IBM QRadar Network Insights
Version 7.3.1

Guide d'utilisation

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 15.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.3.1 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

Table des matières

Avis aux lecteurs canadiens . . . . . **v**

Présentation de l'installation de QRadar Network Insights . . . . . **vii**

1 QRadar Network Insights **1**

2 Scénarios d'utilisation de QRadar Network Insights **3**

3 Contenu QRadar Network Insights **5**

4 Extensions de contenu QRadar Network Insights **9**
Extension de contenu v1.1.0 9
Extension de contenu v1. 2.0. 12
Extension de contenu v1. 3.0. 13
Extension de contenu v1. 4.0. 13

Remarques **15**
Marques 16
Dispositions relatives à la documentation du produit 16
Déclaration IBM de confidentialité en ligne 17

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.

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.

Présentation de l'installation de QRadar Network Insights

Ce guide contient des informations sur l'analyse des données réseau en temps réel à l'aide d'IBM® QRadar Network Insights.

Public visé

Les responsables de l'analyse extraient des informations du trafic réseau et examinent plus particulièrement les incidents de sécurité et les indicateurs de menace.

Documentation technique

Pour rechercher la documentation produit IBM Security QRadar sur le Web, y compris toute la documentation traduite, accédez à IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Pour savoir comment accéder à d'autres documents techniques dans la bibliothèque produit QRadar, voir la note technique Accessing IBM Security Documentation (en anglais) (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

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

Instructions relatives aux bonnes pratiques de sécurité

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.

1 QRadar Network Insights

IBM QRadar Network Insights offre une vision détaillée des communications réseau en temps réel permettant d'étendre les fonctions de votre déploiement IBM Security QRadar.

Via une analyse détaillée de l'activité réseau et du contenu des applications, QRadar Network Insights permet à QRadar Sense Analytics de détecter toute activité de menace.

QRadar Network Insights offre une analyse détaillée des métadonnées réseau et du contenu des applications afin de détecter les activités suspectes camouflées au milieu du trafic normal et d'extraire le contenu afin que QRadar ait une vue d'ensemble des activités de menace réseau. Les informations fournies par QRadar Network Insights s'intègrent en toute transparence à des sources de données standard et à la surveillances des menaces pour étendre les fonctions de détection de menaces, d'analyse et de détection QRadar.

QRadar Network Insights assure la visibilité de différents scénarios d'utilisation, notamment :

- Détection et analyse des logiciels malveillants
- Détection de campagnes et de courriers électroniques d'hameçonnage
- Menaces internes
- Détection d'attaque de mutation latérale
- Protection contre l'exfiltration des données
- Identification des écarts de conformité

Avantages de QRadar Network Insights

La liste suivante présente les avantages de l'utilisation de QRadar Network Insights:

- Inspection de paquet approfondie afin d'identifier les menaces avancées et le contenu malveillant.
- Etend les fonctionnalités de QRadar afin de détecter les attaques par hameçonnage, les intrusions de logiciel malveillant, la mutation latérale et l'exfiltration de données.
- Enregistrement des activités des applications, capture des principaux artefacts et identification des actifs, des applications et des utilisateurs participant aux communications réseau.
- Application de l'analyse de contenu Layer 7 pour une analyse de sécurité avancée.
- Analyse de fichiers et activation du suivi des fichiers.

2 Scénarios d'utilisation de QRadar Network Insights

QRadar Network Insights offre une vue détaillée des communications réseau et du contenu des applications permettant à QRadar Sense Analytics de détecter les activités de menace. Vous pouvez utiliser QRadar Network Insights pour détecter et analyser les logiciels malveillants, l'hameçonnage, les menaces internes, les attaques par mutation latérale, l'exfiltration de données et les écarts de conformité.

