	Dans la zone de liste, vous pouvez sélectionner l'intervalle à partir duquel vous souhaitez filtrer.

Tableau 17. Paramètres des événements regroupés (suite)

Paramètre	Description
Statistiques en cours	Lorsque vous n'êtes pas en mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), les statistiques en cours ci-après s'affichent : **Remarque :** Cliquez sur la flèche à côté de **Statistiques en cours** pour afficher ou masquer les statistiques. • **Résultats totaux** - Indique le nombre total de résultats correspondant à vos critères de recherche. • **Fichiers de données recherchés** - Indique le nombre total de fichiers de données recherchés au cours de l'intervalle de temps spécifié. • **Fichiers de données compressés recherchés** - Indique le nombre total de fichiers de données compressés dans l'intervalle de temps spécifié. • **Nombre de fichiers d'index** - Indique le nombre total de fichiers d'indexation recherchés au cours de l'intervalle de temps spécifié. • **Durée** - Indique la durée de la recherche. **Remarque :** Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service clients pour identifier et résoudre les événements, vous pouvez être invité à fournir des informations sur les statistiques en cours.

Tableau 17. Paramètres des événements regroupés (suite)

Paramètre	Description
Graphiques	Affiche les graphiques configurables qui représentent les enregistrements correspondant à l'intervalle de temps et l'option de regroupement. Cliquez sur **Masquer les graphiques** si vous souhaitez supprimer le graphique de votre affichage. Chaque graphique fournit une légende, qui constitue une référence visuelle pour vous aider à associer les objets de graphique aux paramètres qu'ils représentent. À l'aide de la fonction de légende, vous pouvez effectuer les actions suivantes : • Déplacez le pointeur de votre souris sur un élément de légende pour afficher plus d'informations sur les paramètres qu'il représente. • Cliquez avec le bouton droit de la souris sur l'élément de la légende afin d'étudier cet élément. • Cliquez sur un graphique circulaire pour masquer l'élément dans le graphique. Cliquez de nouveau sur l'élément de légende pour afficher l'élément masqué. Vous pouvez également cliquer sur l'élément de graphique correspondant pour masquer/afficher l'élément. • Cliquez sur **Légende** si vous souhaitez déplacer la légende de votre affichage du graphique. **Remarque :** Les graphiques s'affichent uniquement après avoir sélectionné un délai de type Dernier intervalle (actualisation automatique) au minimum et une option de regroupement à afficher. **Remarque :** Si vous utilisez Mozilla Firefox en tant que navigateur et qu'une extension de navigateur de blocage de publicité est installée, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez supprimer l'extension de navigateur de blocage de publicité. Pour plus d'informations, voir la documentation de votre navigateur.
IP source (Nombre unique)	Indique l'adresse IP source associée à cet événement. S'il existe plusieurs adresses IP associées à cet événement, cette zone indique le terme Multiple et le nombre d'adresses IP.
IP de destination (Nombre unique)	Indique l'adresse IP de destination associée à cet événement. S'il existe plusieurs adresses IP associées à cet événement, cette zone indique le terme Multiple et le nombre d'adresses IP.

Tableau 17. Paramètres des événements regroupés (suite)

Paramètre	Description
Port de destination (Nombre unique)	Indique les ports de destination associés à cet événement. S'il existe plusieurs ports associés à cet événement, cette zone indique le terme Multiple et le nombre de ports.
Nom d'événement	Indique le nom normalisé de l'événement.
Source de journal (Nombre unique)	Indique les sources de journal ayant envoyé l'événement à QRadar. S'il existe plusieurs sources de journal associées à cet événement, cette zone indique le terme Multiple et le nombre de sources de journal.
Catégorie de niveau supérieur (Nombre unique)	Indique la catégorie de haut niveau de cet événement. S'il existe plusieurs catégories associées à cet événement, cette zone indique le terme Multiple et le nombre de catégories. Pour plus d'informations sur les catégories, voir *IBM QRadar Log Manager Administration Guide*.
Catégorie de niveau inférieur (Nombre unique)	Indique la catégorie de bas niveau de cet événement. S'il existe plusieurs catégories associées à cet événement, cette zone indique le terme Multiple et le nombre de catégories.
Protocole (Nombre unique)	Indique l'ID du protocole associé à cet événement. S'il existe plusieurs protocoles associés à cet événement, cette zone indique le terme Multiple et le nombre d'ID du protocole.
Nom d'utilisation (Nombre unique)	Indique le nom d'utilisateur associé à cet événement, s'il est disponible. S'il existe plusieurs noms d'utilisateur associés à cet événement, cette zone indique le terme Multiple et le nombre de noms d'utilisateurs.
Magnitude (Maximum)	Indique l'ampleur maximale calculée pour les événements regroupés. Les variables utilisées pour calculer l'ampleur incluent la crédibilité, la pertinence et la gravité. Pour plus d'informations sur la crédibilité, la pertinence et la gravité, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).
Nombre d'événements (Somme)	Indique le nombre total d'événements regroupés dans cet événement normalisé. Les événements sont regroupés lorsque plusieurs événements du même type pour la même adresse IP source et de destination sont identifiés dans une courte période.
Nombre	Indique le nombre total d'événements normalisés dans ce groupe d'événements.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Dans la zone de liste **Vue**, sélectionnez le délai que vous souhaitez afficher.
3. Dans la zone de liste Affichage, sélectionnez le paramètre selon lequel vous souhaitez regrouper les événements. Voir le Tableau 2. Les groupes d'événements sont répertoriés. Pour plus d'informations sur les groupes d'événements, voir le tableau 1.
4. Pour afficher la page Liste d'événements pour un groupe, cliquez deux fois sur le groupe des événements que vous souhaitez étudier. La page Liste d'événements ne conserve pas les configurations de graphique définies sur l'onglet **Activité du journal**. Pour plus d'informations sur les paramètres de la page Liste d'événements, voir le tableau 1.
5. Pour afficher les détails de l'événement, cliquez deux fois sur l'événement que vous souhaitez étudier. Pour plus d'informations sur les détails de l'événement, voir le tableau 2.

Affichage des détails des événements

Vous pouvez afficher une liste des événements dans différents modes, notamment le mode de diffusion en flux ou groupes d'événements. Quel que soit le mode que vous choisissez pour afficher les événements, vous pouvez localiser et afficher les détails d'un événement unique.

La page des détails d'événement fournit les informations suivantes :

Tableau 18. Détails d'événement

Paramètre	Description
Nom d'événement	Indique le nom normalisé de l'événement.
Catégorie de niveau inférieur	Indique la catégorie de bas niveau de cet événement. Pour plus d'informations sur les catégories, voir *IBM Security QRadar Administration Guide*.
Description de l'événement	Indique une description de l'événement, si disponible.
Magnitude	Indique l'ampleur de cet événement. Pour plus d'informations sur la magnitude, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).
Pertinence	Indique le degré de pertinence de cet événement. Pour plus d'informations sur la pertinence, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).
Gravité	Indique la gravité de cet événement. Pour plus d'informations sur la gravité, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).

Tableau 18. Détails d'événement (suite)

Paramètre	Description
Crédibilité	Indique la crédibilité de cet événement. Pour plus d'informations sur la crédibilité, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).
Nom d'utilisateur	Indique le nom d'utilisateur associé à cet événement, le cas échéant.
Heure de début	Indique l'heure à laquelle l'événement a été reçu de la source du journal.
Heure de stockage	Indique l'heure à laquelle l'événement a été enregistré dans la base de données QRadar.
Heure de la source de journal	Indique l'heure système telle que rapportée par la source de journal dans le contenu d'événement.
Informations de détection des anomalies - Ce volet s'affiche uniquement si cet événement a été généré par une règle de détection des anomalies. Cliquez sur l'icône **Anomalie** pour afficher les résultats de la recherche sauvegardée qui ont entraîné la génération de cet événement par la règle de détection des anomalies.	
Description de la règle	Indique la règle de détection d'anomalie qui a généré cet événement.
Description de l'anomalie	Indique une description du comportement anormal qui a été détecté par la règle de détection des anomalies.
Valeur d'alerte d'anomalie	Indique la valeur d'alerte d'anomalie.
Informations sur la source et la cible	
IP source	Indique l'adresse IP source de l'événement.
IP de destination	Indique l'adresse IP cible de l'événement.
Nom de l'actif source	Indique le nom d'actif de la source de l'événement défini par l'utilisateur. Pour en savoir plus sur les actifs, voir Gestion des actifs.
Nom de l'actif de destination	Indique le nom de l'actif cible de l'événement défini par l'utilisateur. Pour en savoir plus sur les actifs, voir Gestion des actifs.
Port source	Indique le port source de cet événement.
Port de destination	Indique le port de destination de cet événement.
Adresse IP source avant conversion d'adresses réseau	Pour un pare-feu ou un autre périphérique doté de la fonction de conversion d'adresses réseau (NAT), ce paramètre définit l'adresse IP source avant l'application des valeurs NAT. NAT convertit l'adresse IP dans un réseau en une adresse IP différente dans un autre réseau.
Adresse IP de destination avant conversion d'adresses réseau	Pour un pare-feu ou un autre périphérique doté de la fonction NAT, ce paramètre définit l'adresse IP de destination avant l'application des valeurs NAT.

Tableau 18. Détails d'événement (suite)

Paramètre	Description
Port source avant conversion d'adresses réseau	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port source avant que les valeurs soient appliquées.
Port de destination avant conversion d'adresses réseau	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port de destination avant que les valeurs soient appliquées.
Adresse IP source après conversion d'adresses réseau	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit l'adresse IP source avant que les valeurs NAT soient appliquées.
Adresse IP de destination après conversion d'adresses réseau	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit l'adresse IP de destination avant que les valeurs NAT soient appliquées.
Port source après conversion d'adresses réseau	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port source avant que les valeurs NAT soient appliquées.
Port de destination après conversion d'adresses réseau	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port de destination avant que les valeurs NAT soient appliquées.
Port source après conversion d'adresses réseau	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port source avant que les valeurs NAT soient appliquées.
Port de destination après conversion d'adresses réseau	Pour un pare-feu ou un autre périphérique capable d'effectuer la NAT, ce paramètre définit le port de destination avant que les valeurs NAT soient appliquées.
Source IPv6	Indique l'adresse IPv6 source de l'événement.
Destination IPv6	Indique l'adresse IPv6 cible de l'événement.
Adresse MAC source	Indique l'adresse MAC source de l'événement.
Adresse MAC de destination	Indique l'adresse MAC cible de l'événement.
Informations de contenu	
Contenu	Indique le contenu utile de l'événement. Cette zone offre 3 onglets pour afficher le contenu utile : • Format de transformation universel (UTF) - Cliquez sur UTF. • Hexadécimal - Cliquez sur HEX. • Base64 - Cliquez sur Base64.
Informations supplémentaires	
Protocole	Indique le protocole associé à cet événement.

Tableau 18. Détails d'événement (suite)

Paramètre	Description
QID	Indique le QID de cet événement. Chaque événement possède un QID unique. Pour en savoir plus sur le mappage d'un QID, consultez la section Modification du mappage d'événement.
Source de journal	Indique la source de journal ayant envoyé l'événement à QRadar. S'il existe plusieurs sources de journal associées à cet événement, cette zone indique le terme Multiple et le nombre de sources du journal.
Nombre d'événements	Indique le nombre total d'événements regroupés dans cet événement normalisé. Les événements sont regroupés lorsque plusieurs événements du même type pour l'adresse IP source et cible sont détectés dans un court laps de temps.
Règles personnalisées	Indique les règles personnalisées qui correspondent à cet événement. .
Correspondance partielle avec les règles personnalisées	Indique les règles personnalisées qui correspondent partiellement à cet événement.
Annotations	Indique l'annotation pour cet événement. Les annotations sont des descriptions textuelles que les règles peuvent ajouter automatiquement aux événements au sein d'une réponse de règle.
Informations d'identité - QRadar collecte des informations d'identité, le cas échéant, à partir des messages source du journal. Les informations d'identité fournissent des détails supplémentaires sur les actifs de votre réseau. Les sources du journal génèrent des informations d'identité uniquement si le message de journal envoyé à QRadar contient une adresse IP et au moins l'un des éléments suivants : nom d'utilisateur ou adresse MAC. Les sources du journal ne génèrent pas toutes des informations d'identité.	
Nom d'utilisateur de l'identité	Indique le nom d'utilisateur de l'actif associé à cet événement.
IP de l'identité	Indique l'adresse IP de l'actif associé à cet événement.
Nom Net Bios de l'identité	Indique le nom du système d'entrée/sortie de la base du réseau (Net Bios) de l'actif associé à cet événement.
Champ étendu de l'identité	Indique plus d'informations sur l'actif associé à cet événement. Le contenu de cette zone est un texte défini par l'utilisateur et repose sur les périphériques sur votre réseau qui sont disponibles pour fournir des informations d'identité. On peut citer : l'emplacement physique des noms de ports, des politiques pertinentes, des commutateurs de réseau et des noms de port.

Tableau 18. Détails d'événement (suite)

Paramètre	Description
Dispose d'une identité (indicateur)	Indique la valeur Vrai si QRadar a collecté des informations d'identité pour l'actif associé à cet événement. Pour savoir quels périphériques envoient les informations d'identités, voir le *Guide de configuration de services de données IBM QRadar*.
Nom d'hôte de l'identité	Indique le nom d'hôte de l'actif associé à cet événement.
Adresse MAC de l'identité	Indique l'adresse MAC de l'actif associé à cet événement.
Nom de groupe de l'identité	Indique le nom de groupe de l'actif associé à cet événement.

Barre d'outils des détails d'événements

La barre d'outils des détails d'événements offre plusieurs fonctions pour l'affichage des détails d'événements.

La barre d'outils **détails d'événements** offre les fonctions suivantes :

Tableau 19. Barre d'outils des détails d'événements

Retour à la liste d'événements	Cliquez sur **Retour** à la **liste d'événements** pour retourner à la liste d'événements.
Infraction	Cliquez sur **Infraction** pour afficher les infractions associées à l'événement.
Anomalie	Cliquez sur **Anomalie** pour afficher les résultats de recherche enregistrée qui ont entraîné la génération de cet événement par la règle de détection des anomalies. **Remarque :** Cette icône s'affiche uniquement si cet événement a été généré par une règle de détection d'anomalie.
Cartographier l'événement	Cliquez sur **Cartographier l'événement** pour éditer le mappage d'événements. Pour en savoir plus, voir section Modification du mappage d'événements.
Faux positif	Cliquez sur **Faux positif** pour régler QRadar afin d'éviter la génération d'événements de faux positifs dans les infractions.
Extraire la propriété	Cliquez sur **Extraire la propriété** pour créer une propriété d'événement personnalisé à partir de l'événement sélectionné.
Précédent	Cliquez sur **Précédent** pour afficher l'événement précédent dans la liste d'événement.
Suivant	Cliquez sur **Suivant** pour afficher l'événement suivant dans la liste d'événements.

Tableau 19. Barre d'outils des détails d'événements (suite)

Données PCAP	**Remarque :** Cette option s'affiche uniquement si votre console QRadar est configurée pour s'intégrer à Juniper JunOS Platform DSM. Pour en savoir plus sur la gestion des données PCAP, consultez la section Gestion des données PCAP. • **Afficher les informations PCAP** - Sélectionnez cette option pour afficher les informations PCAP. Pour en savoir plus, consultez la section Affichage d'informations PCAP. • **Télécharger le fichier PCAP** - Sélectionnez cette option pour télécharger le fichier PCAP pour votre système de bureau. Pour en savoir plus, consultez la section Téléchargement du fichier PCAP pour votre système de bureau.
Imprimer	Cliquez sur **Imprimer** pour imprimer les détails d'événement.

Affichage des infractions associées

Dans l'onglet Activité du journal, vous pouvez afficher l'infraction associée à l'événement.

Pourquoi et quand exécuter cette tâche

Si un événement correspond à une règle, une infraction peut être générée sur l'onglet **Infractions**.

Pour plus d'informations sur les règles, voir *IBM Security QRadar Administration Guide*.

Lorsque vous affichez une infraction à partir de l'onglet **Activité du journal**, l'infraction risque de ne pas s'afficher si le magistrat n'a pas encore enregistré l'infraction associée à l'événement sélectionné sur le disque ou si l'infraction a été purgée de la base de données. Si cela se produit, le système vous prévient.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Facultatif. Si vous affichez des événements en mode de diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause ce mode.
3. Cliquez sur l'icône **Infraction** à côté de l'événement que vous souhaitez étudier.
4. Affichez l'infraction associée.

Modification de mappage d'événement

Vous pouvez mapper manuellement un événement normalisé ou brut à une catégorie de niveau supérieur ou inférieur (ou QID).

Avant de commencer

Cette opération manuelle permet de mapper des événements de source de journal inconnus à des événements QRadar connus afin de pouvoir les classer et les traiter de façon adéquate.

Pourquoi et quand exécuter cette tâche

A des fins de normalisation, QRadar mappe automatiquement les événements de sources de journal vers des catégories de niveau supérieur et de niveau inférieur.

Pour plus d'informations sur les catégories d'événements, voir *IBM Security QRadar Administration Guide*.

Lorsque QRadar reçoit des événements de sources de journal que le système ne parvient pas à classer, ces événements sont classés comme étant inconnus. Ces événements se produisent pour plusieurs raisons, notamment :

- **Evénements définis par l'utilisateur** - Certaines sources de journal comme Snort, vous permettent de créer des événements définis par l'utilisateur.
- **Nouveaux événements ou événements plus anciens** - Les sources de journal des fournisseurs peuvent mettre à jour leurs logiciels avec des éditions de maintenance pour prendre en charge de nouveaux événements que QRadar ne prend peut-être pas en charge.

Remarque : L'icône **Cartographier l'événement** est désactivée pour les événements lorsque la catégorie de niveau supérieur est SIM Audit ou que le type de source de journal est Simple Object Access Protocol (SOAP).

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Facultatif. Si vous affichez des événements en mode de diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause ce mode.
3. Cliquez deux fois sur l'événement que vous souhaitez mapper.
4. Cliquez sur **Cartographier l'événement**.
5. Si vous connaissez le QID que vous souhaitez mapper à cet événement, entrez le QID dans la zone **Entrez des QID**.
6. Si vous ne connaissez pas le QID à mapper à cet événement, vous pouvez rechercher un QID particulier :
   a. Choisissez l'une des options suivantes : `Pour rechercher un QID par catégorie, sélectionnez la catégorie de niveau supérieur dans la zone de liste Catégorie de niveau supérieur. Pour rechercher un QID par catégorie, sélectionnez la catégorie de niveau inférieur dans la zone de liste Catégorie de niveau inférieur. Pour rechercher un QID par type de source de journal, sélectionnez un type de source de journal dans la zone de liste Type de la source de journal. Pour rechercher un QID par nom, entrez un nom dans la zone QID/Nom.`
   b. Cliquez sur **Rechercher**.
   c. Sélectionnez le **QID** que vous souhaitez associer à cet événement.
7. Cliquez sur **OK**.

Réglage des faux positifs

Vous pouvez utiliser la fonction Ajustement des faux positifs pour éviter que les événements faux positifs ne créent des infractions.

Avant de commencer

Vous pouvez régler les événements faux positifs à partir de la page event list ou event details.

Pourquoi et quand exécuter cette tâche

Vous pouvez régler les événements faux positifs à partir de la page event list ou event details.

Vous devez disposer des droits appropriés pour créer des règles personnalisées afin de régler les faux positifs.

Pour plus d'informations sur les rôles, voir *IBM Security QRadar Administration Guide*.

Pour plus d'informations sur les faux positifs, voir leglossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Facultatif. Si vous affichez des événements en mode de diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause ce mode.
3. Sélectionnez l'événement que vous souhaitez régler.
4. Cliquez sur **Faux positif**.
5. Dans le panneau Propriété d'événement/de flux de la fenêtre Faux positif, sélectionnez l'une des options suivantes :
   - Evénement/Flux avec un QID spécifique de <Evénement>
   - Tout événement/flux avec une catégorie de bas niveau de <Evénement>
   - Tout événement/flux avec une catégorie de haut niveau de <Evénement>
6. Dans le panneau Direction du trafic, sélectionnez l'une des options suivantes :
   - <D'une adresse IP source > vers <une adresse IP de destination>
   - <D'une adresse IP source> vers n'importe quelle destination
   - De n'importe quelle source vers <une adresse IP de destination>
   - De n'importe quelle source vers n'importe quelle destination
7. Cliquez sur **Optimiser**.

Données PCAP

Si votre console QRadar est configurée pour s'intégrer au gestionnaire de services de données Juniper JunOS Platform, les données Packet Capture (PCAP) peuvent être reçues, traitées, puis stockées à partir d'une source de journal Juniper SRX-Series Services Gateway.

Pour plus d'informations sur le gestionnaire de services de données Juniper JunOS Platform, voir le document *IBM QRadar - Guide de configuration du gestionnaire de services de données*.

Affichage de la colonne de données PCAP

La colonne **Données PCAP** ne s'affiche pas par défaut dans l'onglet **Activité du journal**. Lorsque vous créez un critère de recherche, vous devez sélectionner la colonne **Données PCAP** du volet Définition de colonne.

Avant de commencer

Avant de pouvoir afficher des données PCAP dans l'onglet **Activité du journal**, la source du journal de la passerelle de service Juniper SRX-Series doit être configurée à l'aide du protocole PCAP Syslog Combination. Pour plus d'informations sur la configuration des protocoles de sources de journal, voir *Managing Log Sources Guide*.

Pourquoi et quand exécuter cette tâche

Lorsque vous effectuez une recherche incluant la colonne **Données PCAP**, une icône apparaît dans la colonne **Données PCAP** des résultats de la recherche si les données PCAP sont disponibles pour un événement. L'icône **PCAP** vous permet d'afficher des données PCAP ou de télécharger le fichier **PCAP** sur votre système de bureau.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Dans la zone de liste **Rechercher**, sélectionnez **Nouvelle recherche**.
3. Facultatif. Pour rechercher des événements contenant des données PCAP, configurez les critères de recherche suivants :
   a. Dans la première zone de liste, sélectionnez **Données PCAP**.
   b. Dans la deuxième zone de liste, sélectionnez **Est égal à**.
   c. Dans la troisième zone de liste, sélectionnez **Vrai**.
   d. Cliquez sur **Ajouter un filtre**.
4. Configurez vos définitions de colonnes pour inclure la colonne **Données PCAP** :
   a. Dans la liste **Colonnes disponibles** du volet Définition de colonne, cliquez sur **Données PCAP**.
   b. Cliquez sur l'icône **Ajouter une colonne** de l'ensemble d'icônes inférieur pour déplacer la colonne **Données PCAP** vers la liste **Colonnes**.
   c. Facultatif. Cliquez sur l'icône **Ajouter une colonne** de l'ensemble d'icônes supérieur pour déplacer la colonne **Données PCAP** vers la liste **Grouper par**.
5. Cliquez sur **Filtrer**.
6. Facultatif. Si vous affichez des événements en mode de diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause la diffusion en flux.
7. Cliquez deux fois sur l'événement que vous souhaiter étudier.

Que faire ensuite

Pour plus d'informations sur l'affichage et le téléchargement de données PCAP, reportez-vous aux sections suivantes :

- Affichage des informations PCAP
- Téléchargement du fichier PCAP sur votre système de bureau

Affichage des informations PCAP

Dans le menu de la barre d'outils **Données PCAP**, vous pouvez afficher une version lisible des données dans le fichier PCAP ou télécharger le fichier PCAP sur votre système de bureau.

Avant de commencer

Avant de pouvoir afficher des informations PCAP, vous devez effectuer ou sélectionner une recherche qui affiche la colonne **Données PCAP**.

Pourquoi et quand exécuter cette tâche

Avant de pouvoir afficher les données PCAP, le fichier PCAP doit être récupéré pour affichage sur l'interface utilisateur. Si le processus de téléchargement dure longtemps, la fenêtre Téléchargement des informations PCAP s'affiche. Dans la plupart des cas, le processus de téléchargement est rapide et cette fenêtre ne s'affiche pas.

Après avoir récupéré le fichier, une fenêtre contextuelle s'affiche fournissant une version lisible du fichier PCAP. Vous pouvez lire les informations affichées dans la fenêtre ou télécharger les informations sur votre système de bureau.

Procédure

1. Pour l'événement que vous souhaitez étudier, choisissez une des options suivantes :
   - Sélectionnez l'événement et cliquez sur l'icône **PCAP**.
   - Cliquez avec le bouton droit de la souris sur l'icône **PCAP** de l'événement et sélectionnez **Options supplémentaires** > **Afficher les informations PCAP**.
   - Cliquez deux fois sur l'événement que vous souhaitez étudier, puis sélectionnez **Données PCAP** > **Afficher les informations PCAP** dans la barre d'outils des détails d'événement.
2. Si vous souhaitez télécharger les informations sur votre système de bureau, choisissez l'une des options suivantes :
   - Cliquez sur **Télécharger le fichier PCAP** pour télécharger le fichier PCAP d'origine à utiliser dans une application externe.
   - Cliquez sur **Télécharger le texte PCAP** pour télécharger les informations PCAP au format .TXT
3. Sélectionnez une des options suivantes :
   - Si vous souhaitez ouvrir le fichier pour un affichage immédiat, sélectionnez l'option **Ouvrir avec** puis sélectionnez une application dans la zone de liste.
   - Si vous souhaitez enregistrer la liste, sélectionnez l'option **Sauvegarder le fichier**.
4. Cliquez sur **OK**.

Téléchargement du fichier PCAP sur votre système de bureau

Vous pouvez télécharger le fichier PCAP sur votre système de bureau pour stockage ou pour utilisation dans d'autres applications.

Avant de commencer

Avant de pouvoir visualiser des informations PCAP, vous devez effectuer ou sélectionner une recherche affichant la colonne de données PCAP. Voir **Affichage de la colonne de données PCAP**.

Procédure

1. Pour l'événement que vous souhaitez étudier, choisissez l'une des options suivantes :
   - Sélectionnez l'événement et cliquez sur l'icône **PCAP**.
   - Cliquez avec le bouton droit de la souris sur l'icône PCAP de l'événement et sélectionnez **Options supplémentaires** > **Télécharger le fichier PCAP**.
   - Cliquez deux fois sur l'événement que vous souhaitez étudier, puis sélectionnez **Données PCAP** > **Télécharger le fichier PCAP** dans la barre d'outils des détails d'événement.
2. Sélectionnez l'une des options suivantes :
   - Si vous souhaitez ouvrir le fichier pour l'affichage immédiat, sélectionnez l'option **Ouvrir avec** et sélectionnez une application dans la zone de liste.
   - Si vous souhaitez enregistrer la liste, sélectionnez l'option **Sauvegarder le fichier**.
3. Cliquez sur **OK**.

Exportation d'événements

Vous pouvez exporter des événements au format XML (Extensible Markup Language) ou CSV (Comma-Separated Values).

Avant de commencer

La durée nécessaire à l'exportation de vos données dépend du nombre de paramètres spécifiés.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Facultatif. Si vous affichez des événements en mode de diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause ce mode.
3. Dans la zone de liste **Actions**, sélectionnez l'une des options suivantes :
   - **Exporter au format XML** > **Colonnes visibles** - Sélectionnez cette option pour exporter uniquement les colonnes qui sont visibles dans l'onglet Activité du journal. Il s'agit de l'option recommandée.
   - **Exporter au format XML** > **Exportation complète (toutes les colonnes)** - Sélectionnez cette option pour exporter tous les paramètres d'événement. Une exportation complète peut prendre un certain temps.
   - **Exporter au format CSV** > **Colonnes visibles** - Sélectionnez cette option pour exporter uniquement les colonnes visibles dans l'onglet **Activité du journal**. Il s'agit de l'option recommandée.
   - **Exporter au format CSV** > **Exportation complète (toutes les colonnes)** - Sélectionnez cette option pour exporter tous les paramètres d'événement. Une exportation complète peut prendre un certain temps.
4. Si vous souhaitez reprendre vos activités lors de l'exportation, cliquez sur **Aviser à la fin de l'opération**.

Résultats

Lorsque l'exportation est terminée, vous recevez une notification vous informant que l'exportation est terminée. Si vous n'avez pas sélectionné l'icône **Aviser à la fin de l'opération**, la fenêtre de statut s'affiche.

Chapitre 6. Surveillance de l'activité réseau

L'onglet **Activité réseau** vous permet de surveiller et d'étudier l'activité réseau (flux) en temps réel ou d'effectuer des recherches avancées.

Présentation de l'onglet Activité réseau

L'onglet **Activité réseau** vous permet de surveiller et d'étudier l'activité réseau (flux) en temps réel ou d'effectuer des recherches avancées.

L'affichage de l'onglet **Activité réseau** nécessite une autorisation.

Pour plus d'informations sur les autorisations et l'affectation de rôles, voir *IBM Security QRadar Administration Guide*.

Sélectionnez l'onglet **Activité réseau** pour contrôler visuellement et étudier les données de flux en temps réel ou effectuer des recherches avancées pour filtrer les flux affichés. Un flux est une session de communication entre deux hôtes. Vous pouvez afficher les informations des flux afin de déterminer comment le trafic est communiqué et ce qui est communiqué (si l'option de capture de contenu est activée). Les informations sur le flux peuvent également comprendre certains détails tels que les protocoles, les valeurs ASN ou les valeurs IFIndex (Interface Index).

Barre d'outils de l'onglet Activité réseau

Vous pouvez accéder à plusieurs options à partir de la barre d'outils de l'onglet **Activité réseau**.

Vous pouvez accéder aux options suivantes à partir de la barre d'outils de l'onglet **Activité réseau** :

Tableau 20. Options de la barre d'outils de l'onglet Activité réseau

Options	Description
Rechercher	Cliquez sur **Rechercher** pour effectuer des recherches avancées sur les flux. Les options de recherche incluent : • **Nouvelle recherche** - Sélectionnez cette option pour créer une nouvelle recherche de flux. • **Editer la recherche** - Sélectionnez cette option pour sélectionner et modifier la recherche de flux. • **Gérer les résultats de la recherche** - Sélectionnez cette option pour afficher et gérer les résultats de la recherche. Pour plus d'informations sur la fonction de recherche, voir Recherches de données.

© Copyright IBM Corp. 2012, 2017

Tableau 20. Options de la barre d'outils de l'onglet Activité réseau (suite)

Options	Description
Recherches rapides	Dans cette zone de liste, vous pouvez exécuter des recherches précédemment enregistrées. Les options ne sont affichées dans la zone de liste **Recherches rapides** que lorsque vous avez enregistré un critère de recherche qui indique l'option **Inclure dans mes recherches rapides**.
Ajouter un filtre	Cliquez sur **Ajouter un filtre** pour ajouter un filtre aux résultats de recherche actuelle.
Sauvegarder les critères	Cliquez sur **Sauvegarder les critères** pour sauvegarder les critères de la recherche actuelle.
Sauvegarder les résultats	Cliquez sur **Sauvegarder les résultats** pour sauvegarder les résultats de la recherche actuelle. Cette option ne s'affiche qu'après qu'une recherche soit terminée. Cette option est désactivée en mode de diffusion en flux.
Annuler	Cliquez sur **Annuler** pour annuler une recherche en cours. Cette option est désactivée en mode de diffusion en flux.
Faux positif	Cliquez sur **Faux positif** pour ouvrir la fenêtre Ajustement des faux positifs afin de désactiver les flux connus en tant que faux positifs pour les empêcher de créer des infractions. Pour plus d'informations sur les faux positifs, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html). Cette option est désactivée en mode de diffusion en flux. Voir Exportation de flux.

Tableau 20. Options de la barre d'outils de l'onglet Activité réseau (suite)

Options	Description
Règles	L'option **Règles** n'est visible que si vous avez l'autorisation d'afficher des règles personnalisées. Sélectionnez l'une des options suivantes : **Règles** pour afficher ou créer une règle. Si vous êtes autorisé à afficher les règles, la page de synthèse de l'assistant Règles s'affiche. Si vous avez l'autorisation de maintenir des règles personnalisées, vous pouvez modifier la règle. **Remarque :** Les options de règle de détection d'anomalies ne sont visibles que si vous disposez de l'autorisation **Activité réseau** > **Disposer du droit de gestion de règles personnalisées**. Pour activer les options de la règle de détection des anomalies, vous devez sauvegarder les critères de recherche agrégés. Les critères de recherche sauvegardés spécifient les paramètres requis. Sélectionnez l'une des options suivantes **Ajouter une règle de seuil** pour créer une règle de seuil. Une règle de seuil teste le trafic de flux pour une activité qui dépasse un seuil configuré. Les seuils peuvent reposer sur toutes les données collectées. Par exemple, si vous créez une règle de seuil indiquant que le nombre de clients pouvant se connecter au serveur ne doit pas dépasser 220 clients entre 08h00 et 17h00, les règles génèrent une alerte lorsque le 221ème client tente de se connecter. **Ajouter une règle de comportement** pour créer une règle de comportement. Une règle de comportement teste le trafic de flux relatif aux changements de volume dans le comportement qui se produit dans les modèles saisonniers réguliers. Par exemple, si un serveur de messagerie communique généralement avec 100 hôtes par seconde au milieu de la nuit et qu'ensuite il commence soudain à communiquer avec 1000 hôtes par seconde, une règle comportementale génère une alerte. **Ajouter une règle d'anomalie** pour créer une règle d'anomalie. Une règle d'anomalie teste le trafic du flux en vue de détecter une activité anormale, comme par exemple un trafic nouveau ou inconnu. Par exemple, vous pouvez créer une règle d'anomalie pour comparer le volume moyen du trafic des cinq dernières minutes avec le volume moyen du trafic au cours de la dernière heure. S'il existe un changement de plus de 40 %, la règle génère une réponse. Pour plus d'informations, voir *IBM Security QRadar Administration Guide*.

Tableau 20. Options de la barre d'outils de l'onglet Activité réseau (suite)

Options	Description
Actions	Cliquez sur **Actions** pour effectuer les actions suivantes : • **Afficher tout** - Sélectionnez cette option pour supprimer tous les filtres sur le critère de recherche et pour afficher tous les flux non filtrés. • **Imprimer** - Sélectionnez cette option pour imprimer les événements affichés sur la page. • **Exporter au format XML** - Sélectionnez cette option pour exporter les flux au format XML. Voir Exportation de flux. • **Exporter au format CSV** - Sélectionnez cette option pour exporter les flux au format CSV. Voir Exportation de flux . • **Supprimer** - Sélectionnez cette option pour supprimer un résultat de recherche. Voir Recherches de données. • **Envoyer une notification** - Sélectionnez cette option pour indiquer que vous souhaitez recevoir une notification par e-mail à la fin des recherches sélectionnées. Cette option n'est activée que pour les recherches en cours. **Remarque :** Les options **Imprimer**, **Exporter au format XML** et **Exporter au format CSV** sont désactivées en mode de diffusion en flux et lorsque vous affichez des résultats de recherche partielle.
Barre d'outils de recherche	**Recherche avancée** Sélectionnez **Recherche avancée** dans la zone de liste puis entrez une chaîne de recherche AQL (Ariel Query Language) pour indiquer les zones que vous souhaitez renvoyer. **Filtrage rapide** Sélectionnez **Filtrage rapide** dans la zone de liste pour rechercher des contenus à l'aide de mots ou de phrases simples.
Afficher	La vue par défaut sous l'onglet **Activité réseau** est un flux des événements en temps réel. La liste **Vue** contient des options qui permettent d'afficher également des événements au cours de plages de temps spécifiques. Après avoir choisi une plage de temps spécifique dans la liste **Vue**, vous pouvez modifier la plage de temps affichée en changeant les valeurs de date et d'heure dans les zones **Heure de début** et **Heure de fin**.

Options du menu contextuel

Sur l'onglet **Activité réseau**, vous pouvez faire un clic droit sur un flux pour accéder à des critères supplémentaires de filtrage.

Les options du menu contextuel sont :

Tableau 21. Options de menu contextuel

Option	Description
Filtrer sur	Sélectionnez cette option pour filtrer les flux sélectionnés, en fonction du paramètre sélectionné dans le flux.
Faux positif	Sélectionnez cette option pour ouvrir la fenêtre Ajustement des faux positifs, qui vous permet de désactiver les flux connus en tant que faux positifs pour les empêcher de créer des infractions. Cette option est désactivée en mode de diffusion en flux. Voir Exportation de flux.
Options supplémentaires :	Sélectionnez cette option pour étudier une adresse IP. Voir Etude des adresses IP. **Remarque :** Cette option n'est pas affichée en mode de diffusion en flux.
Filtrage rapide	Filtrage des éléments qui correspondent, ou qui ne correspondent pas, à la sélection.

Barre d'état

Lors de la diffusion des flux, la barre d'état affiche la moyenne des résultats reçus par seconde.

Il s'agit du nombre de résultats que la console a reçu avec succès de la part des processeurs d'événement. Si ce nombre est supérieur à 40 résultats par seconde, seulement 40 résultats s'affichent. Le reste est mémorisé dans la mémoire tampon. Pour afficher plus d'informations d'état, déplacez le pointeur de votre souris sur la barre d'état.

Lorsque les flux ne sont pas en cours de diffusion, la barre d'état affiche le nombre de résultats de recherche en cours d'affichage ainsi que le temps nécessaire au traitement des résultats de recherche.

Enregistrements des dépassements

Si vous disposez des autorisations d'administration, vous pouvez indiquer le nombre maximal de flux que vous souhaitez envoyer du QRadar QFlow Collector aux processeurs d'événements.

Si vous disposez des autorisations d'administration, vous pouvez indiquer le nombre maximal de flux que vous souhaitez envoyer du QRadar QFlow Collector aux processeurs d'événements. Toutes les données collectées une fois la limite de flux configurée atteinte sont regroupées dans un enregistrement de flux unique. Cet enregistrement de flux s'affiche ensuite sur l'onglet **Activité réseau** avec l'adresse IP source de 127.0.0.4 et l'adresse IP de destination de 127.0.0.5. Cet enregistrement de flux indique le dépassement sur l'onglet **Activité réseau**.

Surveillance de l'activité réseau

Par défaut, l'onglet **Activité réseau** affiche les flux en mode de diffusion en flux, ce qui vous permet d'afficher les flux en temps réel.

Pour plus d'informations sur la diffusion en flux, voir Affichage des flux de diffusion en flux. Vous pouvez spécifier un intervalle pour filtrer les flux à l'aide de la zone de liste **Vue**.

Si vous avez précédemment configuré des critères de recherche sauvegardés par défaut, les résultats de cette recherche sont automatiquement affichés lorsque vous accédez à l'onglet **Activité réseau**. Pour plus d'informations sur la sauvegarde des critères de recherche, voir Sauvegarde des critères de recherche d'événement et de flux.

Affichage des flux en continu

Le mode d'affichage des flux vous permet d'afficher les données de flux entrantes dans votre système. Ce mode fournit un affichage en temps réel de votre activité de flux en cours en affichant les derniers 50 flux.

Pourquoi et quand exécuter cette tâche

Si vous appliquez un filtre dans l'onglet Activité réseau ou dans vos critères de recherche avant d'activer le mode de diffusion en flux, les filtres sont maintenus en mode de diffusion en flux. Cependant, le mode de diffusion en flux ne prend pas en charge les recherches qui comprennent les flux groupés. Si vous activez le mode de diffusion en flux sur des flux groupés ou des critères de recherche groupés, l'onglet Activité réseau affiche les flux normalisés. Voir Affichage des flux normalisés.

Lorsque vous souhaitez sélectionner un flux pour afficher les détails ou effectuer une action, vous devez mettre en pause ce mode avant de cliquer deux fois sur un événement. Lorsque la diffusion en flux est mise en pause, les derniers 1000 flux s'affichent.

Procédure

1. Cliquez sur l'onglet **Activité réseau**.
2. Dans la zone de liste Vue, sélectionnez **Temps réel (diffusion en flux)**.

Pour plus d'informations sur les options de la barre d'outils, voir la table 5-1. Pour plus d'informations sur les paramètres affichés en mode de diffusion en flux, voir la table 5-3.

3. Facultatif. Mettre en pause ou lire la diffusion en flux. Sélectionnez l'une des options suivantes :
   - Pour sélectionner un enregistrement d'événement, cliquez sur l'icône **Pause** pour suspendre la diffusion en flux.
   - Pour redémarrer le mode de diffusion en flux, cliquez sur l'icône **Play**.

Affichage des flux normalisés

Les flux de données sont collectés, normalisés puis affichés sur l'onglet **Activité réseau**.

Pourquoi et quand exécuter cette tâche

La normalisation implique la préparation des données de flux pour afficher des informations lisibles sur l'onglet.

Remarque : Si vous avez sélectionné un délai à afficher, un graphique de série temporelle s'affiche. Pour plus d'informations sur l'utilisation des graphiques de série temporelle, voir Présentation des graphiques de série temporelle.

L'onglet **Activité réseau** affiche les paramètres suivants lorsque vous consultez les flux normalisés :

Tableau 22. Paramètres de l'onglet Activité réseau

Paramètre	Description
Filtres en cours	Le haut du tableau affiche les détails des filtres appliqués aux résultats de recherche. Pour effacer ces valeurs de filtres, cliquez sur **Effacer le filtre**. **Remarque :** Ce paramètre s'affiche uniquement après avoir appliqué un filtre.
Afficher	Dans la zone de liste, vous pouvez sélectionner l'intervalle à partir duquel vous souhaitez filtrer.
Statistiques en cours	Lorsque vous n'êtes pas en mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), les statistiques en cours ci-après s'affichent : **Remarque :** Cliquez sur la flèche située à côté de Statistiques en cours pour afficher ou masquer les statistiques. • **Résultats totaux** - Indique le nombre total de résultats correspondant à vos critères de recherche. • **Fichiers de données recherchés** - Indique le nombre total de fichiers de données recherchés au cours de l'intervalle de temps spécifié. • **Fichiers de données compressés recherchés** - Indique le nombre total de fichiers compressés recherchés dans l'intervalle de temps spécifié. • **Nombre de fichiers d'index** - Indique le nombre total de fichiers d'indexation recherchés au cours de l'intervalle de temps spécifié. • **Durée** - Indique la durée de la recherche. **Remarque :** Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service client pour identifier et résoudre les flux, vous pouvez être invités à fournir les informations de statistiques en cours.

Tableau 22. Paramètres de l'onglet Activité réseau (suite)

Paramètre	Description
Graphiques	Affiche les graphiques configurables qui représentent les enregistrements correspondant à l'intervalle de temps et l'option de regroupement. Cliquez sur **Masquer les graphiques** si vous souhaitez supprimer les graphiques de votre affichage. Les graphiques s'affichent uniquement après avoir sélectionné un délai de type Dernier intervalle (actualisation automatique) au minimum et une option de regroupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir Configuration des graphiques. **Remarque :** Si vous utilisez Mozilla Firefox en tant que navigateur et qu'une extension de navigateur de blocage de publicité est installée, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez retirer l'extension de navigateur de blocage de publicité. Pour en savoir plus, consultez la documentation de votre navigateur.
Icône **Infractions**	Cliquez sur l'icône **Infractions** pour voir les détails de l'infraction associée à ce flux.
Type de flux	Indique le type de flux. Les types de flux se mesurent par le rapport de l'activité entrante avec l'activité sortante. Les types de flux sont les suivants : • **Flux standard**- Trafic Bidirectionnel • **Type A** - Un-vers-plusieurs (unidirectionnel), par exemple, un hôte unique effectuant une analyse réseau. • **Type B** - Plusieurs-vers-un (unidirectionnel), par exemple, une attaque DoS distribuée (DDoS). • **Type C** - Un-vers-un (unidirectionnel), par exemple, un hôte vers une analyse de port d'hôte.
Heure du premier paquet	Indique la date et l'heure de réception du flux.
Heure de stockage	Indique l'heure à laquelle l'événement a été enregistré dans la base de données QRadar.
IP source	Indique l'adresse IP source du flux.
Port source	Indique le port source du flux.
IP de destination	Indique l'adresse IP de destination du flux.
Port de destination	Indique le port de destination du flux.
Octets source	Indique le nombre d'octets envoyés à partir de l'hôte source.
Octets de destination	Indique le nombre d'octets envoyés à partir de l'hôte de destination.
Nombre total d'octets	Indique le nombre total d'octets associés au flux.

Tableau 22. Paramètres de l'onglet Activité réseau (suite)

Paramètre	Description
Paquets source	Indique le nombre total de paquets envoyés à partir de l'hôte source.
Paquets de destination	Indique le nombre total de paquets envoyés à partir de l'hôte de destination.
Paquets totaux	Indique le nombre total de paquets associés au flux.
Protocole	Indique le protocole associé au flux.
Application	Indique l'application détectée du flux. Pour plus d'informations sur la détection d'applications, voir *IBM Security QRadar Application Configuration Guide*.
Type/Code ICMP	Indique le type et le code Internet Control Message Protocol (ICMP), le cas échéant. Si le flux possède des informations de type ICMP et des informations de code sous un format connu, cette zone s'affiche en tant que Type <A>, Code <B>, où <A> et <B> sont les valeurs numériques du type et du code.
Indicateurs source	Indique les balises de Transmission Control Protocol(TCP) détectées dans le paquet source, le cas échéant.
Indicateurs de destination	Indique les balises TCP détectées dans le paquet de destination, le cas échéant.
QoS source	Indique le niveau de service Quality of service (QoS) du flux. QoS permet au serveur de fournir les différents niveaux de service pour les flux. QoS fournit les différents niveaux des services de base suivants : • **Meilleur effort** - Ce niveau de service ne garantit pas la livraison. La livraison du flux est assurée dans la mesure du possible. • **Service différencié** - Certains flux ont la priorité sur d'autres flux. Cette priorité est accordée en fonction de la classification de trafic. • **Service garanti** - Ce niveau de service garantit la réservation des ressources du réseau pour certains flux.
QoS de destination	Indique le niveau de service QoS pour le flux de destination.
Source de flux	Indique le système qui a détecté le flux.
Interface du flux	Indique l'interface qui reçoit le flux.
Index conditionnel source	Indique le nombre d'index d'interface source (IFIndex).
Index conditionnel de destination	Indique le nombre d'IFIndex de destination.
ASN source	Indique les valeurs Autonomous System Number (ASN) source.

Tableau 22. Paramètres de l'onglet Activité réseau (suite)

Paramètre	Description
ASN de destination	Indique les valeurs ASN de destination.

Procédure

1. Cliquez sur l'onglet **Activité réseau**.
2. Dans la zone de liste **Affichage**, sélectionnez **Par défaut (normalisé)**.
3. Dans la zone de liste **Vue**, sélectionnez le délai que vous souhaitez afficher.
4. Cliquez sur l'icône **Pause** pour mettre en pause la diffusion en flux.
5. Cliquez deux fois sur le flux que vous souhaitez afficher de façon plus détaillée. Voir Détails de flux.

Affichage des flux regroupés

Grâce à l'onglet **Activité réseau**, vous pouvez afficher les flux regroupés selon plusieurs options. A partir de la zone de liste **Afficher**, vous pouvez sélectionner le paramètre par lequel vous souhaitez regrouper les flux.

Pourquoi et quand exécuter cette tâche

La zone de liste **Afficher** ne s'affiche pas en mode de diffusion en flux car ce mode ne prend pas en charge les flux regroupés. Si vous entrez le mode de diffusion en flux à l'aide d'un critère de recherche non groupé, cette option s'affiche.

