Cisco 2018 Security Capabilities Benchmark Study: Defenders report greater reliance on automation and artificial intelligence

Chief information security officers (CISOs) interviewed for the Cisco 2018 Security Capabilities Benchmark Study report that they are eager t

Figure 7 is an overview of web attack methods over a three-year period, from October 2014 to October 2017. Adversaries consistently employed suspicious binaries during this period, primarily to deliver adware and spyware. As discussed in the *Cisco 2017 Midyear Cybersecurity Report*, these types of

Many new domains tied to malvertising campaigns

The resources that RLDs reuse give clues to whether the

Insider threats: Taking advantage of the cloud

Recommendations

Many ICS breaches begin with the compromise of vulnerable

In examining critical advisories (Figure 35), Apache Struts

IoT and library vulnerabilities loomed larger in 2017

Between October 1, 2016, and September 30, 2017, Cisco threat researchers discovered 224 new vulnerabilities in non-Cisco products, of which 40 vulnerabilities were related to third-party software libraries included in these products, and 74 were related to IoT devices (Figure 36).

The relatively large number of vulnerabilities in libraries

Complexity created by vendors in orchestration

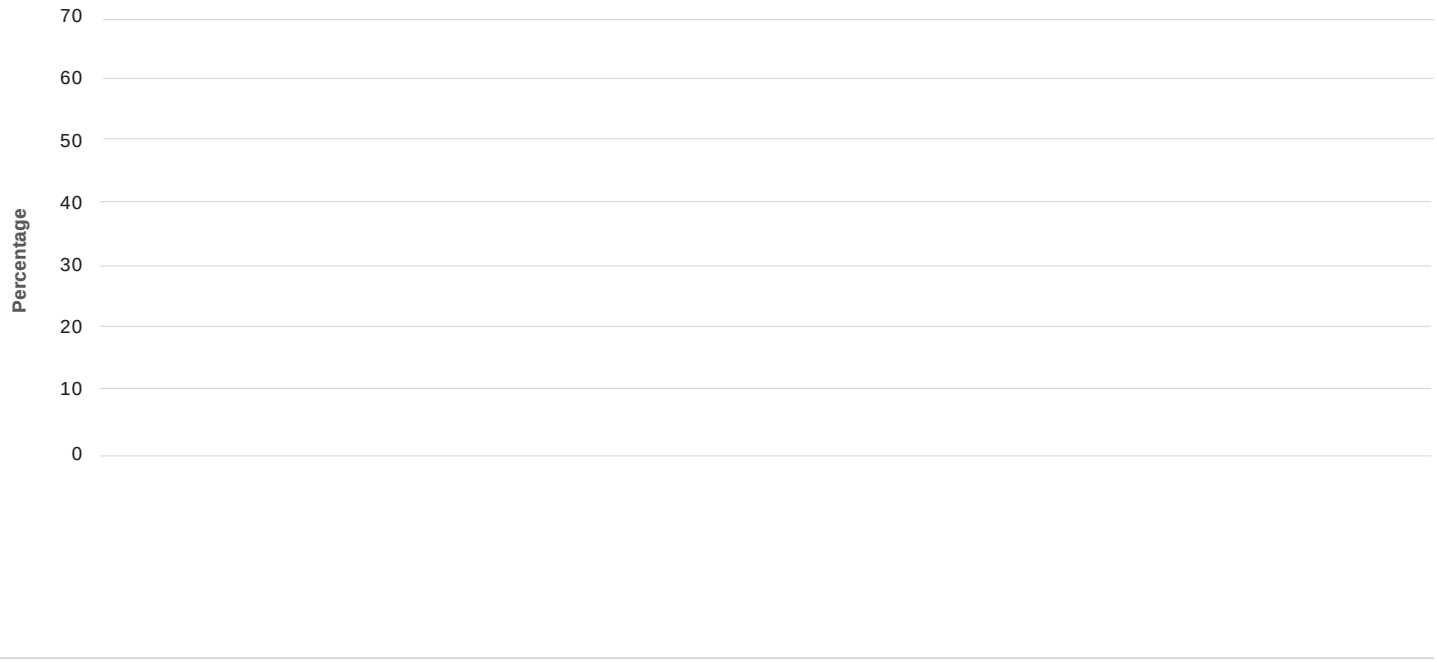
Security professionals expect to spend more on tools that use artificial intelligence and machine learning in a bid to improve defenses and help shoulder the workload. In addition, they plan to invest in tools that will provide safeguards for critical systems, such as critical infrastructure services.

Conclusion

Conclusion

In the modern threat landscape, adversaries are adept at

About Cisco


70
60
50
40
30
20
10
0
Percentage