Détection et analyse des logiciels malveillants

Les logiciels malveillants évoluent fréquemment afin d'éviter d'être détectés. Vous pouvez utiliser QRadar Network Insights pour détecter les logiciels malveillants en fonction des hachages et de l'activité des fichiers et observer et analyser les artefacts, tels les éléments suivants :

- Noms
- Propriétés
- Déplacement
- Contenu suspect

Détection de campagnes et de courriers électroniques d'hameçonnage

L'hameçonnage peut camoufler son activité au milieu de messages électroniques normaux. Vous pouvez vous préparer et réagir aux messages électroniques malveillants en utilisant QRadar Network Insights pour analyser les différents éléments suivants :

- Sources
- Cibles
- Objet
- Contenu

Menaces internes

Vous pouvez intégrer QRadar Network Insights à l'application User Behavior Analytics pour améliorer la détection des menaces. Utilisez l'analyse QRadar Network Insights pour reconnaître les éléments suivants :

- Utilisateurs à haut risque
- Cibles potentielles d'hameçonnage
- Sentiment négatif
- Comportements suspects

Détection d'attaque de mutation latérale

QRadar Network Insights peut effectuer le suivi des communications anormales :

- Reconnaissance
- Transferts de données
- Acteurs malveillants

Protection contre l'exfiltration des données

Les données peuvent être exfiltrées via plusieurs méthodes. Utilisez QRadar Network Insights pour identifier et effectuer le suivi des fichiers suspects, par exemple :

- Anomalies de serveur DNS

- Contenu sensible
- Connexions anormales
- Alias

Identification des écarts de conformité

QRadar Network Insights permet une surveillance continue de la conformité par rapport à l'entreprise, au secteur d'activité et aux lois en vigueur.

3 Contenu QRadar Network Insights

Le contenu QRadar Network Insights chargé dépend du niveau d'inspection et de la disponibilité des données dans le système source.

Par exemple, un certain type de contenu est chargé par le flux X-Force Threat Intelligence mais la zone peut apparaître vide dans QRadar si les informations ne sont pas disponibles dans X-Force.

Pour inclure le contenu dans les recherches, sélectionnez les zones dans la section **Définition de colonne** du générateur de requête QRadar.

Vous pouvez également inclure le contenu dans les recherches avancées. Pour plus d'informations sur la création de recherches avancées, voir le document *IBM Security QRadar Ariel Query Language Guide*.

Contenu du niveau d'inspection de base

Lorsque le niveau d'inspection est **De base**, QRadar Network Insights remplit les zones suivantes :

Tableau 1. Contenu chargé avec le niveau d'inspection **de base**

Nom du générateur de requête	Nom de la recherche avancée	Source de données
Source IP address	`sourceip`	En-tête IPv4 ou IPv6 du paquet de flux
Source port	`sourceport`	En-tête TCP ou UDP du paquet de flux.
Destination IP address	`destinationip`	En-tête IPv4 ou IPv6 du paquet de flux
Destination port	`destinationport`	En-tête TCP ou UDP du paquet de flux.
IP protocol	`protocolid`	En-tête IPv4 ou IPv6 du flux.
Flow ID	`flowid`	Affectation par QRadar Network Insights.
Total Packets	`sourcepackets`, `destinationpackets`	Affectation et gestion par QRadar Network Insights*.
Total bytes per packet	`sourcebytes`, `destinationbytes`	Affectation et gestion par QRadar Network Insights*.
First Packet Time	`firstpackettime`	Affectation par QRadar Network Insights.
Last Packet Time	`lastpackettime`	Affectation par QRadar Network Insights.
Source DSCP	`sourcedscp`	Qualité IP du service dérivée de l'en-tête IPv4 ou IPv6 du paquet de flux*.
Destination DSCP	`destinationdscp`	Qualité IP du service dérivée de l'en-tête IPv4 ou IPv6 du paquet de flux*.
VLAN Tag	`"vlan tag"`	Zone renseignée uniquement lorsque le trafic réseau inclut des en-têtes VLAN.