La zone de liste **Afficher** fournit les options suivantes :

Tableau 23. Options de flux regroupés

Option de groupe	Description
IP source ou de destination	Affiche une liste résumée des flux regroupés par l'adresse IP associée au flux.
IP source	Affiche une liste résumée des flux regroupés par l'adresse IP source du flux.
IP de destination	Affiche une liste résumée des flux regroupés par l'adresse IP de destination du flux.
Port source	Affiche une liste résumée des flux regroupés par le port source du flux.
Port de destination	Affiche une liste résumée des flux regroupés par le port de destination du flux.
Réseau source	Affiche une liste résumée des flux regroupés par le réseau source du flux.
Réseau de destination	Affiche une liste résumée des flux regroupés par le réseau de destination du flux.
Application	Affiche une liste résumée des flux regroupés par l'application qui a généré le flux.
Informations géographiques	Affiche une liste résumée des flux regroupés par emplacement géographique.
Protocole	Affiche une liste résumée des flux regroupés par le protocole associé au flux.
Biais du flux	Affiche une liste résumée des flux regroupés par la direction du flux.

Tableau 23. Options de flux regroupés (suite)

Option de groupe	Description
Type ICMP	Affiche une liste résumée des flux regroupés par le type ICMP du flux.

Après avoir sélectionné une option dans la zone de liste **Afficher**, l'agencement de colonne des données dépend de l'option de groupe choisie. Chaque ligne du tableau de flux représente un groupe de flux. L'onglet **Activité réseau** fournit les informations suivantes pour chaque groupe de flux.

Tableau 24. Paramètres des flux regroupés

En-tête	Description
Groupement par	Indique le paramètre sur lequel la recherche est regroupée.
Filtres en cours	Le haut du tableau affiche les détails du filtre appliqué aux résultats de la recherche. Pour effacer ces valeurs de filtre, cliquez sur **Effacer le filtre**.
Afficher	Dans la zone de liste, vous pouvez sélectionner l'intervalle à partir duquel vous souhaitez filtrer.
Statistiques en cours	Lorsque vous n'êtes pas en mode Temps réel (diffusion en flux) ou Dernière minute (actualisation automatique), les statistiques en cours ci-après s'affichent : **Remarque :** Cliquez sur la flèche à côté de **Statistiques en cours** pour afficher ou masquer les statistiques. • **Résultats totaux** - Indique le nombre total de résultats correspondant à vos critères de recherche. • **Fichiers de données recherchés** - Indique le nombre total de fichiers de données recherchés au cours de l'intervalle de temps spécifié. • **Fichiers de données compressés recherchés** -Indique le nombre total de fichiers de données compressés dans l'intervalle de temps spécifié. • **Nombre de fichiers d'index** - Indique le nombre total de fichiers d'indexation recherchés au cours de l'intervalle de temps spécifié. • **Durée** - Indique la durée de la recherche. **Remarque :** Les statistiques en cours sont utiles pour l'identification et la résolution des problèmes. Lorsque vous contactez le service client pour identifier et résoudre les flux, vous pouvez être invités à fournir les informations de statistiques en cours.

Tableau 24. Paramètres des flux regroupés (suite)

En-tête	Description
Graphiques	Affiche les graphiques configurables représentant les enregistrements correspondant à l'intervalle de temps et l'option de regroupement. Cliquez sur **Masquer les graphiques** si vous souhaitez supprimer les graphiques de votre affichage. Les graphiques s'affichent uniquement après avoir sélectionné un délai de type Dernier intervalle (actualisation automatique) au minimum et une option de regroupement à afficher. Pour plus d'informations sur la configuration des graphiques, voir Configuration des graphiques. **Remarque :** Si vous utilisez Mozilla Firefox en tant que navigateur et qu'une extension de navigateur de blocage de publicité est installée, les graphiques ne s'affichent pas. Pour afficher les graphiques, vous devez supprimer l'extension de navigateur de blocage de publicité. Pour plus d'informations, voir la documentation de votre navigateur.
IP source (Nombre unique)	Indique l'adresse IP source du flux.
IP de destination (Nombre unique)	Indique l'adresse IP de destination du flux. S'il existe plusieurs adresses IP de destination associées à ce flux, cette zone indique le terme Multiple et le nombre d'adresses IP.
Port source (Nombre unique)	Indique le port source du flux.
Port de destination (Nombre unique)	Indique le port de destination du flux. S'il existe plusieurs ports de destination associés à ce flux, cette zone indique le terme Multiple et le nombre de ports.
Réseau source (Nombre unique)	Indique le réseau source du flux. S'il existe plusieurs réseaux source associés à ce flux, cette zone indique le terme Multiple et le nombre de réseaux.
Réseau de destination (Nombre unique)	Indique le port de destination du flux. S'il existe plusieurs réseaux de destination associés à ce flux, cette zone indique le terme Multiple et le nombre de réseaux.
Application (Nombre unique)	Indique l'application détectée des flux. S'il existe plusieurs applications associées à ce flux, cette zone indique le terme Multiple et le nombre d'applications.
Octets source (Somme)	Indique le nombre d'octets de la source.
Octets de destination (Somme)	Indique le nombre d'octets de la destination.
Nombre total d'octets (Somme)	Indique le nombre total d'octets associés au flux.
Paquets source (Somme)	Indique le nombre de paquets de la source.
Paquets source (Somme)	Indique le nombre de paquets de la source.

Tableau 24. Paramètres des flux regroupés (suite)

En-tête	Description
Paquets source (Somme)	Indique le nombre de paquets de la source.
Paquets de destination (Somme)	Indique le nombre de paquets de la destination.
Paquets totaux (Somme)	Indique le nombre total de paquets associés au flux.
Nombre	Indique le nombre de flux envoyés ou reçus.

Procédure

1. Cliquez sur l'onglet **Activité réseau**.
2. Dans la zone de liste **Vue**, sélectionnez le délai que vous souhaitez afficher.
3. Dans la zone de liste **Affichage**, sélectionnez le paramètre selon lequel vous souhaitez regrouper les flux. Voir le tableau 2. Les groupes de flux sont répertoriés. Pour plus d'informations sur les détails de groupe de flux, voir le tableau 1.
4. Pour afficher la page Liste de flux d'un groupe, cliquez deux fois sur le groupe de flux que vous souhaitez étudier. La page Liste de flux ne conserve pas les configurations de graphique que vous avez éventuellement définies sur l'onglet **Activité réseau**. Pour plus d'informations sur les paramètres Liste de flux, voir le tableau 2.
5. Pour afficher les détails d'un flux, cliquez deux fois sur le flux que vous souhaitez étudier. Pour plus d'informations sur la page de détails de flux, voir le tableau 1.

Détails de flux

Vous pouvez afficher une liste de flux dans différents modes, y compris le mode diffusion en flux ou groupes de flux. Quel que soit le mode que vous choisissez pour consulter les flux, vous pouvez localiser et afficher les détails d'un flux unique.

La page de détails de flux fournit les informations suivantes :

Tableau 25. Détails de flux

Paramètre	Description
Informations de flux	
Protocole	Indique le protocole associé à cet événement. Pour plus d'informations sur les protocoles, voir *IBM Security QRadar Application Configuration Guide*.
Application	Indique l'application détectée du flux. Pour plus d'informations sur la détection d'applications, voir *IBM Security QRadar Application Configuration Guide*.
Magnitude	Indique l'ampleur de ce flux. Pour plus d'informations sur la magnitude, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).

Tableau 25. Détails de flux (suite)

Paramètre	Description
Pertinence	Indique la pertinence de ce flux. Pour plus d'informations sur la pertinence, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).
Gravité	Indique la gravité de ce flux. Pour plus d'informations sur la gravité, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).
Crédibilité	Indique la crédibilité de ce flux. Pour plus d'informations sur la crédibilité, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).
Heure du premier paquet	Indique l'heure de début du flux, telle que reportée par la source du flux. Pour plus d'informations sur les sources de flux, voir *IBM Security QRadar Administration Guide*.
Heure du dernier paquet	Indique l'heure de fin du flux, telle que reportée par la source de flux.
Heure de stockage	Indique l'heure à laquelle l'événement a été enregistré dans la base de données QRadar.
Nom d'événement	Indique le nom normalisé du flux.
Catégorie de niveau inférieur	Indique la catégorie de bas niveau de ce flux. Pour plus d'informations sur les catégories, voir *IBM Security QRadar Administration Guide*.
Description de l'événement	Indique une description du flux, si disponible.
Informations sur la source et la destination	
IP source	Indique l'adresse IP de la source du flux.
IP de destination	Indique l'adresse IP de destination du flux.
Nom de l'actif source	Indique le nom d'actif source du flux.
Nom de l'actif de destination	Indique le nom d'actif de destination du flux.
Source IPv6	Indique l'adresse IPv6 de la source du flux.
Destination IPv6	Indique l'adresse IPv6 de la destination du flux.
Port source	Indique le port source du flux.
Port de destination	Indique le port de destination du flux.
QoS source	Indique le niveau de service du flux source.

Tableau 25. Détails de flux (suite)

Paramètre	Description
QoS de destination	Indique le niveau de qualité de service pour le flux de destination.
ASN source	Indique le nombre des valeurs ASN de la source. **Remarque :** Si le flux possède des enregistrements en double provenant des divers sources de flux, les nombres des valeurs ASN source correspondant sont répertoriés.
ASN de destination	Indique le nombre des valeurs ASN de destination. **Remarque :** Si le flux possède des enregistrements en double provenant des diverses sources de flux, les nombres des valeurs ASN de destination correspondant sont répertoriés.
Index conditionnel source	Indique le nombre d'IFIndex source. **Remarque :** Si le flux possède des enregistrements en double provenant de diverses sources de flux, les nombres d'IFIndex source correspondant sont répertoriés.
Index conditionnel de destination	Indique le nombre d'IFIndex de destination. **Remarque :** Si le flux possède des enregistrements en double provenant de diverses sources de flux, les nombres d'IFIndex source correspondant sont répertoriés.
Contenu source	Indique le nombre de paquets et d'octets pour le contenu de la source.
Contenu de destination	Indique le nombre de paquets et d'octets pour le contenu de destination.
Informations sur le contenu	
Contenu source	Indique le contenu de la source du flux. Cette zone offre 3 formats pour afficher le contenu : • Universal Transformation Format (UTF) - Cliquez sur UTF. • Hexadécimal - Cliquez sur HEX. • Base64 - Cliquez sur Base64. **Remarque :** Si votre source de flux est Netflow v9 ou IPFIX, des zones non interprétées de ces sources peuvent être affichées dans la zone **Contenu source**. Le format de cette zone non interprétée est <name>=<value>. Par exemple, `MN_TTL=x`

Tableau 25. Détails de flux (suite)

Paramètre	Description
Contenu de destination	Indique le contenu de la destination du flux. Cette zone offre 3 formats pour afficher le contenu : • Universal Transformation Format (UTF) - Cliquez sur **UTF**. • Hexadécimal - Cliquez sur **HEX**. • Base64 - Cliquez sur **Base64**.
Informations supplémentaires	
Type de flux	Indique le type de flux. Les types de flux sont mesurés par le rapport de l'activité entrante avec l'activité sortante. Les types de flux incluent : • Standard - trafic bidirectionnel • Entrez A - unique vers plusieurs (unidirectionnel) • Entrez B - plusieurs vers unique (unidirectionnel) • Entrez C - unique vers unique (unidirectionnel)
Direction du flux	Indique la direction du flux. Les directions du flux comprennent : • L2L - Trafic interne d'un réseau local vers un autre réseau local. • L2R - Trafic interne d'un réseau local vers un réseau distant. • R2L - Trafic interne d'un réseau distant vers un réseau local. • R2R - Trafic interne d'un réseau distant vers un autre réseau distant.
Règles personnalisées	Indique les règles personnalisées qui correspondent à ce flux. Pour plus d'informations sur les règles, voir *IBM Security QRadar Administration Guide*.
Correspondance partielle avec les règles personnalisées	Indique les règles personnalisées qui correspondent partiellement à ce flux.
Source/interface du flux	Indique le nom de la source du flux du système qui a détecté le flux. **Remarque :** Si ce flux possède plusieurs enregistrements de diverses sources de flux, les sources de flux correspondantes sont répertoriées.
Annotations	Indique l'annotation ou les notes pour ces flux. Les annotations sont des descriptions de texte que les règles peuvent automatiquement ajouter aux flux dans le cadre de la réponse à la règle.

Barre d'outils des détails de flux

La barre d'outils des détails de flux fournit diverses fonctions.

La barre d'outils des détails de flux fournit les fonctions suivantes

Tableau 26. Description de la barre d'outils des détails de flux

Fonction	Description
Retour aux résultats	Cliquez sur **Retour aux résultats** pour retourner à la liste des flux.
Extraire la propriété	Cliquez sur **Extraire la propriété** pour créer une propriété de flux personnalisé à partir du flux sélectionné. Pour plus d'informations, voir les propriétés d'événement personnalisé et de flux.
Faux positif	Cliquez sur **Faux positif** pour ouvrir la fenêtre Ajustement des faux positifs, qui vous permet de désactiver les flux connus en tant que faux positifs pour les empêcher de créer des infractions. Cette option est désactivée en mode de diffusion en flux. Voir Exportation de flux.
Précédent	Cliquez sur **Précédent** pour afficher le flux précédent dans la liste de flux.
Suivant	Cliquez sur **Suivant** pour afficher le flux suivant dans la liste de flux.
Imprimer	Cliquez sur **Imprimer** pour imprimer les détails d'un flux.
Infraction	Si **Infraction** est disponible, cliquez dessus pour afficher la page relative au récapitulatif des infractions.

Réglage des faux positifs

Vous pouvez utiliser la fonction Ajustement des faux positifs pour éviter que les flux faux positifs ne créent des infractions. Vous pouvez régler les flux de faux positifs à partir de la page de liste de flux ou de détails des flux.

Pourquoi et quand exécuter cette tâche

Remarque : Vous pouvez régler les flux des faux positifs à partir de la page des détails.

Vous devez disposer des droits appropriés pour créer des règles personnalisées afin de régler les faux positifs. Pour plus d'informations sur les faux positifs, voir le glossaire (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/r_qradar_siem_glossary.html).

Procédure

1. Cliquez sur l'onglet **Activité réseau**.
2. Facultatif. Si vous affichez les flux en mode de diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause la diffusion en flux.
3. Sélectionnez le flux que vous souhaitez régler.
4. Cliquez sur **Faux positif**.

5. Dans le volet Propriété d'événement/de flux de la fenêtre Faux positif, sélectionnez l'une des options suivantes :
   - Evénement/Flux avec un QID spécifique de <Evénement>
   - Tout événement/flux avec une catégorie de bas niveau de <Evénement>
   - Tout événement/flux avec une catégorie de haut niveau de <Evénement>
6. Dans le volet Direction du trafic, sélectionnez l'une des options suivantes :
   - <D'une adresse IP source > vers <une adresse IP de destination>
   - <D'une adresse IP source> vers n'importe quelle destination
   - De n'importe quelle source vers <une adresse IP de destination>
   - De n'importe quelle source vers n'importe quelle destination
7. Cliquez sur **Optimiser**.

Exportation de flux

Vous pouvez exporter les flux au format XML (Extensible Markup Language) ou CSV (Comma Separated Values). La durée nécessaire à l'exportation de vos données dépend du nombre de paramètres spécifiés.

Procédure

1. Cliquez sur l'onglet **Activité réseau**.
2. Facultatif. Si vous affichez les flux en mode de diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause la diffusion en flux.
3. Dans la zone de liste **Actions**, sélectionnez l'une des options suivantes :
   - **Exporter au format XML** > **Colonnes visibles** - Sélectionnez cette option pour exporter uniquement les colonnes qui sont visibles dans l'onglet Activité du journal. Il s'agit de l'option recommandée.
   - **Exporter au format XML** > **Exportation complète (toutes les colonnes)** - Sélectionnez cette option pour exporter tous les paramètres de flux. Une exportation complète peut prendre un certain temps.
   - **Exporter au format CSV** > **Colonnes visibles** - Sélectionnez cette option pour exporter uniquement les colonnes qui sont visibles dans l'onglet Activité du journal. Il s'agit de l'option recommandée.
   - **Exporter au format CSV** > **Exportation complète (toutes les colonnes)** - Sélectionnez cette option pour exporter tous les paramètres de flux. Une exportation complète peut prendre un certain temps.
4. Si vous souhaitez reprendre vos activités, cliquez sur **Aviser à la fin de l'opération**.

Résultats

Lorsque l'exportation est terminée, vous recevez une notification vous informant que l'exportation est terminée. Si vous n'avez pas sélectionné l'icône **Aviser à la fin de l'opération**, la fenêtre Etat s'affiche.

Chapitre 7. Gestion des actifs

La collecte et la visualisation des données d'actifs vous aident à identifier les menaces et les vulnérabilités. Une base de données exacte d'actifs facilite l'association des infractions qui sont déclenchées dans votre système à des actifs physiques ou virtuels dans votre réseau.

Restriction : QRadar Log Manager effectue un suivi des données d'actif uniquement si QRadar Vulnerability Manager est installé. Pour plus d'informations sur les différences entre IBM Security QRadar SIEM et IBM QRadar Log Manager, voir «Fonctions de votre produit Security Intelligence», à la page 3.

Données d'actif

Un *actif* est tout noeud final du réseau qui envoie ou reçoit des données au sein de votre infrastructure réseau. Par exemple, les ordinateurs portables, les serveurs, les machines virtuelles et les appareils portables sont tous des actifs. Un identifiant unique est attribué à chaque actif dans la base d'actifs de sorte que l'actif peut être distingué des autres enregistrements d'actifs.

La détection des périphériques est également utile dans la construction d'un ensemble de données d'informations historiques sur l'actif. Le suivi des informations sur les actifs lorsqu'elles changent vous aide à surveiller l'utilisation des actifs de votre réseau.

Profils d'actifs

Un *profil d'actif* est une collection de tous les renseignements que IBM Security QRadar SIEM a recueilli au fil du temps sur un actif spécifique. Le profil contient des informations sur les services qui sont exécutés sur l'actif et les informations d'identité connues.

QRadar SIEM crée automatiquement des profils d'actifs à partir d'événements d'identité et de données de flux bidirectionnel ou si elles sont configurées, des analyses d'évaluations de vulnérabilité. Les données sont corrélées à travers un processus qui est appelé *rapprochement des actifs* et le profil est mis à jour lorsque de nouvelles information entrent dans QRadar. Le nom d'actif est dérivé des informations contenues dans la mise à jour d'actifs dans l'ordre de priorité suivant :

- Nom attribué
- Nom d'hôte NETBios
- Nom d'hôte DNS
- Adresse IP

Collecte des données d'actif

Les profils d'actif sont générés de manière dynamique à partir d'informations d'identité qui sont absorbées de façon passive à partir de données d'événement ou de flux, ou à partir de données que QRadar recherche activement pendant une analyse de vulnérabilité. Vous pouvez également importer les données d'actif ou éditer le profil d'actif manuellement.

© Copyright IBM Corp. 2012, 2017

Sources des données d'actif

Les données d'actif sont reçues de plusieurs sources différentes dans votre déploiement IBM Security QRadar.

Les données d'actif sont écrites dans la base de données d'actifs de manière incrémentielles, généralement par incréments de 2 ou 3 données à la fois. À l'exception des mises à jour à partir de scanners de vulnérabilité du réseau, chaque mise à jour d'actifs contient des informations sur un seul actif à la fois.

Les données d'actifs proviennent généralement de l'une des sources de données d'actifs suivantes :

Evénements
Les contenus d'événements, tels que ceux créés par les serveurs DHCP ou d'authentification, contiennent souvent des connexions d'utilisateurs, des adresses IP, des noms d'hôte, des adresses MAC et d'autres informations d'actifs. Ces données sont immédiatement transmises à la base de données d'actifs pour aider à déterminer à quel actif la mise à jour d'actif s'applique.

Les événements sont la principale cause des écarts de croissance d'actifs.

Flux Les contenus de flux contiennent des informations de communication telles que l'adresse IP, le port et le protocole qui sont collectées au cours d'intervalles configurables, réguliers. A la fin de chaque intervalle, les données sont fournies à la base de données d'actifs, une adresse IP à la fois.

Etant donné que les données d'actifs provenant des flux sont jumelées avec un actif sur la base d'un identifiant unique, l'adresse IP, les données de flux ne sont jamais la cause d'écarts de croissance d'actifs.

Programmes d'analyse des vulnérabilités
QRadar s'intègre aux scanners de vulnérabilité IBM et d'autres marques pouvant fournir des données d'actifs telles que le système d'exploitation, les logiciels installés et les informations sur les correctifs. Le type de données varie d'un scanner à l'autre et peut également varier d'une analyse à l'autre. Au fur et à mesure que de nouveaux actifs, informations de port, et vulnérabilités sont découverts, les données sont introduites dans le profil de l'actif sur la base des plages CIDR qui sont définies dans l'analyse.

Certains scanners peuvent intégrer des écarts de croissance d'actifs mais cela est rare.

Interface utilisateur
Les utilisateurs qui disposent du rôle Actifs peuvent importer ou fournir des informations sur les actifs directement vers la base de données d'actifs. Les mises à jour d'actifs fournis directement par un utilisateur concernent un actif spécifique. Par conséquent, la phase de rapprochement des actifs est ignorée.

Les mises à jour d'actifs qui sont fournies par les utilisateurs n'introduisent pas d'écarts de croissance d'actifs.

Données d'actifs de domaine

Quand une source de données d'actifs est configurée avec les informations de domaine, toutes les données d'actifs qui proviennent de cette source de données sont automatiquement marquées avec le même domaine. Etant donné que les

données dans le modèle d'actif sont compatibles avec le domaine, les informations de domaine sont appliquées à tous les composants QRadar y compris les identités, les infractions, les profils d'actifs, et la découverte de serveur.

Lorsque vous affichez le profil d'actifs, certaines zones peuvent être vides. Les zones vides existent lorsque le système n'a pas reçu ces informations dans une mise à jour d'actifs, ou les informations ont dépassé la période de rétention des actifs. La période de rétention par défaut est de 120 jours. Une adresse IP qui apparaît comme 0.0.0.0 indique que l'actif ne contient pas d'information de l'adresse IP.

Flux des données d'actifs entrantes

IBM Security QRadar utilise les informations d'identité d'un contenu d'événement pour déterminer si un nouvel actif doit être créé ou si un actif existant doit être mis à jour.

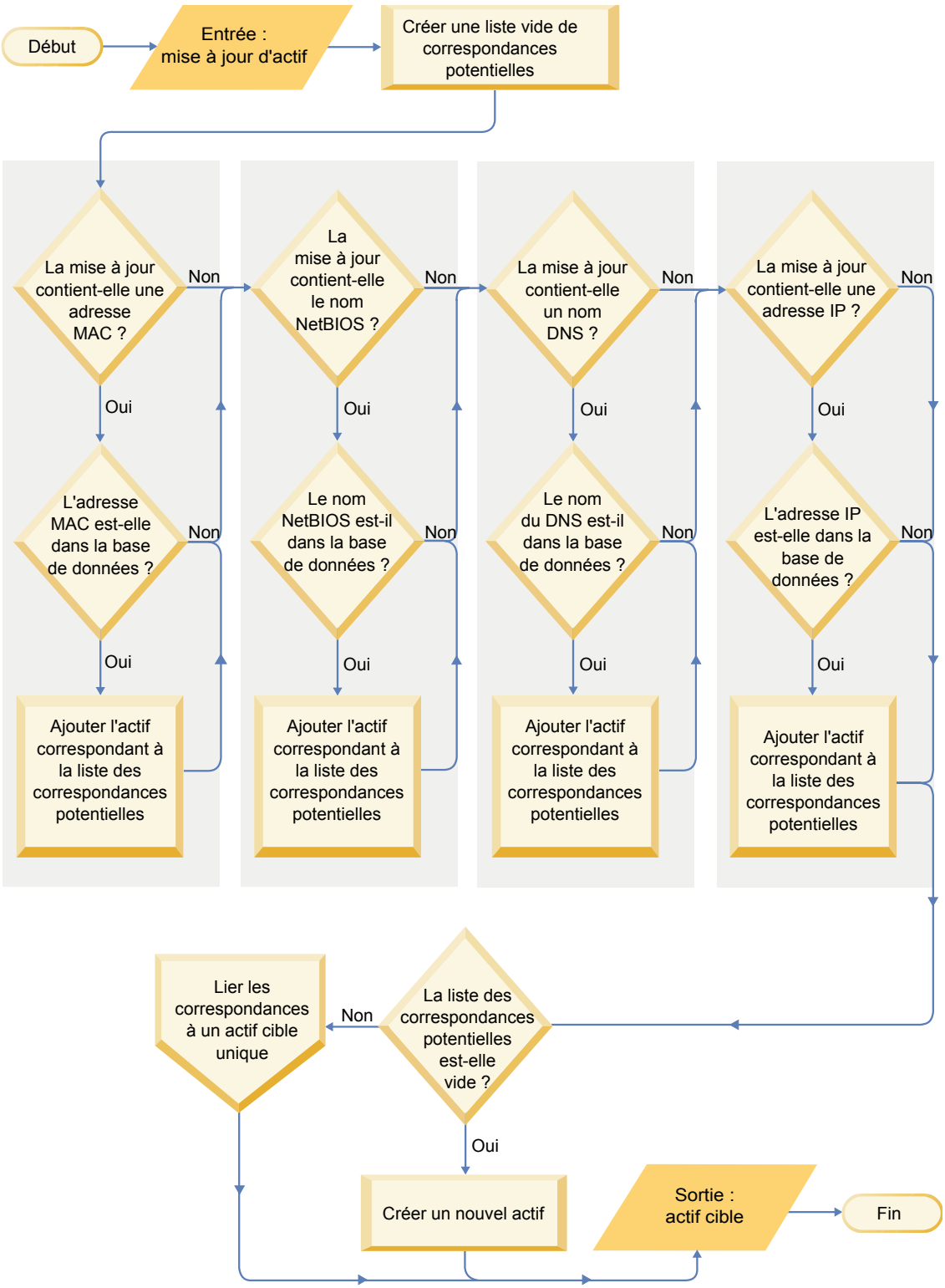

Figure 2. Graphique des flux de données d'actifs

1. QRadar reçoit l'événement. Le profileur d'actifs examine le contenu d'événement pour obtenir des informations d'identité.
2. Si les informations d'identité incluent une adresse MAC, un nom d'hôte NetBIOS ou un nom d'hôte DNS déjà associé à un actif dans la base de données des actifs, cet actif est mis à jour pour inclure les nouvelles informations.
3. Si les seules informations d'identité disponibles sont une adresse IP, le système rapproche la mise à jour de l'actif existant qui a la même adresse IP.
4. Si une mise à jour d'actif contient une adresse IP qui correspond à un actif existant mais les informations d'identité ne correspondent pas, le système utilise d'autres informations pour exclure une correspondance de faux positif avant de mettre à jour l'actif existant.
5. Si les informations d'identité ne correspondent pas à un actif existant dans la base de données, un nouvel actif est créé conformément aux informations du contenu d'événement.

Mises à jour des données d'actifs

IBM Security QRadar utilise les informations d'identité d'un contenu d'événement afin de déterminer si un nouvel actif doit être créé ou si un actif existant doit être mis à jour.

Chaque mise à jour d'actifs doit contenir des informations fiables au sujet d'un actif unique. Lorsque QRadar reçoit une mise à jour d'actif, le système détermine l'actif auquel s'applique la mise à jour.

Le *rapprochement d'actifs* est le processus de détermination de la relation entre les mises à jour d'actifs et l'actif connexe dans la base d'actifs. Le rapprochement d'actifs survient après que QRadar reçoit la mise à jour, mais avant que les informations sont écrites dans la base de données d'actifs

Informations d'identité

Chaque actif doit contenir au moins une donnée d'identité. Les mises à jour ultérieures qui contiennent une ou plusieurs de ces mêmes données d'identité sont rapprochées avec l'actif qui possède ces données. Les mises à jour qui sont basées sur les adresses IP sont manipulées avec précaution pour éviter les correspondances d'actifs faux positifs. Les correspondances d'actifs constituant des faux positifs se produisent lorsqu'un actif physique devient propriétaire d'une adresse IP qui appartenait auparavant à un autre actif du système.

Lorsque plusieurs données d'identités sont fournies, le profileur d'actif classe les informations par ordre de priorité, de la plus déterminante à la moins déterminante, dans l'ordre suivant :

- Adresse MAC
- Nom d'hôte NetBIOS
- Nom d'hôte DNS
- Adresse IP

Les adresses MAC, les noms d'hôte NetBIOS et les noms d'hôte DNS sont uniques et sont par conséquent considérés comme des données d'identité définitives. Les mises à jour entrantes qui correspondent à un actif existant seulement par l'adresse IP sont gérées différemment des mises à jour qui correspondent à des données d'identité plus définitives.

Concepts associés:

«Règles d'exclusion de rapprochement d'actifs»
Avec chaque mise à jour d'actifs qui entre dans IBM Security QRadar, les règles d'exclusion de rapprochement d'actifs effectuent des tests sur l'adresse MAC, le nom d'hôte NetBIOS, le nom d'hôte DNS et l'adresse IP dans la mise à jour d'actifs.

Règles d'exclusion de rapprochement d'actifs

Avec chaque mise à jour d'actifs qui entre dans IBM Security QRadar, les règles d'exclusion de rapprochement d'actifs effectuent des tests sur l'adresse MAC, le nom d'hôte NetBIOS, le nom d'hôte DNS et l'adresse IP dans la mise à jour d'actifs.

Par défaut, chaque donnée d'actif est suivie sur une période de deux heures. Si une donnée d'identité dans la mise à jour d'actifs présente un comportement suspect deux fois ou plus dans les 2 heures, cette donnée est ajoutée aux listes noires d'actifs. Chaque type de données d'actif d'identité testé génère une nouvelle liste noire.

Dans les environnements de domaine, les règles d'exclusion de rapprochement d'actifs suivent le comportement des données d'actifs séparément pour chaque domaine.

Les règles d'exclusion de rapprochement des actifs testent les scénarios suivants :

Tableau 27. Tests de règle et réponses

Scénario	Réponse à la règle
Quand une adresse MAC est associée à trois adresses IP différentes ou plus en 2 heures ou moins	Ajoutez l'adresse MAC à la liste noire MAC du domaine de rapprochement d'actifs
Quand un nom d'hôte DNS est associé à trois adresses IP différentes ou plus en 2 heures ou moins	Ajoutez le nom d'hôte DNS à la liste noire DNS du domaine de rapprochement d'actifs
Quand un nom d'hôte NetBIOS est associé à trois adresses IP différentes ou plus en 2 heures ou moins	Ajoutez le nom d'hôte NetBIOS à la liste noire NetBIOS du domaine de rapprochement d'actifs
Quand une adresse IPv4 est associée à trois adresses MAC différentes ou plus en 2 heures ou moins	Ajoutez l'adresse IP à la liste noire IPv4 du domaine de rapprochement d'actifs
Quand un nom d'hôte NetBIOS est associé à trois adresses MAC différentes ou plus en 2 heures ou moins	Ajoutez le nom d'hôte NetBIOS à la liste noire NetBIOS du domaine de rapprochement d'actifs
Quand un nom d'hôte DNS est associé à trois adresses MAC différentes ou plus en 2 heures ou moins	Ajoutez le nom d'hôte DNS à la liste noire DNS du domaine de rapprochement d'actifs
Quand une adresse IPv4 est associée à trois noms d'hôte DNS différents ou plus en 2 heures ou moins	Ajoutez l'adresse IP à la liste noire IPv4 du domaine de rapprochement d'actifs
Quand un nom d'hôte NetBIOS est associé à trois noms d'hôte DNS différents ou plus en 2 heures ou moins	Ajoutez le nom d'hôte NetBIOS à la liste noire NetBIOS du domaine de rapprochement d'actifs
Quand une adresse MAC est associée à trois noms d'hôte DNS différents ou plus en 2 heures ou moins	Ajoutez l'adresse MAC à la liste noire MAC du domaine de rapprochement d'actifs

Tableau 27. Tests de règle et réponses (suite)

Scénario	Réponse à la règle
Quand une adresse IPv4 est associée à trois noms d'hôte NetBIOS différents ou plus en 2 heures ou moins	Ajoutez l'adresse IP à la liste noire IPv4 du domaine de rapprochement d'actifs
Quand un nom d'hôte DNS est associé à trois noms d'hôte NetBIOS différents ou plus en 2 heures ou moins	Ajoutez le nom d'hôte DNS à la liste noire DNS du domaine de rapprochement d'actifs
Quand une adresse MAC est associée à trois noms d'hôte NetBIOS différents ou plus en 2 heures ou moins	Ajoutez l'adresse MAC à la liste noire MAC du domaine de rapprochement d'actifs

Vous pouvez consulter ces règles sur l'onglet **Infractions** en cliquant sur **Règles** puis en sélectionnant le groupe d'**exclusion de rapprochement d'actifs** dans la liste déroulante.

Concepts associés:

«Exemple : règles d'exclusion d'actifs ajustées pour exclure des adresses IP de la liste noire»
Vous pouvez exclure des adresses IP de la mise sur liste noire en ajustant les règles d'exclusion d'actifs.

Exemple : règles d'exclusion d'actifs ajustées pour exclure des adresses IP de la liste noire

Vous pouvez exclure des adresses IP de la mise sur liste noire en ajustant les règles d'exclusion d'actifs.

En tant qu'administrateur de sécurité réseau, vous gérez un réseau d'entreprise qui comprend un segment de réseau wifi public où les baux d'adresses IP sont généralement courts et fréquents. Les actifs sur ce segment du réseau ont tendance à être transitoires, principalement des ordinateurs portables et des appareils portables qui se connectent et se déconnectent du réseau WiFi public fréquemment. Généralement, une seule adresse IP est utilisée plusieurs fois par différentes unités sur une courte période.

Dans le reste de votre déploiement, vous disposez d'un réseau géré personnalisé constitué uniquement de périphériques de l'entreprise inventoriés. Les baux d'adresses IP sont beaucoup plus longs dans cette partie du réseau, et les adresses IP sont accessibles par l'authentification uniquement. Sur ce segment de réseau, vous voulez savoir immédiatement quand il existe des écarts de croissance d'actifs et vous souhaitez conserver les paramètres par défaut pour les règles d'exclusion de rapprochement d'actifs.

Mise d'adresses IP sur liste noire

Dans cet environnement, les règles d'exclusion de rapprochement d'actifs par défaut mettent en liste noire par inadvertance l'ensemble du réseau dans un court laps de temps.

Votre équipe de sécurité estime que les notifications relatives aux actifs qui sont générées par le segment de wifi constituent une nuisance. Vous souhaitez empêcher le wifi de déclencher davantage de notifications d'écart de croissance d'actifs.

Ajustement de règles de rapprochement d'actifs pour ignorer certaines mises à jour d'actifs

Vous passez en revue le rapport **Écart d'actifs par source de journal** dans la dernière notification du système. Vous déterminez que les données sur la liste noire proviennent du serveur DHCP sur votre réseau wifi.

Les valeurs de la colonne **Nombre d'événements**, **Nombre de flux** et de la colonne **Infractions** pour la ligne correspondant à la règle **AssetExclusion: Exclude IP By MAC Address** indiquent que votre serveur DHCP wifi déclenche cette règle.

Vous ajoutez un test aux règles d'exclusion de rapprochement d'actifs existantes pour faire en sorte que les règles cessent d'ajouter des données Wi-Fi à la liste noire.

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
and when at least 3 events are seen with the same Identity IP and
different Identity MAC in 2 hours.
```

La règle mise à jour teste uniquement les événements des sources de journaux qui ne sont pas sur votre serveur DHCP wifi. Pour éviter que les événements DHCP wifi soient soumis à des tests d'analyse de comportement et à des ensembles de référence plus onéreux, vous avez également déplacé ce test en haut de la pile de tests.

Fusion d'actifs

La *fusion d'actifs* est le processus par lequel les informations d'un actif sont combinées aux informations d'un autre actif en vertu du principe qu'ils sont en fait le même actif physique.

La fusion d'actifs se produit quand une mise à jour d'actifs contient des données d'identité qui correspondent à deux profils d'actifs différents. Par exemple, une seule mise à jour contenant un nom d'hôte NetBIOS qui correspond à un profil d'actifs et une adresse MAC qui correspond à un profil d'actifs différent pourrait déclencher une fusion d'actifs.

Certains systèmes peuvent causer des volumes élevés de fusion d'actifs, car ils ont des sources de données d'actifs qui combinent par inadvertance des informations d'identité de deux actifs physiques différents dans une seule mise à jour d'actifs. Certains exemples de ces systèmes comprennent les environnements suivants :

- Serveurs syslog centraux qui agissent en tant que proxy de l'événement
- Machines virtuelles
- Environnements d'installation automatisée
- Noms d'hôtes non uniques, communs avec des actifs tels que les iPads et les iPhones..
- Réseaux privés virtuels qui présentent des adresses MAC partagées
- Extensions de source de journal dont le champ d'identité est `OverrideAndAlwaysSend=true`

Les actifs qui ont de nombreuses adresses IP, adresses MAC, ou noms d'hôte présentent des écarts de croissance d'actifs et peuvent déclencher des notifications système.

Concepts associés:

«Identification des écarts de croissance d'actifs»
Parfois, les sources de données d'actifs produisent des mises à jour que IBM Security QRadar ne peut pas correctement traiter sans une résolution manuelle. Selon la cause de la croissance d'actifs anormale, vous pouvez corriger la source de données d'actif à l'origine du problème ou vous pouvez bloquer les mises à jour d'actif qui proviennent de cette source de données.

Identification des écarts de croissance d'actifs

Parfois, les sources de données d'actifs produisent des mises à jour que IBM Security QRadar ne peut pas correctement traiter sans une résolution manuelle. Selon la cause de la croissance d'actifs anormale, vous pouvez corriger la source de données d'actif à l'origine du problème ou vous pouvez bloquer les mises à jour d'actif qui proviennent de cette source de données.

Des *écarts de croissance d'actifs* se produisent lorsque le nombre de mises à jour d'actifs pour une seule unité s'accroît au-delà de la limite définie par le seuil de rétention pour un type spécifique d'informations d'identité. Un traitement approprié des écarts de croissance d'actifs est essentiel pour maintenir un modèle d'actif précis.

A la base de chaque écart de croissance d'actifs se trouve une source de données d'actifs dont les données sont peu fiables pour la mise à jour du modèle d'actif. Lorsqu'un écart de croissance d'actifs potentiel est identifié, vous devez examiner la source des informations afin de déterminer s'il y a une explication plausible à l'accumulation par l'actif d'importants volumes de données d'identité. La cause d'un écart de croissance d'actifs est spécifique à chaque environnement.

Exemple de serveur DHCP de croissance d'actifs non naturelle dans un profil d'actifs

Considérons un serveur de réseau privé virtuel (VPN) dans un réseau Dynamic Host Configuration Protocol (DHCP). Le serveur VPN est configuré pour attribuer des adresses IP aux clients VPN entrants par mandatement des requêtes DHCP pour le compte du client vers le serveur DHCP du réseau.

Du point de vue du serveur DHCP, la même adresse MAC demande à plusieurs reprises de nombreuses affectations d'adresses IP. Dans le cadre de l'exploitation du réseau, le serveur VPN délègue les adresses IP aux clients, mais le serveur DHCP ne peut pas distinguer quand une demande est faite par un actif pour le compte d'un autre.

Le journal du serveur DHCP, qui est configuré en tant que source de journal QRadar génère un événement d'accusé de réception DHCP (DHCP ACK) qui associe l'adresse MAC du serveur VPN à l'adresse IP qui est attribuée au client VPN. Lorsque le rapprochement des actifs se produit, le système rapproche cet événement par adresse MAC, qui se traduit par un actif existant unique qui augmente d'une adresse IP pour chaque événement DHCP ACK qui est analysé.

Finalement, un profil d'actifs contient toutes les adresses IP qui ont été allouées au serveur VPN. Cet écart de croissance d'actifs est causé par des mises à jour d'actifs

qui contiennent des informations sur plusieurs actifs.

Paramètres de seuil

Lorsqu'un actif dans la base de données atteint un nombre spécifique de propriétés, telles que des adresses IP ou des adresses MAC multiples QRadar empêche cet actif de recevoir plus de mises à jour.

Les paramètres de seuil Profileur d'actif précisent les conditions dans lesquelles un actif est verrouillé pour empêcher les mises à jour. L'actif est mis à jour normalement jusqu'à la valeur de seuil. Lorsque le système recueille suffisamment de données pour dépasser le seuil, l'actif montre un écart de croissance d'actifs. Les futures mises à jour de l'actif sont bloquées jusqu'à ce que l'écart de croissance soit redressé.

Notifications système indiquant des écarts de croissance d'actifs

IBM Security QRadar génère des notifications système pour vous aider à identifier et à gérer les écarts de croissance d'actifs dans votre environnement.

Les messages système suivants indiquent que QRadar a identifié des écarts potentiels de croissance d'actifs :

- `Le système a détecté des profils d'actifs qui dépassent le seuil de taille normale.`
- `Les règles de la liste noire d'actifs ont ajouté de nouvelles données d'actifs au listes noires d'actifs`

Les messages de notification du système incluent des liens vers des rapports pour vous aider à identifier les actifs présentant des écarts de croissance.

Données d'actif qui changent fréquemment

La croissance d'actifs peut être causée par de gros volumes de données d'actifs qui changent de manière légitime, comme dans les situations suivantes :

- Un appareil mobile qui change souvent de bureau et auquel une adresse IP est affectée à chaque connexion.
- Un appareil qui se connecte à un réseau wifi public avec des baux d'adresses IP courts, par exemple sur un campus d'université, peut collecter de gros volumes de données d'actif sur un semestre.

Exemple : comment les erreurs de configuration pour extensions de source de journal peuvent causer des écarts de croissance d'actifs

Les extensions personnalisées de source de journal qui sont mal configurées peuvent causer des écarts de croissance d'actifs.

Vous configurez une extension de source de journal personnalisée pour fournir des mises à jour d'actifs à IBM Security QRadar en analysant les noms d'utilisateur depuis le contenu d'événement situé sur un serveur central. Vous configurez l'extension de source de journal pour remplacer la propriété de nom d'hôte d'événement de sorte que les mises à jour d'actifs qui sont générées par la source de journal personnalisée précisent toujours le nom d'hôte DNS du serveur central.

Plutôt que QRadar reçoive une mise à jour qui comporte le nom d'hôte de l'actif auquel l'utilisateur s'est connecté, la source de journal génère de nombreuses mises à jour d'actifs qui ont toutes le même nom d'hôte.

Dans ce cas, l'écart de croissance d'actifs est causé par un profil d'actifs qui contient un grand nombre d'adresses IP et de noms d'utilisateur.

Traitement des problèmes des profils d'actifs qui dépassent le seuil de taille normale

IBM Security QRadar génère une notification système lorsque l'accumulation de données sous un seul actif dépasse les seuils limites configurés pour les données d'identité.