Attributs du niveau d'inspection enrichi

Lorsque le niveau d'inspection est **Enrichi**, QRadar Network Insights remplit les zones suivantes :

Tableau 2. Contenu chargé avec le niveau d'inspection **enrichi**

Nom du générateur de requête	Nom de la recherche avancée	Source de données
Application	`applicationid`	Plusieurs sources (inspecteurs et X-Force, par exemple). L'attribut est renseigné par défaut.
Action	`action`	Zone renseignée uniquement lorsque les données X-Force sont disponibles. Les valeurs possibles pour l'action d'application sont les suivantes : • Write/Post/Chat • Stream/Download • Share • Start App • Audio Chat/Video Chat • Software/AV Updates
Password	`password`	Zone renseignée uniquement lorsque l'inspecteur recherche un mot de passe en clair.
File Name	`"file name"`	Zone renseignée uniquement lorsqu'un fichier est trouvé.
DNS Query	`"dns query"`	Zone renseignée uniquement si cet élément est un serveur DNS.
DNS Response	`"dns response"`	Zone renseignée uniquement si cet élément est un serveur DNS.
Recipient Users	`"recipient users"`	Plusieurs sources (messages électroniques ou messages de discussion, par exemple). Zone renseignée uniquement lorsque les données sont disponibles.
File Entropy	`"file entropy"`	Zone renseignée uniquement lorsqu'un fichier est trouvé.
Content Type	`"content type"`	HTTP, Inspecteur de contenu Zone renseignée uniquement lorsque le type de fichier n'est pas reconnu.
Web Categories	`"web categories"`	Zone renseignée uniquement lorsque les données X-Force sont disponibles.
File Hash	`"file hash"`	Zone renseignée uniquement lorsqu'un fichier est trouvé. Par exemple, le hachage de fichier peut être SHA256, MD5 ou SHA1.
File Size	`"file size"`	Zone renseignée uniquement lorsqu'un fichier est trouvé.
HTTP Host	`"http host"`	Zone d'hôte dans la demande HTTP. Zone renseignée uniquement si le protocole HTTP est utilisé.

Tableau 2. Contenu chargé avec le niveau d'inspection **enrichi** *(suite)*

Nom du générateur de requête	Nom de la recherche avancée	Source de données
HTTP Referrer	`"http referrer"`	Zone de référenceur dans la demande HTTP. Zone renseignée uniquement si le protocole HTTP est utilisé.
HTTP Response Code	`"http response code"`	Réponse à la demande HTTP. Zone renseignée uniquement si le protocole HTTP est utilisé.
Search Arguments	`"search arguments"`	Arguments de recherche dans la demande HTTP. Zone renseignée uniquement si le protocole HTTP est utilisé.
HTTP Server	`"http server"`	Zone de serveur dans la demande HTTP. Zone renseignée uniquement si le protocole HTTP est utilisé.
HTTP User Agent	`"http user agent"`	Zone d'agent utilisateur dans la demande HTTP. Zone renseignée uniquement si le protocole HTTP est utilisé.
HTTP Version	`"http version"`	Zone de version dans la demande HTTP. Zone renseignée uniquement si le protocole HTTP est utilisé.
Originating User	`"originating user"`	Plusieurs sources (messages électroniques ou messages de discussion, par exemple). Zone renseignée uniquement lorsque les données sont disponibles.
Request URL	`"request url"`	Chaîne d'URL Zone renseignée uniquement si le protocole HTTP est utilisé.
SMTP Hello	`"smtp hello"`	Demande SMTP Zone renseignée uniquement si le protocole SMTP est utilisé.
Content subject	`"content subject"`	Extrait des données utilisateur, uniquement lorsque les données sont disponibles. Par exemple, l'objet peut provenir d'un message électronique ou être intégré aux métadonnées.
Suspect Content Descriptions	`"suspect content descriptions"`	Plusieurs sources. Par exemple, le contenu suspect peut provenir de la catégorie de site Web, de liens intégrés ou de règles Yara. Zone renseignée uniquement lorsqu'une entité suspecte est détectée. Pour plus d'informations, voir les attributs de niveau d'inspection **avancé**.

Attributs du niveau d'inspection avancé

Le niveau d'inspection **avancé** capture les mêmes attributs de flux de contenu que le niveau d'inspection **enrichi**.

Cependant, lorsque le niveau d'inspection est **avancé** et que la liste de contenu suspect identifie une entité suspecte, les flux sont soumis à des processus d'extraction de contenu plus stricts.

La liste de contenu suspect est renseignée dans les conditions suivantes :

- La réputation de l'adresse IP d'un des noeuds finaux du flux est suspecte.
- La catégorie d'un site Web correspond à un entrée suspecte.
- Contenu suspect détecté dans les informations transférées
- Via l'analyse avec des règles Yara fournies par l'utilisateur.
- Scripts détectés dans les fichiers Office ou PDF.
- Liens intégrés détectés dans les fichiers PDF.
- Nombre excessif d'éléments détectés via la correspondance d'expression régulière.
- Numéros de carte de crédit, numéros de sécurité sociale, adresses IP et adresses électroniques détectés.
- Eléments définis par l'utilisateur détectés via la correspondance d'expression régulière marquée comme suspecte.
- Détection d'un protocole identifié s'exécutant sur un port non standard.
- Détection d'un certificat SSL/TLS utilisé en dehors de ses dates de validité.
- Détection de l'utilisation d'un certificat autosigné dans SSL/TLS.
- Détection de l'utilisation d'une longueur de clé publique insuffisante.

4 Extensions de contenu QRadar Network Insights

L'extension de contenu IBM QRadar Network Insights inclut des règles, des rapports, des recherches et des propriétés personnalisées QRadar supplémentaires pour les administrateurs. Ce contenu personnalisé de moteur de règle permet principalement d'effectuer des analyses, de créer des alertes et des rapports pour les déploiements QRadar Network Insights.

Remarque : Depuis l'extension de contenu v1.3.0, l'extension de contenu QRadar Network Insights est prise en charge uniquement par QRadar V7.3.0 ou version ultérieure.

Extension de contenu v1.1.0

L'extension de contenu IBM QRadar Network Insights v1.1.0 ajoute des règles, des recherches, des rapports et des extractions de propriété personnalisée grâce auxquels QRadar Network Insights peut disposer d'analyses, d'alertes et de rapports.

Cette extension est conçue pour ajouter du contenu destiné aux administrateurs ayant des dispositifs QRadar Network Insights dans leur déploiement (type de dispositif = 1901 ou 1920). Lorsqu'un administrateur installe ce pack de contenu, il est invité à remplacer le contenu existant car certaines propriétés personnalisées sont mises à jour avec ce pack de contenu.

Propriétés d'événement personnalisées ajoutées par l'extension de contenu v1. 1.0

L'extension de contenu QRadar Network Insights V1.1.0 inclut des propriétés d'événement personnalisées (nouvelles et mises à jour) pour la capture de contenu réseau à partir d'événements et de flux, tels que les utilisateurs destinataires, le hachage de fichier, les noms de fichier, le sujet de contenu et le code de rejet.

Tableau 3. Propriétés d'événement personnalisées dans l'extension de contenu v1. 1.0

Nom	Type de propriété	Expression régulière
Action	Flux	`IBM\(APP_ACTION\)=([^;]+);`
Content Subject	Flux	`IBM\(SUBJECT\)=([^;]+);`
Content_Type	Flux	`IBM\(HTTP_CONT_TYPE\)=([^;]+);`
DNS_Query_String	Flux	`IBM\(DNS_QUERY_SDATA\)=\(([^)]+)\);`
DNS_Response_String	Flux	`IBM\(DNS_RESP_SDATA\)=\(([^)]+)\);`
File Hash	Flux	`IBM\(HTTP_FILES_CKSUM\)=0x([^;]+);`
File Name	Flux	`IBM\(CONTENT_FILE_NAME\)=([^;]+);`
File_Size	Flux	`IBM\(HTTP_FILES_SIZE\)=([^;]+);`
HTTP Host	Flux	`IBM\(HTTP_HOST\)=([^;]+);`
HTTP Referrer	Flux	`IBM\(HTTP_REFER\)=([^;]+);`
HTTP Response Code	Flux	`IBM\(HTTP_RETURN_CODE\)=([^;]+);`
HTTP Server	Flux	`IBM\(HTTP_SRV\)=([^;]+);`
HTTP User-Agent	Flux	`IBM\(HTTP_UA\)=([A-Za-z0-9\s\-_.,:;()/\\]+);`
HTTP Version	Flux	`IBM\(HTTP_VRS\)=HTTP/([^;]+);`
IP_Dest_Reputation	Flux	`IBM\(IP_DST_REP\)=([^;]+);`
Originating_User	Flux	`IBM\(ORIG_USER\)=([^;]+);`
Password	Flux	`IBM\(ACTPASSWD\)=([^;]+);`