```
Le système a détecté des profils d'actifs qui dépassent le seuil de taille normale.
```

Explication

Le contenu de la notification montre une liste des cinq actifs présentant le plus souvent un écart et pourquoi le système a marqué chaque actif en tant qu'écart de croissance. Comme le montre l'exemple suivant, le contenu indique également le nombre de fois que l'actif a tenté de croître au-delà du seuil de taille des actifs.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

Lorsque les données d'actifs dépassent le seuil configuré, QRadar empêche les futures mises à jour sur l'actif. Cette intervention empêche le système de recevoir davantage de données corrompues et atténue les impacts de performance qui pourraient survenir si le système tente de rapprocher les mises à jour entrantes avec un profil d'actifs anormalement grand.

Action utilisateur requise

Utilisez les informations du contenu de notification pour identifier les actifs qui contribuent à l'écart de croissance d'actifs et déterminer la cause de la croissance anormale. La notification fournit un lien vers un rapport de tous les actifs qui ont connu un écart de croissance d'actifs au cours des dernières 24 heures.

Après avoir résolu l'écart de croissance d'actifs dans votre environnement, vous pouvez exécuter de nouveau le rapport.

1. Cliquez sur l'onglet **Activité du journal** et cliquez sur **Rechercher** > **Nouvelle recherche**.
2. Sélectionnez la recherche sauvegardée **Croissance d'actifs présentant un écart : rapports d'actifs**.
3. Utilisez le rapport pour identifier et réparer les données d'actifs inexactes qui ont été créées pendant l'écart.

Si les données d'actifs sont valides, les administrateurs QRadar peuvent augmenter les seuils limites pour les adresses IP, les adresses MAC, les noms d'hôte NetBIOS et les noms d'hôte DNS dans la **Configuration du profileur d'actif** dans l'onglet QRadar **Admin**.

De nouvelles données d'actifs sont ajoutées aux listes noires d'actifs

IBM Security QRadar génère une notification système quand une donnée d'actif présente un comportement qui est compatible avec une croissance déviante d'actif.

`Les règles de la liste noire d'actifs ont ajouté de nouvelles données d'actifs aux listes noires d'actifs`

Explication

Les règles d'exclusion d'actifs surveillent les données d'actifs par souci de cohérence et d'intégrité. Les règles suivent des données spécifiques d'actifs au fil du temps afin d'assurer qu'elles sont constamment observées avec le même sous-ensemble de données dans un délai raisonnable.

Par exemple, si une mise à jour d'actif comprend à la fois une adresse MAC et un nom d'hôte DNS, l'adresse MAC est associée à ce nom d'hôte DNS pour une période prolongée. Les mises à jour ultérieures d'actifs qui contiennent cette adresse MAC contiennent également ce même nom d'hôte DNS quand un nom d'hôte est inclus dans la mise à jour d'actif. Si l'adresse MAC est soudainement associée à un nom d'hôte DNS différent pendant une brève période, la modification est surveillée. Si l'adresse MAC change à nouveau dans un court délai, l'adresse MAC est signalée comme contribuant à une instance de croissance d'actifs déviante et anormale.

Action utilisateur requise

Utilisez les informations du contenu de notification pour identifier les règles utilisées pour contrôler les données d'actifs. Cliquez sur le lien **Ecarts d'actifs par source de journal** dans la notification pour voir les écarts d'actifs qui se sont produits dans les dernières 24 heures.

Si les données d'actifs sont valables, les administrateurs QRadar peuvent configurer QRadar pour résoudre le problème.

- Si vos listes noires se remplissent de façon trop rapide, vous pouvez affiner les règles d'exclusion de rapprochement d'actifs qui les remplissent.
- Si vous voulez ajouter les données à la base de données d'actifs, vous pouvez supprimer les données d'actifs de la liste noire et les ajouter à la liste blanche d'actifs correspondante. L'ajout de données d'actifs à la liste blanche les empêche de réapparaître par inadvertance sur la liste noire.

Listes noires et listes blanches d'actifs

IBM Security QRadar utilise un groupe de règles de rapprochement d'actifs pour déterminer si les données d'actif sont considérées comme fiables. Lorsque les données d'actif sont interrogeables, QRadar utilise des listes noires et des listes blanches d'actifs pour déterminer s'il est nécessaire de mettre à jour les profils d'actif avec les données d'actif.

Une *liste noire d'actifs* est une collecte de données que IBM Security QRadar considère peu fiables. Les données dans la liste noire d'actifs sont susceptibles de contribuer à des écarts de croissance d'actifs et QRadar empêche l'ajout de données à la base de données d'actifs.

Une *liste blanche d'actifs* est une collecte de données d'actifs qui ignore la logique du moteur de rapprochement des actifs selon laquelle les données sont ajoutées à

une liste noire d'actifs. Lorsque le système identifie une correspondance de liste noire, il consulte la liste blanche pour voir si la valeur existe. Si la mise à jour d'actif correspond aux données qui figurent dans la liste blanche, la modification est synchronisée et l'actif est mis à jour. Les données d'actifs sur la liste blanche sont appliquées globalement pour tous les domaines.

Votre administrateur QRadar peut modifier les données de la liste noire et de la liste blanche pour éviter les futurs écarts de croissance d'actifs.

Listes noires d'actifs

Une *liste noire d'actifs* est une collecte de données que IBM Security QRadar considère peu fiables sur la base des règles d'exclusion de rapprochement des actifs. Les données dans la liste noire d'actifs sont susceptibles de contribuer à des écarts de croissance d'actifs et QRadar empêche l'ajout de données à la base de données d'actifs.

Chaque mise à jour d'actifs dans QRadar est comparée aux listes noires d'actifs. Les données d'actifs sur la liste noire sont appliquées globalement pour tous les domaines. Si la mise à jour d'actifs contient des informations d'identité (adresse MAC, nom d'hôte NetBIOS, nom d'hôte DNS ou adresse IP) qui se trouvent sur une liste noire, la mise à jour entrante est rejetée et la base de données d'actifs n'est pas mise à jour.

Le tableau suivant indique le nom et le type de la collection de référence pour chaque type de données d'actifs d'identité.

Tableau 28. Noms de collection de référence pour les données de la liste noire d'actifs

Type de données d'identité	**Nom de collection de référence**	**Type de collection de référence**
Adresses IP (v4)	Liste noire IPv4 de rapprochement d'actifs	Ensemble de références [type d'ensemble : IP]
Noms d'hôte DNS	Liste noire DNS de rapprochement d'actifs	Ensemble de références [type d'ensemble : ALNIC*]
Noms d'hôte NetBIOS	Liste noire NetBIOS de rapprochement d'actifs	Ensemble de références [type d'ensemble : ALNIC*]
Adresses Mac	Liste noire MAC de rapprochement d'actifs	Ensemble de références [type d'ensemble : ALNIC*]
* ALNIC est un type alphanumérique qui peut accueillir à la fois le nom d'hôte et les valeurs d'adresse MAC.		

Votre administrateur QRadar peut modifier les entrées de liste noire afin de garantir que les nouvelles données d'actif sont correctement traitées.

Liste blanches d'actifs

Vous pouvez utiliser des listes blanches d'actifs pour éviter que les données d'actif de IBM Security QRadar ne réapparaissent par erreur dans les listes noires d'actifs.

Une *liste blanche d'actifs* est une collecte de données d'actifs qui remplace la logique de moteur de rapprochement d'actifs concernant les données qui sont ajoutées à une liste noire d'actifs. Lorsque le système identifie une correspondance de liste noire, il consulte la liste blanche pour voir si la valeur existe. Si la mise à jour d'actif correspond aux données qui figurent dans la liste blanche, la modification

est synchronisée et l'actif est mis à jour. Les données d'actifs sur la liste blanche sont appliquées globalement pour tous les domaines.

Votre administrateur QRadar peut modifier les entrées de liste blanche afin de garantir que les nouvelles données d'actif sont correctement traitées.

Exemple d'un cas d'utilisation de liste blanche

La liste blanche est utile si vous avez des données d'actif qui continuent de s'afficher dans les listes noires lorsqu'il s'agit d'une mise à jour d'actif valide. Par exemple, si vous avez un équilibrage de charge DNS de rondes qui est configuré pour l'utilisation par rotation d'un ensemble de cinq adresses IP. Les règles Exclusion de rapprochement d'actifs peuvent déterminer que les différentes adresses IP associées au même nom d'hôte DNS sont indicatives d'un écart de croissance d'actifs, et le système peut ajouter l'équilibrage de charge DNS à la liste noire. Pour résoudre ce problème, vous pouvez ajouter le nom d'hôte DNS à la Liste blanche DNS de rapprochement d'actifs.

Entrées de masse dans la liste blanche d'actifs

Une base de données exacte d'actifs facilite l'association des infractions qui sont déclenchées dans votre système à des actifs physiques ou virtuels dans votre réseau. Si les écarts d'actifs sont ignorés par l'ajout d'entrées de masse dans la liste blanche d'actifs, cela ne contribue pas à générer une base de données d'actifs exacte. Au lieu d'ajouter des entrées de liste blanche en masse, passez en revue la liste noire d'actifs afin de déterminer ce qui contribue à l'écart de croissance d'actif, puis déterminez comment résoudre ce problème.

Types de listes blanches d'actifs

Chaque type de données d'identité est conservé dans une liste blanche distincte. Le tableau suivant indique le nom et le type de la collection de référence pour chaque type de données d'actifs d'identité.

Tableau 29. Nom de collection de référence pour les données de la liste blanche d'actifs

Type de données	Nom de collection de référence	Type de collection de référence
Adresses IP	Liste blanche IPv4 de rapprochement d'actifs	Ensemble de références [type d'ensemble : IP]
Noms d'hôte DNS	Liste blanche DNS de rapprochement d'actifs	Ensemble de références [type d'ensemble : ALNIC*]
Noms d'hôte NetBIOS	Liste blanche NetBIOS de rapprochement d'actifs	Ensemble de références [type d'ensemble : ALNIC*]
Adresses MAC	Liste blanche MAC de rapprochement d'actifs	Ensemble de références [type d'ensemble : ALNIC*]
* ALNIC est un type alphanumérique qui peut accueillir à la fois le nom d'hôte et les valeurs d'adresse MAC.		

Profils d'actifs

Les profils d'actif fournissent des informations sur chaque actif connu de votre réseau, y compris les services qui s'exécutent sur chaque actif.

Les informations de profil d'actif sont utilisées à des fins de corrélation pour réduire les faux positifs. Par exemple, si une source tente d'exploiter un service

spécifique en cours d'exécution sur un actif, QRadar détermine si l'actif est vulnérable à cette attaque en mettant en corrélation l'attaque avec le profil d'actif.

Les profils d'actif sont automatiquement reconnus si des données de flux ou des analyses d'évaluation de la vulnérabilité sont configurées. Pour que les données de flux remplissent les profils d'actif, des flux bidirectionnels sont nécessaires. Les profils d'actif peuvent également être créés automatiquement à partir d'événements d'identité. Pour plus d'informations sur l'évaluation de la vulnérabilité, voir le document *IBM QRadar Vulnerability Assessment Guide*.

Pour plus d'informations sur les sources de flux, voir *IBM Security QRadar Administration Guide*.

Vulnérabilités

Vous pouvez utiliser QRadar Vulnerability Manager et des scanners tiers pour identifier les vulnérabilités.

Les scanners tiers identifient et signalent les vulnérabilités détectées à l'aide de références externes, telles que l'Open Source Vulnerability Database (OSVDB), la National Vulnerability Database (NVDB) et Critical Watch. QualysGuard et nCircle ip360 sont des exemples de scanners tiers. La base de données OSVDB assigne un identificateur de référence unique (OSVDB ID) à chaque vulnérabilité. Les références externes affectent un identificateur de référence unique à chaque vulnérabilité. Un ID Common Vulnerability and Exposures (CVE) ou un ID Bugtraq sont des exemples d'ID de référence de données externe. Pour plus d'informations sur les scanners et l'évaluation de la vulnérabilité, voir *IBM Security QRadar Vulnerability Manager - Guide d'utilisation*.

QRadar Vulnerability Manager est un composant que vous pouvez obtenir séparément et activer à l'aide d'une clé de licence. QRadar Vulnerability Manager est une plateforme d'analyse réseau qui permet de détecter les vulnérabilités existant au sein des applications, systèmes ou dispositifs. Une fois que les analyses ont permis d'identifier les vulnérabilités, vous pouvez rechercher et examiner les données de vulnérabilité, corriger les vulnérabilités, puis réexécuter les analyses pour évaluer le nouveau niveau de risque.

Lorsque QRadar Vulnerability Manager est activé, vous pouvez effectuer des tâches d'évaluation de la vulnérabilité dans l'onglet **Vulnérabilités**. Dans l'onglet **Actifs**, vous pouvez exécuter des analyses sur les actifs sélectionnés.

Pour plus d'informations, voir *IBM Security QRadar Vulnerability Manager - Guide d'utilisation*

Présentation de l'onglet Actifs

L'onglet **Actifs** fournit un espace de travail à partir duquel vous pouvez gérer les actifs de votre réseau et étudier les vulnérabilités d'un actif, ainsi que les ports, les applications, l'historique et d'autres associations.

L'onglet **Actifs** vous permet d'effectuer les tâches suivantes :

- Afficher tous les actifs découverts.
- Ajouter manuellement les profils d'actif.
- Rechercher des actifs spécifiques.
- Afficher des informations sur des actifs découverts.
- Modifier les profils d'actif pour les actifs ajoutés ou découverts manuellement.

- Ajuster les vulnérabilités de faux positifs.
- Importer des actifs.
- Imprimer ou exporter des profils d'actif.
- Découvrir des actifs.
- Configurer et gérer le scannage de vulnérabilité de tiers.
- Démarrer les analyses QRadar Vulnerability Manager.

Pour obtenir des informations sur l'option Reconnaissance des serveurs du panneau de navigation, voir *IBM Security QRadar Administration Guide*

Pour plus d'informations sur l'option VA Scan du panneau de navigation, consultez le manuel *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Affichage d'un profil d'actif

Dans la liste d'actifs de l'onglet **Actifs**, vous pouvez sélectionner et afficher un profil d'actif. Un profil d'actif fournit des informations sur chaque profil.

Pourquoi et quand exécuter cette tâche

Les informations de profil d'actif sont automatiquement identifiées par la reconnaissance de serveur ou configurées manuellement. Vous pouvez éditer les informations de profil d'actif générées automatiquement.

La page Profil d'actif fournit des informations sur l'actif, organisées en plusieurs volets. Pour afficher un volet, vous pouvez cliquer sur la flèche **(>)** sur le volet pour afficher plus de détails ou sélectionner le volet dans la zone de liste **Afficher** sur la barre d'outils.

La barre d'outils de la page Profil d'actif fournit les fonctions suivantes :

Tableau 30. Fonctions de la barre d'outils de la page Profil d'actif

Options	Description
Revenir à la liste d'actifs	Cliquez sur cette option pour revenir à la liste d'actifs.
Affichage	Dans la zone de liste, vous pouvez sélectionner le volet que vous voulez afficher sur le volet Profil d'actif. Les volets Récapitulatif de l'actif et Récapitulatif de l'interface réseau sont toujours affichés.
Modifier un actif	Cliquez sur cette option pour éditer le profil d'actif. Voir «Ajout ou édition d'un profil d'actif», à la page 120.
Afficher par réseau	Si cet actif est associé à une infraction, cette option vous permet d'afficher la liste des réseaux associés à celui-ci. Lorsque vous cliquez sur **Afficher par réseau**, la fenêtre Liste de réseaux s'affiche.
Afficher le récapitulatif de la source	Si cet actif est la source d'une infraction, cette option vous permet d'afficher les informations récapitulatives sur la source. Lorsque vous cliquez sur **Afficher le récapitulatif de la source**, le fenêtre Liste d'infractions s'affiche.

Tableau 30. Fonctions de la barre d'outils de la page Profil d'actif (suite)

Options	Description
Afficher le récapitulatif de la destination	Si cet actif correspond à la destination d'une infraction, cette option vous permet d'afficher les informations récapitulatives sur la destination. Lorsque vous cliquez sur **Afficher le récapitulatif de la destination**, la fenêtre Liste des destinations s'affiche.
Historique	Cliquez sur l'option **Historique** pour afficher les informations historiques des événements de cet actif. Lorsque vous cliquez sur l'icône **Historique**, la fenêtre Recherche d'événements s'affiche, préremplie avec les critères de recherche d'événements : Vous pouvez personnaliser les paramètres de recherche, si nécessaire. Cliquez sur **Rechercher** pour afficher les informations historiques d'événement.
Applications	Cliquez sur **Applications** pour afficher les informations d'application de cet actif. Lorsque vous cliquez sur l'icône **Applications**, la fenêtre Recherche de flux s'affiche, préremplie avec les critères de recherche d'événements. Vous pouvez personnaliser les paramètres de recherche, si nécessaire. Cliquez sur **Rechercher** pour afficher les informations de l'application.
Rechercher des connexions	Cliquez sur **Rechercher des connexions** pour rechercher des connexions. La fenêtre Recherche de connexion s'affiche. Cette option s'affiche uniquement si IBM Security QRadar Risk Manager a été acheté et mis sous licence. Pour plus d'informations, voir *IBM Security QRadar Risk Manager - Guide d'utilisation*.
Afficher la topologie	Cliquez sur **Afficher la topologie** pour étudier davantage l'actif. La fenêtre Topologie en cours s'affiche. Cette option s'affiche uniquement si IBM Security QRadar Risk Manager a été acheté et mis sous licence. Pour plus d'informations, voir *IBM Security QRadar Risk Manager - Guide d'utilisation*.
Actions	Dans la liste **Actions**, sélectionnez **Historique des vulnérabilités.** Cette option s'affiche uniquement si IBM Security QRadar Risk Manager a été acheté et mis sous licence. Pour plus d'informations, voir *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**
3. Cliquez deux fois sur l'actif que vous souhaitez afficher.

4. Utilisez les options sur la barre d'outils pour afficher les différents volets des informations de profil d'actif. Voir Edition d'un profil d'actif.
5. Pour rechercher les vulnérabilités associées, cliquez sur chaque vulnérabilité dans le volet Vulnérabilités. Voir le Tableau 10-10
6. Si nécessaire, éditez le profil d'actif. Voir Edition d'un profil d'actif.
7. Cliquez sur **Revenir à la liste d'actifs** pour sélectionner et afficher un autre actif, si nécessaire.

Ajout ou édition d'un profil d'actif

Les profils d'actif sont automatiquement détectés et ajoutés. Néanmoins, il peut être nécessaire d'ajouter un profil manuellement.

Pourquoi et quand exécuter cette tâche

Lorsque des actifs sont détectés à l'aide de l'option Reconnaissance des serveurs, certains détails de profil d'actif sont remplis automatiquement. Vous pouvez ajouter manuellement des informations au profil d'actif et pouvez éditer certains paramètres.

Vous pouvez uniquement éditer les paramètres qui ont été saisis manuellement. Les paramètres gérés par le système s'affichent en italiques et ne sont pas éditables. Vous pouvez supprimer les paramètres générés par le système, si nécessaire.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Sélectionnez l'une des options suivantes :
   - Pour ajouter un actif, cliquez sur **Ajouter un actif** et saisissez l'adresse IP ou la plage CIDR de l'actif dans la zone **Nouvelle adresse IP**.
   - Pour éditer un actif, cliquez deux fois sur l'actif que vous souhaitez afficher, puis cliquez sur **Modifier un actif**.
4. Configurez les paramètres dans le volet Adresse MAC et IP. Configurez une ou plusieurs options parmi les suivantes :
   - Cliquez sur l'icône **Nouvelle adresse MAC** et saisissez une adresse MAC dans la boîte de dialogue.
   - Cliquez sur l'icône **Nouvelle adresse IP** et saisissez une adresse IP dans la boîte de dialogue.
   - Si **Contrôleur NIC inconnu** est disponible, sélectionnez cet élément, cliquez sur l'icône **Editer** et saisissez une nouvelle adresse MAC dans la boîte de dialogue.
   - Sélectionnez une adresse MAC ou IP dans la liste, cliquez sur l'icône **Editer** et saisissez une nouvelle adresse MAC dans la boîte de dialogue.
   - Sélectionnez une adresse MAC ou IP dans la liste, puis cliquez sur l'icône **Retirer**.
5. Configurez les paramètres dans le volet Noms et Description. Configurez une ou plusieurs options parmi les suivantes :

Paramètre	Description
DNS	Choisissez l'une des options suivantes : • Saisissez un nom DNS, puis cliquez sur **Ajouter**. • Sélectionnez un nom DNS dans la liste, puis cliquez sur **Editer**. • Sélectionnez un nom DNS dans la liste, puis cliquez sur **Retirer**.
NetBIOS	Choisissez l'une des options suivantes : • Saisissez un nom NetBIOS, puis cliquez sur **Ajouter**. • Sélectionnez un nom NetBIOS dans la liste, puis cliquez sur **Editer**. • Sélectionnez un nom NetBIOS dans la liste, puis cliquez sur **Retirer**.
Nom attribué	Saisissez le nom de ce profil d'actif.
Emplacement	Saisissez l'emplacement de ce profil d'actif.
Description	Saisissez la description de ce profil d'actif.
AP sans fil	Saisissez le point d'accès sans fil de ce profil d'accès.
SSIS sans fil	Saisissez l'identificateur de sous-système de stockage (SSID) de ce profil d'actif.
ID commutateur	Saisissez l'ID de commutateur de ce profil d'actif.
ID port commutateur	Saisissez l'ID de port de commutateur de ce profil d'actif.

6. Configurez les paramètres dans le volet Système d'exploitation :
   a. Dans la zone de liste **Fournisseur**, sélectionnez un fournisseur de système d'exploitation.
   b. Dans la zone de liste **Produit**, sélectionnez le système d'exploitation pour le profil d'actif.
   c. Dans la zone de liste **Version**, sélectionnez la version du système d'exploitation sélectionné.
   d. Cliquez sur l'icône **Ajouter**.
   e. Dans la zone de liste **Remplacer**, sélectionnez l'une des options suivantes :
      - **Remplacer jusqu'à la prochaine analyse** - Sélectionnez cette option pour indiquer que le scanner fournit des informations sur le système d'exploitation et que les informations peuvent être temporairement éditées. Si vous éditez les paramètres du système d'exploitation, le scanner restaure les informations au moment de sa prochaine analyse.
      - **Remplacer définitivement** - Sélectionnez cette option pour indiquer que vous souhaitez entrer manuellement des informations sur le système d'exploitation et désactiver la mise à jour des informations par le scanner.
   f. Sélectionnez un système d'exploitation dans la liste.
   g. Sélectionnez un système d'exploitation et cliquez sur l'icône **Redéfinir le basculement**.

7. Configurez les paramètres dans le volet CVSS et poids. Configurez une ou plusieurs options parmi les suivantes :

Paramètre	Description
Dommages collatéraux potentiels	Configurez ce paramètre pour indiquer le risque de danger de mort ou de perte d'actifs physiques par endommagement ou vol . Vous pouvez également utiliser ce paramètre pour indiquer le risque de perte économique en termes de productivité ou de recettes. Le risque de dommages collatéraux accru augmente la valeur calculée du paramètre Score CVSS . Dans la zone de liste **Dommages collatéraux potentiels**, sélectionnez l'une des options suivantes : • Aucun • Faible • Faible-Moyen • Moyen-Elevé • Elevé • Non défini Lorsque vous configurez le paramètre **Dommages collatéraux potentiels**, le paramètre **Poids** est automatiquement mis à jour.
Exigences de confidentialité	Configurez ce paramètre pour indiquer l'impact sur la confidentialité d'une vulnérabilité correctement exploitée de cet actif. L'impact de confidentialité accru augmente la valeur calculée du paramètre Score CVSS. Dans la zone de liste **Exigences de confidentialité**, sélectionnez l'une des options suivantes : • Faible • Moyen • Elevé • Non défini

Paramètre	Description
Exigences de disponibilité	Configurez ce paramètre pour indiquer l'impact sur la disponibilité de l'actif lorsqu'une vulnérabilité est correctement exploitée. Les attaques qui consomment de la bande passante réseau, des cycles de processeur ou de l'espace disque ont un impact sur la disponibilité d'un actif. L'impact de disponibilité accru augmente la valeur calculée du paramètre Score CVSS. Dans la zone de liste **Exigences de disponibilité**, sélectionnez l'une des options suivantes : • Faible • Moyen • Elevé • Non défini
Exigences d'intégrité	Configurez ce paramètre pour indiquer l'impact sur l'intégrité de l'actif lorsqu'une vulnérabilité est correctement exploitée. L'intégrité fait référence à la fiabilité et la véracité des informations. L'impact d'intégrité accru augmente la valeur calculée du paramètre Score CVSS. Dans la zone de liste **Exigences d'intégrité**, sélectionnez l'une des options suivantes : • Faible • Moyen • Elevé • Non défini
Poids	Dans la zone de liste **Poids**, sélectionnez le poids de ce profil d'accès. L'intervalle est compris entre 0 et 10. Lorsque vous configurez le paramètre **Poids**, le paramètre **Dommages collatéraux potentiels** est automatiquement mis à jour.

8. Configurez les paramètres dans le volet Propriétaires. Sélectionnez une ou plusieurs options parmi les suivantes :

Paramètre	Description
Propriétaire fonctionnel	Entrez le nom du propriétaire fonctionnel de l'actif. Un directeur de service est un exemple de propriétaire fonctionnel. La longueur maximale est de 255 caractères.
Contact propriétaire fonctionnel	Entrez les informations de contact du propriétaire fonctionnel. La longueur maximale est de 255 caractères.

Paramètre	Description
Propriétaire technique	Entrez le propriétaire technique de l'actif. Un responsable informatique ou un directeur sont des exemples de propriétaire fonctionnel. La longueur maximale est de 255 caractères.
Contact propriétaire technique	Entrez les informations de contact du propriétaire technique. La longueur maximale est de 255 caractères.
Utilisateur technique	Dans la zone de liste, sélectionnez le nom d'utilisateur que vous souhaitez associer à ce profil d'actif. Vous pouvez également utiliser ce paramètre pour activer la correction automatique des vulnérabilités d'IBM Security QRadar Vulnerability Manager. Pour plus d'informations sur la correction automatique, voir le document *IBM QRadar Vulnerability Manager User Guide*.

9. Cliquez sur **Sauvegarder**.

Recherche de profils d'actifs

Vous pouvez configurer les paramètres de recherche pour afficher uniquement les profils d'actifs que vous souhaitez rechercher dans l'onglet **Actifs** de la page Actif.

Pourquoi et quand exécuter cette tâche

Lorsque vous accédez à l'onglet **Actifs**, la page Actif s'affiche, remplie avec tous les actifs détectés dans votre réseau. Configurez les paramètres de recherche pour affiner la liste et afficher uniquement les profils d'actifs à rechercher.

La page Recherche d'actif permet de gérer les groupes de recherche d'actifs. Pour en savoir plus sur les groupes de recherche d'actifs, voir Groupes de recherche d'actifs.

La fonction de recherche vous permet de rechercher des profils d'hôte, des actifs et des informations d'identité. Les informations d'identité fournissent des détails supplémentaires sur les sources de journal de votre réseau, y compris les informations DNS, les connexions utilisateur et les adresses MAC.

La fonction de recherche d'actifs vous permet de rechercher les actifs par références de données externes pour déterminer si des vulnérabilités connues existent dans votre déploiement.

Par exemple :

Vous recevez une notification indiquant que l'ID CVE : est exploité activement dans la zone. Pour vérifier si des hôtes de votre déploiement sont vulnérables à cette exploitation, vous pouvez sélectionner **Référence externe de vulnérabilité** dans la liste des paramètres de recherche, sélectionner **CVE**, puis saisir

```
2010-000
```

Pour afficher une liste de tous les hôtes vulnérables à cet ID CVE spécifique.

Remarque : Pour plus d'informations sur OSVDB, voir le site *http://osvdb.org/* . Pour plus d'informations sur la base de données NVDB, voir le site *http://nvd.nist.gov/* .

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Dans la barre d'outils, cliquez sur **Rechercher** > **Nouvelle recherche**.
4. Sélectionnez l'une des options suivantes :
   - Pour charger une recherche précédemment sauvegardée, passez à l'étape 5.
   - Pour créer une nouvelle recherche, passez à l'étape 6.
5. Sélectionnez une recherche précédemment sauvegardée :
   a. Sélectionnez l'une des options suivantes :
      - Facultatif. Dans la zone de liste **Groupe**, sélectionnez le groupe de recherche d'actifs que vous souhaitez afficher dans la liste **Recherches sauvegardées disponibles**.
      - Dans la liste **Recherches sauvegardées disponibles**, sélectionnez la recherche sauvegardée que vous souhaitez charger.
      - Dans la zone **Saisir une recherche sauvegardée ou effectuer votre sélection dans la liste**, saisissez le nom de la recherche que vous souhaitez charger.

   b. Cliquez sur **Charger**.
6. Dans le volet Paramètres de recherche, définissez vos critères de recherche :
   a. Dans la première zone de liste, sélectionnez le paramètre d'actif que vous souhaitez rechercher. Par exemple, **Nom d'hôte**, **Classification des risques de vulnérabilité**, ou **Propriétaire technique**.
   b. Dans la deuxième zone de liste, sélectionnez le modificateur que vous souhaitez utiliser dans le cadre de la recherche.
   c. Dans la zone d'entrée, saisissez les informations spécifiques associées à votre paramètre de recherche.
   d. Cliquez sur **Ajouter un filtre**.
   e. Répétez ces étapes pour chaque filtre que vous souhaitez ajouter aux critères de recherche.
7. Cliquez sur **Rechercher**.

Résultats

Vous pouvez enregistrer vos critères de recherche d'actifs. Voir Sauvegarde des critères de recherche d'actifs.

Sauvegarde des critères de recherche d'un actif

Dans l'onglet **Actif**, vous pouvez sauvegarder les critères de recherche configurés afin de pouvoir les réutiliser. Les critères de recherche enregistrés n'expirent pas.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Effectuez une recherche.
4. Cliquez sur **Sauvegarder les critères**.

5. Saisissez les valeurs pour ces paramètres :

Paramètre	Description
Entrez le nom de cette recherche	Entrez le nom unique que vous souhaitez affecter à ce critère de recherche.
Gérer les groupes	Cliquez sur **Gérer les groupes** pour gérer des groupes de recherche. Cette option s'affiche uniquement si vous disposez d'autorisations administrateur.
Affecter la recherche au(x) groupe(s)	Cochez la case du groupe auquel vous souhaitez affecter cette recherche sauvegardée. Si vous ne sélectionnez pas de groupe, cette recherche sauvegardée est affectée au groupe **Autre** par défaut.
Inclure dans mes recherches rapides	Cochez cette case pour inclure cette recherche à votre zone de liste **Recherche rapide**, dans la barre d'outils de l'onglet **Actifs**.
Définir par défaut	Cochez cette case pour définir cette recherche comme recherche par défaut lorsque vous accédez à l'onglet **Actifs**.
Partager avec tout le monde	Cochez cette case pour partager ces exigences de recherche avec tous les autres utilisateurs.

Groupes de recherche d'actifs

A l'aide de la fenêtre Groupes de recherche d'actif, vous pouvez créer et gérer des groupes de recherche d'actifs.

Ces groupes vous permettent de localiser facilement des critères de recherche sauvegardés sur l'onglet **Actifs**.

Affichage des groupes de recherche

Utilisez la fenêtre Groupes de recherche d'actif pour afficher un groupe de liste et des sous-groupes.

Pourquoi et quand exécuter cette tâche

Dans la fenêtre Groupes de recherche d'actif, vous pouvez afficher des détails sur chaque groupe, notamment une description et la date de la dernière modification du groupe.

Toutes les recherches sauvegardées qui ne sont pas affectées à un groupe se trouvent dans le groupe **Autre**.

La fenêtre Groupes de recherche d'actif affiche les paramètres suivants pour chaque groupe :

Tableau 31. Fonctions de la barre d'outils de la fenêtre Groupes de recherche d'actif

Fonction	Description
Nouveau groupe	Pour créer un nouveau groupe de recherche, vous pouvez cliquer sur **Nouveau groupe**. Voir Création d'un nouveau groupe de recherche.

Tableau 31. Fonctions de la barre d'outils de la fenêtre Groupes de recherche d'actif (suite)

Fonction	Description
Editer	Pour éditer un groupe de recherche existant, vous pouvez cliquer sur **Editer**. Voir Edition d'un groupe de recherche.
Copier	Pour copier une recherche sauvegardée sur un autre groupe de recherche, vous pouvez cliquer sur **Copier**. Voir Copie d'une recherche sauvegardée vers un autre groupe.
Retirer	Pour supprimer un groupe de recherche ou une recherche sauvegardée à partir d'un groupe de recherche, sélectionnez l'élément que vous souhaitez supprimer, puis cliquez sur **Retirer**. Voir Suppression d'un groupe ou d'une recherche sauvegardée d'un groupe.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Sélectionnez **Rechercher** > **Nouvelle recherche**.
4. Cliquez sur **Gérer les groupes**.
5. Afficher les groupes de recherche.

Création d'un groupe de recherche

Dans la fenêtre Groupes de recherche d'actif, vous pouvez créer un groupe de recherche.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Sélectionnez **Rechercher** > **Nouvelle recherche**.
4. Cliquez sur **Gérer les groupes**.
5. Sélectionnez le dossier du groupe sous lequel vous souhaitez créer le groupe.
6. Cliquez sur **Nouveau groupe**.
7. Dans la zone **Nom**, entrez un nom unique pour le nouveau groupe.
8. Facultatif. Dans la zone **Description**, entrez une description.
9. Cliquez sur **OK**.

Edition d'un groupe de recherche

Vous pouvez éditer les zones **Nom** et **Description** d'un groupe de recherche.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Sélectionnez **Rechercher** > **Nouvelle recherche**.
4. Cliquez sur **Gérer les groupes**.
5. Sélectionnez le groupe que vous souhaitez éditer.
6. Cliquez sur **Editer**.

7. Saisissez un nouveau nom dans la zone **Nom**.
8. Entrez une nouvelle description dans la zone **Description**.
9. Cliquez sur **OK**.

Copie d'une recherche sauvegardée vers un autre groupe

Vous pouvez copier une recherche sauvegardée vers un autre groupe. Vous pouvez également copier la recherche sauvegardée vers plusieurs groupes.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Sélectionnez **Rechercher** > **Nouvelle recherche**.
4. Cliquez sur **Gérer les groupes**.
5. Sélectionnez la recherche sauvegardée que vous souhaitez copier.
6. Cliquez sur **Copier**.
7. Dans la fenêtre Groupes d'éléments, cochez la case du groupe vers lequel vous souhaitez copier la recherche sauvegardée.
8. Cliquez sur **Affecter des groupes**.

Suppression d'un groupe ou d'une recherche sauvegardée dans un groupe

Vous pouvez utiliser l'icône **Retirer** pour supprimer une recherche d'un groupe ou supprimer un groupe de recherche.

Pourquoi et quand exécuter cette tâche

Lorsque vous supprimez une recherche sauvegardée d'un groupe, la recherche sauvegardée n'est pas supprimée de votre système. La recherche sauvegardée est supprimée du groupe et déplacée automatiquement vers le groupe **Autre**.

Vous ne pouvez pas supprimer les groupes suivants de votre système :

- Groupes de recherche d'actif
- Autre

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Sélectionnez **Rechercher** > **Nouvelle recherche**.
4. Cliquez sur **Gérer les groupes**.
5. Sélectionnez la recherche sauvegardée que vous souhaitez supprimer du groupe :
   - Sélectionnez la recherche sauvegardée que vous souhaitez supprimer du groupe.
   - Sélectionnez le groupe que vous souhaitez supprimer.

Tâches de gestion des profils d'actif

Vous pouvez supprimer, importer et exporter des profils d'actif à l'aide de l'onglet Actifs.

Pourquoi et quand exécuter cette tâche

L'onglet **Actifs** vous permet de supprimer, importer et exporter des profils d'actif.

Suppression des actifs

Vous pouvez supprimer des actifs spécifiques ou tous les profils d'actifs répertoriés.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Sélectionnez l'actif que vous souhaitez supprimer, puis sélectionnez **Supprimer un actif** dans la zone de liste **Actions**.
4. Cliquez sur **OK**.

Importation de profils d'actif

Vous pouvez importer des informations de profil d'actif.

Avant de commencer

Le fichier importé doit être un fichier CSV au format suivant :

```
ip,nom,poids,description
```

où :

- **ip** - Indique une adresse IP valide selon la notation décimale à points. Par exemple : 192.168.5.34.
- **nom** - Indique le nom de cet actif pouvant contenir jusqu'à 255 caractères. Les virgules ne sont pas valides dans cette zone et invalident le processus d'importation. Par exemple : WebServer01 est correct.
- **poids** - Indique un nombre compris entre 0 et 10, qui correspond à l'importance de cet actif sur votre réseau. Une valeur égale à 0 représente une importance faible et une valeur égale à 10 une importance très élevée.
- **description** - Indique une description textuelle de cet actif pouvant contenir jusqu'à 255 caractères. Cette valeur est facultative.

Par exemple, les entrées suivantes peuvent être incluses dans un fichier CSV :