Tableau 3. Propriétés d'événement personnalisées dans l'extension de contenu v1. 1.0 (suite)

Nom	Type de propriété	Expression régulière
Recipient User	Evénement	Plusieurs expressions régulières pour Microsoft Exchange, Linux OS, Solaris OS et Barracuda Spam and Virus Firewall.
Recipient Users	Flux	`IBM\(DEST_USER_LIST\)=\(([^)]+)\);`
Reject Code	Evénement	Plusieurs expressions régulières pour Microsoft Exchange, Linux OS, Solaris OS et Barracuda Spam and Virus Firewall.
Request_URL	Flux	`IBM\(REQ_URL\)=([^;]+);`
Search_Arguments	Flux	`IBM\(HTTP_SEARCH_ARGS\)=([^;]+);`
SMTP HELO	Flux	`IBM\(SMTPHELO\)=([^;]+);`
Suspect_Content	Flux	`IBM\(SUSPECT_CONT_LIST\)=\(([^)]+)\);`
Web_Categories	Flux	`IBM\(HTTP_CONT_CATEGORY_LIST\)=\(([^)]+)\);`

Règles ajoutées par l'extension de contenu v1. 1.0

L'extension de contenu QRadar Network Insights V1.1.0 inclut quatre nouvelles règles qui se déclenchent lors du hachage de fichier et de tentatives de courrier indésirable ou d'hameçonnage.

Tableau 4. Règles ajoutées dans l'extension de contenu v1. 1.0

Nom de règle	Description
Observed File Hash Associated with Malware Threat	Cette règle se déclenche lorsque le contenu de flux inclut un hachage de fichier correspondant aux hachages de fichier incorrects connus inclus dans un flux de données Threat Intelligence. Indique qu'une personne a transféré un logiciel malveillant via le réseau.
Observed File Hash Seen Across Multiple Hosts	Cette règle se déclenche lorsqu'il est détecté qu'un même hachage de fichier associé à ce logiciel malveillant a été transféré vers plusieurs destinations.
Potential Spam/Phishing Attempt Detected on Rejected Email Recipient	Cette règle se déclenche lorsqu'il est détecté dans le système que des e-mails envoyés à une adresse de destinataire qui n'existe pas ont été rejetés. Cela peut indiquer un courrier indésirable ou une tentative d'hameçonnage. Configurez le bloc de construction BB:CategoryDefinition: Rejected Email Recipient afin d'inclure des ID QRadar (QID) adaptés à votre entreprise. Cet élément est préchargé avec des ID QID pour la surveillance de Microsoft Exchange, Linux OS [exécutant sendmail], Solaris Operating System Sendmail Logs et Barracuda Spam & Virus Firewall.
Potential Spam/Phishing Subject Detected from Multiple Sending Servers	Cette règle se déclenche lorsque plusieurs serveurs envoient le même sujet de message électronique au cours d'une période, ce qui peut indiquer du courrier indésirable ou des tentatives de hameçonnage.

Recherches ajoutées par l'extension de contenu v1. 1.0

L'extension de contenu QRadar Network Insights V1.1.0 inclut quatre nouvelles recherches. Ces recherches sont conçues pour aider les utilisateurs à trier le contenu de type hameçonnage ou de logiciel malveillant dans les données de flux qui utilisent des informations de fichier et de hachage ou des informations de sujet de contenu dans des messages électroniques.