-
  ```
  192.168.5.34,WebServer01,5,Main Production Web Server
  ```
-
  ```
  192.168.5.35,MailServ01,0,
  ```

Le processus d'importation fusionne les profils d'actif importés avec les informations de profil d'actif actuellement stockées sur le système.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Dans la zone de liste **Actions**, sélectionnez **Importer des actifs**.
4. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier CSV que vous souhaitez importer.
5. Cliquez sur **Importer des actifs** pour commencer le processus d'importation.

Exportation des actifs

Vous pouvez exporter les profils d'actifs répertoriés vers un fichier au format XML ou CSV.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Dans la zone de liste **Actions**, sélectionnez l'une des options suivantes :
   - Exporter au format XML
   - Exporter au format CSV
4. Affichez la fenêtre d'état correspondant au statut du processus d'exportation.
5. Facultatif : Si vous souhaitez utiliser d'autres onglets et pages alors que le processus d'exportation est en cours, cliquez sur le lien **Aviser à la fin de l'opération**.

   Une fois l'exportation terminée, la fenêtre de téléchargement de fichier s'affiche.
6. Dans cette fenêtre, choisissez l'une des options suivantes :
   - **Ouvrir** - Sélectionnez cette option pour ouvrir les résultats de l'exportation dans le navigateur de votre choix.
   - **Sauvegarder** - Sélectionnez cette option pour enregistrer les résultats sur votre bureau.
7. Cliquez sur **OK**.

Recherche de vulnérabilités pour l'actif

Le volet Vulnérabilités de la page Profil d'actif affiche une liste des vulnérabilités découvertes pour l'actif.

Pourquoi et quand exécuter cette tâche

Vous pouvez cliquer deux fois sur la vulnérabilité pour afficher plus de détails.

La fenêtre Groupe de recherche d'actif fournit les détails suivants :

Paramètre	Description
ID de vulnérabilité	Indique l'ID de la vulnérabilité. L'ID de vulnérabilité est un identificateur unique généré par Vulnerability Information System (VIS).
Date de publication	Indique la date à laquelle les détails de la vulnérabilité ont été publiés sur la base de données OSVDB.
Nom	Indique le nom de la vulnérabilité.
Actifs	Indique le nombre d'actifs de votre réseau disposant de cette vulnérabilité. Cliquez sur le lien pour afficher la liste des actifs.
Actifs, y-compris exceptions	Indique le nombre d'actifs de votre réseau disposant d'exceptions de vulnérabilité. Cliquez sur le lien pour afficher la liste des actifs.

Paramètre	Description
CVE	Indique l'identificateur CVE de la vulnérabilité. Les identificateurs CVE sont fournis par la base de données NVDB. Cliquez sur le lien pour obtenir plus d'informations. Le site Web NVDB s'affiche dans une nouvelle fenêtre de navigateur.
xforce	Indique l'identificateur X-Force de la vulnérabilité. Cliquez sur le lien pour obtenir plus d'informations. Lorsque vous cliquez sur le lien, le site Web IBM Internet Security Systems apparaît dans une nouvelle fenêtre de navigateur.
OSVDB	Indique l'identificateur OSVDB de la vulnérabilité. Cliquez sur le lien pour obtenir plus d'informations. Le site Web OSVDB s'affiche dans une nouvelle fenêtre de navigateur.
Détails du plug-in	Indique l'ID de QRadar Vulnerability Manager. Cliquez sur le lien pour afficher les entrées Oval Definitions, Windows Knowledge Base ou les recommandations UNIX pour la vulnérabilité. Cette fonction fournit des informations sur la manière dont QRadar Vulnerability Manager recherche des données de vulnérabilité lors d'une analyse de correctif. Vous pouvez l'utiliser pour identifier la raison pour laquelle une vulnérabilité est apparue ou non sur un actif.

Paramètre	Description
CVSS Score Base	Affiche le score Common Vulnerability Scoring System (CVSS) agrégé des vulnérabilités de cet actif. Un score CVSS est une métrique d'évaluation de la gravité d'une vulnérabilité. Vous pouvez utiliser les scores CVSS pour mesurer les inquiétudes justifiées par une vulnérabilité par rapport à d'autres vulnérabilités. Le score CVSS est calculé à l'aide des paramètres utilisateur suivants : • Dommages collatéraux potentiels • Exigences de confidentialité • Exigences de disponibilité • Exigences d'intégrité Pour plus d'informations sur la configuration de ces paramètres, voir «Ajout ou édition d'un profil d'actif», à la page 120. Pour plus d'informations sur CVSS, voir *http://www.first.org/cvss/*.
Impact	Affiche le type de préjudice ou de dommage attendu si cette vulnérabilité était exploitée.
Métriques de base CVSS	Affiche les métriques utilisées pour calculer le score CVSS de base, notamment : • Vecteur d'accès • Complexité d'accès • Authentification • Impact sur la confidentialité • Impact sur l'intégrité • Impact sur la disponibilité
Description	Indique une description de la vulnérabilité détectée. Cette valeur est uniquement disponible lorsque votre système intègre les outils VA.
Problème	Indique les effets que la vulnérabilité peut avoir sur votre réseau.
Solution	Suivez les instructions fournies pour résoudre la vulnérabilité.
Correctif virtuel	Affiche les informations de correctif virtuel associées à cette vulnérabilité, le cas échéant. Un correctif virtuel est une solution de réduction à court terme pour une vulnérabilité récemment découverte. Ces informations proviennent des événements IPS (Intrusion Protection System). Si vous souhaitez installer le correctif virtuel, reportez-vous aux informations de votre fournisseur IPS.

Paramètre	Description
Référence	Affiche la liste des références externes, notamment : • **Type de référence** - Indique le type de référence répertoriée, tel qu'une adresse URL recommandée ou une liste de messages. • **URL** - Indique l'adresse URL sur laquelle vous pouvez cliquer pour afficher la référence. Cliquez sur le lien pour obtenir plus d'informations. Lorsque vous cliquez sur le lien, la ressource externe s'affiche dans une nouvelle fenêtre de navigateur.
Produits	Affiche la liste des produits associés à cette vulnérabilité. • **Fournisseur** - Indique le fournisseur du produit. • **Produit** - Indique le nom du produit. • **Version** - Indique le numéro de version du produit.

Procédure

1. Cliquez sur l'onglet **Actifs**.
2. Dans le menu de navigation, cliquez sur **Profils d'actifs**.
3. Sélectionnez un profil d'actif.
4. Dans le volet Vulnérabilités, cliquez sur la valeur de paramètre **ID** ou **Vulnérabilité** de la vulnérabilité que vous souhaitez étudier.

Chapitre 8. Gestion des graphiques

Vous pouvez afficher vos données à l'aide de diverses options de configuration de graphique.

Grâce aux graphiques sur les onglets **Activité du journal** et **Activité réseau**, vous pouvez afficher vos données à l'aide de diverses options de configuration de graphique.

Gestion des graphiques

Vous pouvez utiliser diverses options de configuration des graphiques pour afficher vos données.

Si vous sélectionnez un délai ou une option de groupement pour afficher vos données, les graphiques s'affichent au-dessus de la liste d'événements ou de flux.

Les graphiques ne s'affichent pas lors du mode de diffusion en flux.

Vous pouvez configurer un graphique pour sélectionner les données que vous souhaitez tracer. Vous pouvez configurer des graphiques sans tenir compte des autres pour afficher vos résultats de recherche à partir de perspectives différentes.

Les types de graphiques incluent :

- graphique à barres - affiche les données dans un graphique à barres. Cette option est uniquement disponible pour les événements groupés.
- graphique circulaire - affiche les données dans un graphique circulaire. Cette option est uniquement disponible pour les événements groupés.
- tableau - affiche les données dans un tableau. Cette option est uniquement disponible pour les événements groupés.
- séries temporelles - affiche un graphique à courbes interactif qui représente les enregistrements mis en corrélation par un intervalle de temps spécifié. Pour en savoir plus sur la configuration des critères de recherche des séries temporelles, consultez la section Présentation de graphique de séries temporelles.

Après avoir configuré un graphique, les configurations de votre graphique sont conservées lorsque vous :

- modifiez votre affichage à l'aide de la zone de liste **Afficher**.
- appliquez un filtre.
- sauvegardez votre critère de recherche.

Vos configurations de graphique ne sont pas conservées lorsque vous :

- démarrez une nouvelle recherche.
- accédez à une recherche rapide.
- affichez les résultats groupés dans une fenêtre d'affiliation.
- sauvegardez les résultats de votre recherche.

Remarque : Si vous utilisez le navigateur Web Mozilla Firefox et qu'une extension de navigateur de blocage de publicité est installée, les graphiques ne

© Copyright IBM Corp. 2012, 2017

s'affichent pas. Pour afficher les graphiques, vous devez retirer l'extension de navigateur de blocage de publicité. Pour en savoir plus, consultez la documentation de votre navigateur.

Présentation des graphiques de série temporelle

Les graphiques de série temporelle sont des représentations graphiques de votre activité au fil du temps.

Les sommets et les creux correspondent aux volumes d'activité élevés et faibles. Les graphiques de série temporelle sont utiles à l'analyse des tendances de données à court et à long terme.

A l'aide des graphiques de séries temporelles, vous pouvez accéder, naviguer et étudier le journal ou l'activité réseau à partir des divers affichages et perspectives.

Remarque : Vous devez disposer des autorisations appropriées pour gérer et afficher des graphiques de série temporelle.

Pour afficher les graphiques de série temporelle, vous devez créer et sauvegarder une recherche qui comprend les séries temporelles et les options de groupement. Vous pouvez enregistrer jusqu'à 100 recherches de séries temporelles.

Les recherches de séries temporelles enregistrées par défaut sont accessibles à partir de la liste des recherches disponibles sur la page de recherche d'événements ou de flux.

Vous pouvez facilement identifier les recherches de séries temporelles enregistrées dans le menu **Recherches rapides** car le nom de la recherche est ajouté à la plage de temps spécifiée dans les critères de recherche.

Si vos paramètres de recherche correspondent à une recherche déjà sauvegardée pour les options de groupement et de définition, un graphique de série temporelle peut s'afficher automatiquement pour vos résultats de recherche. Si un graphique de série temporelle ne s'affiche pas automatiquement pour vos critères de recherche non sauvegardés, il n'existe aucune recherche sauvegardée correspondant aux paramètres de recherche. Si cela se produit, vous devez activer la capture des données de série temporelle et sauvegarder vos critères de recherche.

Vous pouvez agrandir et analyser un diagramme pour étudier l'activité. Le tableau suivant fournit des fonctions vous permettant d'afficher des graphiques de série temporelle.

Tableau 32. Fonctions des graphiques de série temporelle

Fonction	Description
Afficher les données avec plus de détails	A l'aide de la fonction de zoom, vous pouvez étudier les plus petites tranches horaires du trafic de l'événement. • Placez le pointeur de votre souris sur le graphique et utilisez la molette pour agrandir le graphique (faire rouler la molette de la souris vers le haut). • Mettez en évidence la zone du graphique que vous souhaitez agrandir. Lorsque vous relâchez le bouton de la souris, le graphique affiche un segment temporel plus petit. Vous pouvez maintenant cliquer sur le graphique et le déplacer pour l'analyser. Lorsque vous agrandissez le graphique de série temporelle, le graphique s'actualise pour afficher un segment de temps plus petit.
Afficher un intervalle de temps de données plus large	A l'aide de la fonction de zoom, vous pouvez rechercher des segments de temps plus larges ou retourner à l'intervalle maximal. Vous pouvez étendre un intervalle de temps en utilisant l'une des options suivantes : • Cliquez sur Réinitialiser le zoom dans le coin supérieur gauche du graphique. • Placez le pointeur de votre souris sur le graphique, puis utilisez la molette pour agrandir l'affichage (faire rouler la molette vers le bas).
Analyser le graphique	Lorsque vous avez agrandi un graphique de série temporelle, vous pouvez cliquer sur le graphique et le déplacer vers la gauche ou la droite pour analyser le diagramme.

Légendes des graphiques

Chaque graphique fournit une légende, qui est une référence visuelle pour vous aider à associer les objets de graphique pour les paramètres qu'ils représentent.

À l'aide de la fonction de légende, vous pouvez effectuer les actions suivantes :

- Déplacez le pointeur de votre souris sur un élément de légende ou le bloc de couleurs de légende pour afficher plus d'informations sur les paramètres qu'il représente.
- Cliquez avec le bouton droit de la souris sur l'élément de la légende afin d'étudier cet élément.
- Cliquez sur un graphique circulaire ou un diagramme à barres pour masquer l'élément dans le graphique. Cliquez de nouveau sur l'élément de légende pour afficher l'élément masqué. Vous pouvez également cliquer sur l'élément de graphique correspondant pour masquer/afficher l'élément.

- Cliquez sur **Légende**, ou sur la flèche à côté si vous souhaitez supprimer la légende de votre affichage du graphique.

Configuration des graphiques

Vous pouvez utiliser les options de configuration pour modifier le type de graphique, le type d'objet à représenter sous forme de graphique et le nombre d'objets représentés sur le graphique. Vous pouvez également sélectionner un intervalle pour les graphiques de série temporelle et activer une capture de données de série temporelle

Pourquoi et quand exécuter cette tâche

Les données peuvent être cumulées de sorte que lorsque vous exécutez une recherche de série temporelle, il existe une mémoire cache des données pour afficher les données relatives à la période précédente. Après avoir activé la capture de données de série temporelle pour un paramètre sélectionné, un astérisque (*) est affiché à côté du paramètre dans la zone de liste Valeur vers graphique.

Restriction : Les graphiques ne sont pas affichés lorsque vous affichez des événements ou des flux en temps réel (streaming). Pour afficher les graphiques, vous devez accéder à l'onglet **Activité du journal** ou **Activité réseau** et réaliser une recherche groupée spécifiant un intervalle de temps.

Procédure

1. Cliquez sur l'onglet **Activité du journal** ou **Activité réseau**.
2. Pour créer une recherche groupée, procédez comme suit :
   a. Dans la barre d'outils, cliquez sur **Rechercher** > **Nouvelle recherche**.
   b. Sous **Recherches sauvegardées disponibles**, sélectionnez une recherche et cliquez sur **Charger**.
   c. Accédez au panneau Définition de colonne et si la zone de liste **Grouper par** est vide, dans la liste **Colonnes disponibles**, sélectionnez une colonne.
   d. Cliquez sur **Rechercher**.
3. Pour utiliser une recherche groupée, sur la barre d'outils, cliquez sur **Recherches rapides** et sélectionnez une recherche groupée.
4. Dans le panneau Graphiques, cliquez sur l'icône **Configurer** ( ).
5. Configurez les paramètres suivants :

Paramètre	Description
Valeur vers graphique	Type d'objet que vous souhaitez représenter sur l'axe Y du graphique. Les options incluent tous les paramètres d'événements ou de flux normalisés ou personnalisés inclus dans vos paramètres de recherche.
Afficher les meilleurs	Nombre d'objets que vous souhaitez afficher dans le graphique. La valeur par défaut est 10. Si vous incluez plus de 10 éléments dans votre graphique, vos données risquent d'être illisibles.

Paramètre	Description
Type de graphique	Si votre graphique à barre, votre graphique circulaire ou votre graphique en forme de tableau est basé sur des critères de recherche sauvegardée et porte sur un intervalle supérieur à 1 heure, vous devez cliquer sur **Mettre à jour les détails** pour mettre à jour le graphique et compléter les détails de l'événement.
Capture des données de séries temporelles	Permet la capture des données de série temporelles. Lorsque vous cochez cette case, le graphique commence à accumuler des données pour les graphiques de séries temporelles. Cette option est désactivée par défaut. Cette option est uniquement disponible sur les graphiques de série temporelle.
Intervalle	Intervalle que vous souhaitez afficher. Cette option est uniquement disponible sur les graphiques de série temporelle.

6. Si vous avez l'option de graphique **Série temporelle** et activé l'option **Capture des données de séries temporelles**, dans le panneau Graphiques, cliquez sur **Sauvegarder**.
7. Pour afficher la liste des événements ou flux dans le cas où votre intervalle est supérieur à une heure, cliquez sur **Mettre à jour les détails**.

Chapitre 9. Recherches

Utilisez les options de recherche et d'indexation de IBM Security QRadar pour améliorer les performances de recherche et renvoyer des résultats plus rapides. Pour trouver des critères spécifiques, les recherches avancées utilisent les chaînes de recherche AQL.

Sur les onglets **Activité du journal**, **Activité réseau** et **Infractions**, vous pouvez définir des critères pour la recherche d'événements, de flux et d'infractions.

Recherches d'événement et de flux

Vous pouvez effectuer des recherches dans les onglets **Activité du journal**, **Activité réseau** et **Infractions**.

Si votre administrateur QRadar a configuré des restrictions de ressource afin de définir des limitations d'heure ou de données pour les recherches d'événement et de flux, l'icône de restriction de ressource ( ) s'affiche en regard des critères de recherche.

Après avoir effectué une recherche, vous pouvez sauvegarder les critères de recherche et les résultats de la recherche.

Création d'une recherche personnalisée

Vous pouvez chercher des données correspondant à vos critères en utilisant des options de rechercher plus spécifiques. Par exemple, vous pouvez spécifier des colonnes pour votre recherche, que vous pouvez regrouper et réorganiser pour consulter plus efficacement vos résultats de la recherche.

Pourquoi et quand exécuter cette tâche

La durée de votre recherche dépend de la taille de votre base de données.

Vous pouvez ajouter de nouvelles options de recherche pour filtrer les résultats de la recherche afin de trouver un événement ou un flux spécifique que vous cherchez.

Le tableau ci-dessous décrit les options de recherche que vous pouvez utiliser pour rechercher des données d'événement et de flux :

Tableau 33. Options de recherche

Options	Description
Groupe	Cette option vous permet de sélectionner un groupe de recherche d'événement ou de flux pour afficher la liste **Recherches sauvegardées disponibles**.
Saisir une recherche sauvegardée ou effectuer votre sélection dans la liste	Entrez le nom d'une recherche sauvegardée ou un mot-clé pour filtrer la liste **Recherches sauvegardées disponibles**.

© Copyright IBM Corp. 2012, 2017

Tableau 33. Options de recherche (suite)

Options	Description
Recherches sauvegardées disponibles	Cette liste affiche toutes les recherches disponibles, sauf si vous lui appliquez un filtre en utilisant les options **Groupe ou Saisir une recherche sauvegardée** ou **Effectuer votre sélection dans la liste**. Vous pouvez sélectionner une recherche sauvegardée sur cette liste à afficher ou éditer.
Rechercher	L'icône **Rechercher** est disponible dans plusieurs volets de la page de recherche. Vous pouvez cliquer sur Rechercher une fois que vous avez terminé la configuration de la recherche et que vous souhaitez afficher les résultats.
Inclure dans mes recherches rapides	Cochez cette case pour inclure cette recherche à votre menu **Recherche rapide**.
Inclure dans mon tableau de bord	Cette case vous permet d'inclure les données de vos recherches sauvegardées à l'onglet **Tableau de bord**. Pour plus d'informations sur l'onglet **Tableau de bord**, voir Gestion du tableau de bord. **Remarque :** Ce paramètre ne s'affiche que si la recherche est regroupée.
Définir par défaut	Cochez cette case pour définir cette recherche comme votre recherche par défaut.
Partager avec tout le monde	Cochez cette case pour partager cette recherche avec tous les autres utilisateurs.
Temps réel (diffusion en flux)	Affiche les résultats en mode de diffusion en flux. **Remarque :** Quand l'option Temps réel (diffusion en flux) est activée, il est impossible de grouper vos résultats de recherche. Si vous sélectionnez n'importe quelle option de groupement dans le volet Définition de colonne, un message d'erreur apparaît.
Dernier intervalle (actualisation automatique)	Les onglets **Activité du journal** et **Activité réseau** sont actualisés à intervalles d'une minute pour afficher les toutes dernières informations.
Récent	Une fois que vous avez choisi cette option, vous devez sélectionner l'un des intervalles dans la liste. **Remarque :** Les résultats de la dernière minute ne sont peut-être pas disponibles. Sélectionnez l'option <*Intervalle spécifique*> si vous souhaitez afficher tous les résultats.
Intervalle spécifique	Une fois que vous avez choisi cette option, vous devez sélectionner la plage de date et d'heure dans les agendas **Heure de début** et **Heure de fin**.

Tableau 33. Options de recherche (suite)

Options	Description
Accumulation des données	Cette option s'affiche lorsque vous chargez une recherche enregistrée. Si aucune donnée n'est cumulée pour cette recherche sauvegardée, le message d'information suivant s'affiche : `Les données ne sont pas cumulées pour cette recherche`. Si les données s'accumulent pour cette recherche enregistrée, les options suivantes s'affichent : Lorsque vous cliquez sur le lien de la colonne ou que vous passez la souris dessus, une liste des colonnes cumulant les données s'affiche. Cliquez sur le lien **Activer/Désactiver les comptages uniques** pour afficher les comptages d'événements et de flux uniques au lieu des comptages moyens dans le temps. Une fois que vous cliquez sur le lien **Activer les comptages uniques**, une boîte de dialogue s'ouvre et indique les recherches et les rapports sauvegardés qui partagent les données accumulées. Cliquez sur le lien **Activer/Désactiver les comptages uniques** pour afficher les comptages d'événements uniques au lieu des comptages moyens dans le temps. Une fois que vous cliquez sur le lien **Activer les comptages uniques**, une boîte de dialogue s'ouvre et indique les recherches et les rapports sauvegardés qui partagent les données accumulées.
Filtres en cours	Affiche les filtres appliqués à cette recherche.
Enregistrer les résultats une fois la recherche terminée	Enregistre les résultats de la recherche.
Afficher	Spécifie une colonne prédéfinie, définie de manière à s'afficher dans les résultats de la recherche.
Nom	Nom de l'agencement de colonne personnalisé.
Sauvegarder la présentation de colonne	Enregistre un agencement de colonne personnalisé que vous avez modifié.
Supprimer la présentation de colonne	Supprime un agencement de colonne personnalisé enregistré.
Saisir une colonne ou effectuer votre sélection dans la liste	Filtrez les colonnes répertoriées dans la liste Colonnes disponibles. Par exemple, saisissez `Périphérique` pour afficher la liste des colonnes contenant Périphérique dans leur nom.

Tableau 33. Options de recherche (suite)

Options	Description
Colonnes disponibles	Les colonnes en cours d'utilisation pour cette recherche sauvegardée sont mises en évidence et affichées dans la liste **Colonnes**.
Flèches Ajouter une colonne et Retirer la colonne (ensemble supérieur)	Le premier ensemble de flèches vous permet de personnaliser la liste **Grouper par**. • Pour ajouter une colonne, sélectionnez une ou plusieurs colonnes dans la liste **Colonnes disponibles** et cliquez sur la flèche droite. • Pour retirer une colonne, sélectionnez une ou plusieurs colonnes dans la liste **Grouper par** et cliquez sur la flèche gauche.
Flèches Ajouter une colonne et Retirer la colonne (ensemble inférieur)	Le dernier ensemble de flèches vous permet de personnaliser la liste **Colonnes**. • Pour ajouter une colonne, sélectionnez une ou plusieurs colonnes dans la liste **Colonnes disponibles** et cliquez sur la flèche droite. • Pour retirer une colonne, sélectionnez une ou plusieurs colonnes dans la liste **Colonnes** et cliquez sur la flèche gauche.
Grouper par	Spécifie les colonnes dans lesquelles la recherche enregistrée regroupe les résultats. • Pour déplacer une colonne vers le haut de la liste de priorité, sélectionnez une colonne et cliquez sur la flèche haut. Vous pouvez également faire glisser la colonne vers le haut de la liste. • Pour déplacer une colonne vers le bas de la liste de priorité, sélectionnez une colonne et cliquez sur la flèche bas. Vous pouvez également faire glisser la colonne vers le bas de la liste. La liste de priorité indique l'ordre dans lequel les résultats sont groupés. Les résultats de recherche sont groupés dans la première colonne de la liste **Grouper par** puis dans la colonne suivante.

Tableau 33. Options de recherche (suite)

Options	Description
Colonnes	Indique les colonnes choisies pour la recherche. Vous pouvez sélectionner plus de colonnes dans la liste **Colonnes disponibles**. Vous pouvez personnaliser davantage la liste **Colonnes**en utilisant les options suivantes : • Pour déplacer une colonne vers le haut de la liste de priorité, sélectionnez une colonne et cliquez sur la flèche haut. Vous pouvez également faire glisser la colonne vers le haut de la liste. • Pour déplacer une colonne vers le bas de la liste de priorité, sélectionnez une colonne et cliquez sur la flèche bas. Vous pouvez également faire glisser la colonne vers le bas de la liste. Si le type de colonne est numérique ou temporel et qu'une entrée figure dans la liste **Regrouper par**, la colonne contient une liste, qui vous permet de choisir le mode de groupement de la colonne. Si la colonne est de type groupement, la colonne inclut une liste pour sélectionner le nombre de niveaux à inclure pour le regroupement.
Déplacer des colonnes entre la liste Grouper par et la liste Colonnes	Déplacez les colonnes entre la liste **Regrouper par** et la liste **Colonnes** en sélectionnant une colonne dans une liste et en la faisant glisser vers l'autre liste.
Trier par	Dans la première liste, sélectionnez la colonne dans laquelle vous souhaitez trier les résultats de recherche. Puis, dans la deuxième liste, sélectionnez l'ordre dans lequel vous souhaitez afficher les résultats de la recherche.

Tableau 33. Options de recherche (suite)

Options	Description
Limite de résultats	Spécifie le nombre de ligne renvoyées par le recherche dans la fenêtre Modifier la recherche. La zone **Limite de résultats** apparaît également dans la fenêtre Résultats. • Pour une recherche enregistrée, la limite est stockée dans la recherche enregistrée et réappliquée lorsque la recherche est chargée. • Dans les résultats de la recherche, lorsque vous triez une colonne comportant une limite de lignes, le tri est effectué dans les lignes limitées, affichées dans la grille de données. • Pour une recherche regroupée, dans laquelle le graphique de série temporelle est activé, la limite de lignes ne concerne que la grille de données. La liste **N premiers** dans le graphique de série temporelle contrôle le nombre de séries temporelles figurant dans le graphique.

Procédure

1. Sélectionnez une option de recherche :
   - Pour rechercher des événements, cliquez sur l'onglet **Activité du journal**.
   - Pour rechercher des flux, cliquez sur l'onglet **Activité réseau**.
2. Dans la liste **Rechercher**, sélectionnez **Nouvelle recherche**.
3. Sélectionnez une recherche précédemment sauvegardée.
4. Pour créer une recherche, dans le volet Intervalle, sélectionnez les options de l'intervalle à capturer pour cette recherche.

   Remarque : L'intervalle sélectionné peut avoir un impact sur les performances, lorsque l'intervalle est important.
5. Activez les comptages uniques dans le volet **Accumulation des données**.

   Remarque : L'activation des comptages uniques dans les données accumulées, qui est partagée avec de nombreuses autres recherches et de nombreux autres rapports, peut réduire les performances système.
6. Dans le volet Paramètres de recherche, définissez vos critères de recherche.
   a. Dans la première liste, sélectionnez un paramètre à rechercher,
   b. Dans la deuxième liste, sélectionnez le modificateur que vous voulez utiliser pour la recherche.
   c. Dans la zone de saisie, entrez les informations spécifiques liées à votre paramètre de recherche.
   d. Cliquez sur **Ajouter un filtre**.
   e. Répétez cette procédure pour chaque filtre que vous ajoutez aux critères de recherche.
7. Pour sauvegarder automatiquement les résultats de la recherche lorsqu'elle est terminée, cochez la case **Enregistrer les résultats une fois la recherche terminée**, puis saisissez un nom pour la recherche sauvegardée.

8. Dans le volet Définition de colonne, définissez les colonnes et l'agencement de colonne à utiliser pour afficher les résultats :
   a. Dans la liste **Afficher**, sélectionnez la colonne préconfigurée devant être associée à cette recherche.
   b. Cliquez sur la flèche située en regard de **Définition de vue avancée** afin d'afficher les paramètres de recherche avancée.
   c. Personnalisez les colonnes à afficher dans les résultats de recherche.
   d. Dans la zone **Limite de résultats**, entrez le nombre de lignes devant être renvoyées par la recherche.
9. Cliquez sur **Filtrer**.

Création d'une présentation de colonne personnalisée

Créez une présentation de colonne personnalisée en ajoutant ou en retirant des colonnes dans une présentation existante.

Procédure

1. Sous l'onglet **Activité du journal** ou **Activité réseau**, cliquez sur **Rechercher** > **Editer la recherche**.
2. Dans le volet **Définition de colonne**, sélectionnez une présentation de colonne existante dans la liste **Afficher**.

   Lorsque vous modifiez la présentation, son nom dans la liste **Afficher** devient automatiquement *Personnalisé*.
3. Modifiez le regroupement de recherche.
   a. Pour ajouter une colonne à votre groupe de recherche, sélectionnez une colonne dans la liste **Colonnes disponibles** et cliquez sur la flèche droite afin de déplacer la colonne dans la liste **Grouper par**.
   b. Pour déplacer une colonne de la liste **Colonnes** vers votre groupe de recherche, sélectionnez une colonne de la liste **Colonnes** et faites-la glisser dans la liste **Grouper par**.
   c. Pour retirer une colonne de votre groupe de recherche, sélectionnez la colonne dans la liste **Grouper par** et cliquez sur la flèche gauche.
   d. Pour modifier l'ordre de vos groupes de colonnes, utilisez les flèches haut et bas et faites glisser les colonnes vers l'emplacement souhaité.
4. Modifiez la présentation de colonne.
   a. Pour ajouter une colonne à votre présentation personnalisée, sélectionnez une colonne dans la liste **Colonnes disponibles** et cliquez sur la flèche droite afin de déplacer la colonne vers la liste **Colonnes**.
   b. Pour déplacer une colonne de la liste **Grouper par** vers votre présentation personnalisée, sélectionnez une colonne de la liste **Grouper par** et faites-la glisser vers la liste **Colonnes**.
   c. Pour retirer une colonne de votre présentation personnalisée, sélectionnez la colonne dans la liste **Colonnes** et cliquez sur la flèche gauche.
   d. Pour modifier l'ordre de vos colonnes, utilisez les flèches haut et bas et faites glisser les colonnes vers l'emplacement souhaité.
5. Dans la zone **Nom**, entrez le nom de votre présentation de colonne personnalisé.
6. Cliquez sur **Sauvegarder la présentation**.

Suppression d'une présentation de colonne personnalisée

Vous pouvez supprimer une présentation de colonne existante créée par un utilisateur.

Procédure

1. Sous l'onglet **Activité du journal** ou **Activité réseau**, cliquez sur **Rechercher** > **Editer la recherche**.
2. Dans le volet **Définition de colonne**, sélectionnez une présentation de colonne existante créée par un utilisateur dans la liste **Afficher**.
3. Cliquez sur **Supprimer la présentation**.

Sauvegarde des critères de recherche

Vous pouvez enregistrer les critères de recherche configurés de sorte que vous puissiez réutiliser les critères et utiliser les critères de recherche sauvegardée dans les autres composants, tels que les rapports. Les critères de recherche sauvegardée n'expirent pas.

Pourquoi et quand exécuter cette tâche

Si vous indiquez un intervalle pour votre recherche, le nom de la recherche est accolé à l'intervalle spécifié. Par exemple, une recherche sauvegardée nommée Utilisations par source comprenant un intervalle des 5 dernières minutes devient Utilisations par source - 5 dernières minutes.

Si vous modifiez un ensemble de colonnes dans une recherche sauvegardée précédemment et que vous sauvegardez les critères de recherche sous le même nom, vous perdez les cumuls précédents de graphique de série temporelle.

Procédure

1. Sélectionnez l'une des options suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Effectuez une recherche.
3. Cliquez sur **Sauvegarder les critères**.
4. Saisissez les valeurs de ces paramètres :

Option	Description
Paramètre	Description
Nom de la recherche	Saisissez le nom unique que vous souhaitez affecter à ce critère de recherche.
Affecter la recherche au(x) groupe(s)	Cochez la case du groupe auquel vous souhaitez affecter cette recherche sauvegardée. Si vous ne sélectionnez aucun groupe, cette recherche sauvegardée est affectée par défaut au groupe Autre. Pour plus d'informations, voir Gestion des groupes de recherche.
Gérer les groupes	Cliquez sur **Gérer les groupes** pour gérer des groupes de recherche. Pour plus d'informations, voir Gestion des groupes de recherche.

Option	Description
Options d'intervalle :	Sélectionnez l'une des options suivantes : • **Temps réel (diffusion en flux)** - Sélectionnez cette option pour filtrer vos résultats de recherche en mode de diffusion en flux. • **Dernier intervalle (actualisation automatique)** - Sélectionnez cette option pour filtrer vos résultats de recherche en mode d'actualisation automatique. Les onglets **Activité du journal** et **Activité réseau** s'actualisent toutes les minutes pour afficher les informations les plus récentes. • **Récent** - Sélectionnez cette option puis, dans cette zone de liste, sélectionnez l'intervalle que vous souhaitez filtrer. • **Intervalle spécifique** - Sélectionnez cette option et, à partir de l'agenda, sélectionnez la date et l'intervalle que vous souhaitez filtrer.
Inclure dans mes recherches rapides	Cochez cette case pour inclure cette recherche à votre zone de liste **Recherche rapide** de la barre d'outils.
Inclure dans mon tableau de bord	Cette case vous permet d'inclure les données de vos recherches sauvegardées à l'onglet **Tableau de bord**. Pour plus d'informations sur l'onglet **Tableau de bord**, voir Gestion du tableau de bord. **Remarque :** Ce paramètre ne s'affiche que si la recherche est regroupée.
Définir par défaut	Cochez cette case pour définir cette recherche comme votre recherche par défaut.
Partager avec tout le monde	Cochez cette case pour partager ces exigences de recherche avec tous les autres utilisateurs.

5. Cliquez sur **OK**.

Recherche planifiée

Cette option vous permet de planifier une recherche et d'afficher les résultats.

Vous pouvez planifier une recherche qui s'exécute à un moment précis du jour ou de la nuit.

Exemple :
Si vous planifiez une recherche qui doit s'exécuter dans la nuit, vous pouvez l'étudier le matin. Contrairement aux rapports, vous avez la possibilité de regrouper les résultats de recherche et d'effectuer des investigations supplémentaires. Vous pouvez effectuer des recherches sur le nombre d'échecs de connexion dans votre groupe réseau. Si le résultat est généralement 10 et que le résultat de la recherche est 100, vous pouvez regrouper les résultats de la recherche pour simplifier les investigations. Pour voir quel est l'utilisateur qui à le plus d'échecs de connexion, vous pouvez regrouper par nom d'utilisateur. Vous pouvez ensuite approfondir la recherche.

Vous pouvez planifier une recherche sur des événements ou des flux à partir de l'onglet **Rapports** . Vous devez sélectionner un ensemble de critères de recherche précédemment enregistrés.

1. Création d'un rapport

   Indiquez les informations suivantes dans la fenêtre **Assistant Création de rapports** :

   - Le type de diagramme est Evénements/journaux ou Flux.
   - Le rapport est basé sur une recherche sauvegardée.
   - Génération d'une infraction.

     Vous pouvez choisir l'option permettant de **créer une infraction** ou d'**ajouter un résultat à une infraction existante**.

     Vous pouvez également générer une recherche manuelle.
2. Affichage des résultats de la recherche

Vous pouvez afficher les résultats de votre recherche planifiée depuis l'onglet **Infractions**.

- Les infractions de recherche planifiée sont identifiées par la colonne **Type d'infraction**.

  Si vous créez une infraction, elle est générée à chaque exécution du rapport. Si vous ajoutez le résultat de la recherche sauvegardée à une infraction existante, une infraction est créée à la première exécution du rapport. Les exécutions de rapports suivantes s'ajoutent à cette infraction. Si aucun résultat n'est renvoyé, le système n'ajoute ni ne crée aucune infraction.
- Pour afficher les résultats de la recherche la plus récente dans la fenêtre Récapitulatif des infractions, cliquez deux fois sur une infraction de recherche planifiée dans la liste des infractions. Pour afficher la liste de toutes les exécutions de recherche planifiées, cliquez sur **Résultats de la recherche** dans le panneau **5 derniers résultats de recherche**.

Vous pouvez affecter une infraction de recherche planifiée à un utilisateur.

Tâches associées:

«Création d'une recherche personnalisée», à la page 141
Vous pouvez chercher des données correspondant à vos critères en utilisant des options de rechercher plus spécifiques. Par exemple, vous pouvez spécifier des colonnes pour votre recherche, que vous pouvez regrouper et réorganiser pour consulter plus efficacement vos résultats de la recherche.

«Affectation d'infractions aux utilisateurs», à la page 52
Par défaut, toutes les nouvelles infractions ne pas affectées. Vous pouvez affecter une infraction à un utilisateur IBM Security QRadar à des fins d'investigation.

Options de recherches avancées

Utilisez la zone **Recherche avancée** pour entrer une requête AQL (Ariel Query Language) spécifiant les zones souhaitées et comment vous voulez les regrouper pour lancer une requête.

Remarque : Lorsque vous saisissez une requête AQL, utilisez des guillemets simples pour une comparaison de chaînes, et des guillemets pour une comparaison de valeur de propriété.

La zone **Recherche avancée** offre une fonction de remplissage automatique et de mise en évidence de syntaxe

Utilisez la fonction de remplissage automatique et de mise en évidence de syntaxe pour aider à créer des requêtes. Pour connaître les navigateurs Web pris en charge, voir «Navigateurs Web pris en charge», à la page 4

Remarque : Si vous utilisez un filtre rapide sur l'onglet **Activité du journal**, vous devez actualiser votre fenêtre de navigation avant d'exécuter une recherche avancée.

Accès à la recherche avancée

Accédez à l'option **Recherche avancée** à partir de la barre d'outils **Recherche** située sur les onglets **Activité réseau** et **Activité du journal** pour entrer une requête AQL.

Sélectionnez **Recherche avancée** dans la zone de liste de la barre d'outils **Recherche**.

Développez la zone **Recherche avancée** comme suit :

1. Faites glisser l'icône Développer située à droite de la zone.
2. Appuyez sur Maj + Entrée pour passer à la ligne suivante.
3. Appuyez sur Entrée.

Vous pouvez cliquer sur une valeur du résultat de la recherche avec le bouton droit de la souris et appliquer un filtre sur cette valeur.

Double-cliquez sur n'importe quelle ligne du résultat de la recherche pour afficher plus de détails.

Toutes les recherches, y compris les recherches AQL sont incluses dans le journal d'audit.

Exemples de chaînes de recherche AQL

Le tableau suivant fournit des exemples de chaînes de recherche AQL.

Tableau 34. Exemples de chaînes de recherche AQL

Description	Exemple

Sélection des colonnes par défaut des événements.
 	
Sélection des colonnes par défaut des flux.
	`SELECT * FROM events`
	
	`SELECT * FROM flows`

Sélection de colonnes spécifiques.	`SELECT sourceip, destinationip FROM events`
Sélection de colonnes spécifiques et filtrage des résultats.	`SELECT sourceip, destinationip FROM events ORDER BY destinationip`
Exécution d'une requête de recherche agrégée.	`SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip`
Exécution d'un appel de fonction dans une clause SELECT.	`SELECT CATEGORYNAME(category) AS namedCategory FROM events`
Filtrage des résultats de recherche à l'aide d'une clause WHERE.	`SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1`

Tableau 34. Exemples de chaînes de recherche AQL (suite)

Description	Exemple
Recherche d'événements ayant déclenché une règle spécifique à partir du nom de règle ou d'un texte partiel du nom de règle.	`SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'`
Référencement des noms de zones contenant des caractères spéciaux, tels que des caractères arithmétiques ou des espaces, en plaçant le nom de la zone entre guillemets.	`SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'`

Le tableau suivant fournit des exemples de chaînes de recherche AQL pour X-Force.

Tableau 35. Exemples de chaînes de recherche AQL pour X-Force

Description	Exemple
Comparer une adresse IP à une catégorie X-Force avec une valeur de confiance.	`select * from events where XFORCE_IP_CONFIDENCE('Spam',sourceip)>3`
Rechercher les catégories d'URL X-Force associées à une URL.	`select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL`
Extraire les catégories IP X-Force qui sont associées à une adresse IP.	`select sourceip, XFORCE_IP_CATEGORY(sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL`

Pour en savoir plus sur les fonctions, les zones et les opérateurs de recherche, reportez-vous au *Guide du langage de requête Ariel*.

Exemples de chaînes de recherche AQL

Utilisez le langage AQL (Ariel Query Language) pour extraire des zones spécifiques des événements, flux et tables simarc dans la base de données Ariel.

Remarque : Lors de la création d'une requête AQL, si vous copiez du texte provenant d'un document et contenant des apostrophes et que vous le collez dans IBM Security QRadar, votre requête ne sera pas analysée. Pour remédier à cette situation, vous pouvez coller le texte dans QRadar et entrer à nouveau les apostrophes ou vous pouvez copier et coller le texte à partir d'IBM Knowledge Center.

Génération de rapports sur l'utilisation d'un compte

Les différentes communautés d'utilisateurs peuvent avoir des indicateurs de menace et d'utilisation différents.

Utilisez les données de référence pour générer des rapports sur plusieurs propriétés utilisateurs, par exemple le nom du département, l'emplacement ou le chef. Vous pouvez utiliser des données de référence externes.

La requête suivante renvoie des informations de métadonnées sur l'utilisateur à partir de ses événements de connexion.

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
```

```
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

Connaissance de plusieurs identificateurs de comptes

Dans cet exemple, les utilisateurs individuels ont plusieurs comptes dans le réseau. L'organisation a besoin d'obtenir une vue unique des activités de l'utilisateur.

Utilisez les données de référence pour mapper les ID utilisateurs locaux à un ID global.

La requête suivante renvoie les comptes utilisateurs utilisés par un ID global sur des événements signalés comme suspects.

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

La requête suivante montre les activités réalisées par un ID global.

```
SELECT
QIDNAME(qid) as 'Event name',
starttime as 'Time',
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event Username',
REFERENCEMAP('GlobalID_Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

Identification d'un balisage de longue durée suspect

De nombreuses menaces utilisent des commandes et des contrôles pour communiquer de façon régulière, durant plusieurs jours, plusieurs semaines et plusieurs mois.

Les recherches avancées peuvent identifier les modèles de connexion au fil du temps. Par exemple, vous pouvez analyser les connexions cohérentes, courtes, de faible volume, le nombre de connexions par jour/mois/an entre les adresses IP ou une adresse IP et un emplacement géographique.

La requête suivante détecte les instances potentielles d'un balisage s'effectuant toutes les heures.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'HH')) as 'different hours',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection = 'L2R'
GROUP BY sourceip, destinationip
HAVING "different hours" > 20
AND "total flows" < 25
LAST 24 hours
```

Conseil : Vous pouvez modifier cette requête pour travailler sur des journaux de proxy ou autres types d'événements.

La requête suivante détecte des instances potentielles de balisage quotidien.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'dd'))as 'different days',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection='L2R'
GROUP BY sourceip, destinationip
HAVING "different days" > 4
AND "total flows" < 14
LAST 7 days
```

La requête suivante détecte un balisage quotidien entre un IP de source et un IP de destination. Les horaires de balisage varient tous les jours. L'intervalle de temps séparant deux balisages est court.

```
SELECT
sourceip,
LONG(DATEFORMAT(starttime,'hh')) as hourofday,
(AVG( hourofday*hourofday) - (AVG(hourofday)^2))as variance,
COUNT(*) as 'total flows'
FROM flows
GROUP BY sourceip, destinationip
HAVING variance < 01 and "total flows" < 10
LAST 7 days
```

La requête suivante détecte un balisage quotidien vers un domaine à l'aide d'événements de journaux de proxy. Les horaires de balisage varient tous les jours. L'intervalle de temps séparant deux balisages est court.

```
SELECT sourceip,
LONG(DATEFORMAT(starttime,'hh')) as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and "total events" < 10
LAST 7 days
```

La propriété **url_domain** est une propriété personnalisée des journaux de proxy.

Intelligence de menace externe

Les données d'utilisation et de sécurité en corrélation avec des données d'intelligence de menace externe peuvent fournir des indicateurs de menace importants.

Des recherches avancées peuvent croiser des indicateurs d'intelligence de menace externe avec d'autres événements de sécurité et données d'utilisation.

Cette requête montre comment vous pouvez analyser des données de menace externe durant plusieurs jours, plusieurs semaines ou plusieurs mois afin d'identifier le niveau de risque des actifs et des comptes et de définir des priorités.

```
Select
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
```

```
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

Intelligence des actifs et configuration

Les indicateurs de menace et d'utilisation varient en fonction du type d'accès, du système d'exploitation, de la posture de vulnérabilité, du type de serveur, de la classification et d'autres paramètres.

Dans cette requête, les recherches avancées et le modèle d'actif offrent une connaissance opérationnelle d'un emplacement.

La fonction **Assetproperty** extrait les valeurs de propriétés des actifs et vous permet d'inclure les données d'actif dans les résultats.

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

La requête suivante vous montre comment vous pouvez utiliser les recherches avancées et le suivi de l'identité des utilisateurs dans le modèle d'actif.

La fonction **AssetUser** extrait le nom d'utilisateur de la base de données des actifs.

```
SELECT
APPLICATIONNAME(applicationid) as App,
ASSETUSER(sourceip, now()) as srcAssetUser,
COUNT(*) as 'Total Flows'
FROM flows
WHERE srcAssetUser IS NOT NULL
GROUP BY App, srcAssetUser
ORDER BY "Total Flows" DESC
LAST 3 HOURS
```

Fonction de recherche réseau

Vous pouvez utiliser la fonction de recherche réseau **Network LOOKUP** pour extraire le nom de réseau associé à une adresse IP.

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

Fonction de recherche de règle

Vous pouvez utiliser la fonction de recherche de règle **Rule LOOKUP** pour extraire le nom d'une règle à l'aide de son ID.

```
SELECT RULENAME(123) FROM events
```

La requête suivante renvoie les événements ayant déclenché un nom de règle spécifique.

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

Recherche en texte intégral (Full TEXT SEARCH)

Vous pouvez utiliser l'opérateur TEXT SEARCH pour faire des recherches en texte intégral en utilisant l'option **Recherche avancée**.

Dans cet exemple, il existe un certain nombre d'événements qui contiennent le terme "firewall" dans le contenu. Vous pouvez rechercher ces événements en utilisant l'option **Filtre rapide** et l'option **Recherche avancée** de l'onglet **Activité du journal**.

- Pour utiliser l'option **Filtre rapide**, entrez le texte suivant dans la case **Filtre rapide** : `'firewall'`
- Pour utiliser l'option **Recherche avancée**, entrez la requête suivante dans la case **Recherche avancée** :