Les recherches suivantes ont été ajoutées dans l'extension de contenu v1. 1.0 :

- Malware Distribution by File and Hash
- Malware by Hash and Source Asset
- Malware Traffic Summary

- Phishing Subjects by Recipient User

Rapports ajoutés par l'extension de contenu v1. 1.0

L'extension de contenu QRadar Network Insights V1.1.0 inclut trois nouveaux rapports pour les équipes de sécurité. Ces rapports exécutent des recherches qui identifient l'hameçonnage en fonction du contenu d'objet et du logiciel malveillant utilisant des informations de fichier et de hachage disponibles dans les données de flux. Ces nouveaux rapports s'exécutent une fois par semaine ou une fois par jour.

Tableau 5. Rapports ajoutés dans l'extension de contenu v1. 1.0

Nom de rapport	Planification de rapport
Top Phishing Subjects by Recipient User (QNI)	Hebdomadaire
Top Malware by Asset (QNI)	Quotidienne
Malware Distribution by File (QNI)	Quotidienne

Fonctions personnalisées ajoutées par l'extension de contenu v1. 1.0

Une fonction AQL personnalisée *EMAIL::ISREPLY* pour les sujets de contenu peut être appelée. Elle utilise une recherche avancée de l'onglet Activité réseau. Le but de cette fonction personnalisée est d'identifier les objets de courrier électronique qui sont des réponses à des courriers électroniques. Par exemple, une requête AQL peut permettre aux administrateurs de rechercher des données de flux et de renvoyer des résultats pour les objets de courrier électronique qui ne sont pas vides (aucun objet de courrier électronique) et les objets de courrier électronique qui ne sont pas des réponses RE: [objet de courrier électronique]. Ainsi, les utilisateurs peuvent rechercher au sein de l'entreprise les courriers étant des réponses (RE:) aux courriers d'hameçonnage car la fonction recherche dans les données de flux les objets de courrier électronique contenant "RE:".

Tableau 6. Fonctions personnalisées ajoutées dans l'extension de contenu v1. 1.0

Nom de la fonction de l'objet de contenu	Description
Custom Function	`isReply()`
Usage	`EMAIL::ISREPLY(Content_Subject)`
Namespace	`Email`
Name/Execute Function Name	`isReply`
Description	Cette fonction vérifie si la propriété, Content_Subject, inclut Re:

Autre contenu de référence requis par l'extension de contenu v1. 1.0

Dans la plupart des cas, ces blocs de constructions et ces ensembles de données de référence sont présents dans QRadar, ce qui fait qu'aucune nouvelle mise à jour n'est requise. Toutefois, ce contenu est requis pour les règles, les recherches, les rapports et les propriétés personnalisées incluses dans le pack de contenu QRadar Network Insights. Si le contenu ci-dessous n'existe pas dans QRadar, il est créé par ce pack de contenu.

Blocs de construction requis par l'extension de contenu QRadar Network Insights :

- BB:HostDefinition: Mail Servers
- BB:HostReference: Mail Servers
- BB:PortDefinition: Mail Ports

Données de référence requises par l'extension de contenu QRadar Network Insights :

- Malware Hashes SHA
- Malware Hashes MD5
- Phishing Subjects
- Mail Servers

Extension de contenu v1. 2.0

L'extension de contenu IBM QRadar Network Insights V1.2.0 ajoute des règles et des extractions de propriété personnalisée grâce auxquelles QRadar Network Insights peut disposer d'analyses, d'alertes et de rapports.

Cette extension est conçue pour ajouter du contenu destiné aux administrateurs ayant des dispositifs QRadar Network Insights dans leur déploiement (type de dispositif = 1901 ou 1920).

Remarque : Certaines propriétés personnalisées sont mises à jour dans ce pack de contenu. Il peut être nécessaire de remplacer le contenu existant.
Lorsqu'un administrateur installe ce pack de contenu, il est invité à remplacer le contenu existant car certaines propriétés personnalisées sont mises à jour avec ce pack de contenu.

Règles et propriétés d'événement personnalisées ajoutées par l'extension de contenu v1. 2.0

Tableau 7. Règles et propriétés d'événement personnalisées

Type	Contenu mis à jour	Description de la modification
Propriété personnalisée	**File_Size (Flux)** Mise à jour de l'action de règle afin de sélectionner "Vérifier que l'élément événement détecté fait partie d'une infraction". Dans la version 1.1.0, cette case à cocher n'était pas sélectionnée. Ce point a été corrigé dans la version 1.2.0 afin de garantir que des infractions sont créées.	Mise à jour de la propriété personnalisée File_Size (flux) afin de changer le type de zone d'alphanumérique en numérique. Cette mise à jour optimise également la propriété personnalisée pour le contenu source et le contenu cible.
Règle	**Potential Spam/Phishing Attempt Detected on Rejected Email Recipient**	Mise à jour de l'action de règle afin de sélectionner "Vérifier que l'élément événement détecté fait partie d'une infraction". Dans la version 1.1.0, cette case à cocher n'était pas sélectionnée. Ce point a été corrigé dans la version 1.2.0 afin de garantir que des infractions sont créées.
Règle	**Access to Improperly Secured Service - Certificate Invalid**	Nouvelle règle ajoutée pour QRadar Network Insights afin de détecter les sessions SSL/TLS utilisant des certificats non valides.
Règle	**Access to Improperly Secured Service - Weak Public Key Length**	Nouvelle règle ajoutée pour QRadar Network Insights afin de détecter les sessions SSL/TLS utilisant des longueurs de clé publique insuffisantes.
Règle	**Access to Improperly Secured Service - Certificate Expired**	Nouvelle règle ajoutée pour QRadar Network Insights afin de détecter les sessions SSL/TLS utilisant des certificats arrivés à expiration.
Règle	**Access to Improperly Secured Service - Self Signed Certificate**	Nouvelle règle ajoutée pour QRadar Network Insights afin de détecter les sessions SSL/TLS utilisant un certificat autosigné.

Extension de contenu v1. 3.0

L'extension de contenu IBM QRadar Network Insights V1.3.0 assure la prise en charge de QRadar versions 7.3.0 et versions ultérieures.

Cette extension constitue un support pour les administrateurs ayant des dispositifs QRadar Network Insights dans leur déploiement (type de dispositif = 1901 ou 1920). Les propriétés personnalisées des versions précédentes de l'extension de contenu QRadar Network Insights sont désormais des zones TLV.

Remarque : Certaines propriétés personnalisées sont mises à jour dans ce pack de contenu. Il peut être nécessaire de remplacer le contenu existant.

Extension de contenu v1. 4.0

L'extension de contenu IBM QRadar Network Insights V1.4.0 ajoute des règles, des rapports, des recherches sauvegardées et des blocs de constructions grâce auxquels QRadar Network Insights peut disposer d'analyses, d'alertes et de rapports.

L'extension de contenu QRadar Network Insights V1.4.0 ajoute des recherches sauvegardées, des rapports, des règles et des blocs de construction. De plus, elle permet l'intégration entre QRadar Network Insights et les règles User Behavior Analytics. Ces dernières sont activées par défaut mais si vous utilisez l'application User Behavior Analytics, vous pouvez les désactiver. Le tableau suivant présente les modifications effectuées dans l'extension de contenu QRadar Network Insights V1.4.0.