```
SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
```

Propriété personnalisée

Vous pouvez accéder aux propriétés personnalisées pour les événements et les flux lorsque vous utilisez l'option **Recherche avancée**.

La requête suivante utilise la propriété personnalisée "MyWebsiteUrl" pour trier les événements par une URL Web :

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

Tâches associées:

«Création d'une propriété personnalisée basée sur une expression régulière», à la page 182
Vous pouvez créer une propriété personnalisée basée sur une expression régulière afin que les contenus d'événements ou de flux correspondent à une expression régulière.

Options de recherche du filtrage rapide

Vous pouvez rechercher vos contenus d'événements et de flux en tapant une chaîne de recherche de texte utilisant des mots ou des phrases simples.

Le filtrage rapide est l'une des méthodes les plus rapides qui existe pour rechercher des contenus d'événements ou de flux pour des données spécifiques. Par exemple, vous pouvez utiliser le filtrage rapide pour rechercher les types d'informations suivants :

- Chaque périphérique pare-feu assigné à une plage d'adresses spécifique au cours de la dernière semaine
- Une série de fichiers PDF envoyés par un compte Gmail au cours des 5 derniers jours
- Tous les enregistrements effectués sur une période de deux mois qui correspondent exactement à un nom d'utilisateur séparé par des tirets
- Une liste des adresses de sites qui se terminent par .ca

Vous pouvez filtrer vos recherches à partir des emplacements suivants :

A partir de la barre d'outils Activité du journal et des barres d'outils Activités réseau Sélectionnez **Filtrage rapide** dans la zone de liste de la barre d'outils **Recherche** pour entrer une chaîne de recherche de texte. Cliquez sur l'icône **Filtrage rapide** pour appliquer votre **Filtrage rapide** à la liste des événements ou des flux.

A partir de la boîte de dialogue Ajouter un filtre

Cliquez sur l'icône **Ajouter un filtre** de l'onglet **Activité du journal** ou **Activité réseau**.

Sélectionnez **Filtrage rapide** en tant que paramètre de filtre et entrez une chaîne de recherche de texte.

A partir des pages Recherche de flux

Ajoutez un filtrage rapide à votre liste de filtres.

Lorsque vous affichez des **flux** en temps réel (diffusion en flux) ou en mode dernier intervalle, vous pouvez taper uniquement des mots ou des phrases simples dans la zone **Filtrage rapide**. Lorsque vous affichez des **événements** ou des **flux** avec un intervalle, suivez les instructions de syntaxe suivantes :

Tableau 36. Instructions relatives à la syntaxe du filtrage rapide

Description	Exemple
Inclure un texte en clair de tout type que vous souhaitez trouver dans le contenu.	`Pare-feu`
Rechercher des phrases exactes en incluant plusieurs termes entre guillemets.	`"Refus de pare-feu"`
Inclure un ou plusieurs caractères génériques. Le terme de recherche ne peut pas commencer par un caractère générique.	`P?re-feu` ou `P??e-f*`
Regrouper des termes avec des expressions logiques, telles que AND, OR et NOT. Pour être reconnues comme expressions logiques et non comme termes de recherche, la syntaxe et les opérateurs doivent apparaître en majuscules.	`(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`
Lorsque vous créez un critère de recherche incluant l'expression logique NOT, vous devez inclure au moins un autre type d'expression logique, sinon aucun résultat ne sera renvoyé.	`(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
Les caractères suivants doivent être précédés d'une barre oblique inversée afin d'indiquer que le caractère fait partie de votre terme de recherche : `+ - && || ! () {} [] ^ " ~ * ? : \.`	`"%PIX\-5\-304001"`

Limitations

Les recherches à filtrage rapide s'effectuent sur les données de journal des événements et des flux bruts et ne font pas de distinction entre les zones. Par exemple, les recherches à filtrage rapide renvoient des correspondances à la fois pour une adresse IP source et une adresse IP de destination, à moins que des termes permettant d'affiner les résultats soient entrés.

Les termes de recherche sont mis en correspondance dans l'ordre à partir du premier caractère du mot ou phrase du contenu. Le terme de recherche `user` correspond à `user_1` et `user_2` mais ne correspond pas aux phrases suivantes : `ruser`, `myuser` ou `anyuser`.

Les recherches de filtre rapide utilisent l'environnement local anglais. *Environnement local* est le paramètre qui identifie une langue ou une zone

géographique et détermine les conventions de format telles que le classement, la conversion de casse, la classification des caractères, la langue des messages, la représentation de la date et de l'heure, et la représentation numérique.

L'environnement local est défini par votre système d'exploitation. Vous pouvez configurer QRadar pour remplacer le paramètre d'environnement local du système d'exploitation. Par exemple, vous pouvez définir l'environnement local sur **English** et QRadar Console sur **Italiano (Italien)**.

Si vous utilisez des caractères Unicode dans votre requête de recherche à filtrage rapide, des résultats de recherches inattendus peuvent être renvoyés.

Si vous sélectionnez un environnement local qui n'est pas l'anglais, vous pouvez utiliser l'option de recherche avancée dans QRadar pour la recherche d'événement et les données de charge.

Comment fonctionnent les recherches à filtrage rapide et les jetons de contenus ?

Le texte inclus dans le contenu est constitué de mots, de phrases, de symboles et d'autres éléments. Ces jetons sont délimités par des espaces et des signes de ponctuation. Les jetons ne correspondent pas toujours au termes de recherche spécifiés par l'utilisateur, et par conséquent que certains termes ne sont pas trouvés lorsqu'ils ne correspondent pas au jeton généré. Les caractères délimiteurs sont ignorés mais des exceptions existent, par exemple :

- Les points non suivis d'un blanc sont inclus comme faisant partie du jeton.

  Par exemple, `1.2.3.4:56` est segmenté comme jeton d'hôte `1.2.3.4` et comme jeton de port `56`.
- Les mots sont divisés en cas de traits d'union, à moins que le mot contienne un nombre, auquel cas le jeton n'est pas divisé et les nombres et traits d'union sont conservés comme un seul jeton.
- Les noms de domaines Internet et les adresses de courrier électronique sont conservés comme un seul jeton.

  `1.2.3.4/home/www` est segmenté comme un seul jeton et l'URL n'est pas séparée.

  `1.2.3.7:/calling1/www2/scp4/path5/fff` est segmenté comme hôte `1.2.3.7` et la suite forme un seul et même jeton `/calling1/www2/scp4/path5/fff`

Les noms de fichiers et d'URL contenant plusieurs traits de soulignement sont divisé avant un point (.).

Exemple de plusieurs traits de soulignement dans un nom de fichier :

Si vous utilisez `hurricane_katrina_ladm118.jpg` comme terme de recherche, le terme sera divisé en deux jetons :

- `hurricane`
- `katrina_ladm118.jpg`

Recherchez le contenu du terme de recherche complet en plaçant des guillemets doubles avant et après le terme de recherche : `"hurricane_katrina_ladm118.jpg"`

Exemple de traits de soulignement multiples dans un chemin d'accès à un fichier relatif :

thumb.ladm1180830/thumb.ladm11808301806.hurricane_katrina_ladm118.jpg est divisé en deux jetons :

- thumb.ladm1180830/thumb.ladm11808301806.hurricane
- katrina_ladm118.jpg

Pour rechercher hurricane_katrina_ladm118.jpg, qui se compose d'un jeton partiel et d'un jeton complet, placez un astérisque avant le terme de recherche : *hurricane_katrina_ladm118.jpg

Concepts associés:

Chapitre 9, «Recherches», à la page 141
Utilisez les options de recherche et d'indexation de IBM Security QRadar pour améliorer les performances de recherche et renvoyer des résultats plus rapides. Pour trouver des critères spécifiques, les recherches avancées utilisent les chaînes de recherche AQL.

Recherches d'infractions

Vous pouvez rechercher des infractions au moyen de critères spécifiques pour afficher des infractions qui correspondent à des critères de recherche dans une liste de résultats.

Vous pouvez créer ou charger un ensemble de critères de recherche précédemment enregistrés.

Recherche d'infractions dans les pages Mes Infractions et Toutes les infractions

Dans les pages Mes Infractions et Toutes les infractions de l'onglet **Infraction**, vous pouvez rechercher les infractions correspondant à vos critères.

Pourquoi et quand exécuter cette tâche

Le tableau suivant décrit les options de recherche que vous pouvez utiliser pour rechercher les données relatives aux infractions sur les pages **Mes Infractions** et **Toutes les infractions**.

Pour obtenir des informations sur les catégories, consultez le *IBM Security QRadar Administration Guide*.

Tableau 37. Options de recherche des pages Mes Infractions et Toutes les infractions

Options	Description
Groupe	Cette zone de liste vous permet de sélectionner un groupe de recherche d'infractions pour l'afficher dans la liste **Recherches sauvegardées disponibles**.
Saisir une recherche sauvegardée ou effectuer votre sélection dans la liste	Cette zone vous permet de saisir le nom d'une recherche sauvegardée ou d'un mot-clé pour filtrer la liste **Recherches sauvegardées disponibles**.

Tableau 37. Options de recherche des pages Mes Infractions et Toutes les infractions (suite)

Options	Description
Recherches sauvegardées disponibles	Cette liste affiche toutes les recherches disponibles, sauf si vous lui appliquez un filtre en utilisant les options Groupe ou Saisir une recherche sauvegardée ou effectuer votre sélection dans la liste. Vous pouvez sélectionner une recherche sauvegardée sur cette liste à afficher ou éditer.
Toutes les infractions	Cette option vous permet de rechercher toutes les infractions sans tenir compte de l'intervalle.
Récent	Cette option vous permet de sélectionner un intervalle prédéfini pour votre filtre. Une fois que vous avez choisi cette option, vous devez sélectionner l'un des intervalles dans la zone de liste.
Intervalle spécifique	Cette option vous permet de configurer un intervalle personnalisé pour votre recherche. Une fois que vous avez choisi cette option, vous devez sélectionner l'une des options suivantes. • **Date de début entre** - Cochez cette case pour rechercher des infractions qui ont commencé pendant une période définie. Une fois que vous avez coché cette case, utilisez les zones de liste pour sélectionner les dates que vous souhaitez rechercher. • **Dernier événement/flux entre** - Cochez cette case pour rechercher des infractions dont le dernier événement détecté s'est déroulé dans une période définie. Une fois que vous avez coché cette case, utilisez les zones de liste pour sélectionner les dates que vous souhaitez rechercher.
Rechercher	L'icône **Rechercher** est disponible dans plusieurs volets de la page de recherche. Vous pouvez cliquer sur **Rechercher** lorsque vous avez terminé de configurer la recherche et que vous souhaitez afficher les résultats.
ID d'infraction	Dans cette zone, vous pouvez saisir l'ID de l'infraction que vous souhaitez rechercher.
Description	Dans cette zone, vous pouvez saisir la description que vous souhaitez rechercher.
Affecté à l'utilisateur	Dans cette zone de liste, vous pouvez sélectionner le nom d'utilisateur que vous souhaitez rechercher.

Tableau 37. Options de recherche des pages Mes Infractions et Toutes les infractions (suite)

Options	Description
Direction	Dans cette zone de liste, vous pouvez sélectionner le sens de l'infraction que vous souhaitez rechercher. Les options incluent : • Local à local • Local à distant • Distant à local • Distant à distant • Local à distant ou local • Distant à distant ou local
IP Source	Dans cette zone, vous pouvez saisir l'adresse IP source ou la plage CIDR que vous souhaitez rechercher.
IP de destination	Dans cette zone, vous pouvez saisir l'adresse IP de destination ou la plage CIDR que vous souhaitez rechercher.
Magnitude	Dans cette zone de liste, vous pouvez spécifier une amplitude, puis choisir d'afficher uniquement les infractions dont l'amplitude est égale, inférieure ou supérieure à la valeur configurée. L'intervalle est compris entre 0 et 10.
Gravité	Dans cette zone de liste, vous pouvez indiquer une gravité puis choisir de n'afficher que les infractions dont la gravité est égale, inférieure ou supérieure à la valeur configurée. L'intervalle est compris entre 0 et 10.
Crédibilité	Dans cette zone de liste, vous pouvez indiquer une crédibilité et choisir de n'afficher que les infractions dont la crédibilité est égale, inférieure ou supérieure à la valeur configurée. L'intervalle est compris entre 0 et 10.
Pertinence	Dans cette zone de liste, vous pouvez indiquer une pertinence et choisir de n'afficher que les infractions qui sont égales, inférieures ou supérieures à la valeur configurée. L'intervalle est compris entre 0 et 10.
Contient le nom d'utilisateur	Dans cette zone, vous pouvez saisir une expression régulière (regex) pour rechercher les infractions contenant un nom d'utilisateur spécifique. Lorsque vous définissez des modèles d'expression régulière personnalisés, vous devez accepter les règles d'expression régulière telles que définies par le langage de programmation Java™. Pour plus d'informations, vous pouvez vous référer aux tutoriels d'expressions régulières disponibles sur le Web.

Tableau 37. Options de recherche des pages Mes Infractions et Toutes les infractions (suite)

Options	Description
Réseau source	Dans cette zone de liste, vous pouvez sélectionner le réseau source que vous souhaitez rechercher.
Réseau de destination	Dans cette zone de liste, vous pouvez sélectionner le réseau de destination que vous souhaitez rechercher.
Catégorie de niveau supérieur	Dans cette zone de liste, vous pouvez sélectionner la catégorie de niveau supérieur que vous souhaitez rechercher .
Catégorie de niveau inférieur	Dans cette zone de liste, vous pouvez sélectionner la catégorie de niveau inférieur que vous souhaitez rechercher.
Exclure	Les options de ce volet vous permettent d'exclure des infractions des résultats de la recherche. Ces options incluent : • Infractions actives • Infractions masquées • Infractions fermées • Infractions inactives • Infractions protégées
Fermé par l'utilisateur	Ce paramètre ne s'affiche que lorsque la case **Infractions fermées** n'est pas cochée dans le volet Exclure. Dans cette zone de liste, vous pouvez sélectionner le nom d'utilisateur pour lequel vous souhaitez rechercher les infractions clôturées ou sélectionner Any pour afficher toutes les infractions clôturées.
Motif de la fermeture	Ce paramètre ne s'affiche que lorsque la case **Infractions fermées** n'est pas cochée dans le volet Exclure. Dans cette zone de liste, vous pouvez sélectionner une raison pour laquelle vous souhaitez rechercher des infractions clôturées ou sélectionner **All** pour afficher toutes les infractions clôturées.
Evénements	Dans cette zone de liste, vous pouvez indiquer un nombre d'événements et choisir de n'afficher que les infractions dont le nombre d'événements est égal, inférieur ou supérieur à la valeur configurée.
Flux	Dans cette zone de liste, vous pouvez indiquer un nombre de flux puis choisir d'afficher uniquement les infractions dont le nombre de flux est égal, inférieur ou supérieur à la valeur configurée.

Tableau 37. Options de recherche des pages Mes Infractions et Toutes les infractions (suite)

Options	Description
Evénements/flux totaux	Dans cette zone de liste, vous pouvez indiquer un nombre total d'événements et de flux puis choisir de n'afficher que les infractions dont le nombre total d'événements et de flux est égal, inférieur ou supérieur à la valeur configurée.
Destinations	Dans cette zone de liste, vous pouvez indiquer un nombre d'adresses IP de destination puis choisir d'afficher uniquement les infractions dont le nombre d'adresses IP de destination est égal, inférieur ou supérieur à la valeur configurée.
Groupe de source de journal	Dans cette zone de liste, vous pouvez sélectionner un groupe de sources de journal contenant la source de journal que vous souhaitez rechercher. La zone de liste **Source de journal** affiche toutes les sources de journal affectées au groupe de sources de journal sélectionné.
Source de journal	Dans cette zone de liste, vous pouvez sélectionner la source de journal que vous souhaitez rechercher.
Groupe de règles	Dans cette zone de liste, vous pouvez sélectionner un groupe de règles contenant la règle de contribution que vous souhaitez rechercher. La zone de liste **Règle** affiche toutes les règles affectées au groupe de règles sélectionné.
Règle	Dans cette zone de liste, vous pouvez sélectionner la règle de contribution que vous souhaitez rechercher.
Type d'infraction	Dans cette zone de liste, vous pouvez sélectionner un type d'infraction que vous souhaitez rechercher. Pour plus d'informations sur les options de la zone de liste **Type d'infraction**, voir le Tableau 2.

Le tableau suivant décrit les options disponibles dans la zone de liste **Type d'infraction** :

Tableau 38. Options de type d'infraction

Type d'infraction	Description
Tout	Cette option recherche toutes les sources d'infraction.
IP Source	Pour rechercher des infractions avec une adresse IP source spécifique, vous pouvez sélectionner cette option, puis saisir l'adresse IP source que souhaitez rechercher.

Tableau 38. Options de type d'infraction (suite)

Type d'infraction	Description
IP de destination	Pour rechercher des infractions avec une adresse IP de destination spécifique, vous pouvez sélectionner cette option, puis saisir l'adresse IP de destination que vous souhaitez rechercher.
Nom d'événement	Pour rechercher des infractions avec un nom d'événement spécifique, vous pouvez cliquer sur l'icône **Parcourir** pour ouvrir le navigateur d'événement et sélectionner le nom de l'événement (QID) que vous souhaitez rechercher. Vous pouvez rechercher un QID particulier à l'aide de l'une des options suivantes : • Pour rechercher un QID par catégorie, cochez la case **Parcourir par catégorie** et sélectionnez la catégorie de niveau supérieur ou inférieur dans les zones de liste. • Pour rechercher un QID par type de source de journal, cochez la case **Parcourir par Type de source de journal** et sélectionnez un type de source de journal dans la zone de liste **Type de la source de journal**. • Pour rechercher un QID par type de source de journal, cochez la case **Parcourir par Type de source de journal** et sélectionnez un type de source de journal dans la zone de liste **Type de la source de journal**. • Pour rechercher un QID par nom, cochez la case **Recherche de QID** et saisissez un nom dans la zone **QID/Nom**.
Nom d'utilisateur	Pour rechercher des infractions avec un nom d'utilisateur spécifique, vous pouvez sélectionner cette option puis saisir le nom d'utilisateur que vous souhaitez rechercher.
Adresse MAC source	Pour rechercher des infractions avec une adresse MAC source spécifique, vous pouvez sélectionner cette option puis saisir l'adresse MAC source que vous souhaitez rechercher.
Adresse MAC de destination	Pour rechercher des infractions avec une adresse MAC de destination spécifique, vous pouvez sélectionner cette option puis saisir l'adresse MAC de destination que vous souhaitez rechercher.

Tableau 38. Options de type d'infraction (suite)

Type d'infraction	Description
Source de journal	Dans la zone de liste **Groupe de source de journal**, vous pouvez sélectionner le groupe de sources de journal contenant la source de journal que vous souhaitez rechercher. La zone de liste **Source de journal** affiche toutes les sources de journal affectées au groupe de sources de journal sélectionné. Dans la zone de liste **Source de journal**, vous pouvez sélectionner la source de journal que vous souhaitez rechercher.
Nom d'hôte	Pour rechercher des infractions avec un nom d'hôte spécifique, vous pouvez sélectionner cette option puis saisir le nom d'hôte que vous souhaitez rechercher.
Port source	Pour rechercher les infractions avec un port source spécifique, vous pouvez sélectionner cette option puis saisir le port source que vous souhaitez rechercher.
Port de destination	Pour rechercher des infractions avec un port de destination spécifique, vous pouvez sélectionner cette option puis saisir le port de destination que vous souhaiter rechercher.
IPv6 source	Pour rechercher des infractions avec une adresse IPv6 source spécifique, vous pouvez sélectionner cette option et saisir l'adresse IPv6 source que vous souhaitez rechercher.
IPv6 de destination	Pour rechercher des infractions avec une adresse IPv6 de destination spécifique, vous pouvez sélectionner cette option puis saisir l'adresse IPv6 de destination que vous souhaitez rechercher.
ASN source	Pour rechercher des infractions avec un avis préalable d'expédition source spécifique, vous pouvez sélectionner ce dernier dans la zone de liste **ASN source**.
ASN de destination	Pour rechercher des infractions avec un ASN de destination spécifique, vous pouvez sélectionner celui-ci dans la zone de liste **ASN de destination**.
Règle	Pour rechercher des infractions associées à une règle spécifique, vous pouvez sélectionner le groupe de règles contenant la règle que vous souhaitez rechercher dans la zone de liste **Groupe de règles**. La zone de liste **Groupe de règles** affiche toutes les règles affectées au groupe de règles sélectionné. Dans la zone de liste **Règle**, vous pouvez sélectionner la règle que vous souhaitez rechercher.

Tableau 38. Options de type d'infraction (suite)

Type d'infraction	Description
ID application	Pour rechercher des infractions avec un ID d'application, vous pouvez sélectionner l'ID d'application dans la zone de liste **ID application**.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Dans la zone de liste **Rechercher**, sélectionnez **Nouvelle recherche**.
3. Sélectionnez l'une des options suivantes :
   - Pour charger une recherche sauvegardée précédemment, passez à l'étape 4.
   - Pour créer une nouvelle recherche, passez à l'étape 7.
4. Sélectionnez une recherche sauvegardée précédemment à l'aide de l'une des options suivantes :
   - Dans la liste **Recherches sauvegardées disponibles**, sélectionnez la recherche sauvegardée que vous souhaitez charger.
   - Dans la zone **Saisir une recherche sauvegardée** ou **effectuer votre sélection dans la liste**, saisissez le nom de la recherche que vous voulez charger.
5. Cliquez sur **Charger**.
6. Facultatif. Cochez la case **Définir par défaut** dans le volet Editer la recherche pour définir cette recherche comme votre recherche par défaut. Si vous définissez cette recherche comme la recherche par défaut, la recherche s'effectue automatiquement et affiche des résultats à chaque fois que vous accédez à l'onglet **Infractions**.
7. Dans le volet Intervalle, sélectionnez une option pour l'intervalle que vous souhaitez capturer pour cette recherche. Voir le Tableau 1.
8. Dans le volet Paramètres de recherche, définissez les critères de recherche spécifiques. Voir le Tableau 1.
9. Sur le panneau Source d'infraction, indiquez le type d'infraction et la source d'infraction que vous souhaitez rechercher :
   a. Dans la zone de liste, sélectionnez le type d'infraction que vous souhaitez rechercher.
   b. Saisissez vos paramètres de recherche. Voir le Tableau 2.
10. Dans le volet Définition de colonne, définissez l'ordre dans lequel vous souhaitez trier les résultats :
    a. Dans la première zone de liste, sélectionnez la colonne dans laquelle vous souhaitez trier les résultats de la recherche.
    b. Dans la deuxième zone de liste, sélectionnez l'ordre dans lequel vous souhaitez afficher les résultats de recherche. Les options comprennent Ordre décroissant et Ordre croissant.
11. Cliquez sur **Rechercher**.

Que faire ensuite

Sauvegarde des critères de recherche sur l'onglet Infraction

Recherche d'infractions dans la page Par adresse IP source

Cette rubrique présente la procédure permettant de rechercher des infractions sur la page **Par adresse IP source** de l'onglet **Infraction**.

Pourquoi et quand exécuter cette tâche

Le tableau suivant décrit les options de recherche que vous pouvez utiliser pour rechercher des infractions sur la page Par adresse IP source :

Tableau 39. Options de recherche de la page Par adresse IP source

Options	Description
Toutes les infractions	Vous pouvez sélectionner cette option pour rechercher toutes les adresses IP source sans tenir compte de l'intervalle.
Récent	Vous pouvez sélectionner cette option et, dans cette zone de liste, sélectionner l'intervalle que vous souhaitez rechercher.
Intervalle spécifique	Pour indiquer un intervalle à rechercher, vous pouvez sélectionner cette option, puis l'une des options suivantes : • **Date de début entre** - Cochez cette case pour rechercher des adresses IP source associées à des infractions qui ont commencé pendant une période définie. Une fois que vous avez coché cette case, utilisez les zones de liste pour sélectionner les dates que vous souhaitez rechercher. • **Dernier événement/flux entre** - Cochez cette case pour rechercher les adresses IP source associées à des infractions dont le dernier événement détecté s'est déroulé dans une période définie. Une fois que vous avez coché cette case, utilisez les zones de liste pour sélectionner les dates que vous souhaitez rechercher.
Rechercher	L'icône **Rechercher** est disponible dans plusieurs volets de la page de recherche. Vous pouvez cliquer sur **Rechercher** lorsque vous avez terminé de configurer la recherche et que vous souhaitez afficher les résultats.
IP source	Dans cette zone, vous pouvez saisir l'adresse IP source ou la plage CIDR que vous souhaitez rechercher.
Magnitude	Dans cette zone de liste, vous pouvez indiquer une amplitude et choisir de n'afficher que les infractions dont l'amplitude est égale, inférieure ou supérieure à la valeur configurée. L'intervalle est compris entre 0 et 10.
Risque de l'analyse des vulnérabilités	Dans cette zone de liste, vous pouvez indiquer un risque VA et choisir de n'afficher que les infractions dont le risque VA est égal, inférieur ou supérieur à la valeur configurée. L'intervalle est compris entre 0 et 10.

Tableau 39. Options de recherche de la page Par adresse IP source (suite)

Options	Description
Evénements/Flux	Dans cette zone de liste, vous pouvez indiquer un nombre d'événements ou de flux et choisir de n'afficher que les infractions dont l'amplitude est égale, inférieure ou supérieure à la valeur configurée.
Exclure	Vous pouvez cocher les cases pour les infractions que vous souhaitez exclure des résultats de recherche. Ces options incluent : • **Infractions actives** • **Infractions masquées** • **Infractions fermées** • **Infractions inactives** • **Infractions protégées**

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Cliquez sur **Par adresse IP source**.
3. Dans la zone de liste **Rechercher**, sélectionnez **Nouvelle recherche**.
4. Dans le volet Intervalle, sélectionnez une option pour l'intervalle que vous souhaitez capturer pour cette recherche. Voir le Tableau 1.
5. Dans le volet Paramètres de recherche, définissez les critères de recherche spécifiques. Voir le Tableau 1.
6. Dans le volet Définition de colonne, définissez l'ordre dans lequel vous souhaitez trier les résultats :
   a. Dans la première zone de liste, sélectionnez la colonne dans laquelle vous souhaitez trier les résultats de la recherche.
   b. Dans la deuxième zone de liste, sélectionnez l'ordre dans lequel vous souhaitez afficher les résultats de recherche. Les options comprennent **Ordre décroissant** et **Ordre croissant**.
7. Cliquez sur **Rechercher**.

Que faire ensuite

Sauvegarde des critères de recherche sur l'onglet Infraction

Recherche d'infractions dans la page Par adresse IP de destination

Sur la page **Par adresse IP de destination** de l'onglet **Infraction**, vous pouvez rechercher des infractions groupées par adresse IP de destination.

Pourquoi et quand exécuter cette tâche

Le tableau suivant décrit les options de recherche que vous pouvez utiliser pour rechercher des infractions sur la page Par adresse IP de destination :

Tableau 40. Options de recherche de la page Par adresse IP de destination

Options	Description
Toutes les infractions	Vous pouvez sélectionner cette option pour rechercher toutes les adresses IP de destination sans tenir compte de l'intervalle.
Récent	Vous pouvez sélectionner cette option et, dans cette zone de liste, sélectionner l'intervalle que vous souhaitez rechercher.
Intervalle spécifique	Pour spécifier un intervalle à rechercher, vous pouvez sélectionner l'option **Intervalle spécifique**, puis l'une des options suivantes : • Pour spécifier un intervalle à rechercher, vous pouvez sélectionner l'option **Intervalle spécifique**, puis l'une des options suivantes : • **Dernier événement/flux entre** - Cochez cette case pour rechercher les adresses IP de destination associées à des infractions dont le dernier événement détecté s'est déroulé dans une période définie. Une fois que vous avez coché cette case, utilisez les zones de liste pour sélectionner les dates que vous souhaitez rechercher.
Rechercher	L'icône **Rechercher** est disponible dans plusieurs volets de la page de recherche. Vous pouvez cliquer sur **Rechercher** lorsque vous avez terminé de configurer la recherche et que vous souhaitez afficher les résultats.
IP de destination	Vous pouvez saisir l'adresse IP de destination ou la plage CIDR que vous souhaitez rechercher.
Magnitude	Dans cette zone de liste, vous pouvez indiquer une amplitude et choisir de n'afficher que les infractions dont l'amplitude est égale, inférieure ou supérieure à la valeur configurée.
Risque de l'analyse des vulnérabilités	Dans cette zone de liste, vous pouvez indiquer un risque VA et choisir de n'afficher que les infractions dont le risque VA est égal, inférieur ou supérieur à la valeur configurée. L'intervalle est compris entre 0 et 10.
Evénements/Flux	Dans cette zone de liste, vous pouvez indiquer une amplitude de nombre d'événements ou de flux puis choisir de n'afficher que les infractions dont le nombre d'événements ou de flux est égal, inférieur ou supérieur à la valeur configurée.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Dans le menu de navigation, cliquez sur **Par adresse IP de destination**.
3. Dans la zone de liste **Rechercher**, sélectionnez **Nouvelle recherche**.

4. Dans le volet Intervalle, sélectionnez une option pour l'intervalle que vous souhaitez capturer pour cette recherche. Voir le Tableau 1.
5. Dans le volet Paramètres de recherche, définissez les critères de recherche spécifiques. Voir le Tableau 1.
6. Dans le volet Définition de colonne, définissez l'ordre dans lequel vous souhaitez trier les résultats :
   a. Dans la première zone de liste, sélectionnez la colonne dans laquelle vous souhaitez trier les résultats de la recherche.
   b. Dans la deuxième zone de liste, sélectionnez l'ordre dans lequel vous souhaitez afficher les résultats de recherche. Les options comprennent **Ordre décroissant** et **Ordre croissant**.
7. Cliquez sur **Rechercher**.

Que faire ensuite

Sauvegarde des critères de recherche sur l'onglet Infraction

Recherche d'infractions dans la page Par réseau

Sur la page **Par réseau** de l'onglet **Infraction**, vous pouvez rechercher des infractions groupées par les réseaux associés.

Pourquoi et quand exécuter cette tâche

Le tableau suivant décrit les options de recherche que vous pouvez utiliser pour rechercher des infractions sur la page Par réseau :

Tableau 41. Options pour rechercher des infractions sur la page Par réseau

Option	Description
Réseau	Dans cette zone de liste, vous pouvez sélectionner le réseau que vous souhaitez rechercher.
Magnitude	Dans cette zone de liste, vous pouvez indiquer une amplitude et choisir de n'afficher que les infractions dont l'amplitude est égale, inférieure ou supérieure à la valeur configurée.
Risque de l'analyse des vulnérabilités	Dans cette zone de liste, vous pouvez indiquer un risque VA et choisir de n'afficher que les infractions dont le risque VA est égal, inférieur ou supérieur à la valeur configurée.
Evénement/Flux	Dans cette zone de liste, vous pouvez indiquer un nombre d'événements ou de flux puis choisir de n'afficher que les infractions dont le nombre d'événements ou de flux est égal, inférieur ou supérieur à la valeur configurée.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Cliquez sur **Par réseau**.
3. Dans la zone de liste **Rechercher**, sélectionnez **Nouvelle recherche**.

4. Dans le volet Paramètres de recherche, définissez les critères de recherche spécifiques. Voir le Tableau 1.
5. Dans le volet Définition de colonne, définissez l'ordre dans lequel vous souhaitez trier les résultats :
   a. Dans la première zone de liste, sélectionnez la colonne dans laquelle vous souhaitez trier les résultats de recherche.
   b. Dans la deuxième zone de liste, sélectionnez l'ordre dans lequel vous souhaitez afficher les résultats de recherche. Les options comprennent **Ordre décroissant** et **Ordre croissant**.
6. Cliquez sur **Rechercher**.

Que faire ensuite

Sauvegarde des critères de recherche sur l'onglet Infraction

Sauvegarde de critères de recherche sur l'onglet Infractions

Dans l'onglet **Infractions**, vous pouvez sauvegarder les critères de recherche configurés afin de pouvoir les réutiliser. Les critères de recherche sauvegardés n'expirent pas.

Procédure

1. Procédure
2. Effectuez une recherche. Voir Recherches d'infractions.
3. Cliquez sur **Sauvegarder les critères**.
4. entrez les valeurs pour les paramètres suivants :

Option	Description
Paramètre	Description
Nom de la recherche	Saisissez un nom que vous souhaitez attribuer à ces critères de recherche.
Gérer les groupes	Cliquez sur **Gérer les groupes** pour gérer des groupes de recherche. Voir Gestion des groupes de recherche.

Option	Description
Options d'intervalle :	Sélectionnez l'une des options suivantes : • **Toutes les infractions** - Sélectionnez cette option pour rechercher toutes les infractions, quel que soit leur intervalle. • **Récent** - Sélectionnez cette option puis, dans cette zone de liste, sélectionnez l'intervalle que vous souhaitez rechercher. • **Intervalle spécifique** - Pour spécifier un intervalle à rechercher, sélectionnez l'option **Intervalle spécifique**, puis l'une des options suivantes : Date de début entre - Cochez cette case pour rechercher des infractions qui ont commencé pendant une période définie. Une fois que vous avez coché cette case, utilisez les zones de liste pour sélectionner les dates que vous souhaitez rechercher. Dernier événement/flux entre - Sélectionnez cette case pour rechercher des infractions dont le dernier événement détecté s'est déroulé au cours d'une période définie. Après avoir sélectionné cette case à cocher, utilisez les zones de liste pour sélectionner les dates pour lesquelles vous voulez effectuer la recherche.Dernier événement entre - Sélectionnez cette case pour rechercher des infractions dont le dernier événement détecté s'est déroulé au cours d'une période définie. Une fois que vous avez coché cette case, utilisez les zones de liste pour sélectionner les dates que vous souhaitez rechercher.
Définir par défaut	Cochez cette case pour définir cette recherche comme votre recherche par défaut.

5. Cliquez sur **OK**.

Recherche d'infractions indexées sur une propriété personnalisée

Définissez des critères de recherche pour filtrer la liste des infractions et reconnaître plus facilement les infractions devant faire l'objet d'une examen. Vous pouvez utiliser le type d'infraction dans vos critères de recherche pour trouver toutes les infractions basées sur une propriété personnalisée. Vous pouvez filtrer les résultats de la requête pour afficher les infractions ayant un résultat de capture de propriétés personnalisées spécifique.

Avant de commencer

La propriété personnalisée doit être utilisée comme index de règle. Pour plus d'informations, voir «Indexation des infractions», à la page 36.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Dans la liste **Rechercher**, sélectionnez **Nouvelle recherche**.
3. Sur le panneau **Source de l'infraction**, sélectionnez la propriété personnalisée dans la liste **Type d'infraction**.

   La liste **Type d'infraction** affiche uniquement les zones normalisées et les propriétés personnalisées utilisées comme index de règles. Vous ne pouvez pas utiliser **Source de l'infraction** pour rechercher des propriétés `DateTime`.
4. Facultatif : Pour rechercher des infractions ayant une valeur spécifique dans le résultat de capture des propriétés personnalisées, entrez la valeur que vous souhaitez rechercher dans la zone de filtre.
5. Configurez d'autres paramètres de recherche pour répondre à vos besoins de recherche.
6. Cliquez sur **Rechercher**.

Résultats

Toutes les infractions répondant aux critères de recherche s'affichent dans la liste des infractions. Lorsque vous affichez le récapitulatif des infractions, la propriété personnalisée recherchée s'affiche dans la zone **Type d'infraction**. Le résultat de capture de propriété personnalisée s'affiche dans la zone **Valeur de propriété personnalisée** du panneau Récapitulatif des sources des infractions.

Recherche rapide des indicateurs de compromis avec la recherche flexible

Vous pouvez utiliser la *recherche flexible* de IBM Security QRadar pour rechercher un indicateur de compromis (IOC), comme par exemple un trafic réseau sortant inhabituel ou des anomalies dans l'activité d'un compte d'utilisateur privilégié.

Avant de commencer

La *recherche flexible* renvoie les 1000 premiers événements associés au critère de recherche. Par exemple, si vous avez besoin de rechercher un MD5 particulier dans le cadre d'une enquête sur l'apparition de logiciels malveillants, vous n'avez pas besoin de passer en revue chaque événement associé. Effectuez une *recherche flexible* pour renvoyer rapidement un ensemble de résultats limité.

Pour profiter des avantages offerts par la *recherche flexible*, vous devez posséder un profil de sécurité d'administrateur ou un profil de sécurité de non administrateur configuré de la manière suivante :

- Priorité d'autorisation définie sur **Aucune restriction**.
- Accès à tous les réseau et à toutes les sources de journal.

La recherche flexible ne peut pas être utilisée par des utilisateurs ayant des profiles de sécurité non administrateurs sur des réseaux sur lesquels des domaines sont configurés.

Procédure

1. Pour effectuer une recherche flexible pour les filtre rapides, procédez comme suit :
   a. Sur l'onglet **Activité du journal**, dans la zone **Filtrage rapide**, entrez une valeur.

b. Dans la liste **Afficher**, sélectionnez un intervalle de temps.

2. Pour effectuer une recherche flexible en cas de recherches de base, procédez comme suit :
   a. Sur l'onglet Activité du journal, cliquez sur **Rechercher** > **Nouvelle recherche**.
   b. Sélectionnez un intervalle **Récent** ou définissez un **Intervalle spécifique**.
   c. Vérifiez que la valeur de la zone **Classer par** est défini sur `Heure de début` et que la valeur de la zone **Limite de résultats** est inférieure ou égale à `1000`. Les colonnes agrégées ne doivent pas être comprises dans la recherche.
   d. Entrez une valeur pour le paramètre **Filtrage rapide** et cliquez sur **Ajouter un filtre**.
3. Pour désactiver complètement la recherche flexible, procédez comme suit :
   a. Cliquez sur **Paramètres système** sur l'onglet **Admin**.
   b. Dans la fenêtre Paramètres système, supprimez toute valeur dans la zone **Nombre limité de recherches par défaut**.

Suppression des critères de recherche

Vous pouvez supprimer des critères de recherche.

Pourquoi et quand exécuter cette tâche

Lorsque vous supprimez une recherche sauvegardée, il se peut que les objets qui lui sont associés ne fonctionnent pas. Les rapports et les règles de détection des anomalies correspondent aux objets QRadar utilisant des critères de recherche sauvegardée. Une fois la recherche sauvegardée supprimée, éditez les objets associés pour vous assurer qu'ils continuent de fonctionner.

Procédure

1. Sélectionnez l'une des options suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Dans la zone de liste **Rechercher**, sélectionnez **Nouvelle recherche** ou **Editer la recherche**.
3. Dans le volet Recherches sauvegardées, sélectionnez une recherche sauvegardée dans la zone de liste **Recherches sauvegardées disponibles**.
4. Cliquez sur **Supprimer**.
   - Si les critères de la recherche sauvegardée ne sont pas associés à d'autres objets QRadar, une fenêtre de confirmation s'affiche.
   - Si les critères de la recherche sauvegardée sont associés à d'autres objets, la fenêtre Supprimer la recherche sauvegardée est affichée. La fenêtre répertorie les objets associés à la recherche sauvegardée que vous souhaitez supprimer. Notez les objets associés.
5. Cliquez sur **OK**.
6. Sélectionnez l'une des options suivantes :
   - Cliquez sur **OK** pour poursuivre.
   - Cliquez sur **Annuler** pour fermer la fenêtre Supprimer la recherche sauvegardée.

Que faire ensuite

Si les critères de la recherche sauvegardée étaient associés à d'autres objets QRadar, accédez aux objets associés que vous avez notés et éditez-les pour supprimer ou remplacer l'association par la recherche sauvegardée supprimée.

Utilisation d'une sous-recherche pour affiner les résultats de recherche

Vous pouvez utiliser une sous-recherche pour effectuer des recherches dans un ensemble de résultats de recherche terminée. La sous-recherche permet d'affiner les résultats de recherche et d'éviter de lancer une nouvelle recherche dans la base de données.

Avant de commencer

Lors de la définition d'une recherche que vous souhaitez utiliser comme base de la sous-recherche, assurez-vous que l'option Temps réel (diffusion en flux) est désactivée et que la recherche n'est pas groupée.

Pourquoi et quand exécuter cette tâche

Cette fonction n'est pas disponible pour les recherches groupées, les recherches en cours ou en mode de diffusion en flux.

Procédure

1. Sélectionnez l'une des options suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Effectuez une recherche.
3. Lorsque vous terminez votre recherche, ajoutez un autre filtre :
   a. Cliquez sur **Ajouter un filtre**.
   b. Dans la première zone de liste, sélectionnez un paramètre que vous souhaitez rechercher.
   c. Dans la deuxième zone de liste, sélectionnez le modificateur que vous voulez utiliser pour la recherche. La liste des modificateurs disponibles dépend de l'attribut sélectionné dans la première liste.
   d. Dans la zone de saisie, entrez des informations spécifiques liées à votre recherche.
   e. Cliquez sur **Ajouter un filtre**.

Résultats

Le volet Filtres originaux indique les filtres d'origine appliqués à la recherche de base. Le volet Filtres en cours indique les filtres appliqués à la sous-recherche. Vous pouvez supprimer les filtres de sous-recherche sans relancer la recherche de base. Cliquez sur le lien **Effacer le filtre** situé en regard du filtre que vous souhaitez supprimer. La recherche de base est relancée lorsque vous désactivez un filtre dans le volet Filtres originaux.

Si vous supprimez les critères de recherche de base des critères de sous-recherche sauvegardée, vous avez toujours accès aux critères de sous-recherche sauvegardée. Si vous ajoutez un filtre, la sous-recherche porte sur l'ensemble de la base de

données car la fonction de recherche n'est plus basée sur un ensemble de données précédemment recherchées.

Que faire ensuite

Sauvegarde des critères de recherche

Gestion des résultats de recherche

Vous pouvez lancer plusieurs recherches, puis naviguer vers d'autres onglets pour effectuer d'autres tâches tandis que vos recherches s'exécutent en arrière-plan.

Vous pouvez configurer une recherche de sorte qu'une notification par courrier électronique vous soit envoyée lorsque cette recherche se termine.

A tout moment, pendant qu'une recherche est en cours, vous pouvez retourner sur les onglets **Activité du journal** ou **Activité réseau** pour afficher des résultats de recherche partiels ou complets.

Annulation d'une recherche

Lorsqu'une recherche est en attente ou en cours, vous pouvez l'annuler depuis la page Gérer les résultats de la recherche.

Pourquoi et quand exécuter cette tâche

Si la recherche est en cours au moment où vous l'annulez, les résultats accumulés sont maintenus.

Procédure

1. Sélectionnez une des options suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Dans le menu **Rechercher**, sélectionnez **Gérer les résultats de la recherche**.
3. Sélectionnez le résultat de la recherche en attente ou en cours que vous souhaitez annuler.
4. Cliquez sur **Annuler**.
5. Cliquez sur **Oui**.

Suppression d'une recherche

Si le résultat de la recherche n'est plus nécessaire, vous pouvez le supprimer depuis la page Gérer les résultats de la recherche.

Procédure

1. Sélectionnez l'une des options suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Dans le menu **Rechercher**, sélectionnez **Gérer les résultats de la recherche**.
3. Sélectionnez le résultat de la recherche que vous souhaitez supprimer.
4. Cliquez sur **Supprimer**.
5. Cliquez sur **Oui**.

Gestion des groupes de recherche

La fenêtre Groupes de recherche vous permet de créer et de gérer les groupes de recherche d'événement, de flux et d'infraction.

Ces groupes vous permettent de localiser facilement des critères de recherche sauvegardés dans les onglets **Activité du journal**, **Activité réseau** et **Infractions** ainsi que dans l'assistant de rapport.

Affichage des groupes de recherche

Un ensemble par défaut de groupes et de sous-groupes est disponible.

Pourquoi et quand exécuter cette tâche

Vous pouvez afficher des groupes de recherche dans les fenêtres Groupe de recherche d'événements, Groupe de recherche de flux ou Groupe de recherche d'infractions.

Toutes les recherches enregistrées qui ne sont pas affectées à un groupe se trouvent dans le groupe **Autre**.

Les fenêtres Groupe de recherche d'événements, Groupe de recherche de flux et Groupe de recherche d'infractions affichent les paramètres suivants pour chaque groupe.

Tableau 42. Paramètres de la fenêtre Groupe de recherche

Paramètre	Description
Nom	Indique le nom du groupe de recherche.
Utilisateur	Indique le nom de l'utilisateur qui a créé le groupe de recherche.
Description	Indique la description du groupe de recherche.
Date de modification	Indique la date à laquelle le groupe de recherche a été modifié.

Les fenêtre Groupes de recherche d'événements, Groupe de recherche de flux et Groupe de recherche d'infractions proposent les fonctions suivantes.

Tableau 43. Les fonctions de la barre d'outils Groupe de recherche

Fonction	Description
Nouveau groupe	Pour créer un groupe de recherche, vous pouvez cliquer sur **Nouveau groupe**. Voir Création d'un nouveau groupe de recherche.
Editer	Pour éditer un groupe de recherche existant, vous pouvez cliquer sur **Editer**. Voir Edition d'un groupe de recherche.
Copier	Pour copier une recherche enregistrée dans un autre groupe de recherche, vous pouvez cliquer sur **Copier**. Voir Copie d'une recherche enregistrée dans un autre groupe.

Tableau 43. Les fonctions de la barre d'outils Groupe de recherche (suite)

Fonction	Description
Retirer	Pour supprimer un groupe de recherche ou une recherche enregistrée d'un groupe de recherche, sélectionnez l'élément que vous souhaitez supprimer, puis cliquez sur **Retirer**. Voir Suppression d'un groupe ou d'une recherche enregistrée d'un groupe.

Procédure

1. Choisissez l'une des options suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. **Sélectionnez Rechercher** > **Editer la recherche**.
3. Cliquez sur **Gérer les groupes**.
4. Afficher les groupes de recherche.

Création d'un groupe de recherche

Vous pouvez créer un nouveau groupe de recherche.

Procédure

1. Sélectionnez l'une des options suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. **Sélectionnez Rechercher Editer la recherche**.
3. Cliquez sur **Gérer les groupes**.
4. Sélectionnez le dossier du groupe sous lequel vous souhaitez créer le groupe.
5. Cliquez sur **Nouveau groupe**.
6. Dans la zone **Nom**, entrez un nom unique pour le nouveau groupe.
7. Facultatif. Dans la zone **Description**, entrez une description.
8. Cliquez sur **OK**.

Edition d'un groupe de recherche

Vous pouvez éditer les zones **Nom** et **Description** d'un groupe de recherche.

Procédure

1. Sélectionnez l'une des options suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Sélectionnez **Rechercher** > **Editer la recherche**.
3. Cliquez sur **Gérer les groupes**.
4. Sélectionnez le groupe que vous souhaitez éditer.
5. Cliquez sur **Editer**.
6. Modifiez les paramètres :
   - Saisissez un nouveau nom dans la zone **Nom**.
   - Saisissez une nouvelle description dans la zone **Description**.
7. Cliquez sur **OK**.

Copie d'une recherche sauvegardée vers un autre groupe

Vous pouvez copier une recherche sauvegardée vers un ou plusieurs groupes.

Procédure

1. Sélectionnez une des options suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Sélectionnez **Rechercher** > **Editer la recherche**.
3. Cliquez sur **Gérer les groupes**.
4. Sélectionnez la recherche sauvegardée que vous souhaitez copier.
5. Cliquez sur **Copier**.
6. Dans la fenêtre Groupes d'éléments, sélectionnez la case du groupe vers lequel vous souhaitez copier la recherche sauvegardée.
7. Cliquez sur **Affecter des groupes**.

Suppression d'un groupe ou d'une recherche sauvegardée dans un groupe

Vous pouvez utiliser l'icône **Retirer** pour supprimer une recherche d'un groupe ou supprimer un groupe de recherche.

Pourquoi et quand exécuter cette tâche

Lorsque vous supprimez une recherche sauvegardée d'un groupe, celle-ci n'est pas supprimée de votre système. La recherche sauvegardée est supprimée du groupe et déplacée automatiquement vers le groupe **Autre**.

Vous ne pouvez pas supprimer les groupes suivants de votre système :

- Groupes de recherche d'événements
- Groupes de recherche de flux
- Groupes de recherche d'infractions
- Autre

Procédure

1. Sélectionnez l'une des options suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Sélectionnez **Rechercher** > **Editer la recherche**.
3. Cliquez sur **Gérer les groupes**.
4. Sélectionnez l'une des options suivantes :
   - Sélectionnez la recherche sauvegardée que vous souhaitez supprimer du groupe.
   - Sélectionnez le groupe que vous souhaitez supprimer.
5. Cliquez sur **Retirer**.
6. Cliquez sur **OK**.

Exemple de recherche : Rapports quotidiens sur les employés

L'exemple suivant décrit comment utiliser une requête de recherche avancée complexe pour afficher des informations spécifiques sur un employé.

A des fins de gestion des identités, vous décidez de générer un rapport quotidien sur l'activité d'un utilisateur dans QRadar. Le rapport doit contenir des informations sur l'employé, comme par exemple ses noms d'utilisateur, son numéro de série, le nom de son supérieur, et ses activités.

Un employé peut avoir plusieurs noms d'utilisateurs dans QRadar. Vous devez utiliser l'API RESTful pour créer une mappe de référence qui renvoie toutes les noms d'utilisateurs associés au nom de l'employé, `Global_User`. Pour le numéro de série et le nom du supérieur, vous devez créer une autre jeu de données de référence et l'ajouter à la mappe de référence.

Les activités d'un employé peuvent aller des échecs de connexion aux tâches de QRadar, comme par exemple la suppression d'objets. Ces événements sont enregistrés par QRadar. En spécifiant la fréquence des événements dans la mappe, vous pouvez mesurer quand une activité suspecte se produit. Vous devez regrouper les données par nom d'employé et par nom d'événement puis les trier par ordre de fréquence d'événement élevée au cours d'un intervalle de 24 heures.

Pour afficher ce rapport quotidien, connectez vous à QRadar Console. Dans la zone de texte Recherche avancée de l'onglet **Activité du journal**, entrez la requête de recherche suivante :