Tableau 8. Contenu mis à jour par QRadar Network Insights V1.4.0

Type	Contenu mis à jour	Description de la modification
Recherche sauvegardée	**File Transfer by Originating User and Content Type**	Cette recherche de journal et d'activité réseau correspond aux transferts de fichier en fonction des utilisateurs d'origine et des types de contenu.
Recherche sauvegardée	**File Transfer by Source IP and Content Type**	Cette recherche de journal et d'activité réseau correspond aux transferts de fichier en fonction des IP source et des types de contenu.
Rapport	**User File Transfer by Content Type**	Affiche les 20 principaux transferts de fichier utilisateur par type de contenu, en regroupant les recherches de journal et d'activité réseau suivantes : • **File Transfer by Originating User and Content Type** • **File Transfer by Source IP and Content Type**
Règle	**QNI: Confidential Content Being Transferred to Foreign Geography**	Recherche un contenu confidentiel transféré vers les pays/régions avec un accès restreint.
Règle	**UBA : QNI - Confidential Content Being Transferred to Foreign Geography**	Envoie des événements à l'application User Behavior Analytics en fonction de la règle **QNI: Confidential Content Being Transferred to Foreign Geography**. A cette règle est affectée une valeur **senseValue**, qui est utilisée lorsque l'application User Behavior Analytics calcule un score de risque pour un utilisateur.
Règle	**UBA : QNI - Potential Spam/Phishing Subject Detected from Multiple Sending Servers**	Envoie des événements à l'application User Behavior Analytics en fonction de la règle **QNI: Potential Spam/Phishing Subject Detected from Multiple Sending Servers**. A cette règle est affectée une valeur **senseValue**, qui est utilisée lorsque l'application User Behavior Analytics calcule un score de risque pour un utilisateur.

Tableau 8. Contenu mis à jour par QRadar Network Insights V1.4.0 (suite)

Type	Contenu mis à jour	Description de la modification
Règle	**UBA : QNI - Potential Spam/Phishing Attempt Detected on Rejected Email Recipient**	Envoie des événements à l'application User Behavior Analytics en fonction de la règle **QNI: Potential Spam/Phishing Attempt Detected on Rejected Email Recipient**. A cette règle est affectée une valeur **senseValue**, qui est utilisée lorsque l'application User Behavior Analytics calcule un score de risque pour un utilisateur.
Règle	**UBA : QNI - Observed File Hash Associated with Malware Threat**	Envoie des événements à l'application User Behavior Analytics en utilisant la règle **QNI: Observed File Hash Associated with Malware Threat** avec la valeur senseValue. Cette valeur est utilisée lorsque l'application User Behavior Analytics calcule un score de risque pour un utilisateur.
Règle	**UBA : QNI - Observed File Hash Seen Across Multiple Hosts**	Envoie des événements à l'application User Behavior Analytics en utilisant la règle **QNI: Observed File Hash Seen Across Multiple Hosts** avec la valeur senseValue. Cette valeur est utilisée lorsque l'application User Behavior Analytics calcule un score de risque pour un utilisateur.
Règle	**UBA : QNI - Access to Improperly Secured Service - Weak Public Key Length**	Envoie des événements à l'application User Behavior Analytics en fonction de la règle **QNI: Access to Improperly Secured Service - Weak Public Key Length**. A cette règle est affectée une valeur **senseValue**, qui est utilisée lorsque l'application User Behavior Analytics calcule un score de risque pour un utilisateur.
Règle	**UBA : QNI - Access to Improperly Secured Service - Certificate Invalid**	Envoie des événements à l'application User Behavior Analytics en fonction de la règle **QNI: Access to Improperly Secured Service - Weak Public Key Length**. A cette règle est affectée une valeur **senseValue**, qui est utilisée lorsque l'application User Behavior Analytics calcule un score de risque pour un utilisateur.
Règle	**UBA : QNI - Access to Improperly Secured Service - Certificate Expired**	Envoie des événements à l'application User Behavior Analytics en fonction de la règle **QNI: Access to Improperly Secured Service - Certificate Expired**. A cette règle est affectée une valeur **senseValue**, qui est utilisée lorsque l'application User Behavior Analytics calcule un score de risque pour un utilisateur.
Règle	**UBA : QNI - Access to Improperly Secured Service - Self Signed Certificate**	Envoie des événements à l'application User Behavior Analytics en fonction de la règle **QNI: Access to Improperly Secured Service - Self Signed Certificate**. A cette règle est affectée une valeur **senseValue**, qui est utilisée lorsque l'application User Behavior Analytics calcule un score de risque pour un utilisateur.
Bloc de construction	**BB: Category Definition: Countries/Regions with Restricted Access**	Editez ce bloc de construction afin d'inclure un emplacement géographique qui généralement n'est pas autorisé à accéder à l'entreprise. Une fois qu'il est configuré, vous pouvez activer la règle **Confidential Content Being Transferred to Foreign Geography**.

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.

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 produit 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.

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).