```
select REFERENCEMAP('GlobalID_Mapping', username) as Global_User,
QIDNAME(qid) as 'Event Name', count(*) as 'Event Count', FIRST(username) as
UserId, REFERENCETABLE('employee_data','SerialNum', Global_user) as 'Serial
Number', REFERENCETABLE('employee_data','Manager',Global_User) as Manager
from events where (Global_User IS NOT NULL) GROUP BY Global_user,'Event
Name' ORDER BY 'Event Count' DESC last 1 DAYS
```

Chapitre 10. Propriétés d'événementet de flux personnalisés

Utilisez les propriétés d'événement et de flux personnalisées pour rechercher, afficher et signaler des informations présentes dans les journaux que QRadar ne normalise et n'affiche pas d'habitude.

Vous pouvez créer des propriétés d'événement et de flux personnalisées à partir de plusieurs emplacements sur les onglets **Activité du journal** ou **Activité réseau** :

- Dans l'onglet **Activité du journal**, cliquez deux fois sur un événement puis cliquez sur **Extraire la propriété**.
- Dans l'onglet **Activité réseau**, cliquez deux fois sur un flux puis cliquez sur **Extraire la propriété**.
- Vous pouvez créer ou éditer une propriété d'événement ou de flux personnalisée à partir de la page Rechercher. Quand vous créez une propriété personnalisée à partir de la page Rechercher, la propriété n'est pas dérivée d'un événement ou d'un flux particulier ; par conséquent, la fenêtre Propriétés d'événement personnalisées n'est pas en mesure de se préremplir. Vous pouvez copier et coller les informations du contenu depuis une autre source.

Autorisations obligatoires

Permet de créer des propriétés personnalisées si vous possédez les autorisations appropriées.

Vous devez disposer de l'autorisation Propriétés d'événement définies par l'utilisateur ou Propriétés de flux définies par l'utilisateur.

Si vous possédez des droits d'administration, vous pouvez également créer et modifier des propriétés personnalisées à partir de l'onglet Admin.

Cliquez sur **Admin** > **Sources de données** > **Propriétés d'événement personnalisées** > ou sur **Admin** > **Sources de données** > **Propriétés de flux personnalisées**.

Vérifiez auprès de votre administrateur que vous possédez les droits requis.

Pour plus d'informations, voir *IBM Security QRadar Administration Guide*.

Types de propriétés personnalisées

Vous pouvez créer un type de propriété personnalisé.

Lorsque vous créez une propriété personnalisée, vous pouvez créer une expression régulière ou un type de propriété calculé.

A l'aide des instructions d'expression régulière (Regex), vous pouvez extraire des données non normalisées à partir des contenus d'événement ou de flux.

Par exemple, un rapport est créé pour signaler tous les utilisateurs qui apportent des changements aux droits d'utilisateur sur un serveur Oracle. Une liste des utilisateurs est créée et le nombre de fois où ceux-ci ont apporté une modification au droit d'un autre compte est signalé. Cependant, généralement le compte

© Copyright IBM Corp. 2012, 2017

utilisateur réel ou le droit ayant été modifié ne peut pas s'afficher. Vous pouvez créer une propriété personnalisée pour extraire ces informations dans les journaux et utiliser ensuite la propriété pour les recherches et les rapports. L'utilisation de cette fonction nécessite une connaissance approfondie des expressions régulières (regex).

L'expression régulière définit la zone que vous souhaitez définir en tant que propriété personnalisée. Après avoir entré une instruction d'expression régulière, vous pouvez la valider par rapport au contenu. Lorsque vous définissez des modèles d'expression régulière personnalisés, vous devez accepter les règles d'expression régulière telles que définies par le langage de programmation Java.

Pour en savoir plus, vous pouvez vous référer aux tutoriels d'expressions régulières disponibles sur le Web. Une propriété personnalisée peut être associée à plusieurs expressions régulières.

Lorsqu'un événement ou un flux est analysé, chaque modèle d'expression régulière est testé sur l'événement ou sur le flux jusqu'à ce qu'un modèle d'expression régulière corresponde au contenu. Le premier modèle d'expression régulière correspondant au contenu d'événement ou de flux détermine les données à extraire.

A l'aide des propriétés personnalisées basées sur des calculs, vous pouvez effectuer des calculs sur un événement numérique existant ou sur des propriétés d'événement ou de flux afin de produire une propriété calculée.

Par exemple, vous pouvez créer une propriété qui affiche un pourcentage en divisant une propriété numérique par une autre.

Création d'une propriété personnalisée basée sur une expression régulière

Vous pouvez créer une propriété personnalisée basée sur une expression régulière afin que les contenus d'événements ou de flux correspondent à une expression régulière.

Pourquoi et quand exécuter cette tâche

Quand vous configurez une propriété personnalisée basée une expression régulière, les fenêtres Propriétés d'événement personnalisées ou Propriétés de flux personnalisées fournissent les paramètres suivants. Le tableau suivant décrit certains de ces paramètres.

Tableau 44. Paramètres de la fenêtre Propriétés personnalisées (expressions régulières)

Paramètre	Description
Champ de test	Indique le contenu qui a été extrait de l'événement ou du flux non normalisé.

Tableau 44. Paramètres de la fenêtre Propriétés personnalisées (expressions régulières) (suite)

Paramètre	Description
Nouvelle propriété	Le nom de la nouvelle propriété ne peut pas être le nom d'une propriété normalisée, comme `Nom d'utilisateur`, `IP source` ou `IP de destination`. **Remarque :** Les caractères ci-dessous entraînent une erreur s'ils sont utilisés pour créer un nom de propriété : barre oblique inverse (\), virgule (,), point (.), esperluète (&), apostrophe ('), guillemet double ("), parenthèse (()) et crochets doubles ([]). **Important :** Pour les CEP et les CFP incluant ces caractères, vous devez créer un doublon de la propriété et enregistrer le nom de la nouvelle propriété sans utiliser les caractères mentionnés. Ensuite, modifiez toutes les dépendances de l'ancienne propriété de manière à faire référence à la nouvelle propriété. Enfin, supprimez l'ancienne propriété.
Optimiser l'analyse syntaxique pour les règles, rapports et recherches	Analyse et stocke la propriété la première fois que l'événement ou le flux est reçu. Lorsque vous sélectionnez cette case à cocher, la propriété ne nécessite pas d'analyse supplémentaire pour les tests de rapport, de recherche ou de règle. Si vous la décochez, la propriété est analysée chaque fois qu'un test de rapport, de recherche ou de règle est effectué.
Source de journal	Si plusieurs sources de journal sont associées à cet événement, cette zone indique le terme Multiple et le nombre de sources du journal.

Tableau 44. Paramètres de la fenêtre Propriétés personnalisées (expressions régulières) (suite)

Paramètre	Description
Expression régulière	Expression régulière que vous voulez utiliser pour extraire les données du contenu. Les expressions régulières sont sensibles à la casse. Des expressions régulières exemple sont présentées ci-après. • E-mail : `(.+@[^\.].*\.[a-z]{2,}$)` • URL : `(http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\S*)?$)` • Nom de domaine : `(http[s]?://(.+?)["/?:])` • Nombre en virgule flottante : `([-+]?\d*\.?\d*$)` • Entier : `([-+]?\d*$)` • Adresse IP : `(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)` Les groupes de capture doivent être mis entre parenthèses.
Groupe de capture	Les groupes de capture traitent les caractères multiples en tant qu'unité unique. Dans un groupe de capture, les caractères sont groupés entre parenthèses.
Activé	Si vous décochez cette case, cette propriété personnalisée ne s'affiche pas dans les filtres de recherche ou les listes de colonnes, et elle n'est pas analysée à partir du contenu.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Si vous affichez les événements en mode diffusion en flux, cliquez sur l'icône **Pause** pour mettre en pause la diffusion en flux.
3. Cliquez deux fois sur l'événement sur lequel vous souhaitez baser la propriété personnalisée.
4. Cliquez sur **Extraire la propriété**.
5. Dans le panneau **Sélection du type de propriété**, sélectionnez l'option **Expression régulière**.
6. Configurez les paramètres de propriété personnalisée.
7. Cliquez sur **Test** pour tester l'expression régulière par rapport au contenu.
8. Cliquez sur **Sauvegarder**.

Résultats

La propriété personnalisée s'affiche en tant qu'option dans la liste des colonnes disponibles sur la page de recherche. Pour inclure une propriété personnalisée dans une liste d'événements ou de flux, vous devez sélectionner la propriété personnalisée dans la liste des colonnes disponibles lorsque vous créez une recherche.

Concepts associés:

«Exemples de chaînes de recherche AQL», à la page 152
Utilisez le langage AQL (Ariel Query Language) pour extraire des zones spécifiques des événements, flux et tables simarc dans la base de données Ariel.

Création d'une propriété personnalisée basée sur le calcul

Vous pouvez créer une propriété client basée sur le calcul pour faire correspondre les contenus à une expression régulière.

Pourquoi et quand exécuter cette tâche

Lorsque vous configurez une propriété personnalisée basée sur un calcul, la fenêtre Propriété d'événement personnalisée ou Propriété de flux personnalisée fournit les paramètres répertoriés dans le tableau 1 :

Tableau 45. Paramètres de la fenêtre de définition des propriétés personnalisées (calcul)

Paramètre	Description
Définition de propriété	
Nom de la propriété	Entrez un nom unique pour cette propriété personnalisée. Le nouveau nom de propriété ne peut pas être le nom d'une propriété normalisée telle que Nom d'utilisateur, IP source ou IP de destination. **Remarque :** Les caractères ci-dessous entraînent une erreur s'ils sont utilisés pour créer un nom de propriété : barre oblique inverse (\), virgule (,), point (.), esperluète (&), apostrophe ('), guillemet double ("), parenthèse (()) et crochets doubles ([]). **Important :** Pour les CEP et les CFP incluant ces caractères, vous devez créer un doublon de la propriété et enregistrer le nom de la nouvelle propriété sans utiliser les caractères mentionnés. Ensuite, modifiez toutes les dépendances de l'ancienne propriété de manière à faire référence à la nouvelle propriété. Enfin, supprimez l'ancienne propriété.
Description	Entrez une description de cette propriété personnalisée.
Définition de calcul de propriété	

Tableau 45. Paramètres de la fenêtre de définition des propriétés personnalisées (calcul) (suite)

Paramètre	Description
Propriété 1	Dans la zone de liste, sélectionnez la première propriété que vous souhaitez utiliser dans votre calcul. Les options incluent toutes les propriétés personnalisées et normalisées numériques. Vous pouvez également indiquer une valeur numérique spécifique. Dans la zone de liste **Propriété 1**, sélectionnez l'option **Défini par l'utilisateur**. Le paramètre **Propriété numérique** s'affiche. Entrez une valeur numérique spécifique.
Opérateur	Dans la zone de liste, sélectionnez l'opérateur que vous souhaitez appliquer aux propriétés sélectionnées du calcul. Ces options incluent : • Ajouter • Soustraire • Multiplier • Diviser
Propriété 2	Dans la zone de liste, sélectionnez la seconde propriété que vous souhaitez utiliser dans votre calcul. Les options incluent toutes les propriétés personnalisées et normalisées numériques. Vous pouvez également indiquer une valeur numérique spécifique. Dans la zone de liste **Propriété 1**, sélectionnez l'option **Défini par l'utilisateur**. Le paramètre **Propriété numérique** s'affiche. Entrez une valeur numérique spécifique.
Activé	Sélectionnez cette option pour activer cette propriété personnalisée. Si vous désélectionnez cette option, cette propriété personnalisée ne s'affiche pas dans les filtres de recherche d'événement ou de flux ou les listes de colonnes et la propriété d'événement ou de flux n'est pas analysée à partir du contenu.

Procédure

1. Choisissez l'un des éléments suivants : cliquez sur l'onglet **Activité du journal**.
2. Facultatif. Si vous affichez des événements ou des flux en streaming, cliquez sur l'icône **Pause** pour mettre ce mode en pause.
3. Cliquez deux fois sur l'événement ou le flux sur lequel vous souhaitez baser la propriété personnalisée.
4. Cliquez sur **Extraire la propriété**.

5. Dans le volet Sélection du type de propriété, sélectionnez l'option **Calcul**.
6. Configurez les paramètres de la propriété personnalisée.
7. Cliquez sur **Test** pour tester l'expression régulière par rapport au contenu.
8. Cliquez sur **Sauvegarder**.

Résultats

La propriété personnalisée s'affiche en tant qu'option dans la liste des colonnes disponibles sur la page de recherche. Pour inclure une propriété personnalisée dans une liste d'événements ou de flux, vous devez sélectionner la propriété personnalisée dans la liste des colonnes disponibles lorsque vous créez une recherche.

Modification d'une propriété personnalisée

Vous pouvez modifier une propriété personnalisée.

Pourquoi et quand exécuter cette tâche

Les fenêtres Propriétés d'événement personnalisées ou Propriétés de flux personnalisées permettent de modifier une propriété personnalisée.

Les propriétés personnalisées sont décrites dans le tableau suivant.

Tableau 46. Colonnes des fenêtres de propriétés personnalisées

Colonne	Description
Nom de la propriété	Indique un nom unique pour cette propriété personnalisée
Type	Indique le type de cette propriété personnalisée.
Description de la propriété	Indique une description de cette propriété personnalisée.
Type de la source de journal	Indique le nom du type de source de journal auquel s'applique cette propriété personnalisée. Cette colonne ne s'affiche que dans la fenêtre Propriétés d'événement personnalisées.
Source de journal	Indique la source de journal à laquelle s'applique cette propriété personnalisée. S'il existe plusieurs sources de journal associées à cet événement ou à ce flux, cette zone indique le terme Multiple et le nombre de sources de journal. Cette colonne ne s'affiche que dans la fenêtre Propriétés d'événement personnalisées.

Tableau 46. Colonnes des fenêtres de propriétés personnalisées (suite)

Colonne	Description
Expression	Indique l'expression de cette propriété personnalisée. L'expression dépend du type de propriété personnalisée : Pour une propriété personnalisée basée sur les expressions régulières, ce paramètre définit l'expression régulière à utiliser pour extraire les données du contenu. Pour une propriété personnalisée basée sur le calcul, ce paramètre spécifie le calcul à utiliser pour créer une valeur de propriété personnalisée.
Nom d'utilisateur	Indique le nom de l'utilisateur qui a créé cette propriété personnalisée.
Activé	Indique si cette propriété personnalisée est activée. Cette zone indique Vrai ou False.
Date de création	Indique la date à laquelle cette propriété personnalisée a été créée.
Date de modification	Indique la date de la dernière modification de la propriété personnalisée.

Les barres d'outils Propriété d'événement personnalisée et Propriété de flux personnalisée fournissent les fonctions suivantes :

Tableau 47. Options de la barre d'outils de propriétés personnalisées

Option	Description
Ajouter	Cliquez sur **Ajouter** pour ajouter une nouvelle propriété personnalisée.
Editer	Cliquez sur **Editer** pour éditer la propriété personnalisée sélectionnée.
Copier	Cliquez sur **Copier** pour copier les propriétés personnalisées sélectionnées.
Supprimer	Cliquez sur **Supprimer** pour supprimer les propriétés personnalisées sélectionnées.
Activer/Désactiver	Cliquez sur **Activer/Désactiver** pour activer ou désactiver les propriétés personnalisées sélectionnées pour l'analyse syntaxique et l'affichage des filtres de recherche ou des listes de colonne.

Procédure

1. Choisissez l'une des opérations suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Dans la zone de liste **Rechercher**, sélectionnez **Editer la recherche**.
3. Cliquez sur **Gérer les propriétés personnalisées**.
4. Sélectionnez la propriété personnalisée que vous souhaitez éditer, puis cliquez sur **Editer**.

5. Modifiez les paramètres nécessaires.
6. Facultatif. Si vous avez modifié l'expression régulière, cliquez sur **Test** pour tester l'expression régulière par rapport au contenu.
7. Cliquez sur **Sauvegarder**.

Copie d'une propriété personnalisée

Pour créer une nouvelle propriété personnalisée basée sur une propriété existante, vous pouvez copier la propriété personnalisée existante, puis modifier les paramètres.

Procédure

1. Choisissez l'une des opérations suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Dans la zone de liste **Rechercher**, sélectionnez **Editer la recherche**.
3. Cliquez sur **Gérer les propriétés personnalisées**.
4. Sélectionnez la propriété personnalisée que vous souhaitez copier, puis cliquez sur **Copier**.
5. Modifiez les paramètres nécessaires.
6. Facultatif. Si vous avez modifié l'expression régulière, cliquez sur **Test** pour la tester par rapport au contenu.
7. Cliquez sur **Sauvegarder**.

Suppression d'une propriété personnalisée

Vous pouvez supprimer une propriété personnalisée, à condition qu'elle n'ait pas de dépendance.

Procédure

1. Choisissez l'une des opérations suivantes :
   - Cliquez sur l'onglet **Activité du journal**.
   - Cliquez sur l'onglet **Activité réseau**.
2. Cliquez sur l'onglet **Activité du journal**.
3. Dans la zone de liste **Rechercher**, sélectionnez **Editer la recherche**.
4. Cliquez sur **Gérer les propriétés personnalisées**.
5. Sélectionnez la propriété personnalisée que vous souhaitez supprimer et cliquez sur **Supprimer**.
6. Cliquez sur **Oui**.

Chapitre 11. Règles

Les règles, parfois appelées règles de corrélation, sont appliquées aux événements, aux flux ou aux infractions pour rechercher ou détecter des anomalies. Si toutes les conditions d'un test sont remplies, la règle génère une réponse.

Qu'entend-t-on par règles ?

Les règles personnalisées testent les événements, les flux et les infractions afin de détecter toute activité anormale sur votre réseau. Vous pouvez créer des nouvelles règles à l'aide des combinaisons AND et OR des règles existantes. Les règles de détection des anomalies effectuent des tests sur les résultats de recherche d'événement ou de flux enregistrés comme un moyen de détecter les modèles de trafic inhabituels dans votre réseau. Ces règles nécessitent une recherche sauvegardée qui est regroupée autour d'un paramètre commun.

Les QRadar Event Collectors rassemblent des événements des sources locales et distantes, normalisent ces événements et les classent par catégories de niveau inférieur et de niveau supérieur. Pour les flux, les Collecteurs QRadar QFlow lisent les paquets du câble et reçoivent les flux des autres périphériques puis convertissent les données réseau en enregistrements de flux. Chaque processeur d'événements traite les données d'événements et de flux obtenus des QRadar Event Collectors. Les Processeurs d'événement examinent les informations et les mettent en corrélation pour indiquer les changements de comportement ou les violations de règles. Le moteur de règles personnalisées (CRE) traite les événements et les compare aux règles définies en vue de détecter des anomalies. Lorsqu'une condition de règle est remplie, le processeur d'événements génère une action qui est définie dans la réponse à la règle. Le moteur CRE effectue le suivi des systèmes impliqués dans des incidents, donne des événements aux infractions et génère des notifications.

Qu'entend-t-on par blocs de construction ?

Un bloc de construction est une collecte de tests qui ne génère aucune réponse ni aucune action.

Un bloc de construction regroupe les tests utilisés communément pour construire une logique complexe, afin de pouvoir les réutiliser dans des règles. Un bloc de construction teste souvent les adresse IP, les noms des utilisateurs privilégiés ou les collectes de noms d'événements. Par exemple, un bloc de construction peut inclure l'adresse IP de tous les serveurs DNS. Les règles peuvent ensuite utiliser ce bloc de construction.

QRadar contient des règles par défaut et vous pouvez également télécharger d'autres règles du IBM Security App Exchange pour créer de nouvelles règles.

Comment les règles fonctionnent-elles ?

Les QRadar Event Collectors rassemblent des événements des sources locales et distantes, normalisent ces événements et les classent par catégories de niveau inférieur et de niveau supérieur. Pour les flux, les Collecteurs QRadar QFlow lisent les paquets du câble et reçoivent les flux des autres périphériques puis convertissent les données réseau en enregistrements de flux. Chaque processeur

© Copyright IBM Corp. 2012, 2017

d'événements traite les données d'événements et de flux obtenus des QRadar Event Collectors. Les processeurs de flux examinent les informations et les mettent en corrélation pour indiquer les changements de comportement ou les violations de règles. Le moteur de règles personnalisées (CRE) traite les événements et les compare aux règles définies en vue de détecter des anomalies. Lorsqu'une condition de règle est remplie, le processeur d'événements génère une action qui est définie dans la réponse à la règle. Le moteur CRE effectue le suivi des systèmes impliqués dans des incidents, donne des événements aux infractions et génère des notifications.

Comment une infraction est-elle créée à partir d'une règle ?

QRadar crée une infraction lorsque des événements et/ou des flux répondent aux critères de test spécifiés dans les règles.

QRadar analyse les informations suivantes :

- Evénements et flux entrants
- Informations sur les actifs
- Vulnérabilités connues

La règle qui a créé l'infraction définit le type d'infraction.

Le magistrat classe les infractions par ordre de priorité et assigne la valeur de magnitude en fonction de plusieurs facteurs, notamment le nombre d'événements, la gravité, la pertinence et la crédibilité.

Règles personnalisées

IBM Security QRadar comprend les règles qui permettent de détecter une large gamme d'activités, comme les refus excessifs de pare-feu, les tentatives répétées de connexion ayant échoué et une éventuelle activité botnet. Vous pouvez également créer vos propres règles pour détecter une activité inhabituelle.

Qu'entend-t-on par règles personnalisées ?

Vous pouvez personnaliser les règles par défaut pour détecter des activités inhabituelles dans votre réseau.

Types de règles

Chaque type de règle d'événement, de flux, commune ou d'infraction teste les données entrantes venant de différentes sources en temps réel. Il existe plusieurs types de tests de règles. Certains vérifient des propriétés simples de l'ensemble de données. D'autres tests de règles sont plus compliqués. Ils effectuent le suivi de plusieurs séquences d'événements, de flux et d'infraction pendant une durée déterminée et utilisent un "compteur" sur un ou plusieurs paramètres avant de déclencher une réponse à la règle.

Règles d'événement
Test des données des sources de journal entrantes qui sont traitées en temps réel par le processeur d'événements QRadar. Vous pouvez créer une règle d'événement pour détecter un événement unique ou des séquences d'événements. Par exemple, vous pouvez créer une règle d'événement pour surveiller les échecs de tentatives de connexions sur votre réseau, l'accès à

plusieurs hôtes ou un événement de reconnaissance suivi d'une utilisation. Les règles d'événement créent généralement des infractions à titre de réponse.

Règles de flux
Test des données de flux entrantes traitées par le processeur de flux QRadar. Vous pouvez créer une règle de flux pour détecter un flux unique ou des séquences de flux. Les règles de flux créent généralement des infractions à titre de réponse.

Règles communes
Test des données d'événements et de flux. Par exemple, vous pouvez créer une règle commune pour détecter des événements et des flux ayant une adresse IP source spécifique. Les règles communes créent généralement des infractions à titre de réponse.

Règles d'infraction
Test des paramètres d'une infraction pour déclencher plus de réponses. Par exemple, une réponse est générée lorsqu'une infraction se produit à une date et à une heure spécifique. Une règle d'infraction traite uniquement les infractions lorsque des modifications sont réalisées sur l'infraction. Par exemple, lorsque de nouveaux événements sont ajoutés ou lorsque le système a planifié l'infraction pour une réévaluation. Il est fréquent que les règles d'infraction envoient une notification par e-mail comme réponse.

Gestion des règles

Vous pouvez créer, éditer, assigner des règles à des groupes et supprimer des groupes de règles. La catégorisation de vos règles ou les éléments structurants de vos groupes vous permettent d'afficher et de contrôler efficacement vos règles. Par exemple, vous pouvez visualiser toutes les règles relatives à la conformité.

Règles spécifiques à un domaine

Si une règle comporte un test de domaine, vous pouvez restreindre cette règle afin qu'elle ne s'applique qu'aux événements qui se produisent au sein d'un domaine spécifié. Un événement ayant une balise de domaine différente du domaine qui est défini sur la règle ne déclenche pas de réponse.

Pour créer une règle testant les conditions sur l'ensemble du système, définissez la condition de domaine sur **Tout domaine**.

Conditions de règles

La plupart des tests de règle évaluent une seule condition, comme l'existence d'un élément dans une collecte de données de référence ou le test d'une valeur par rapport à la propriété d'un événement. Pour les comparaisons complexes, vous pouvez tester des règles d'événement en créant une requête AQL (Ariel Query Language) avec les conditions de clause WHERE. Vous pouvez utiliser toutes les fonctions de la clause WHERE pour écrire des critères complexes et éviter d'avoir à exécuter un grand nombre de tests individuels. Par exemple, utilisez une clause AQL WHERE pour vérifier si le trafic SSL ou Web entrant est suivi dans un ensemble de références.

Vous pouvez exécuter des tests sur la propriété d'un événement, d'un flux ou d'une infraction, comme l'adresse IP source, la gravité de l'événement ou l'analyse du débit.

Avec des fonctions, vous pouvez utiliser des blocs de construction et d'autres règles pour créer les fonctions suivantes : multi-événement , multi flux ou multi-infraction. Vous pouvez connecter les règles en utilisant des fonctions prenant en charge les opérateurs booléens, tels que OR et AND. Par exemple, si vous souhaitez connecter des règles d'événements, vous pouvez utiliser la fonction **when an event matches any | all of the following rules**.

Création d'une règle personnalisée

IBM Security QRadar comprend les règles qui permettent de détecter une large gamme d'activités, comme les refus excessifs de pare-feu, les tentatives répétées de connexion ayant échoué et une éventuelle activité botnet. Vous pouvez également créer vos propres règles pour détecter une activité inhabituelle.

Avant de commencer

Avant de commencer à créer une nouvelle règle, vous devez obtenir le droit d'accès à **Infractions** > **Gérer les règles personnalisées**.

Pourquoi et quand exécuter cette tâche

Lorsque vous définissez des tests de règles, testez le moins de données possible. Les tests réalisés de cette manière favorisent les performances des tests de règles et évitent de créer des règles coûteuses. Pour optimiser les performances, commencez par utiliser des catégories générales qui réduisent les données évaluées par le test de règle. Par exemple, commencez par un test de règle pour un type de source de journal, un emplacement réseau, une source de flux ou un contexte spécifiques (R2L, L2R, L2L). Les tests de niveau moyen peuvent inclure des adresses IP, le trafic de port ou tout autre test associé. Les tests de contenus et d'expressions régulières doivent être le dernier test de règle.

Les règles similaires sont groupées par catégories. Par exemple, Audit, Exploit, DDoS, Recon, entre autres. Lorsque vous supprimez un élément d'un groupe, la règle ou le bloc de construction est uniquement supprimé(e) du groupe. Il reste disponible sur la page Règles. Lorsque vous supprimez un groupe, les règles ou les éléments structurants de ce groupe restent disponibles sur la page Règles.

Procédure

1. Depuis les onglets **Infractions**, **Activité du journal** ou **Activité réseau**, cliquez sur **Règles**.
2. Dans la liste **Afficher**, sélectionnez **Règles** pour créer une nouvelle règle.
3. Facultatif : Dans la liste **Afficher**, sélectionnez **Blocs de construction** pour créer une nouvelle règle à l'aide des blocs de construction.
4. Dans la liste **Actions**, sélectionnez un type de règle.

   Chaque type de règle teste les données entrantes de différentes sources en temps réel. Par exemple, les tests de règle d'événement testent les données de source de journal entrantes et les règles d'infraction testent les paramètres d'une infraction pour déclencher davantage de réponses.
5. Dans la page Editeur de pile de test de règles, volet Règle, saisissez un nom unique que vous voulez affecter à cette règle dans la zone de texte **Appliquer**.
6. Dans la zone de liste, sélectionnez **Local** ou **Global**.
   - Si vous sélectionnez **Local**, toutes les règles sont traitées sur le processeur d'événements sur lequel elles ont été reçues et des infractions sont uniquement créées pour les événements qui sont traités localement.

- Si vous sélectionnez **Global**, tous les événements correspondant sont envoyés à la console QRadar Console en vue d'être traités et par conséquent la console QRadar Console utilise une largeur de bande et des ressources de traitement plus importantes.

Détails des règles locales et globales :

Tests des règles globales

Utilisez les règles globales pour détecter des choses comme les "échecs de connexions utilisateurs multiples" lorsque les événements de cet utilisateur peuvent apparaître sur plusieurs Processeurs d'événement. Par exemple, si vous avez configuré cette règle pour 5 échecs de connexion en 10 minutes du même nom d'utilisateur, et si la règle est définie comme règle **locale**, ces 5 échecs de connexion doivent apparaître sur le même processeur d'événements. Par conséquent, si trois échecs de connexion apparaissent sur un processeur d'événements et les deux autres sur un processeur différent, aucune infraction n'est générée. Cependant, si vous avez défini cette règle sur **Global**, elle génère une infraction.

7. Dans la liste **Groupe de test**, sélectionnez un ou plusieurs tests que vous voulez ajouter à cette règle. Le moteur CRE évalue les tests de règle ligne par ligne dans l'ordre. Le premier test est évalué et lorsqu'il est vérifié, la ligne suivante est évaluée jusqu'à ce que le test final soit atteint.

   Si vous sélectionnez le test **lorsque l'événement correspond à cette requête de filtre AQL** pour une nouvelle règle d'événement, entrez une requête de clause AQL WHERE dans la zone de texte **Entrer une requête de filtre AQL**.

   En savoir plus sur l'utilisation de règles pour des événements qui ne sont pas détectés :

   Les tests de règle présentés ci-dessus peuvent être déclenchés individuellement sans que les tests de règle suivants de la même pile de tests de règle soient exécutés.

   - **lorsque le ou les événements n'ont pas été détectés par un ou plusieurs de ces types de source de journal pendant ce nombre de secondes**
   - **lorsque le ou les événements n'ont pas été détectés par une ou plusieurs de ces sources du journal pendant ce nombre de secondes**
   - **lorsque le ou les événements n'ont pas été détectés par un ou plusieurs de ces groupes de sources de journal pendant ce nombre de secondes**

   Ces tests de règle ne sont pas activés par un événement entrant mais sont activés lorsqu'un événement spécifique n'est pas détecté pendant un intervalle de temps donné configuré par vos soins. QRadar utilise une *tâche d'observation* qui demande régulièrement l'heure à laquelle l'événement a été vu pour la dernière fois et stocke cette heure pour l'événement, pour chaque source de journal. La règle est déclenchée lorsque la différence entre cette heure et l'heure actuelle est supérieure au nombre de secondes configuré dans la règle.
8. Pour exporter la règle configurée en tant qu'éléments structurants à utiliser avec d'autres règles :
9. Sur la page Réponses à la règle, configurez les réponses que vous souhaitez que cette règle génère.

   En savoir plus sur les paramètres de la page Réponse à la règle :

Tableau 48. Paramètres des pages Evénement , Flux, Règles communes et Réponse à la règle d'infraction

Paramètre	Description
Supprimer l'événement détecté	Force un événement normalement envoyé au magistrat à être envoyé à la base de données Ariel en vue d'une génération de rapport ou d'une recherche. L'événement supprimé est écrit dans l'espace de stockage et il ignore les tests sur les règles. Cet événement ne s'affiche pas sur l'onglet **Infractions**.
Attribuer le nouvel événement	Cochez cette case pour envoyer un nouvel événement en plus de l'événement ou du flux d'origine, qui est traité comme tous les autres événements du système. Attribue un nouvel événement à l'événement original et est traité comme tous les autres événements du système. Les paramètres **Attribuer le nouvel événement** s'affichent lorsque vous cochez cette case. Par défaut, la case est décochée.
Gravité	Niveau de gravité que vous souhaitez affecter à l'événement. L'intervalle est compris entre 0 (minimum) et 10 (maximum) et la valeur par défaut est 0. La gravité s'affiche dans le panneau Annotation des détails de l'événement.
Crédibilité	Crédibilité que vous souhaitez affecter à la source de journal. Par exemple, la source de journal est-elle bruyante ou coûteuse ? L'intervalle est compris entre 0 (minimum) et 10 (maximum) et la valeur par défaut est 10. La crédibilité s'affiche dans le panneau Annotation des détails de l'événement.
Pertinence	Pertinence que vous souhaitez affecter au poids de l'actif. Par exemple, l'actif a-t-il une grande importance pour vous ? L'intervalle est compris entre 0 (minimum) et 10 (maximum) et la valeur par défaut est 10. Pertinence s'affiche dans le panneau des détails de l'événement Annotation.
E-mail	Pour modifier le paramètre **Environnement local du courrier électronique**, sélectionnez **Paramètres système** sur l'onglet **Admin**.
Entrer les adresses électroniques à notifier	Utilisez des virgules pour séparer plusieurs adresses électroniques.
Alerte SNMP	Activez cette règle pour envoyer une notification SNMP (message d'alerte). La sortie de l'alerte SNMP comprend l'heure système, l'ID objet de l'alerte et les données de notification telles que définies par la base d'informations de gestion. Vous pouvez accéder à la base d'informations de gestion dans `/opt/qradar/conf/Q1LABS-MIB.txt`.

Tableau 48. Paramètres des pages Evénement , Flux, Règles communes et Réponse à la règle d'infraction (suite)

Paramètre	Description
Envoyer au SysLog local	Cochez cette case si vous souhaitez enregistrer localement l'événement ou le flux. Par défaut, cette case est décochée. **Remarque :** Seuls les événements normalisés peuvent être consignés localement sur un dispositif. Si vous souhaitez envoyer les données d'événement brutes, utilisez l'option Envoyer aux destinations de réacheminement pour envoyer les données à un hôte syslog distant.
Envoyer aux destinations de réacheminement	Cette case s'affiche uniquement pour les règles d'événement. Cochez cette case si vous voulez enregistrer l'événement ou le flux ou le transférer à une destination de réacheminement. Une destination de réacheminement est un système de fournisseur, tel que SIEM, la demande de service ou les systèmes d'alerte. Lorsque vous cochez cette case, une liste des destinations de réacheminement s'affiche. Pour ajouter, modifier ou supprimer une destination de réacheminement, cliquez sur le lien **Gérer les destinations**.
Envoyer une notification	Affiche les événements générés par cette règle dans l'élément Notifications système de l'onglet Tableau de bord. Si vous activez les notifications, configurez le paramètre **Limiteur de réponse**.
Ajouter à l'ensemble de référence	Ajoute des événements générés en tant que résultat de cette règle dans un ensemble de référence. Vous devez être un administrateur pour ajouter des données à un ensemble de référence. Pour ajouter des données à un ensemble de référence, procédez comme suit : 1. Dans la première liste, sélectionnez la propriété de l'événement ou du flux que vous souhaitez ajouter. 2. Dans la seconde liste, sélectionnez l'ensemble de référence auquel vous souhaitez ajouter les données spécifiées.
Ajouter aux données de référence	Pour utiliser cette réponse à la règle, vous devez créer la collection des données de référence.

Tableau 48. Paramètres des pages Evénement , Flux, Règles communes et Réponse à la règle d'infraction (suite)

Paramètre	Description
Retirer de l'ensemble de référence	Cochez cette case si vous souhaitez que cette règle supprime des données d'un ensemble de référence. Pour supprimer des données d'un ensemble de référence : 1. Dans la première zone de liste, sélectionnez la propriété de l'événement ou du flux que vous souhaitez supprimer. Les options incluent toutes les données normalisées ou personnalisées. 2. Dans la seconde zone de liste, sélectionnez l'ensemble de référence dont vous souhaitez supprimer les données spécifiées. La réponse à la règle **Retirer de l'ensemble de référence** fournit la fonction suivante : **Actualiser** Cliquez sur **Actualiser** pour actualiser la première zone de liste et s'assurer que la liste est à jour.
Retirer des données de référence	Pour utiliser cette réponse à la règle, vous devez avoir une collecte de données de référence.
Exécuter une action personnalisée	Vous pouvez écrire des scripts qui exécutent des actions spécifiques en réponse à des événements de réseau. Par exemple, vous pouvez écrire un script pour créer une règle de pare-feu qui bloque une adresse IP source particulière de votre réseau en réponse à des échecs répétés de tentative de connexion. Vous pouvez ajouter et configurer des actions personnalisées à l'aide de l'icône **Définir des actions** sous l'onglet **Admin**.
Publier sur le serveur IF-MAP	Si les paramètres IF-MAP sont configurés et déployés dans les paramètres du système, sélectionnez cette option pour publier les informations d'événement sur le serveur IF-MAP.
Limiteur de réponse	Configure la fréquence à laquelle vous souhaitez que cette règle réponde.
Nom de l'infraction	Si vous souhaitez que les informations de la zone **Nom d'événement** contribue au nom de l'infraction, sélectionnez l'option **Ces informations doivent contribuer au nom de l'infraction**. Si vous souhaitez que le **Nom d'événement** configuré corresponde au nom de l'infraction, sélectionnez l'option **Ces informations doivent définir ou remplacer le nom de l'infraction**.

Une notification SNMP peut se présenter comme suit :

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
 ICMP Destination Unreachable Communication with Destination Host is
 Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
 Offense description"
```

Une sortie syslog peut se présenter comme suit :

```
Sep 28 12:39:01 localhost.localdomain ECS:
 Rule 'Name of Rule' Fired: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
 1000398, Category: 1011, Notes: Event description
```

Configuration d'un événement ou d'un flux en tant que faux positif

Il peut arriver qu'un trafic réseau légitime déclenche des faux positifs de flux et d'événement qui compliquent l'identification des véritables incidents de sécurité. Vous pouvez éviter que des événements ou des flux ne soient associés à des infractions en les configurant en tant que faux positifs.

Procédure

1. Depuis les onglets **Activité du journal**, ou **Activité réseau**, cliquez sur le bouton de pause dans l'angle supérieur droit afin d'arrêter en temps réel la diffusion en flux des événements ou des flux.
2. Sélectionnez l'événement que vous souhaitez régler.
3. Cliquez sur **Faux positif**.
4. Sélectionnez une option de propriété d'événement ou de flux.
5. Sélectionnez une option de direction du trafic.
6. Cliquez sur **Optimiser**.

Résultats

L'événement ou le flux répondant aux critères spécifiés n'est plus associé à des infractions. Pour éditer l'ajustement des faux positifs, utilisez le bloc **User-BB_FalsePositive : User Defined Positive Tunings building** dans la section **Règles** de l'onglet **Infractions**.

Règles de détection des anomalies

Les règles de détection des anomalies effectuent des tests sur les résultats de recherche d'événement ou de flux enregistrés comme un moyen de détecter les modèles de trafic inhabituels dans votre réseau.

les règles de détection des anomalies nécessitent une recherche sauvegardée qui est regroupée autour d'un paramètre commun, ainsi qu'un graphique de série temporelle qui est activé. Généralement, la recherche a besoin d'accumuler des données avant que la règle d'anomalie renvoie un résultat identifiant des modèles pour les anomalies, les seuils ou les changements de comportement.

Règles d'anomalie

Ces règles testent le trafic d'événements ou de flux afin d'identifier des changements dans des événements à court terme par rapport à une période de temps plus longue. Il peut s'agir, par exemple, de nouveaux services ou de nouvelles applications qui apparaissent au sein d'un réseau, d'un serveur Web qui tombe en panne, de pare-feux qui commencent tous à refuser du trafic.

Exemple : Vous souhaitez être averti lorsque l'un de vos périphériques de pare-feu génère des rapports plus souvent que d'habitude car votre réseau peut faire l'objet d'une attaque. Vous souhaitez être averti lorsque vous recevez le double d'événement en 1 heure. Pour ceci, effectuez les étapes suivantes :

1. Créez et sauvegardez une recherche groupant par source de journal et affichant uniquement la colonne Nombre.

2. Appliquez la recherche sauvegardée à une règle d'anomalie, ajoutez le test de règle**et lorsque la valeur moyenne (par intervalle) du comptage au cours de la** dernière heure **diffère d'au moins** 100% **de la valeur moyenne (par intervalle) de la même propriété au cours des dernières** 24 heures.

Règles de seuil

Vous pouvez effectuer un test des événements ou des flux pour une activité qui ne respecte pas une plage spécifique. Utilisez ces règles pour détecter les changements d'utilisation de la bande passante dans les applications, les services défaillants, le nombre d'utilisateurs connectés à un VPN et pour la détection des gros transferts sortants.

Exemple : Un utilisateur ayant été impliqué dans un incident antérieur possède un transfert sortant élevé.

Lorsqu'un utilisateur est impliqué dans une infraction antérieure, définissez automatiquement la réponse de règle de sorte à être ajoutée au jeu de références. Si vous possédez une liste de surveillance des utilisateurs, ajoutez-les au jeu de références. Réglez les limites acceptables dans la règle de seuil.

Un jeu de référence, WatchUsers et Key:username sont requis pour votre recherche.

Effectuez la recherche suivante, puis appliquez-la à une règle de seuil.

```
select assetuser(sourceip, now()) as 'srcAssetUser',
Aplicationname(applicationid)as 'AppName', long)sum(sourcebytes
+destinationbytes)) as 'flowsum' from flows where flowdirection = 'L2R' and
REFERENCESETCONTAINS('Watchusers', username)group by 'srcAssetUser',
applicationid order by 'flowsum' desc last 24 hours
```

Règles de comportement

Ces règles testent les événements ou les flux afin d'identifier les modifications de volume qui se produisent dans des modèles réguliers afin de détecter des valeurs extrêmes. Il peut s'agir, par exemple, d'un serveur de messagerie qui comporte un relais ouvert et communique soudain avec de nombreux hôtes ou d'un IPS (système de protection contre les intrusions) qui commence à générer un grand nombre d'activités d'alerte.

Règle de comportement enregistrant le classement ou le volume d'une propriété au cours d'une saison prédéfinie. La saison définit le calendrier de comparaison de base sur lequel porte l'évaluation. Lorsque vous définissez une saison d'une semaine, le comportement de la propriété au cours de cette semaine est enregistré et vous utilisez ensuite des tests de règles pour vous avertir de tout changement.

Lorsqu'un règle de comportement est définie, les saisons sont automatiquement ajustées. Comme les données de la saison sont enregistrées et sont continuellement évaluées afin de décrire la croissance de l'entreprise au cours de la saison, vous n'avez pas besoin de modifier vos règles. Plus une règle de comportement s'exécute dans le temps, plus elle est précise. Vous pouvez ensuite régler les réponses aux règles pour capturer des changements plus subtiles.

Vous souhaitez détecter les changements se produisant au niveau du trafic ou des propriétés qui sont toujours présents, tels que le trafic de courrier, le trafic de pare-feu, les octets transférés par les protocoles communs comme le trafic du port 443 ou les application communes de votre réseau. Définissez un modèle, un type

de trafic ou un type de données que vous pouvez suivre pour générer une tendance générale ou une analyse d'historique. Assignez des tests de règles par rapport à ce modèle pour être averti en cas de conditions spéciales.

Exemple : Vous ajoutez **et lorsque l'importance du** niveau de trafic actuel **(sur une échelle de 0 à 100) est de** 70 par rapport aux tendances de trafic et au comportement appris par rapport au test de règle, le système envoie un avertissement lorsque le trafic défini dans votre délai de saison est de +70 ou -70 du comportement appris.

Le tableau suivant décrit les options des paramètres de test de la règle de comportement.

Tableau 49. Définitions des tests des règles de comportement

Paramètre de test de la règle	Description
Saison	Il s'agit de la valeur la plus importante. La saison définit le comportement de base de la propriété que vous testez, et que les autres tests de règles utilisent. Pour définir une saison, tenez compte du type de trafic que vous surveillez. Par exemple, pour le trafic réseau ou les processus qui incluent une interaction humaine, 1 semaine est une période de temps adéquate. Pour analyser les services automatisés où les modèles sont cohérents, vous pouvez créer une saison de seulement 1 jour pour définir ce modèle de comportement.
Niveau de trafic en cours	Poids des données d'origine avec changement saisonnier et erreur aléatoire prise en compte. Ce test de règle pose la question "Les données sont-elles les mêmes qu'hier à la même heure ?"
Tendance de trafic en cours	Poids des changements dans les données pour chaque intervalle de temps. Ce test de règle pose la question "Dans quelle proportion les données changent-elles si on compare cette minute à la minute précédente ?"
Comportement du trafic en cours	Poids de l'effet saisonnier pour chaque période. Ce test de règle pose la question : "Les données ont-elles augmenté dans les mêmes quantités de la semaine 2 à la semaine 3, que de la semaine 1 à la semaine 2 ?"
Valeur prédite	Utilisez les valeurs prédites pour mettre à l'échelle les lignes de base afin de rendre les avertissements plus ou moins sensibles.

Création d'une règle de détection des anomalies

Les règles de détection des anomalies testent le résultats des recherches de flux ou d'événements sauvegardées en vue d'identifier les modèles de trafic inhabituels qui se produisent dans votre réseau. Les règles de comportement testent le trafic d'événement et de flux en fonction des tendances et des niveaux de trafic

"saisonniers". Les règles de seuil teste les trafics d'événements et de flux inférieurs, égaux ou supérieurs à un seuil configuré ou compris à l'intérieur d'une plage spécifiée.

Avant de commencer

Pour créer des règles de détection des anomalies dans l'onglet **Activité du journal**, vous devez disposer des droits d'utilisation **Activité du journal Gestion de règles personnalisées**.

Pour créer des règles de détection des anomalies dans l'onglet **Activité réseau**, vous devez disposer des droits d'utilisation **Activité réseau Gestion de règles personnalisées**.

Pour gérer les règles de détection des anomalies par défaut ou les règles précédemment créées, utilisez la page **Règles** de l'onglet **Infractions**.

Pourquoi et quand exécuter cette tâche

Lorsque vous créez un règle de détection des anomalies, la règle est renseignée avec une pile de tests par défaut basée sur les critères de vos recherches sauvegardées. Vous pouvez modifier les tests par défaut ou ajouter des tests à la pile de tests. Un test **Propriété accumulée** doit être inclus dans la pile de tests au minimum.

L'option **Testez la valeur [Propriété accumulée sélectionnée] de chaque [groupe] séparément** est sélectionnée par défaut sur la page Editeur de pile de test de règles.

Une règle de détection des anomalies teste la propriété accumulée sélectionnée de chaque groupe d'événements ou de flux séparément. Par exemple, si la valeur accumulée sélectionnée est **UniqueCount(sourceIP)**, la règle test chaque adresse IP source unique de chaque groupe d'événements ou de flux.

L'option **Testez la valeur [Propriété accumulée sélectionnée] de chaque [groupe] séparément** est dynamique. La valeur **[Propriété accumulée sélectionnée]** dépend de l'option que vous sélectionnez pour la zone **ce test de propriété accumulée** de la pile de tests par défaut. La valeur **[groupe]** dépend des options de regroupement spécifiées dans les critères de recherche enregistrés. Si plusieurs options de regroupement sont incluses, le texte peut être tronqué. Placez le pointeur de votre souris sur le texte pour afficher tous les groupes.

Procédure

1. Cliquez sur l'onglet **Activité du journal** ou **Activité réseau**.
2. Effectuez une recherche agrégée.

   Vous pouvez ajouter une propriété à **grouper par** dans une nouvelle recherche d'historique ou sélectionner une propriété dans la liste **Afficher** de la page de recherche en cours.
3. Sur la page de résultat de la recherche, cliquez sur **Configurer**, puis configurez les options suivantes :
   a. Sélectionnez une propriété dans la liste **Valeur à représenter**.
   b. Sélectionnez **séries temporelles** comme type de graphique dans la liste **Valeur à représenter**
   c. Cochez la case **Capture des données de séries temporelles**.

d. Cliquez sur **Sauvegarder**, puis entrez un nom pour votre recherche.
e. Cliquez sur **OK**.
f. Sélectionnez 5 dernière minutes dans la liste **Intervalle** en attendant que le graphique des séries temporelles s'affiche.

Vous devez avoir des données de séries temporelles pour la propriété que vous avez sélectionnée dans la liste **Value to Graph** pour exécuter un test de règle sur cette propriété accumulée.

4. Dans le menu **Règles**, sélectionnez le type de règle que vous souhaitez créer.
   - Ajouter une règle d'anomalie
   - Ajouter une règle de seuil
   - Ajouter une règle de comportement
5. Sur la page Editeur de pile de test de règles, dans la zone **entrez le nom de la règle ici**, entrez un nom unique que vous souhaitez attribuer à cette règle.
6. Pour appliquer votre règle à l'aide du test par défaut, sélectionnez la première règle dans la liste **Groupe de test** des anomalies.

   Il est possible que vous ayez besoin de définir le paramètre de propriété accumulée sur la propriété que vous avez sélectionnée dans la liste **Valeur à représenter** sauvegardée dans le critère de recherche. Si vous souhaitez voir le résultat plus tôt, définissez le pourcentage sur une valeur inférieure, comme 10% par exemple. Redéfinissez **24 dernière heures** sur un intervalle moindre, comme 1 heure par exemple. Comme la détection des anomalies teste les valeurs agrégées en temps réel pour vous signaler les activités anormales sur votre réseau, vous pouvez augmenter ou diminuer les événements ou les flux sur votre trafic réseau, si vous le souhaitez.
7. Ajoutez un test à une règle.
   a. Pour filtrer les options de la liste **Groupe de test**, entrez le texte que vous souhaitez pouvoir filtrer dans la zone **Type à filtrer**.
   b. Dans la liste **Groupe de test**, sélectionnez le type de test que vous souhaitez ajouter à cette règle.
   c. Facultatif : Pour identifier un test en tant que test exclu, cliquez sur **ET** au début du test dans le panneau Règle. Le terme **ET** s'affiche comme **ET NON**.
   d. Cliquez sur les paramètres configurables soulignés pour personnaliser les variables du test.
   e. Dans la boîte de dialogue, sélectionnez les valeurs pour la variable, puis cliquez sur **Soumettre**.
8. Pour tester l'ensemble des propriétés accumulées sélectionnées de chaque groupe d'événements ou de flux, désactivez **Testez la valeur [Propriété accumulée sélectionnée] de chaque [groupe] séparément**.
9. Dans le panneau Groupes, activez les groupes auxquels vous souhaitez affecter cette règle.
10. Dans la zone **Remarques**, entrez les remarques que vous souhaitez inclure pour cette règle, puis cliquez sur **Suivant**.
11. Sur la page Réponses à la règle, configurez les réponses que vous souhaitez que cette règle génère.

Détails des paramètres de la page Réponse à la règle des règles de détection des anomalies :

Le tableau suivant fournit les paramètres de la page Réponse à la règle lorsque le type de règle est Anomalie.

Tableau 50. Paramètres de la page Réponse à la règle de détection d'anomalie

Paramètre	Description
Attribuer le nouvel événement	Indique que cette règle envoie un nouvel événement avec l'événement ou le flux d'origine qui est traité comme tous les autres événements du système. Par défaut cette case est sélectionnée et ne peut pas être décochée.
Désignation de l'infraction	Si vous souhaitez que les informations de la zone Nom d'événement soit reflété dans le nom de l'infraction, sélectionnez l'option **Ces informations doivent contribuer au nom de l'infraction ou des infractions associées**. Si vous souhaitez que le nom d'événement configuré contribue à l'infraction, sélectionnez **Ces informations doivent définir ou remplacer l'infraction ou les infractions associées**. **Remarque :** Après le remplacement du nom de l'infraction, le nom ne change pas tant que l'infraction n'est pas fermée. Par exemple, si une infraction est associée à plusieurs règles et que le dernier événement ne déclenche pas la règle configurée pour remplacer le nom de l'infraction, ce dernier n'est pas mis à jour par le dernier événement. Le nom est toujours celui défini par la règle de remplacement.
Gravité	Niveau de gravité que vous souhaitez affecter à l'événement. L'intervalle est compris entre 0 (minimum) et 10 (maximum) et la valeur par défaut est 5. Gravité s'affiche dans le panneau Annotations des détails d'événement.
Crédibilité	Crédibilité que vous souhaitez affecter à la source de journal. Par exemple, la source de journal est-elle bruyante ou coûteuse ? Dans les zones de liste, sélectionnez la crédibilité d'événement. L'intervalle est compris entre 0 (minimum) et 10 (maximum) et la valeur par défaut est 5. La crédibilité s'affiche dans le panneau Annotations des détails de l'événement.
Pertinence	Pertinence que vous souhaitez affecter au poids de l'actif. Par exemple, l'actif a-t-il une grande importance pour vous ? Dans la zone de liste, sélectionnez la pertinence de l'événement. L'intervalle est compris entre 0 (minimum) et 10 (maximum) et la valeur par défaut est 5. La pertinence s'affiche dans le panneau Annotations des détails de l'événement.
Vérifier que l'événement attribué fait partie d'une infraction	Comme résultat de cette règle, l'événement est renvoyé au magistrat. Si une infraction existe, cet événement est ajouté. Si aucune infraction n'a été créée sur l'onglet Infractions, une nouvelle infraction est créée.
Envoyer une notification	Les événements générés comme résultats de cette règle s'affichent dans l'élément Notifications système de l'onglet **Tableau de bord**. Si vous activez les notifications, configurez le paramètre **Limiteur de réponse**.

Tableau 50. Paramètres de la page Réponse à la règle de détection d'anomalie (suite)

Paramètre	Description
Envoyer au SysLog local	Cochez cette case si vous souhaitez enregistrer localement l'événement ou le flux. Par défaut, la case est décochée. **Remarque :** Seuls les événements normalisés peuvent être connectés localement sur un dispositif QRadar. Si vous souhaitez envoyer des données d'événements bruts, vous devez utiliser l'option **Envoyer aux destinations de réacheminement** pour envoyer les données à un hôte syslog distant.
Ajouter à l'ensemble de références	Ajoute des événements générés en tant que résultat de cette règle dans un ensemble de références. Vous devez être un administrateur pour ajouter des données à un ensemble de références. Pour ajouter des données à un ensemble de références, procédez comme suit : 1. Dans la première liste, sélectionnez la propriété de l'événement ou du flux que vous souhaitez ajouter. 2. Dans la seconde liste, sélectionnez l'ensemble de références auquel vous souhaitez ajouter les données spécifiées.
Ajouter aux données de référence	Pour utiliser cette réponse à la règle, vous devez créer la collection des données de référence.
Retirer de l'ensemble de références	Cochez cette case si vous souhaitez que cette règle supprime des données d'un ensemble de références. Pour supprimer des données d'un ensemble de références, procédez comme suit : 1. Dans la première liste, sélectionnez la propriété de l'événement ou du flux que vous souhaitez supprimer. 2. Dans la seconde liste, sélectionnez l'ensemble de références dont vous souhaitez supprimer les données spécifiées.
Retirer des données de référence	Pour utiliser cette réponse à la règle, vous devez avoir une collecte de données de référence.
Exécuter une action personnalisée	Vous pouvez écrire des scripts qui exécutent des actions spécifiques en réponse à des événements de réseau. Par exemple, vous pouvez écrire un script pour créer une règle de pare-feu qui bloque une adresse IP source particulière de votre réseau en réponse à des échecs répétés de tentative de connexion. Sélectionnez cette case à cocher et choisissez une action personnalisée dans la liste **Action personnalisée à exécuter**. Vous pouvez ajouter et configurer des actions personnalisées à l'aide de l'icône **Définir des actions** sous l'onglet **Admin**.
Publier sur le serveur IF-MAP	Si les paramètres IF-MAP sont configurés et déployés dans les paramètres du système, sélectionnez cette option pour publier les informations relatives à l'événement sur le serveur IF-MAP.
Limiteur de réponse	Cochez cette case puis utilisez les zones de liste pour configurer la fréquence à laquelle vous voulez que cette règle réponde.

Tableau 50. Paramètres de la page Réponse à la règle de détection d'anomalie (suite)

Paramètre	Description
Activer la règle	Cochez cette case pour activer cette règle. Par défaut, la case est cochée.

Une notification SNMP peut se présenter comme suit :

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
 ICMP Destination Unreachable Communication with Destination Host is
 Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
 Offense description"
```

Une sortie syslog peut se présenter comme suit :

```
Sep 28 12:39:01 localhost.localdomain ECS:
 Rule 'Name of Rule' Fired: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
 1000398, Category: 1011, Notes: Event description
```

12. Cliquez sur **Suivant**.
13. Cliquez sur **Terminer**.

Configuration d'une réponse à la règle pour ajouter des données à une collecte de données de référence

Définissez des règles utilisant des données de référence pour vous avertir d'une activité suspecte. Par exemple, incluez une liste d'utilisateurs privilégiés dans les données de référence puis configurez une règle qui est déclenchée pour vous avertir lorsque des anomalies se produisent sur un utilisateur privilégié.

Avant de commencer

Avant d'envoyer des données à un ensemble de références, votre administrateur QRadar doit le créer.

Pourquoi et quand exécuter cette tâche

QRadar prend en charge les types de collectes de données suivants :

Ensemble de références
Ensemble d'éléments, comme une liste d'adresses IP ou de noms d'utilisateurs, qui sont dérivés d'événements ou de flux se produisant sur votre réseau.

Mappage de références
Les données sont stockées dans des enregistrements qui mappent une clé à une valeur. Par exemple, pour corréler l'activité d'un utilisateur sur votre réseau, vous créez une mappe de référence utilisant le paramètre **Nom d'utilisateur** comme clé et l'**ID global** de l'utilisateur comme valeur.

Mappage de références d'ensembles
Les données sont stockées dans des enregistrements qui mappent une clé à plusieurs valeurs. Par exemple, pour tester l'accès autorisé à un brevet, utilisez une propriété d'événement personnalisée pour **ID brevet** comme clé et le paramètre **Nom d'utilisateur** comme valeur. Utilisez un mappage d'ensembles pour établir une liste d'utilisateurs autorisés.

Mappage de références de mappes
Les données sont stockées dans des enregistrements qui mappent une clé à une autre clé, laquelle est à son tour mappée à une valeur unique. Par exemple, pour tester les violations de la bande passante du réseau, vous créez une mappe de mappes. Utilisez le paramètre **IP source** en tant que première clé, le paramètre **Application** en tant que seconde clé et le paramètre **Nombre total d'octets** en tant que valeur.

Table de référence
Dans une table de référence, les données sont stockées dans une table qui mappe une clé à une autre clé, qui est à son tour mappée à une valeur unique. La seconde clé a un type qui lui est affecté. Ce mappage est similaire à une table de base de données où chaque colonne de la table est associée à un type. Par exemple, vous créez une table de référence qui stocke le paramètre **Nom d'utilisateur** en tant que première clé et possède plusieurs clés secondaires ayant un type assigné défini par l'utilisateur comme **Type de protocole IP** avec le paramètre **IP source** ou **Port source** comme valeur. Vous pouvez configurer une réponse à la règle pour ajouter une ou plusieurs clés définies dans la table. Vous pouvez également ajouter des valeurs personnalisées à la réponse à la règle. La valeur personnalisée doit être valide pour le type de la clé secondaire.

Procédure

1. Créez la collecte de données de référence à l'aide du widget **Gestion de l'ensemble de référence** sur l'onglet **Admin**.

   Vous pouvez également créer une collecte de données de référence à l'aide du script `ReferenceDataUtil.sh`.
2. Créez une règle à l'aide de l'assistant **Règles**.
3. Créez une réponse à la règle qui envoie des données à une collecte de données de référence. Vous pouvez ajouter les données sous forme de données partagées ou de données spécifiques au domaine.

   Détails des paramètres de Ajouter aux données de référence :

   Ajouter à une mappe de références
   Envoie des données à une collecte de paires Clé unique/Valeurs multiples. Vous devez sélectionner la clé et la valeur de l'enregistrement de données puis sélectionner la mappe de référence à laquelle vous souhaitez ajouter l'enregistrement de données.

   Ajouter à une mappe d'ensembles de référence
   Envoie des données à une collecte de paires Clé/Valeur unique. Vous devez sélectionner la clé et la valeur de l'enregistrement de données et sélectionner la mappe d'ensembles de référence à laquelle vous souhaitez ajouter l'enregistrement de données.

   Ajouter à une mappe de mappes de référence
   Envoie des données à une collecte de paires Clé multiple/Valeur unique. Vous devez sélectionner une clé pour la première mappe, une clé pour la deuxième mappe puis la valeur de l'enregistrement de données. Vous devez également sélectionner la mappe des mappes de référence auxquelles vous souhaitez ajouter l'enregistrement de données.

   Ajouter à une table de référence
   Envoie des données à une collecte de paires Clés multiples/Valeur unique, où un type a été affecté aux clés secondaires. Sélectionnez la

table de référence à laquelle vous souhaitez ajouter les données, puis sélectionnez une clé primaire. Sélectionnez vos clés internes (clés secondaires) et leurs valeurs pour les enregistrements de données.

Edition d'éléments structurants

Vous pouvez éditer l'un des blocs de construction par défaut pour l'utiliser dans plusieurs règles ou pour construire des règles ou des logiques complexes. Vous pouvez enregistrer un groupe de tests en tant que blocs de construction pour une utilisation avec des règles.

Par exemple, vous pouvez éditer le bloc de construction **BB:HostDefinition: Mail Servers** pour identifier tous les serveurs de messagerie de votre déploiement. Ensuite, vous pouvez configurer toute règle permettant d'exclure vos serveurs de messagerie des tests de règles.

Procédure

1. Cliquez sur l'onglet **Infractions** ou **Activité réseau**.
2. Cliquez sur **Règles**.
3. Dans la liste **Afficher**, sélectionnez **Blocs de construction**.
4. Cliquez deux fois sur l'élément structurant que vous souhaitez éditer.
5. Mettez à jour le bloc de construction, au besoin.
6. Cliquez sur **Suivant**.
7. Continuez à progresser dans l'assistant.
8. Cliquez sur **Terminer**.

Chapitre 12. Corrélation d'historique

Utilisez la corrélation d'historique pour exécuter les événements et les flux passés à travers le moteur de règles personnalisées (CRE) afin d'identifier les menaces ou les incidents de sécurité qui se sont déjà produits.

Restriction : Vous ne pouvez pas utiliser des corrélations d'historique dans IBM QRadar Log Manager. Pour plus d'informations sur les différences entre IBM Security QRadar SIEM et IBM QRadar Log Manager, voir «Fonctions de votre produit Security Intelligence», à la page 3.

Par défaut, un déploiement IBM Security QRadar SIEM analyse les informations qui sont collectées à partir de sources de journaux et des sources de flux en temps quasi réel. Avec la corrélation d'historique, vous pouvez corréler soit par heure de début, soit heure d'unité. L'*heure de début* est l'heure à laquelle l'événement a été reçu par QRadar. L'*Heure d'unité* est l'heure à laquelle l'événement s'est produit sur l'unité.

La corrélation d'historique peut être utile dans les situations suivantes :

Analyse des données en masse
Si vous chargez des données en masse dans votre déploiement QRadar, vous pouvez utiliser la corrélation d'historique pour corréler les données par rapport à des données qui ont été collectées en temps réel. Par exemple, pour éviter une dégradation des performances lors des heures normales, vous pouvez charger les événements à partir de plusieurs sources de journal tous les jours à minuit. Vous pouvez utiliser des corrélations d'historique pour corréler les données par heure de l'unité et afficher la séquence des événements de réseau qui se sont produits au cours des dernières 24 heures.

Test des nouvelles règles
Vous pouvez exécuter la corrélation d'historique pour tester de nouvelles règles. Par exemple, l'un de vos serveurs a été récemment attaqué par de nouveaux logiciels malveillants pour lesquels vous n'avez pas de règles en place. Vous pouvez créer une règle à tester pour ce logiciel malveillant. Ensuite, vous pouvez utiliser la corrélation d'historique pour vérifier la règle par rapport aux données d'historique et voir si la règle déclenche une réponse si celle-ci a été configurée au moment de l'attaque. De même, vous pouvez utiliser la corrélation d'historique pour déterminer quand l'attaque s'est produite en premier lieu ou la fréquence de l'attaque. Vous pouvez continuer d'optimiser la règle puis la déplacer dans un environnement de production.

Re-création de délits perdus ou purgés

Si votre système a perdu des infractions en raison d'une indisponibilité ou de toute autre raison, vous pouvez recréer les infractions en exécutant la corrélation d'historique sur des événements ou des flux arrivant dans ce délai.

Identification de menaces précédemment masquées
Dès que des informations sont connues à propos des dernières menaces de sécurité, vous pouvez utiliser la corrélation d'historique pour identifier les événements de réseau qui se sont déjà produits mais qui n'ont pas

© Copyright IBM Corp. 2012, 2017

déclenché un événement. Vous pouvez rapidement tester les menaces qui ont déjà endommagé le système ou les données de votre organisation.

Présentation de la corrélation d'historique

Vous pouvez configurer un profil de corrélation d'historique pour indiquer les données d'historique que vous voulez analyser et l'ensemble de règles que vous voulez utiliser pour le test. Lorsqu'une règle est déclenchée, une infraction est créée. Vous pouvez affecter l'infraction pour surveillance et résolution.

Sélection de données

Le profil utilise une recherche sauvegardée pour collecter les données d'événement et flux d'historique à utiliser lors de l'exécution. Assurez-vous que votre profil de sécurité accorde les droits pour l'affichage des événements et des flux que vous voulez inclure dans l'exécution de la corrélation d'historique.

Sélection et traitement des règles

La console QRadar traite les données par rapport uniquement aux règles qui sont spécifiées dans le profil de corrélation d'historique.

Les règles communes testent les données à la fois dans les événements et dans les flux. Vous devez avoir le droit d'afficher à la fois les événements et les flux avant de pouvoir ajouter des règles communes au profil. Lorsqu'un profil est édité par un utilisateur qui n'a pas le droit d'afficher les événements et les flux, les règles communes sont automatiquement retirées du profil.

Vous pouvez inclure des règles désactivées dans un profil de corrélation d'historique. Lorsque le profile s'exécute, la règle désactivée est évaluée par rapport aux événements et aux flux entrants. Si la règle est déclenchée, et si l'action de règle est de générer une infraction, l'infraction est créée même lorsque la règle est désactivée. Pour éviter de générer d'inutiles distractions, les réponses aux règles, comme la génération de rapport et les notifications par e-mail, sont ignorées pendant la corrélation d'historique.

Parce que le traitement de la corrélation d'historique se produit dans un emplacement unique, les règles qui sont incluses dans le profil sont traitées comme des règles globales. Le traitement ne modifie pas la règle de locale en globale, mais gère la règle comme si elle était globale pendant l'exécution de la corrélation d'historique. Certaines règles, telles que les règles avec état, peuvent ne pas déclencher la même réponse comme elles le feraient dans une corrélation normale qui est exécutée sur un processeur d'événements locaux. Par exemple, une règle avec état locale qui suit cinq échecs de connexion en 5 minutes, provenant du même nom d'utilisateur, se comporte différemment dans des exécutions de corrélation normale et d'historique. Dans une corrélation normale, cette règle locale gère un compteur du nombre d'échecs de connexion qui sont reçus par chaque processeur d'événements locaux. Dans la corrélation d'historique, cette règle gère un compteur unique pour l'ensemble du système QRadar. Dans cette situation, les infractions peuvent être créées différemment par rapport à une exécution de corrélation normale.

Création d'une infraction

Les exécutions de corrélation d'historique créent des fonctions uniquement lorsqu'une règle est déclenchée et que l'action de règle indique qu'une infraction

doit être créée. Une exécution de corrélation d'historique ne participe pas à une infraction en temps réel, et ne contribue pas à une infraction qui a été créée à partir d'une précédente exécution de corrélation d'historique, même si le même profil est utilisé.

Le nombre maximum d'infractions pouvant être créées par une exécution de corrélation d'historique est de 100. L'exécution de corrélation d'historique s'arrête lorsque la limite est atteinte.

Vous pouvez afficher les infractions d'historique dans le tableau de bord Surveillance des menaces et de la sécurité et sous l'onglet **Infractions** en même temps que vous affichez les infractions en temps réel.

Création d'un profil de corrélation d'historique

Vous créez un profil de corrélation d'historique pour exécuter de nouveau des événements et des flux passés à travers le moteur de règles personnalisées (CRE). Le profil comporte des informations sur l'ensemble de données et les règles à utiliser pendant l'exécution.

Restriction : Vous pouvez créer les profils d'historique dans IBM Security QRadar SIEM. Vous ne pouvez pas créer de profils d'historique dans IBM QRadar Log Manager.

Avant de commencer

Les règles communes testent les données à la fois dans les événements et dans les flux. Vous devez avoir le droit d'afficher à la fois les événements et les flux avant de pouvoir ajouter des règles communes au profil. Lorsqu'un profil est édité par un utilisateur qui n'a pas le droit d'afficher les événements et les flux, les règles communes sont automatiquement retirées du profil.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer un profil pour effectuer une corrélation par heure de début ou heure de l'unité. L'*Heure de début* est l'heure à laquelle les événements parviennent au niveau du collecteur d'événements. L'*Heure d'unité* est l'heure à laquelle l'événement s'est produit sur l'unité. Les événements peuvent être corrélés par heure de début ou heure d'unité. Les flux peuvent être corrélés par date et heure de début uniquement.

Vous pouvez inclure des règles désactivées dans le profil. Les règles qui son désactivées sont indiquées dans les listes de règles par la mention **(désactivé)** en regard u nom de règle.

Une exécution de corrélation d'historique ne participe pas à une infraction en temps réel, et ne contribue pas à une infraction qui a été créée à partir d'une précédente exécution de corrélation d'historique, même si le même profil est utilisé.

Procédure

1. Ouvrez la boîte de dialogue Corrélation d'historique.
   - Sur l'onglet **Activité du journal**, cliquez sur **Actions** > **Corrélation d'historique**.
   - Sur l'onglet **Activité réseau**, cliquez sur **Actions** > **Corrélation d'historique**.

- Sur l'onglet **Infractions**, cliquez sur **Règles** > **Actions** > **Corrélation d'historique**.

2. Cliquez sur **Ajouter** et sélectionnez **Profil d'événement** ou **Profil de flux**.
3. Entrez un nom pour le profil et sélectionnez une recherche sauvegardée. Vous pouvez utiliser uniquement des recherches sauvegardées non regroupées.
4. Sous l'onglet **Règles**, sélectionnez les règles à exécuter sur les données d'historique, puis choisissez l'heure de la corrélation.

   Si vous sélectionnez l'option **Utiliser toutes les règles activées**, vous ne pouvez pas inclure des règles désactivées dans le profil. Si vous souhaitez inclure les règles actives et inactives dans le profil, vous devez les sélectionner de manière individuelle dans la liste de règles et sélectionner **Ajouter la sélection**.
5. Sous l'onglet **Planification**, entrez l'intervalle de la recherche sauvegardée et définissez les paramètres de la planification de profil.
6. Sur l'onglet **Récapitulatif**, passez en revue la configuration et indiquez si le profil doit être exécuté immédiatement.
7. Cliquez sur **Sauvegarder**.

   Le profil est placé dans une file d'attente pour être traité. Les profils en file d'attente basés sur un planning défini sont prioritaires sur les exécutions manuelles.

Affichage des informations relatives aux exécutions de corrélation d'historique

Consultez l'historique d'un profil de corrélation d'historique pour obtenir des informations sur les exécutions passées du profil. Vous pouvez voir la liste des infractions qui ont été créées durant l'exécution et le catalogue des événements ou des flux qui correspondent aux règles déclenchées dans le profil. Vous pouvez voir l'historique des exécutions de corrélation d'historique qui sont en file d'attente, en cours d'exécution, terminées avec des erreurs et annulées.

Pourquoi et quand exécuter cette tâche

Un catalogue de corrélation d'historique est créé pour chaque règle qui est déclenchée pour chaque adresse IP source unique lors de l'exécution, même si aucune infraction n'a été créée. Le catalogue contient tous les événements ou flux qui correspondent pour tout ou partie à la règle déclenchée.

Vous ne pouvez pas générer des rapports directement à partir de données de corrélation d'historique de QRadar. Si vous souhaitez utiliser les programmes tiers pour créer des rapports, vous pouvez exporter les données depuis QRadar.

Procédure

1. Ouvrez la boîte de dialogue Corrélation d'historique.
   - Sur l'onglet **Activité du journal**, cliquez sur **Actions** > **Corrélation d'historique**.
   - Sur l'onglet **Activité réseau**, cliquez sur **Actions** > **Corrélation d'historique**.
   - Sur l'onglet **Infractions**, cliquez sur **Règles** > **Actions** > **Corrélation d'historique**.
2. Sélectionnez un profil et cliquez sur **Afficher l'historique**.
   a. Si l'état de la corrélation d'historique est **Terminé** et que l'option **Nombre d'infractions** est définie sur 0, les règles de profil n'ont déclenché aucune infraction.

b. Si la corrélation d'historique a créé des infractions, dans la colonne **Nombre d'infractions**, cliquez sur le lien pour afficher une liste des infractions qui ont été créées. Si une seule infraction a été créée, le récapitulatif des infractions s'affiche.

3. Dans la colonne **Catalogues**, cliquez sur les liens pour afficher la liste des événement qui correspondent en tout ou partie aux règles de profil.

   La colonne **Heure de début** dans la liste d'événements représente l'heure à laquelle QRadar a reçu l'événement.

4. Cliquez sur **Fermer**.

Chapitre 13. Intégration de IBM X-Force

Les experts en matière de sécurité IBM X-Force utilisent une série de centre de données internationaux pour collecter des dizaines de milliers d'exemplaires de logiciels malveillants, analyser les pages Web et les URL ainsi que pour exécuter les analyses permettant de hiérarchiser les URL et les adresses IP potentiellement malveillantes. Vous pouvez utiliser ces données pour identifier et résoudre l'activité indésirable dans votre environnement avant qu'elle ne menace la stabilité de votre réseau.

Vous pouvez, par exemple, identifier et hiérarchiser ces types d'incident :

- Une série de tentatives de connexions pour une plage dynamique d'adresses IP
- Une connexion proxy anonyme à un portail de partenaire commercial
- Une connexion entre un point de terminaison interne et une commande de réseau de zombies connue
- Une communication entre un point de terminaison et un site de distribution de logiciels malveillants connu

Centre d'informations sur les menaces Internet - Widget du tableau de bord

Le widget Centre d'informations sur les menaces Internet du tableau de bord Surveillance des menaces et de la sécurité utilise des données X-Force pour fournir les recommandations les plus récentes concernant les questions de sécurité, des évaluations de menaces quotidiennes, des informations en matière de sécurité et des référentiels de menace.

Le widget de tableau de bord utilise un flux RSS intégré pour afficher les données X-Force dans le widget de tableau de bord. La console QRadar Console doit avoir accès à Internet pour pouvoir recevoir des données du serveur de mises à jour X-Force (www.iss.net).

Le tableau de bord utilise quatre images de niveau de menace AlertCon afin de fournir un indicateur visuel du niveau de menace en cours.

Tableau 51. Niveaux de menace AlertCon

Niveau	Type	Description
1	Menaces normales	Activité ordinaire visant à compromettre les réseaux non protégés, survenant dans une période allant de quelques minutes à plusieurs heures suivant la connexion de QRadar à Internet.
2	Vigilance accrue	Vulnérabilités ou menaces en ligne pour les réseaux nécessitant une évaluation de la vulnérabilité et une action corrective.
3	Attaques ciblées	Vulnérabilités et faiblesse spécifiques constituant la cible des attaques Internet et nécessitant une action défensive immédiate.
4	Menace catastrophique	Situations de sécurité critiques dans un réseau qui exigent une action défensive immédiate et ciblée. Cette condition peut être imminente ou en cours.

© Copyright IBM Corp. 2012, 2017

Pour plus d'informations sur le niveau menace en cours, cliquez sur le lien **En savoir plus** pour ouvrir la page des activités de menace en cours sur le site Web IBM X-Force Exchange.

Pour afficher un récapitulatif des recommandations en cours, cliquez sur la flèche en regard de la recommandation. Pour examiner l'intégralité de la recommandation, cliquez sur le lien associé.

Application IBM Security Threat Content

L'application IBM Security Threat Content disponible dans IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub) contient des règles, des blocs de construction et des propriétés personnalisées conçus pour une utilisation avec X-Force.

Les données X-Force incluent une liste des URL et des adresses IP potentiellement malveillantes avec un score de menace correspondant. Utilisez les règles X-Force pour marquer automatiquement les données d'activité réseau ou d'événement de sécurité qui impliquent les adresses et pour hiérarchiser les incidents avant de commencer à les examiner.

La liste suivante présente des exemples d'incident que vous pouvez identifier en utilisant les règles X-Force :

- **when the *[source IP | destinationIP | anyIP]* is part of any of the following *[remote network locations]***
- **when *[this host property]* is categorized by X-Force as *[Anonymization Servers | Botnet C&C | DynamicIPs | Malware | ScanningIPs | Spam]* with confidence value *[equal to] [this amount]***
- **when *[this URL property]* is categorized by X-Force as *[Gambling | Auctions | Job Search | Alcohol | Social Networking | Dating]***

L'administrateur QRadar doit installer l'application IBM Security Threat Content pour que les règles s'affichent dans le groupe **Menaces** dans la fenêtre Liste de règles. Pour pouvoir utiliser les règles, il est nécessaire de les activer.

Activation des règles X-Force dans IBM Security QRadar

Lorsque vous ajoutez l'application IBM Security Threat Content à votre système QRadar, les règles X-Force sont automatiquement ajoutées à la Liste de règles. Pour pouvoir utiliser les règles, il est nécessaire de les activer.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Dans la barre d'outils, cliquez sur **Règles** > **Règles**.
3. Dans le menu **Groupe**, cliquez sur **Menaces**.

   La colonne **Groupe** affiche peut-être les règles existantes et les règles étendues. Par défaut, les règles X-Force existantes sont désactivées. Vous pouvez cependant voir des règles existantes qui sont activées. Utilisez les nouvelles règles étendues dans le groupe **Menaces** et non les règles existantes qui utilisent les réseaux éloignés.
4. Sélectionnez les règles **X-Force** dans le groupe **Menaces** puis cliquez sur **Actions** > **Activer/Désactiver**.

Catégories d'adresses IP et d'URL

X-Force Threat Intelligence catégorise les informations relatives aux adresses IP et aux URL.

Les adresses IP sont regroupées dans les catégories suivantes :

- Hôtes de logiciels malveillants
- Sources de courriers indésirables
- Adresses IP dynamiques
- Proxys anonymes
- Commande de réseau de zombies
- Numérisation d'adresses IP

Le flux X-Force Threat Intelligence catégorise également les adresses URL. Par exemple, les adresses URL peuvent être catégorisées comme sites de rencontre, de jeux d'argent ou de pornographie. Pour afficher une liste complète des catégories de la classification d'URL, reportez-vous au site Web IBM X-Force Exchange (https://exchange.xforce.ibmcloud.com/faq).

Recherche d'informations sur les adresses IP et les URL dans X-Force Exchange

Utilisez les options du menu contextuel dans IBM Security QRadar pour rechercher des informations sur les adresses IP et les URL qui se trouvent sur IBM Security X-Force Exchange. Vous pouvez utiliser les informations de vos recherches, infractions et règles QRadar pour rechercher des informations supplémentaires ou pour ajouter des informations sur les adresses IP ou des URL à une collection X-Force Exchange.

Pourquoi et quand exécuter cette tâche

Vous pouvez apporter des informations publiques ou privées pour suivre les données dans des collections lorsque vous recherchez des problèmes de sécurité.

Une *collection* est un référentiel où vous stockez les informations qui sont trouvées au cours d'une étude. Vous pouvez utiliser une collection pour enregistrer des rapports, des commentaires X-Force Exchange ou tout autre contenu. Un rapport X-Force Exchange contient à la fois une version du rapport à partir du moment où il a été enregistré, et un lien vers la version actuelle du rapport. La collection contient une section avec un bloc-notes sous forme de wiki dans lequel vous pouvez ajouter des commentaires relatifs à la collection.

Pour plus d'informations sur X-Force Exchange, voir X-Force Exchange (https://exchange.xforce.ibmcloud.com/).

Procédure

1. Pour rechercher une adresse IP dans X-Force Exchange à partir de QRadar, procédez comme suit :
   a. Sélectionnez l'onglet **Activité du journal** ou **Activité réseau**.
   b. Faites un clic droit sur l'adresse IP que vous voulez visualiser dans X-Force Exchange et sélectionnez **Options supplémentaires** > **Options de plug-in** > **X-Force Exchange Lookup** pour ouvrir l'interface X-Force Exchange.
2. Pour rechercher une adresse URL dans X-Force Exchange à partir de QRadar, procédez comme suit :

a. Sélectionnez l'onglet **Infractions** ou les fenêtres de détails d'événement disponibles sur l'onglet **Infractions**.
b. Cliquez avec le bouton droit sur l'URL que vous souhaitez rechercher dans X-Force Exchange et sélectionnez **Options de plug-in > X-Force Exchange Lookup** pour ouvrir l'interface X-Force Exchange.

Création d'une règle de catégorisation pour surveiller l'accès à certains types de site Web

Vous pouvez créer une règle envoyant une notification par courrier électronique si les utilisateurs du réseau interne accèdent à des adresses URL classées comme sites Web associés à des jeux d'argent.

Avant de commencer

Pour utiliser des données X-Force dans des règles, votre administrateur doit configurer QRadar afin qu'il charge des données à partir des serveurs X-Force.

Pour créer une règle, vous devez disposer des droits **Infractions** > **Gestion de règles personnalisées**.

Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Dans le menu de navigation, cliquez sur **Règles**.
3. Dans la zone de liste **Actions**, sélectionnez **Nouvelle règle d'événement**.
4. Lisez le texte d'introduction de l'assistant Règle et cliquez sur **Suivant**.
5. Cliquez sur **Evénements**, puis sur **Suivant**.
6. Dans la zone de liste **Groupe de test**, sélectionnez **X-Force Tests**.
7. Cliquez sur le signe plus (+) en regard du test indiquant **quand l'URL (personnalisée) est classée par X-Force comme l'une des catégories suivantes**.
8. Dans la zone **entrez le nom de la règle ici** du volet Règle, entrez le nom unique que vous souhaitez affecter à cette règle.
9. Dans la zone de liste, sélectionnez **Local** ou **Global**.
10. Cliquez sur les paramètres configurables soulignés pour personnaliser les variables du test.
    a. Cliquez sur **URL (personnalisé)**.
    b. Sélectionnez la propriété d'URL contenant l'adresse URL qui a été extraite du contenu et cliquez sur **Soumettre**.
    c. Cliquez sur **l'une des catégories suivantes**.
    d. Sélectionnez **Jeux d'argent / Loterie** dans les catégories d'URL X-Force, puis cliquez sur **Ajouter +** et sur **Soumettre**.
11. Pour exporter la règle configurée en tant que bloc de construction à utiliser avec d'autres règles :
    a. Cliquez sur **Exporter sous forme de bloc de construction**.
    b. Entrez un nom unique pour ce bloc de construction.
    c. Cliquez sur **Sauvegarder**.
12. Dans le volet Groupes, cochez les cases des groupes auxquels vous souhaitez affecter cette règle.
13. Dans la zone **Remarques**, entrez la remarque que vous souhaitez ajouter à cette règle, puis cliquez sur **Suivant**.

14. Sur la page Réponses à la règle, cliquez sur **E-mail** et entrez les adresses e-mail recevant la notification.
15. Cliquez sur **Suivant**.
16. Si la règle est correcte, cliquez sur **Terminer**.

Facteur de fiabilité et réputation de l'adresse IP

Les données de réputation de l'adresse IP sont évaluées en fonction de l'heure de détection et du volume de messages ou de données. X-Force classifie les données de réputation d'adresse IP et affecte une valeur de facteur de fiabilité comprise entre 0 et 100 (0 = aucune fiabilité et 100 = fiabilité maximale). Par exemple, X-Force peut catégoriser une adresse IP source comme IP de numérisation avec un facteur de fiabilité de 75, ce qui est un niveau de fiabilité modérément élevé.

Détermination d'un seuil

A titre d'exemple, les spams présentant une entrée de réputation d'adresse IP de 0 indiquent que le trafic d'adresse IP source ne constitue pas un spam, alors qu'une entrée de 100 indique un trafic spam certain. Par conséquent, une valeur inférieure à 50 indique que le message a une faible probabilité d'être un spam et une valeur supérieure à 50 indique que le message a plus de probabilité d'être un spam. Une valeur de 50 ou plus correspond à la limite à partir de laquelle vous pouvez considérer d'intervenir sur une règle déclenchée.

Ces probabilités sont basées sur des données Web en cours que IBM Security X-Force Threat Intelligence collecte et analyse en continu de par le monde dans les centres de données X-Force. Alors que les données sont collectées, le système évalue combien de spams sont reçus d'une adresse IP particulière ou avec quelle fréquence l'adresse IP signalée se trouve dans la catégorie de la réputation d'adresse IP. Plus le nombre d'apparitions est élevé, plus le facteur de fiabilité est défini à la hausse par le système.

Réglage des faux positifs à l'aide de la définition du facteur de fiabilité

Utilisez le facteur de fiabilité pour limiter le nombre d'infractions créées par les règles déclenchées. Suivant le niveau de protection souhaité, vous pouvez régler les valeurs de fiabilité sur le niveau qui correspond le mieux à votre environnement réseau.

Pourquoi et quand exécuter cette tâche

Lorsque vous ajustez des règles, envisagez une échelle où 50 est le point critique. Sur les actifs ayant une importance moindre, vous pouvez pondérer une règle X-Force afin qu'elle se déclenche à un facteur de fiabilité plus élevé pour certaines catégories, par exemple pour les spams. Par exemple, si vous définissez une règle en attribuant un facteur de fiabilité de 75, la règle sera uniquement déclenchée lorsque X-Force détectera une adresse IP avec un facteur de fiabilité égal ou supérieur à 75. Ce réglage réduit le nombre d'infractions générées sur les systèmes de faible priorité et sur les actifs non critiques. Par contre, un système important ou un actif métier critique avec un facteur de fiabilité de 50 déclenche une infraction à un niveau inférieur et attire plus rapidement l'attention sur un problème.

Pour votre zone démilitarisée, sélectionnez une valeur de fiabilité supérieure, comme 95% ou plus. Le nombre d'infractions à examiner n'est pas élevé dans cette

zone. Avec un niveau de fiabilité élevé, les adresses IP sont plus susceptibles de correspondre à la catégorie affichée. S'il est certain à 95% qu'un hôte héberge des logiciels malveillants, vous devez en être informé.

Pour les zones du réseau plus sécurisées, comme un pool de serveurs par exemple, réduisez la valeur de fiabilité. Le nombre de menaces potentielles identifiées est supérieur et l'examen est moins étendu car la menace appartient à un segment de réseau spécifique.

Pour un réglage optimum des faux positif, gérez vos déclencheurs de règle par segment. Explorez votre infrastructure réseau et décidez quels actifs ont besoin d'un niveau de protection supérieur. Vous pouvez appliquer différentes valeurs de fiabilité pour les différents segments de réseau. Utilisez les blocs de construction pour grouper les tests utilisés communément pour les utiliser dans des règles.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Dans la barre d'outils, cliquez sur **Règles** > **Règles**.
3. Cliquez deux fois sur une règle pour démarrer l'assistant de création de règle.
4. Dans la zone de filtre, entrez le texte suivant :

   ```
   when this host property is categorized by X-Force as this category with
   confidence value equal to this amount
   ```
5. Cliquez sur l'icône **Ajouter un test à la règle (+)**.
6. Dans la section Règle, cliquez sur le lien `this amount`.
7. Entrez une valeur de fiabilité.
8. Cliquez sur **Soumettre**.
9. Cliquer sur **Terminer** pour sortir de l'assistant de création de règle.

Recherche de données dans IBM X-Force Exchange avec des critères de recherche avancés

Pour les requêtes complexes, vous pouvez rechercher et filtrer des données dans X-Force Exchange à l'aide des expressions de recherche avancée.

Pourquoi et quand exécuter cette tâche

Les recherches avancées renvoient les données de l'onglet **Activité du journal** ou de l'onglet **Activité réseau** dans QRadar.

Les recherches d'URL ne peuvent pas être renvoyées de l'onglet **Activité réseau** car les informations sur l'URL sont fournies par les données d'événement.

Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Sur la barre d'outils **Rechercher**, sélectionnez **Recherche avancée**.
3. Entrez une expression de requête AQL.

   En savoir plus sur les expressions de recherche :

   Le tableau suivant décrit quelques expressions de recherche communes.

Tableau 52. Expressions de recherche avancées X-Force

Description	Exemple
Recherches d'adresses IP source ayant un facteur de fiabilité supérieur à 50.	`select * from events where XFORCE_IP_CONFIDENCE('Spam',sourceip)>50`
Recherches associées à un URL.	`select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL`
Recherches associées à une adresse IP source.	`select sourceip, XFORCE_IP_CATEGORY(sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL`

4. Cliquez sur **Rechercher**.

Chapitre 14. Gestion de rapports

L'onglet **Rapports** vous permet de créer, éditer, distribuer et gérer des rapports.

Des options de rapports flexibles détaillées permettent de satisfaire diverses normes de réglementation, telles que la conformité PCI.

Vous pouvez créer vos propres rapports personnalisés ou utiliser un rapport par défaut. Vous pouvez personnaliser et rebaptiser les rapports par défaut puis les distribuer à d'autres utilisateurs.

L'onglet **Rapports** peut nécessiter une longue période de temps pour s'actualiser si votre système inclut plusieurs rapports.

Remarque : Si vous utilisez Microsoft Exchange Server 5.5, les caractères de police non disponibles peuvent être affichés dans la ligne d'objet des rapports envoyés par e-mail. Pour résoudre ce problème, téléchargez et installez le Service Pack 4 de Microsoft Exchange Server 5.5. Pour plus d'informations, contactez le support Microsoft.

Considérations relatives aux fuseaux horaires

Afin de garantir que la fonction Rapports utilise la date et l'heure correctes pour le rapport de données, votre session doit être synchronisée avec votre fuseau horaire.

Lors de l'installation et de la configuration des produits QRadar, le fuseau horaire est configuré. Vérifiez auprès de votre administrateur que votre session QRadar est bien synchronisée avec votre fuseau horaire.

Autorisations de l'onglet Rapports

Les administrateurs peuvent afficher tous les rapports créés par d'autres utilisateurs.

Les utilisateurs non administrateurs peuvent afficher les rapports qu'ils ont créés uniquement ou les rapports partagés par les autres utilisateurs.

Paramètres de l'onglet Rapport

L'onglet **Rapports** affiche une liste de rapports personnalisés par défaut.

Dans l'onglet **Rapports**, vous pouvez visualiser des informations statistiques sur le modèle de rapports, effectuer des actions sur les modèles de rapports, afficher les rapports générés et supprimer le contenu généré.

Si un rapport n'indique pas une planification par intervalle, vous devez générer manuellement le rapport.

Vous pouvez pointer votre souris sur un rapport pour prévisualiser un résumé du rapport dans une infobulle. Le résumé indique la configuration du rapport et le type de contenu que génère le rapport.

© Copyright IBM Corp. 2012, 2017

Présentation de rapport

Un rapport peut être constitué de plusieurs éléments de données et peut représenter un réseau et des données de sécurité dans une variété de styles, tels que des tableaux, des graphiques linéaires, des graphiques circulaires et des histogrammes.

Lorsque vous sélectionnez l'agencement d'un rapport, considérez le type de rapport que vous souhaitez créer. Par exemple, ne choisissez pas un petit conteneur de tableau pour un contenu graphique qui affiche un plusieurs objets. chaque graphique comprend une légende et une liste de réseaux dont le contenu est dérivé, choisissez un conteneur assez grand pour contenir les données. Pour prévisualiser comment chaque graphique affiche un ensemble de données, voir Graph types.

Types de graphique

Lorsque vous créez un rapport, vous devez choisir un type de graphique pour chaque graphique que vous y ajoutez.

Le type de graphique détermine la façon dont les données et les objets réseau sont présentés dans le rapport.

Vous pouvez utiliser tous les types de graphique suivants :

Tableau 53. Types de graphique

Type de graphique	Description
Aucun	Utilisez cette option pour créer un espace blanc dans votre rapport. Si vous sélectionnez l'option Aucun pour tout conteneur, aucune configuration supplémentaire n'est nécessaire pour ce conteneur.
Vulnérabilités des actifs	Utilisez cette option pour afficher les données de vulnérabilité pour chaque actif défini dans votre déploiement. Vous pouvez générer des graphiques de vulnérabilité de l'actif lorsque les vulnérabilités ont été détectées par une analyse VA. Ce graphique est disponible après avoir installé IBM Security QRadar Vulnerability Manager.
Connexions	Cette option s'affiche uniquement si vous avez acheté et mis sous licence IBM Security QRadar Risk Manager. Pour plus d'informations, voir *IBM Security QRadar Risk Manager - Guide d'utilisation*.
Règles de périphérique	Cette option s'affiche uniquement si vous avez acheté et mis sous licence IBM Security QRadar Risk Manager. Pour plus d'informations, voir *IBM Security QRadar Risk Manager - Guide d'utilisation*.
Objets non utilisés du périphérique	Cette option s'affiche uniquement si vous avez acheté et mis sous licence IBM Security QRadar Risk Manager. Pour plus d'informations, voir *IBM Security QRadar Risk Manager - Guide d'utilisation*.

Tableau 53. Types de graphique (suite)

Type de graphique	Description
Evénements/Journaux	Utilisez cette option pour afficher des informations liées à un événement. Vous pouvez baser un graphique sur des données provenant des recherches enregistrées dans l'onglet **Activité du journal**. Vous pouvez configurer le graphique pour tracer des données sur une période de temps configurable afin de détecter les tendances d'événement. Pour plus d'informations sur les recherches enregistrées, voir Recherches de données.
Sources de journal	Utilisez cette option pour exporter ou générer des rapports sur des sources de journal. Sélectionnez les sources de journal et les groupes de sources de journal qui doivent figurer dans le rapport. Triez les sources de journal par colonnes de rapport. Incluez les sources de journal pour lesquelles aucun rapport n'a été généré pendant une période définie. Incluez les sources de journal qui ont été créées à un moment donné.
Flux	Utilisez cette option pour afficher des informations liées aux flux. Vous pouvez baser un graphique sur des données provenant des recherches enregistrées dans l'onglet **Activité réseau**. Vous pouvez configurer le graphique pour tracer des données de flux sur une période de temps configurable afin de détecter les tendances de flux. Pour plus d'informations sur les recherches enregistrées, voir Recherches de données.
IP cibles de référence	Utilisez cette option pour afficher la destination principale des adresses IP dans les emplacements réseau que vous sélectionnez.
Principales infractions	Utilisez cette option pour afficher les infractions principales qui se produisent à l'heure actuelle pour les emplacements réseau que vous sélectionnez.
Infractions au fil du temps	Utilisez cette option pour afficher toutes les infractions dont l'heure de début figure dans un intervalle de temps défini pour les emplacements réseau que vous sélectionnez.
IP sources de référence	Utilisez cette option pour afficher et trier les sources d'infractions principales (adresses IP) qui attaquent votre réseau ou les actifs de l'entreprise.

Tableau 53. Types de graphique (suite)

Type de graphique	Description
Vulnérabilités	L'option Vulnérabilités s'affiche uniquement si IBM Security QRadar Vulnerability Manager a été acheté et mis sous licence. Pour plus d'informations, voir *IBM Security QRadar Vulnerability Manager - Guide d'utilisation*.

Tableau 54. Types de graphique

Type de graphique	Description
Aucun	Utilisez cette option pour créer un espace blanc dans votre rapport. Si vous sélectionnez l'option Aucun pour tout conteneur, aucune configuration supplémentaire n'est nécessaire pour ce conteneur.
Vulnérabilités des actifs	Utilisez cette option pour afficher les données de vulnérabilité pour chaque actif défini dans votre déploiement. Vous pouvez générer des graphiques de vulnérabilité de l'actif lorsque les vulnérabilités ont été détectées par une analyse VA. Ce graphique est disponible après avoir installé IBM Security QRadar Vulnerability Manager.
Vulnérabilités	L'option Vulnérabilités s'affiche uniquement si IBM Security QRadar Vulnerability Manager a été acheté et mis sous licence. Pour plus d'informations, voir *IBM Security QRadar Vulnerability Manager - Guide d'utilisation*.

Barre d'outils de l'onglet Rapport

Vous pouvez utiliser la barre d'outils pour effectuer un certain nombre d'actions sur les rapports.

Le tableau suivant identifie et décrit les options de la barre d'outils Rapports.

Tableau 55. Options de la barre d'outils Rapports

Option	Description
Groupe	
Gérer les groupes	Cliquez sur **Gérer les groupes** pour gérer des groupes de rapports. Grâce à la fonction Gérer les groupes, vous pouvez organiser vos rapports en groupes fonctionnels. Vous pouvez partager des groupes de rapports avec d'autres utilisateurs.

Tableau 55. Options de la barre d'outils Rapports (suite)

Option	Description
Actions	Cliquez sur **Actions** pour effectuer les actions suivantes : • **Créer** - Sélectionnez cette option afin de créer un nouveau rapport. • **Editer** - Sélectionnez cette option afin d'éditer le rapport sélectionné. Vous pouvez également cliquer deux fois sur un rapport afin d'éditer son contenu. • **Dupliquer** - Sélectionnez cette option pour dupliquer ou renommer le rapport sélectionné. • **Affecter des groupes** - Sélectionnez cette option afin d'affecter le rapport sélectionné à un groupe de rapports. • **Partager** - Sélectionnez cette option afin de partager le rapport sélectionné avec d'autres utilisateurs. Vous devez disposer de privilèges administratifs afin de partager des rapports. • **Basculer la planification** - Sélectionnez cette option afin de basculer le rapport sélectionné vers l'état Actif ou Inactif. • **Exécuter le rapport** - Sélectionnez cette option afin de générer le rapport sélectionné. Pour générer plusieurs rapports, maintenez la touche de contrôle enfoncée et cliquez sur le rapport que vous souhaitez générer. • **Exécuter le rapport sur des données brutes** - Sélectionnez cette option afin de générer le rapport sélectionné à l'aide de données brutes. Cette option est utile lorsque vous souhaitez générer un rapport avant que les données accumulées nécessaires ne soient disponibles. Par exemple, si vous voulez exécuter un rapport hebdomadaire avant qu'une semaine entière ne se soit écoulée depuis que vous avez créé le rapport, vous pouvez générer le rapport à l'aide de cette option. • **Supprimer le rapport**- Sélectionnez cette option afin de supprimer le rapport sélectionné. Pour supprimer plusieurs rapports, maintenez la touche de contrôle enfoncée et cliquez sur les rapports que vous souhaitez supprimer. • **Supprimer le contenu généré** - Sélectionnez cette option afin de supprimer tous les contenus générés pour les lignes sélectionnées. Pour supprimer plusieurs rapports générés, maintenez la touche de contrôle enfoncée et cliquez sur les rapports générés que vous souhaitez supprimer.

Tableau 55. Options de la barre d'outils Rapports (suite)

Option	Description
Masquer les rapports inactifs	Sélectionnez cette case afin de masquer les modèles de rapports inactifs. L'onglet **Rapports** s'actualise automatiquement et affiche uniquement les rapports actifs. Décochez la case afin d'afficher les rapports inactifs masqués.
Rechercher des rapports	Entrez vos critères de recherche dans la zone **Rechercher des rapports** puis cliquez sur l'icône **Rechercher des rapports**. Une recherche est effectuée concernant les paramètres suivants pour déterminer lequel correspond à vos critères spécifiés : • Titre du rapport • Description du rapport • Groupe de rapports • Groupes de rapports • Nom d'utilisateur de l'auteur du rapport

Types de graphique

Chaque type de graphique prend en charge divers types de graphique que vous pouvez utiliser pour afficher des données.

Les fichiers de configuration de réseau déterminent les couleurs que les tableaux utilisent pour représenter le trafic réseau. Chaque adresse IP est représentée à l'aide d'une couleur unique. Le tableau suivant donne des exemples sur la manière dont les données réseau et de sécurité sont utilisées dans les graphiques. Le tableau décrit les types de graphique disponibles pour chaque type de graphique.

Tableau 56. Types de graphique

Types de graphique	Types de graphique disponibles
Ligne	• Evénements/Journaux • Flux • Connexions • Vulnérabilités
Courbes superposées	• Evénements/Journaux • Flux • Connexions • Vulnérabilités
Barre	• Evénements/Journaux • Flux • Connexions des vulnérabilités des actifs • Connexions • Vulnérabilités

Tableau 56. Types de graphique (suite)

Types de graphique	Types de graphique disponibles
Barre horizontale	• IP sources de référence • Principales infractions • Infractions au fil du temps • IP cibles de référence
Barres empilées	• Evénements/Journaux • Flux • Connexions
Graphique circulaire	• Evénements/Journaux • Flux • Vulnérabilités des actifs • Connexions • Vulnérabilités
Tableau	• Evénements/Journaux • Flux • IP sources de référence • Principales infractions • Infractions au fil du temps • IP cibles de référence • Connexions • Vulnérabilités Pour afficher le contenu d'un tableau, vous devez concevoir le rapport avec un conteneur de largeur pleine page.
Table d'agrégation	Disponible avec le graphique Vulnérabilités des actifs. Pour afficher le contenu d'un tableau, vous devez concevoir le rapport avec un conteneur de largeur pleine page.

Les types de graphiques suivants sont disponibles pour les rapports QRadar Log Manager :

- Ligne
- Courbes superposées
- Barre
- Barres empilées
- Graphique circulaire
- Tableau

Remarque : Lorsque vous créez des rapports sous forme de graphique à barres ou de graphique à barres empilées, le format de la légende est fixe. Les barres ou les sections à barres sont alors représentées par des libellés codés en couleur dans la plupart des cas. Si vous sélectionnez la durée comme valeur pour l'axe des X, vous pouvez créer des intervalles de temps sur l'axe des X.

Création de rapports personnalisés

L'assistant de création de rapports vous permet de créer et de personnaliser un nouveau rapport.

Avant de commencer

Vous devez disposer des autorisations réseau appropriées pour partager les rapports générés avec d'autres utilisateurs.

Pour plus d'informations sur les autorisations, voir *IBM Security QRadar Administration Guide*.

Pourquoi et quand exécuter cette tâche

L'assistant de création de rapports fournit un guide étape par étape sur la conception, la planification et la génération des rapports.

L'assistant utilise les éléments clés suivants permettant de vous aider à créer un rapport :

- **Présentation** - Position et taille de chaque conteneur
- **Conteneur** - Marque de réservation du contenu proposé
- **Contenu** - Définition du graphique placé dans le conteneur

Après avoir créé un rapport qui est généré hebdomadairement ou mensuellement, la date prévue doit être écoulée avant que le rapport généré renvoie des résultats. Pour un rapport planifié, vous devez attendre l'heure planifiée pour l'élaboration des résultats. Par exemple, une recherche hebdomadaire nécessite sept jours pour l'élaboration des données. Cette recherche renvoie des résultats après un délai de 7 jours.

Lorsque vous spécifiez le format de sortie du rapport, n'oubliez pas que la taille du fichier des rapports générés peut être d'un ou de deux mégaoctets, en fonction du format de sortie sélectionné. Le format PDF est de taille plus réduite et n'occupe pas une grande quantité d'espace de stockage sur le disque.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Dans la zone de liste **Actions**, sélectionnez **Créer**.
3. Dans la fenêtre Bienvenue dans l'assistant de création de rapports !, cliquez sur **Suivant**.
4. Sélectionnez l'une des options suivantes :

Option	Description
Manuelle	Par défaut, le rapport est généré une fois. Vous pouvez générer le rapport aussi souvent que vous le voulez.
Horaire	Planifie la génération du rapport pour la fin de chaque heure. Les données de l'heure précédente sont utilisées. Dans les zones de liste, sélectionnez une période pour indiquer le début et la fin du cycle de génération de rapports. Un rapport est généré à chaque heure de cette période. Il est possible de sélectionner une heure par incréments d'une demi-heure. La valeur par défaut est 1:00 a.m pour les zones **De** et **A**.

Option	Description
Quotidienne	Planifie le rapport à générer à la fin de chaque journée. Les données de la veille sont utilisées. Dans les zones de liste, sélectionnez l'heure et les jours de la semaine au cours desquels vous souhaitez exécuter le rapport.
Hebdomadaire	Planifie la génération de rapports hebdomadaires à l'aide des données de la semaine précédente. Sélectionnez le jour de votre choix pour générer le rapport. La valeur par défaut est le lundi. Dans la zone de liste, sélectionnez l'heure de début du cycle de génération de rapports. Il est possible de sélectionner une heure par incréments d'une demi-heure. La valeur par défaut est 1:00 a.m.
Mensuelle	Planifie la génération de rapports mensuels à l'aide des données du mois précédent. Dans la zone de liste, sélectionnez la date à laquelle vous souhaitez générer le rapport. La valeur par défaut est le premier jour du mois. Sélectionnez l'heure de début du cycle de génération de rapports. Il est possible de sélectionner une heure par incréments d'une demi-heure. La valeur par défaut est 1:00 a.m.

5. Dans le volet **Autoriser la génération manuelle de ce rapport**, sélectionnez **Oui** ou **Non**.
6. Configurez la présentation de votre rapport :
   a. Dans la liste **Orientation**, sélectionnez **Portrait** ou **Paysage** pour l'orientation de la page.
   b. Sélectionnez l'une des six options d'agencement affichées dans l'assistant de création de rapports.
   c. Cliquez sur **Suivant**.
7. Indiquez des valeurs des paramètres suivants :

Paramètre	Valeurs
Titre du rapport	Ce titre peut comporter jusqu'à 100 caractères. N'utilisez pas de caractères spéciaux.
Logo	Dans la zone de liste, sélectionnez un logo.
Options de pagination	Dans la zone de liste, sélectionnez un emplacement pour les numéros de page à afficher dans le rapport. Vous pouvez choisir de ne pas afficher des numéros de page.

Paramètre	Valeurs
Classification de rapports	Entrez une classification pour ce rapport. Vous pouvez entrer jusqu'à 75 caractères. Vous pouvez utiliser les espaces de début, des caractères spéciaux, et les caractères sur deux octets. La classification de rapport s'affiche dans l'en-tête et le pied de page du rapport. Vous pouvez classifier votre rapport comme `confidentiel`, `hautement confidentiel`, `sensible`, ou `interne`.

8. Configurez chaque conteneur du rapport :
   a. Dans la zone de liste **Type de graphique**, sélectionnez un type de graphique.
   b. Sur la fenêtre Détails de conteneur, configurez les paramètres de graphique.

      Remarque : Vous pouvez également créer des recherches sauvegardées de l'actif. Dans la zone de liste **Recherche à utiliser**, sélectionnez votre recherche sauvegardée.
   c. Cliquez sur **Sauvegarder les détails du conteneur**.
   d. Si vous avez sélectionné plus d'un conteneur, répétez les étapes a à c.
   e. Cliquez sur **Suivant**.
9. Prévisualisez la page Aperçu de la disposition, puis cliquez sur **Suivant**.
10. Cochez les cases correspondant aux formats de rapport que vous voulez générer, puis cliquez sur **Suivant**.

    Important : Le langage XML est disponible uniquement pour les tableaux.
11. Sélectionnez les canaux de distribution de votre rapport, puis cliquez sur **Suivant**. Les options incluent les canaux de distribution suivants :

Option	Description
Console de rapports	Cochez cette case pour envoyer le rapport généré vers l'onglet **Rapports**. La **Console de rapports** est le canal de distribution par défaut.
Sélectionnez les utilisateurs pouvant consulter la sortie générée par ce rapport.	Cette option s'affiche une fois que vous avez coché la case **Console de rapports**. Dans la liste des utilisateurs, sélectionnez les utilisateurs auxquels vous souhaitez accorder le droit d'afficher les rapports générés.
Sélectionner tous les utilisateurs	Cette option s'affiche uniquement une fois que vous avez coché la case **Console de rapports**. Cochez cette case si vous voulez accorder le droit à tous les utilisateurs d'afficher les rapports générés. Vous devez disposer des autorisations réseau appropriées pour partager les rapports générés avec d'autres utilisateurs.
Messagerie électronique	Cochez cette case si vous voulez distribuer les rapports générés par e-mail.

Option	Description
Entrez les adresses e-mail de destination du rapport	Cette option s'affiche uniquement une fois que vous avez coché la case **E-mail**. Saisissez l'adresse e-mail de chaque destinataire des rapports générés ; séparez la liste d'adresses e-mail par des virgules. Le nombre maximum de caractères pour ce paramètre est 255. Les destinataires reçoivent cet e-mail de no_reply_reports@qradar.
Inclure le rapport sous forme de pièce jointe (non-HTML uniquement)	Cette option s'affiche uniquement une fois que vous avez coché la case **E-mail**. Cochez cette case pour envoyer le rapport généré en tant que pièce jointe.
Inclure un lien vers la console de rapports	Cette option s'affiche uniquement une fois que vous avez coché la case **E-mail**. Cochez cette case pour inclure un lien vers Console de rapports dans l'e-mail.

12. Sur la page Fin, entrez les valeurs des paramètres suivants.

Option	Description
Description de rapports	Saisissez une description pour ce rapport. La description est affichée dans la page Récapitulatif et dans l'e-mail de distribution des rapports générés.
Sélectionnez les groupes auxquels vous souhaitez que ce rapport appartienne	Sélectionnez les groupes auxquels vous voulez affecter ce rapport. Pour plus d'informations sur les groupes, voir Groupes de rapports.
Voulez-vous exécuter ce rapport maintenant ?	Cochez cette case si vous souhaitez générer le rapport lorsque l'assistant est terminé. Par défaut, cette case est cochée.

13. Cliquez sur **Suivant** afin d'afficher le rapport récapitulatif.
14. Sur la page Récapitulatif, sélectionnez les onglets disponibles sur le rapport récapitulatif afin de prévisualiser votre configuration de rapport.

Résultats

Le rapport est immédiatement généré. Si vous décochez la case **Voulez-vous exécuter ce rapport maintenant ?**, sur la page finale de l'assistant, le rapport est sauvegardé et généré à l'heure planifiée. Le titre du rapport est le titre par défaut du rapport généré. Si vous reconfigurez un rapport afin d'entrer un nouveau titre, le rapport est enregistré en tant que nouveau rapport sous le nouveau nom, mais le rapport d'origine reste le même.

Edition d'un rapport

A l'aide de l'assistant de création de rapports, vous pouvez éditer n'importe quel rapport par défaut ou personnalisé à modifier.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser ou personnaliser un nombre important de rapports par défaut. L'onglet par défaut **Rapports** affiche la liste des rapports. Chaque rapport capture et affiche les données existantes.

Remarque : Lorsque vous personnalisez un rapport planifié pour générer manuellement, sélectionnez l'intervalle de temps **Date de fin** avant de sélectionner la **Date de début**.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Cliquez deux fois sur le rapport que vous souhaitez personnaliser.
3. Sur l'assistant de création de rapports, changez les paramètres permettant de personnaliser le rapport afin de générer le contenu dont vous avez besoin.

Résultats

Si vous reconfigurez un rapport afin d'entrer un nouveau titre, le rapport est enregistré en tant que nouveau rapport sous le nouveau nom, mais le rapport d'origine reste le même.

Affichage de rapports générés

Dans l'onglet **Rapports**, une icône s'affiche dans la colonne **Formats** si un rapport a généré du contenu. Vous pouvez cliquer sur l'icône pour afficher le rapport.

Pourquoi et quand exécuter cette tâche

Lorsqu'un rapport a généré du contenu, la colonne **Rapports générés** affiche une zone de liste. La zone de liste affiche tout le contenu généré, organisé par l'horodatage du rapport. Les rapports les plus récents sont affichés en haut de la liste. Si un rapport ne génère pas de contenu, la valeur **Aucun** est affichée dans la colonne **Rapports générés**.

Les icônes représentant le format de rapport du rapport généré s'affichent dans la colonne **Formats**.

Les rapports peuvent être générés aux formats PDF, HTML, RTF, XML et XLS.

Remarque : Les formats XML et XLS sont disponibles uniquement pour les rapports qui utilisent un format de table de graphiques unique (portrait ou paysage).

Vous pouvez afficher uniquement les rapports auxquels l'administrateur vous a autorisé à accéder. Les administrateurs peuvent accéder à tous les rapports.

Si vous utilisez le navigateur Web Mozilla Firefox et que vous sélectionnez le format de rapport RTF, le navigateur Web Mozilla Firefox lance une nouvelle fenêtre de navigateur. Le lancement de cette nouvelle fenêtre est le résultat de la configuration du navigateur Web Mozilla Firefox et n'affecte pas QRadar. Vous pouvez fermer la fenêtre et poursuivre votre session QRadar.

Procédure

1. Cliquez sur l'onglet **Rapports**.

2. Dans la zone de liste de la colonne **Rapports générés**, sélectionnez l'horodatage du rapport que vous souhaitez afficher.
3. Cliquez sur l'icône du format que vous souhaitez afficher.

Suppression du contenu généré

Lorsque vous supprimez du contenu généré, tous les rapports générés depuis le canevas de rapport sont supprimés, mais le canevas de rapport est conservé.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Sélectionnez les rapports dont vous souhaitez supprimer le contenu généré.
3. Dans la zone de liste **Actions**, cliquez sur **Supprimer le contenu généré**.

Génération manuelle d'un rapport

Vous pouvez configurer un rapport pour sa génération automatique ; cependant, vous pouvez générer un rapport manuellement, à n'importe quel moment.

Pourquoi et quand exécuter cette tâche

Pendant que le rapport est généré, la colonne Heure de la prochaine exécution affiche l'un des trois messages suivants :

- **Génération de** - Le rapport est en cours de génération.
- **En file d'attente (position dans la file d'attente)** - Le rapport est mis en file d'attente pour la génération. Le message indique la position du rapport dans la file d'attente. Par exemple, 1 de 3.
- **(x heure(s) x min y s)** - L'exécution du rapport est planifiée. Le message est un compte à rebours qui indique quand le rapport suivant sera exécuté.

Vous pouvez sélectionner l'icône **Actualiser** pour actualiser la vue, y compris les informations de la colonne **Heure de la prochaine exécution**.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Sélectionnez le rapport que vous souhaitez générer.
3. Cliquez sur **Exécuter le rapport**.

Que faire ensuite

Après la génération d'un rapport, vous pouvez afficher le rapport généré dans la colonne Rapports générés.

Duplication d'un rapport

Pour créer un rapport qui présente une forte ressemblance avec un rapport existant, vous pouvez dupliquer le rapport que vous souhaitez modéliser, puis le personnaliser.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Sélectionnez le rapport que vous souhaitez dupliquer.
3. Dans la zone de liste **Actions**, cliquez sur **Dupliquer**.

4. Entrez un nouveau nom, sans espace, pour le rapport.

Que faire ensuite

Vous pouvez personnaliser le rapport dupliqué.

Partage d'un rapport

Vous pouvez partager des rapports avec d'autres utilisateurs. Lorsque vous partagez un rapport, vous devez fournir une copie du rapport sélectionné à un autre utilisateur en vue de sa modification ou planification.

Pourquoi et quand exécuter cette tâche

Toutes les mises à jour effectuées par l'utilisateur sur un rapport partagé n'affectent pas la version originale du rapport.

Vous devez disposer de privilèges d'administration pour partager des rapports. En outre, pour qu'un nouvel utilisateur puisse afficher et accéder aux rapports, un administrateur doit partager tous les rapports nécessaires avec le nouvel utilisateur.

Vous pouvez uniquement partager le rapport avec les utilisateurs possédant les droits d'accès appropriés.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Sélectionnez les rapports que vous souhaitez partager.
3. Dans la zone de liste **Actions**, cliquez sur **Share**.
4. Dans la liste des utilisateurs, sélectionnez les utilisateurs avec lesquels vous souhaitez partager ce rapport.

Personnalisation de rapports

Pour personnaliser des rapports, vous pouvez importer des logos et des images spécifiques. Pour personnaliser des rapports à l'aide de logos personnalisés, vous devez télécharger et configurer les logos avant de commencer à utiliser l'assistant de création de rapports.

Avant de commencer

Nous vous recommandons l'utilisation de graphiques 144 x 50 pixels avec un fond blanc.

Pour vous assurer que votre navigateur affiche le nouveau logo, visez le cache de votre navigateur.

Pourquoi et quand exécuter cette tâche

La personnalisation de rapports est bénéfique pour votre entreprise si vous prenez en charge plus d'un seul logo. Lorsque vous téléchargez une image, elle est automatiquement enregistrée en tant que Portable Network Graphic (PNG).

Lorsque vous téléchargez une nouvelle image et que vous la définissez comme image par défaut, la nouvelle image par défaut n'est pas appliquée aux rapports

qui ont été précédemment générés. La mise à jour du logo sur les rapports précédemment générés nécessite la génération manuelle d'un nouveau contenu dans le rapport.

Si vous téléchargez une image dont la longueur ne peut être prise en charge par l'en-tête du rapport, l'image est automatiquement redimensionnée pour s'adapter à l'en-tête, soit une hauteur d'environ 50 pixels.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Dans le menu de navigation, cliquez sur **Personnalisation**.
3. Cliquez sur **Parcourir** pour accéder aux fichiers de votre système.
4. Sélectionnez le fichier qui contient le logo que vous souhaitez télécharger. Cliquez sur **Ouvrir**.
5. Cliquez sur **Charger une image**.
6. Sélectionnez le logo que vous souhaitez utiliser par défaut, puis cliquez sur **Définir une image par défaut**.

Groupe de rapports

Vous pouvez trier des rapports dans des groupes fonctionnels. Si vous classez les rapports en groupes, vous pouvez efficacement organiser et trouver des rapports.

Par exemple, vous pouvez afficher tous les rapports relatifs à la conformité PCIDSS (Payment Card Industry Data Security Standard).

Par défaut, l'onglet **Rapports** affiche la liste de tous les rapports ; cependant, vous pouvez classer les rapports dans des groupes tels que :

- Conformité
- Administratif
- Sources de journal
- Gestion de réseau
- Sécurité
- VoIP
- Autre

Lorsque vous créez un nouveau rapport, vous pouvez affecter le rapport à un groupe existant ou créer un nouveau groupe. Vous devez disposer d'un accès administratif afin de créer, modifier ou supprimer des groupes.

Pour plus d'informations sur les rôles d'utilisateurs, voir *IBM Security QRadar Administration Guide*.

Création d'un groupe de rapports

Vous pouvez créer de nouveaux groupes.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Cliquez sur **Gérer les groupes**.
3. Dans l'arborescence de navigation, sélectionnez le groupe dans lequel vous souhaitez créer un nouveau groupe.

4. Cliquez sur **Nouveau groupe**.
5. Entrez les valeurs pour les paramètres suivants :
   - **Nom** - Entrez le nom du nouveau groupe. Ce nom peut contenir jusqu'à 225 caractères.
   - **Description** - Facultatif. Entrez une description pour ce groupe. La description peut contenir jusqu'à 255 caractères.
6. Cliquez sur **OK**.
7. Pour changer l'emplacement du nouveau groupe, cliquez sur le nouveau groupe et faites glisser le dossier vers le nouvel emplacement dans l'arborescence de navigation.
8. Fermez la fenêtre Groupes de rapports.

Modification d'un groupe

Vous pouvez éditer un groupe de rapports pour changer le nom ou la description.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Cliquez sur **Gérer les groupes**.
3. Dans l'arborescence de navigation, sélectionnez le groupe que vous souhaitez éditer.
4. Cliquez sur **Editer**.
5. Mettez les valeurs des paramètres à jour, si nécessaire :
   - **Nom** - Entrez le nom pour le nouveau groupe. Le nom peut contenir jusqu'à 225 caractères.
   - **Description** - Facultatif. Saisissez une description pour ce groupe. La description peut contenir jusqu'à 255 caractères. Cette zone est facultative.
6. Cliquez sur **OK**.
7. Fermez la fenêtre Groupes de rapports.

Partage des groupes de rapports

Vous pouvez partager des groupes de rapports avec d'autres utilisateurs.

Avant de commencer

Vous devez disposer de droits d'administration pour le partage d'un groupe de rapports avec d'autres utilisateurs.

Pour plus d'informations sur les autorisations, voir *IBM Security QRadar Administration Guide*.

Vous ne pouvez pas utiliser l'outil de gestion de contenu (CMT) pour partager les groupes de rapports.

Pour plus d'informations sur l'outil de gestion de contenu (CMT), voir *IBM Security QRadar Administration Guide*.

Pourquoi et quand exécuter cette tâche

Dans la fenêtre Groupes de rapports, les utilisateurs partagés peuvent voir le groupe de rapports dans la liste de rapports.

Toutes les mises à jour effectuées par l'utilisateur sur un groupe de rapports partagé n'affectent pas la version originale du rapport. Seul le propriétaire peut supprimer ou modifier.

Une copie du rapport est créée lorsqu'un utilisateur duplique ou exécute le rapport partagé. L'utilisateur peut modifier ou planifier des rapports dans le groupe de rapports copié.

L'option de partage de groupe remplace les options de partage de rapport précédentes configurées pour les rapports dans le groupe.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Sur la fenêtre **Rapports**, cliquez sur **Gérer les groupes**.
3. Sur la fenêtre **Groupes de rapports**, sélectionnez le groupe de rapports que vous souhaitez partager et cliquez sur **Partager**.
4. Dans la fenêtre **Options de partage**, sélectionnez l'une des options suivantes.

Option	Description
Défaut (hérité du parent)	Le groupe de rapports n'est pas partagé. Tout groupe de rapports copié ou rapport généré reste dans la liste de rapports des utilisateurs. Chaque rapport dans le groupe se voit affecter une option de partage de rapport parent qui a été configurée.
Partager avec tout le monde	Le groupe de rapports est partagé avec tous les utilisateurs.
Partager avec des utilisateurs correspondant aux critères suivants...	Le groupe de rapports est partagé avec des utilisateurs spécifiques. **Rôles utilisateur** Sélectionnez dans la liste des rôles utilisateur et cliquez sur l'icône ajouter (symbole +). **Profils de sécurité** Sélectionnez à partir de la liste de profils de sécurité et cliquez sur l'icône ajouter (le symbole +).

5. Cliquez sur **Sauvegarder**.

Résultats

Sur la fenêtre Groupes de rapports, les utilisateurs partagés voient le groupe de rapports dans la liste de rapports. Les rapports générés affichent du contenu en fonction de la configuration du profil de sécurité.

Affectation d'un rapport à un groupe

Vous pouvez utiliser l'option **Affecter des groupes** pour affecter un rapport à un autre groupe.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Sélectionnez le rapport que vous souhaitez affecter à un groupe.
3. A partir de la zone de liste **Actions**, sélectionnez **Affecter des groupes**.
4. Dans la liste **Groupes d'éléments**, sélectionnez la case du groupe auquel vous souhaitez attribuer ce rapport.
5. Cliquez sur **Affecter des groupes**.

Copie d'un rapport vers un autre groupe

L'icône **Copier** permet de copier un rapport vers un ou plusieurs groupes de rapports.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Cliquez sur **Gérer les groupes**.
3. Dans l'arborescence de navigation, sélectionnez le rapport que vous souhaitez copier.
4. Cliquez sur **Copier**.
5. Sélectionnez le groupe ou les groupes vers lesquels vous souhaitez copier le rapport.
6. Cliquez sur **Affecter des groupes**.
7. Fermez la fenêtre Groupes de rapports.

Suppression d'un rapport

Vous pouvez utiliser l'icône **Retirer** pour supprimer un rapport d'un groupe.

Pourquoi et quand exécuter cette tâche

Lorsque vous supprimez un rapport d'un groupe, ce rapport existe toujours dans l'onglet **Rapports**. Le rapport n'est pas supprimé de votre système.

Procédure

1. Cliquez sur l'onglet **Rapports**.
2. Cliquez sur **Gérer les groupes**.
3. Dans l'arborescence de navigation, accédez au dossier qui contient le rapport que vous souhaitez supprimer.
4. Dans la liste des groupes, sélectionnez le rapport que vous souhaitez supprimer.
5. Cliquez sur **Retirer**.
6. Cliquez sur **OK**.
7. Fermez la fenêtre Groupes de rapports.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties tacites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

© Copyright IBM Corp. 2012, 2017

Toute référence à ces informations sur des sites web non-IBM est fournie par souci de commodité uniquement et ne constitue en aucun cas une adhésion au contenu de ces sites web. Les documents sur ces sites web ne font pas partie des documents de ce produit IBM et l'utilisation de ces sites web se fait à vos propres risques.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance et les exemples client ne sont présentés qu'à des fins d'illustration. Les résultats des performances réelles peuvent varier en fonction des configurations et des conditions de fonctionnement spécifiques.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Tous ces noms sont fictifs, et toute ressemblance avec des noms de personnes ou de sociétés réelles serait purement fortuite.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de service peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité

Ces dispositions viennent s'ajouter à toute autre condition d'utilisation applicable au site web IBM.

Utilisation personnelle

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer ou publier tout ou partie de ces publications ou en produire des oeuvres dérivées sans le consentement exprès d'IBM.

Utilisation commerciale

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas reproduire, distribuer ou afficher tout ou partie de ces publications en dehors de votre entreprise ou en tirer des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Exception faite des droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, tacite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Déclaration IBM de confidentialité en ligne

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Selon la configuration déployée, la présente Offre Logiciels peut utiliser des cookies de session et des cookies persistants destinés à collecter le nom et le mot de passe des utilisateurs pour les fonctions de gestion des session et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet (http://www.ibm.com/privacy/fr/fr) et la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet sur le site http://www.ibm.com/privacy/details/fr/fr, ainsi que la section "IBM Software Products and Software-as-a-Service Privacy Statement" sur le site http://www.ibm.com/software/info/product-privacy (en anglais).

Glossaire

Ce glossaire contient les termes utilisés dans les logiciels et les produits IBM Security QRadar SIEM, et leur définition.

Les références croisées suivantes sont utilisées :

- *Voir* renvoie d'un terme peu utilisé au terme généralement utilisé ou d'une abréviation à la forme développée.
- *Voir aussi* renvoie à un terme connexe ou à un antonyme.

Pour tout autre terme et définition, veuillez vous référer au site Web de terminologie IBM (ouvre une nouvelle fenêtre).

«A» «C» «D», à la page 246 «E», à la page 246 «F» , à la page 246 «G», à la page 247 «H», à la page 247 «I», à la page 247 «J», à la page 247 «L», à la page 247 «M», à la page 248 «N», à la page 248 «O», à la page 249 «P», à la page 249 «R», à la page 249 «S», à la page 250 «T», à la page 251 «V», à la page 251

A

accumulateur
Registre dans lequel une opérande d'une opération peut être stockée et remplacée ensuite par le résultat de cette opération.

actif Objet gérable qui est déployé ou destiné à être déployé dans un environnement opérationnel.

adresse IP virtuelle du cluster
Adresse IP partagée entre l'hôte principal ou secondaire et le cluster haute disponibilité.

agrégation de liens
Regroupement des cartes d'interface réseau physique, telles que les câbles ou les ports, en une seule interface réseau logique. L'agrégation de lien permet d'augmenter la bande passante et la disponibilité du réseau.

ampleur
Mesure de l'importance relative d'une infraction. L'ampleur est une valeur pondérée calculée à partir des mesures de pertinence, de gravité et de crédibilité.

analyse immédiate
Analyse de vulnérabilité qui génère des données de rapport à partir de résultats d'analyse d'après le nom de session.

anomalie
Ecart par rapport au comportement attendu du réseau.

ARP Voir protocole de résolution d'adresse.

ASN Voir numéro de système autonome.

C

capture de contenu
Processus permettant de capturer une quantité configurable de contenus et de stocker ensuite les données dans un journal de flux.

chiffrement
Dans le cadre de la sécurité informatique, processus de conversion de données dans une forme inintelligible, de sorte que les données d'origine ne puissent pas être obtenues ou puisse l'être uniquement via un processus de déchiffrement.

cible hors site
Périphérique situé en dehors du site principal recevant des événements ou des flux de données d'un collecteur d'événements.

CIDR Voir routage CIDR.

client Programme logiciel ou ordinateur demandant des services à un serveur.

cluster à haute disponibilité
Une configuration haute disponibilité se compose d'un serveur principal et d'un serveur secondaire.

code d'authentification de message basé sur le hachage (HMAC)
Code cryptographique qui utilise une fonction de hachage chiffrée et une clé secrète.

comportement
Effets observables d'une opération ou d'un événement, y compris de ses résultats.

© Copyright IBM Corp. 2012, 2017

console
Clavier-écran à partir duquel un opérateur peut contrôler et observer le fonctionnement du système.

contexte d'hôte
Service surveillant les composants pour s'assurer que chaque composant fonctionne comme prévu.

Conversion d'adresses réseau (NAT)
Dans un pare-feu, la conversion d'adresses de protocole Internet (IP) sécurisées à des adresses enregistrées externes. Ceci permet la communication avec des réseaux externes mais masque les adresses IP utilisées à l'intérieur du pare-feu.

couche réseau
Dans une architecture OSI, couche fournissant des services pour établir un chemin d'accès entre les systèmes ouverts avec une qualité de service prévisible.

crédibilité
Classement numérique compris entre 0 et 10, utilisé pour déterminer l'intégrité d'un événement ou la présence d'une infraction. La crédibilité augmente lorsque plusieurs sources signalent le même événement ou la même infraction.

CVSS Voir système de notation de vulnérabilité commune.

D

destination d'acheminement
Système d'un ou plusieurs fournisseurs recevant des données brutes et normalisées de sources de journal et de sources de flux.

dispositif d'analyse externe
Machine qui est connectée au réseau pour la collecte de données de vulnérabilité concernant des actifs du réseau.

distant à distant (R2R)
Trafic externe entre un réseau distant et un autre réseau distant.

distant à local (R2L)
Trafic externe entre un réseau distant et un réseau local.

DNS Voir système de noms de domaine.

données d'identification
Ensemble d'informations accordant certains droits d'accès à un utilisateur ou à un processus.

données utiles
Données d'application contenues dans un flux IP, excluant l'en-tête et les informations administratives.

DSM Voir module de support de périphérique.

Dynamic Host Configuration Protocol (DHCP)
Protocole de communication utilisé pour gérer les informations de configuration de façon centralisée. Par exemple, DHCP affecte automatiquement des adresses IP aux ordinateurs d'un réseau.

E

ensemble de référence
liste d'éléments uniques dérivés d'événements ou de flux sur un réseau (liste d'adresses IP ou liste de noms d'utilisateur, par exemple).

extension de source de journal
Fichier XML qui inclut l'ensemble des schémas d'expression régulière requis pour identifier et catégoriser les événements de contenu d'événement.

F

faux positif
Résultat de test classé comme positif (indiquant que le site est vulnérable aux attaques) et que l'utilisateur décide de classer comme négatif (il ne s'agit pas d'une vulnérabilité).

feuille Dans une arborescence, entrée ou noeud ne possédant pas d'enfant.

fichier de clés
Dans le domaine de la sécurité informatique, fichier qui contient des clés publiques et privées, des clés d'authentification et des certificats.

flux Transmission de données unique passant par un lien lors d'une conversation.

flux double
Plusieurs instances de la même transmission de données provenant de sources de flux distinctes.

fournisseur d'accès à Internet (FAI)
Organisation fournissant un accès à Internet.

G

gravité
Mesure de la menace relative qu'une source représente pour une destination.

H

HA Voir haute disponibilité.

haute disponibilité (HA)
Se dit d'un système en cluster reconfiguré en cas de défaillance d'un noeud ou d'un démon, de telle sorte que la charge puisse être redistribuée entre les autres noeuds du cluster.

HMAC
Voir code d'authentification de message basé sur le hachage.

hôte à haute disponibilité principal
Ordinateur principal connecté au cluster haute disponibilité.

hôte à haute disponibilité secondaire
Ordinateur de secours connecté au cluster haute disponibilité. L'hôte à haute disponibilité secondaire assume la responsabilité de l'hôte à haute disponibilité principal en cas de défaillance de ce dernier.

I

ICMP Voir protocole de message de gestion inter-réseau.

identité
Collection d'attributs provenant d'une source de données et représentant une personne, une organisation, un lieu ou un élément.

IDS Voir système de détection d'intrusion.

infraction
Message envoyé ou événement généré en réponse à une condition contrôlée. Par exemple, une infraction indiquera si une règle a été violée ou si le réseau se trouve en état d'attaque.

interconnexion de systèmes ouverts
Interconnexion de systèmes ouverts conforme aux normes ISO (International Organization for Standardization) pour l'échange d'informations.

interface liée
Voir agrégation de liaisons.

intervalle de coalescence
Fréquence à laquelle les événements sont regroupés. Le regroupement d'événements se produit à des intervalles de 10 secondes et commence avec le premier événement qui ne correspond à aucun événement de coalescence en cours. A l'intérieur de l'intervalle de coalescence, les trois premiers événements correspondants sont regroupés et envoyés au processeur d'événement.

intervalle de rapport
Intervalle de temps configurable au terme duquel le processeur d'événement doit envoyer la totalité des données d'événements et de flux capturés à la console.

IP Voir protocole Internet.

IPS Voir système de prévention contre les intrusions.

ISP Voir fournisseur d'accès à Internet.

J

journal de flux
Collection d'enregistrements de flux.

L

LAN Voir réseau local.

LDAP Voir protocole LDAP (Lightweight Directory Access Protocol).

L2L Voir local à local.

local à distant (L2R)
Concerne le trafic interne d'un réseau local à un autre réseau distant.

local à local (L2L)
Concerne le trafic interne d'un réseau local à un autre réseau local.

L2R Voir local à distant.

M

magasin de clés certifiées
Fichier clé de base de données qui contient les clés publiques d'une entité certifiée.

magistrat
Composant interne analysant le trafic réseau et les événements de sécurité à l'aide de règles personnalisées définies.

mappe de références
enregistrement de données d'un mappage direct d'une clé à une valeur (un nom d'utilisateur vers un ID global, par exemple).

mappe de références de mappes
enregistrement de données de deux clés mappées à un grand nombre de valeurs (mappage, par exemple, du nombre d'octets total d'une application vers un IP source.

mappe de références d'ensembles
enregistrement de données d'une clé mappée à un grand nombre de valeurs (mappage, par exemple, d'une liste d'utilisateurs privilégiés à un hôte).

mappe QID
Taxonomie identifiant chaque événement unique et mappant les événements à des catégories de bas niveau et de haut niveau afin de déterminer la façon dont un événement doit être corrélé et organisé.

masque de sous-réseau
Pour la mise en sous-réseau Internet, masque de 32 bits permettant d'identifier les bits d'adresse de sous-réseau de la partie hôte d'une adresse IP.

minuteur d'actualisation
Périphérique interne déclenché manuellement ou automatiquement à des intervalles temporisés, mettant à jour les données d'activité réseau en cours.

module de support de périphérique (DSM)
Fichier de configuration analysant les événements reçus de plusieurs sources de journal et les convertissant à un format de taxonomie standard affichable comme sortie.

multi-diffusion IP
Transmission d'un datagramme IP (Internet Protocol) à une série de systèmes constituant un groupe de multi-diffusion unique.

N

NAT Voir conversion d'adresses réseau.

NDQC
Voir nom de domaine qualifié complet.

NetFlow
Protocole de réseau Cisco surveillant les données de flux du trafic réseau. Les données NetFlow contiennent des informations sur le client et le serveur, les ports utilisés et le nombre d'octets et de paquets circulant via les commutateurs et routeurs connectés à un réseau. Les données sont envoyées aux connecteurs NetFlow où l'analyse des données se produit.

noeud final
Adresse d'une API ou service dans un environnement. Une API expose un noeud final et en même temps appelle les noeuds finaux d'autres services.

nom de domaine qualifié complet (NDQC)
Dans les communications Internet, le nom d'un système hôte qui inclut tous les sous-noms du nom de domaine. rchland.vnet.ibm.com est un exemple de nom de domaine complet.

nom de réseau qualifié complet (NDQC)
Dans une hiérarchie de réseau, le nom d'un objet comprenant tous les services. Exemple de nom de réseau qualifié complet : CompanyA.Department.Marketing.

NRQC
Voir nom de réseau qualifié complet.

numéro de système autonome (ASN)
Dans TCP/IP, numéro affecté à un système autonome par la même autorité centrale que celle qui affecte les adresses IP. Le numéro de système autonome permet aux algorithmes de routage automatique de distinguer les systèmes autonomes.

O

objet Noeud terminal de la base de données
Objet de terminal ou noeud dans une hiérarchie de base de données.

objet réseau
Composant d'une hiérarchie réseau.

Open Source Vulnerability Database (OSVDB)
Créée par et pour la communauté de sécurité réseau, cette base de données open source fournit des informations techniques sur les vulnérabilités de la sécurité réseau.

ordre d'analyse syntaxique
Définition de source de journal dans laquelle l'utilisateur peut définir l'ordre d'importance pour les sources de journal qui partagent une adresse IP ou un nom d'hôte communs.

OSI Voir interconnexion de systèmes ouverts.

OSVDB
Voir Open Source Vulnerability Database.

P

partage administratif
Ressource réseau qui est masquée aux utilisateurs ne disposant pas de privilèges d'administration. Les partages administratifs donne accès aux administrateurs à toutes les ressources sur un système réseau.

passerelle
Périphérique ou programme permettant de connecter des réseaux ou des systèmes à des architectures réseau différentes.

pertinence
Mesure de l'impact relatif d'un événement, d'une catégorie ou d'une infraction sur le réseau.

point de données
Valeur calculée d'une mesure à un moment donné.

protocole
Ensemble de règles gérant les communications et le transfert de données entre plusieurs unités ou systèmes, dans un réseau de communication.

protocole de message de gestion inter-réseau (ICMP)
Protocole Internet utilisé par une passerelle pour communiquer avec un hôte source, par exemple, pour signaler une erreur dans un datagramme.

protocole de résolution d'adresse (ARP)
Protocole qui établit une correspondance dynamique entre une adresse IP et une adresse d'adaptateur de réseau dans un réseau local.

protocole DHCP
Voir Dynamic Host Configuration Protocol.

protocole Internet (IP)
Protocole acheminant les données via un réseau ou des réseaux interconnectés. Ce protocole joue le rôle d'intermédiaire entre les couches de protocole de niveau supérieur et le réseau physique. Voir aussi protocole TCP.

protocole LDAP (Lightweight Directory Access Protocol)
Protocole ouvert utilisant TCP/IP pour fournir l'accès aux annuaires qui prennent en charge un modèle X.500 et pour lequel les ressources exigées par le protocole X.500 DAP (Directory Access Protocol) plus complexe ne sont pas requises. Par exemple, le protocole LDAP peut être utilisé pour localiser des personnes, des organisations et d'autres ressources dans un annuaire Internet ou Intranet.

R

rafale Accroissement soudain du taux d'événements ou de flux entrants qui entraîne un dépassement de la limite de flux ou de taux d'événement sous licence.

rapport
Dans la gestion des requêtes, données dont la mise en forme résulte de l'exécution d'une requête et de l'application d'un formulaire particulier aux enregistrements renvoyés par cette requête.

recon Voir reconnaissance.

reconnaissance (recon)
Méthode par laquelle les informations appartenant à l'identité des ressources réseau sont collectées. L'analyse réseau et d'autres techniques sont utilisées pour compiler une liste d'événements de

ressource réseau auxquels un niveau de sécurité est ensuite affecté.

redirection du protocole de résolution d'adresse
Méthode du protocole ARP permettant de notifier l'hôte en cas de problème sur un réseau.

règle Ensemble d'instructions conditionnelles permettant à des systèmes informatiques d'identifier des relations et d'exécuter les réponses automatisées correspondantes.

règle de routage
Condition qui, lorsque ses critères sont satisfaits par les données d'événement, entraîne une collection de conditions et le routage conséquent.

réseau local
Réseau reliant plusieurs périphériques dans une zone limitée (telle qu'un bâtiment ou un campus) et pouvant être connecté à un réseau plus grand.

R2L Voir local à local.

routage CIDR
Méthode d'ajout d'adresses IP (Internet Protocol) de classe C. Les adresses sont fournies aux fournisseurs de services Internet (ISP) pour une utilisation par leurs clients. Les adresses CIDR réduisent la taille des tables de routage et augmentent le nombre d'adresses IP disponibles au sein des organisations.

R2R Voir distant à distant.

S

scanner
Programme de sécurité automatisée qui recherche les vulnérabilités logicielles au sein d'applications Web.

serveur whois
Serveur utilisé pour récupérer les informations sur des ressources Internet enregistrées, telles que les allocations de noms de domaine et adresses IP.

signature d'application
Ensemble unique de caractéristiques dérivées de l'examen de contenus de paquets puis utilisées pour identifier une application spécifique.

Simple Network Management Protocol (SNMP)
Ensemble de protocoles permettant de surveiller les systèmes et les périphériques dans des réseaux complexes. Les informations sur les périphériques gérés sont définies et stockées dans une base d'informations de gestion.

SNMP
Voir Simple Network Management Protocol.

SOAP Protocole simple reposant sur XML pour l'échange d'informations dans un environnement réparti décentralisé. Le protocole SOAP peut être utilisé pour rechercher et renvoyer des informations et pour appeler des services via Internet.

source de journal
Equipement de sécurité ou équipement réseau duquel un journal d'événement provient.

source hors site
Périphérique situé en dehors du site principal renvoyant les données normalisées à un collecteur d'événements.

sources de flux
Origine du flux capturé. Une source de flux est classée comme interne lorsque le flux provient d'un matériel installé sur un hôte géré et comme externe lorsque le flux est envoyé à un collecteur de flux.

sous-recherche
Fonction permettant d'effectuer une requête de recherche sur un ensemble de résultats de recherche terminés.

sous-réseau
Réseau divisé en plusieurs sous-groupes indépendants de plus petite taille, connectés entre eux.

structure hiérarchique du réseau
Type de conteneur représentant une collection hiérarchique d'objets réseau.

subnet
Voir sous-réseau.

super-flux
Flux unique composé de plusieurs flux aux propriétés similaires permettant d'améliorer la capacité de traitement en réduisant les contraintes de stockage.

système actif
Dans un cluster haute disponibilité, système ayant tous ses services en cours d'exécution.

système de détection d'intrusion (IDS)
Logiciel détectant les tentatives d'attaques ou attaques réussies sur les ressources surveillées d'un réseau ou d'un système hôte.

système de noms de domaine (DNS)
Système de base de données répartie qui mappe des noms de domaine à des adresses IP.

système de notation de vulnérabilité commune (CVSS)
Système d'évaluation permettant de mesurer la gravité d'une vulnérabilité.

système de prévention contre les intrusions (IPS)
Système essayant de refuser les activités potentiellement malveillantes. Les mécanismes de refus peuvent impliquer le filtrage, le suivi ou la définition de limites de débit.

système de secours
Système s'activant automatiquement en cas de défaillance du système actif. Si la réplication de disque est activée, il réplique les données du système actif.

T

table de référence
tableau dans lequel l'enregistrement de données mappe les clés qui ont un type affecté à d'autres clés, qui sont ensuite mappées à une valeur unique.

TCP Voir Transmission Control Protocol.

Transmission Control Protocol (TCP)
Protocole de communication utilisé sur Internet et dans tout réseau respectant les normes IETF (Internet Engineering Task Force) relatives au protocole inter-réseau. TCP constitue un protocole hôte à hôte fiable dans les réseaux à commutation de paquets et dans les systèmes interconnectés de ces réseaux. Voir aussi Protocole Internet.

V

violation
Acte visant à détourner ou contourner les règles de l'entreprise.

vue système
Représentation visuelle de l'hôte principal et de l'hôte géré composant un système.

vulnérabilité
Risque lié à la sécurité dans un système d'exploitation, un logiciel système ou un composant de logiciel d'application.

Index

A

actifs 8, 16, 19
actions sur une infraction 49
activité du journal 12, 16, 19, 29, 33, 55, 78, 79, 135, 136, 175, 176, 177, 178, 179, 181
  critères de recherche 148
  présentation 55
Activité du journal 135, 176
activité réseau 12, 16, 19, 20, 29, 33, 85, 90, 135, 136, 148, 175, 176, 178, 179, 181
Activité réseau 90, 135, 174, 176
actualiser des données 12
affichage dans une nouvelle fenêtre 32
affichage de données PCAP 81
affichage des éléments 27
affichage des événements de diffusion en continu 61
Affichage des flux en continu 90
affichage des flux regroupés 94
affichage des groupes de recherche 126, 177
affichage des infractions associées aux événements 77
afficher des événements groupés 67
afficher le tableau de bord 20, 29, 32, 33
afficher les messages 10
afficher les notifications système 33
afficher un profil d'actif 118
aide 16
aide en ligne 16
ajout d'éléments 33
ajout d'éléments d'événement 33
ajout d'éléments de recherche de flux 33
ajout de filtre 175
ajouter un actif 120
ajouter un élément 20
ajouter un élément de tableau de bord 19
ampleur 40
annulation d'une recherche 176
annuler la protection des infractions 39
application 19
assistant de règles personnalisées 10, 27
assistant règle de détection des anomalies 202

B

barre d'état 61, 89
barre d'outils 55
barre d'outils de l'onglet Activité réseau 85
barre d'outils des détails d'événements 76
Barre d'outils des détails de flux 101

C

centre de documentation des menaces Internet 29
chargement en bloc
  analyse d'événements et de flux 209
  corrélation d'historique 209
collecteur QFlow 89
colonne de données PCAP 80, 82
commandes 10
configuration de l'activité du journal 30
configuration de l'activité réseau 30
configuration des connexions 30
configuration des éléments de tableau de bord 30
configurer et gérer les réseaux, les plug-ins ainsi que les composants 9
configurer et gérer les systèmes 9
configurer et gérer les utilisateurs 9
configurer la taille de page 19
conformité 19
conservation d'infraction 39
contenus d'aide 16
copie d'une recherche sauvegardée 179
copier une recherche sauvegardée 128
corrélation d'historique
  création d'un profil 211
  heure de début 209
  heure de l'unité 209
  informations sur les exécutions passées 212
  infractions 212
  traitement des règles 209
création d'un groupe de recherche 178
création de groupes de recherche 177
crédibilité 40
créer des rapports 8
créer un groupe de recherche 127
critères de filtrage de flux 88
critères de recherche
  disponible sauvegardé 174
  onglet Activité du journal 174
  sauvegarde 148
  suppression 174
critères de recherche enregistré 20

D

dernière minute (actualisation automatique) 12
description d'événement 72
détachement d'un élément de tableau de bord 32
détails d'événement unique 72
détails d'événements 76
détails de flux 90, 97
détails de la vulnérabilité 130
diffusion en temps réel (en flux) 12
dispositif 9
données d'événements bruts 65
données d'événements non analysées 65
données de configuration 9
données Packet Capture (PCAP) 80
Données PCAP 80, 81
dupliquer un rapport 235

E

éditer un actif 120
éditer un groupe 238
éditer un groupe de recherche 127, 178
élément de tableau de bord 33
élément de tableau de bord Notification système 27
élément de tableau de bord Récapitulatif du système 23
éléments d'infraction 21
éléments de recherche de connexion 24
éléments de tableau de bord Activité du journal 22
éléments de tableau de bord liés à l'infraction. 21
en temps réel 61
enregistrements des dépassements 89
étude de l'activité du journal 55
étude des événements 22
étude des infractions 7, 40
étudier 85
étudier l'activité réseau 85
étudier les flux 8
étudier les journaux d'événements 8
événement de mappe 78
événements 23, 77, 141
événements de diffusion en flux 61
événements normalisés 62
excludes option 39
exécution d'une sous-recherche 175
exportation d'événements 82
exportation d'un profil d'actif 129
exportation de flux 102
exportation des actifs 130
exporter au format CSV 102
exporter au format XML 102
exporter des infractions 52

F

faux positif 79, 101
faux positifs 116
fenêtre groupes de recherche 177
fermeture d'infractions 51
filtre rapide 141
flux 23, 85, 141, 149
flux continu 89
flux normalisés 90
flux X-Force Threat Intelligence
  exemple 218
fonctions de barre d'outils des détails d'événements 76

© Copyright IBM Corp. 2012, 2017

G

générer un rapport manuellement 235
gérer des groupes de recherche 171
gérer des rapports 8, 226
gérer les groupes 128
Gérer les résultats de la recherche 176
gestion des graphiques 135
gestion des groupes de recherche 177
gestion des infractions 35
gestion des risques
  surveillance de la conformité aux règles 24
  surveillances des modifications de risques 26
gestion des tableaux de bord 19
glossaire 245
graphique de série temporelle 136
gravité 40
groupe
  suppression 179
groupe de recherche
  création 178
  édition 178
groupe de recherche d'événements 177, 178
groupe de recherche d'infractions 178
groupe de recherche de flux 177, 178
groupes de flux 97
groupes de rapports 238
groupes de recherche
  affichage 177
  gestion 177
groupes de recherche d'actifs 126

H

heure de début 209
heure de l'unité 209
heure de la console 15
heure système 15
hôtes 8

I

IBM Security QRadar Risk Manager 9
icône Retirer 128
image
  rapports
    personnalisation 236
  téléchargement 236
importation d'un profil d'actif 129
importer des actifs 129
Indicateur 27
informations utilisateur 16
infraction 77
  ampleur 40
  études 40
infractions 19, 39, 177, 178, 179
  affectation aux utilisateurs 52
  corrélation d'historique 212
infractions mises à jour 23
interface utilisateur 7

L

légendes de graphique 137
lire des données 12
liste d'événements 72
liste des flux dans différents modes 97

M

manage search results 176
masquer une infraction 50
menace 19
menu contextuel 60, 88
menu Messages 10
message de notification 27
mettre à jour les détails de l'utilisateur 16
mettre en pause des données 12
mode d'affichage des flux en continu 90
mode document
  navigateur Web Internet Explorer 5
mode navigateur
  navigateur Web Internet Explorer 5
modifier un mappage d'événement 78

N

niveau de menace actuelle 29
nombre de résultats de recherche 89
notification système 33
notifications système 10
nouveau tableau de bord 29
nouvelle recherche 127

O

objets de graphique 137
onglet Actif 117, 126
onglet Actifs 8, 118, 120, 126, 127, 128, 129
onglet activité du journal 141
onglet Activité du journal 8, 12, 60, 61, 62, 65, 67, 77, 80, 82, 141
Onglet Activité du journal 55
onglet Activité réseau 8, 12, 85, 88, 89, 94, 102, 141
Onglet Activité réseau 90, 101
Onglet Admin 9
onglet de tableau de bord 19, 20, 29, 32
onglet Infraction 167, 168, 170
onglet infractions 12, 39, 50, 51, 52
onglet Infractions 7, 171
onglet par défaut 7
onglet rapports 8, 12
onglet report 226
onglet Risques 24
onglet tableau de bord 29, 32, 33
onglet Tableau de bord 7, 10, 19, 21, 22, 24
onglets 7
onglets d'interface utilisateur 7
onglets de l'interface utilisateur 10
options des événements groupés 67
organiser les éléments de votre tableau de bord 19

P

page de détails d'événement 72
page de recherche d'actifs 124
page IP Source 167
page Par adresse IP de destination 168
Page Par réseau 170
page Profil d'actif 130
paramètres des événements groupés 67
partage de groupes de rapports 238
partager des rapports 236
personnaliser l'élément de tableau de bord 20
personnaliser les tableaux de bord 20
pertinence 40
plusieurs tableaux de bord 19
Présentation de rapport 224
présentation des graphiques 135
processeur d'événements 89
processeurs d'événements 89
profil d'actif 118, 120
profils d'actif 116, 125, 127, 128, 129
profils d'actifs 126, 127, 128, 130
propriété
  copie de propriété personnalisée 189
  modification de propriété personnalisée 187
propriété d'expression régulière 182
propriété de calcul 185
propriété personnalisée 189
propriétés d'événement et de flux personnalisées 181
protection des infractions 39

Q

QID 78
QRadar Vulnerability Manager 117

R

rapport
  édition 234
rapport réparti 8
rapports 16, 19
  affichage 234
  corrélation d'historique 212
Rapports générés les plus récents 23
rapports personnalisés 230
récapitulatif de l'activité au cours des dernières 24 heures 23
recherche 127, 141
  copie vers un groupe 179
recherche d'événement et de flux 141
recherche d'infractions 167, 168, 170
recherche de flux 20
recherche de profils d'actifs 124
recherche planifiée
  événements 149
  recherche 149
  recherche enregistrée 149
recherches d'infractions 159
redimensionner des colonnes 16
réglage des faux positifs 79
Réglage des faux positifs 101
règle de détection des anomalies 202
règles 192, 199

règles personnalisées
création 194
renommer un tableau de bord 32
réseau 19
résultats de processeur d'événement 61
résultats de recherche
annuler 176
gestion 176
suppression 176

S

sauvegarde de critères 125
sauvegarde de critères de recherche 171
sauvegarde des critères de recherche d'événements et de flux 61
sauvegarde des critères de recherche d'un actif 125
sauvegarder les critères 171
scanners tiers 117
sécurité 19
serveurs 8
source de journal 65
spécification du nombre d'objets de données à afficher 30
spécification du type de graphique 30
suppression d'un profil d'actif 129
suppression d'un tableau de bord 33
suppression d'une recherche 176
suppression des actifs 129
supprimer un élément du tableau de bord 32
supprimer un groupe 128, 179
supprimer une recherche sauvegardée 128
supprimer une recherche sauvegardée d'un groupe 179
surveillance de l'activité réseau 90
surveillance des événements 22
surveiller 85
surveiller l'activité réseau 85
surveiller les infractions 49
système 19

T

tableau de bord 33
tableau de bord du gestionnaire de risques
création 26
tableau de bord Gestion des vulnérabilités 27
tableau de bord personnalisé 19, 24, 29
tableau de bord Surveillance des risques 24
tableaux 19
tableaux de bord de surveillance des risques
création 24
téléchargement d'un fichier PCAP 82
téléchargement du fichier de données PCAP 81
test de règle 209
tri des résultats dans les tables 12
type de propriété calculé 181
type de propriété d'expression régulière 181
types de graphique 224
types de graphiques 228
types de propriétés 181

V

vulnérabilités 117
vulnérabilités pour l'actif 130

Z

zone de liste afficher 67
zone de liste Afficher 94