Flyer
Security

Adding Intelligence to Your SIEM: What Threat Intelligence Is and Why It Is Important

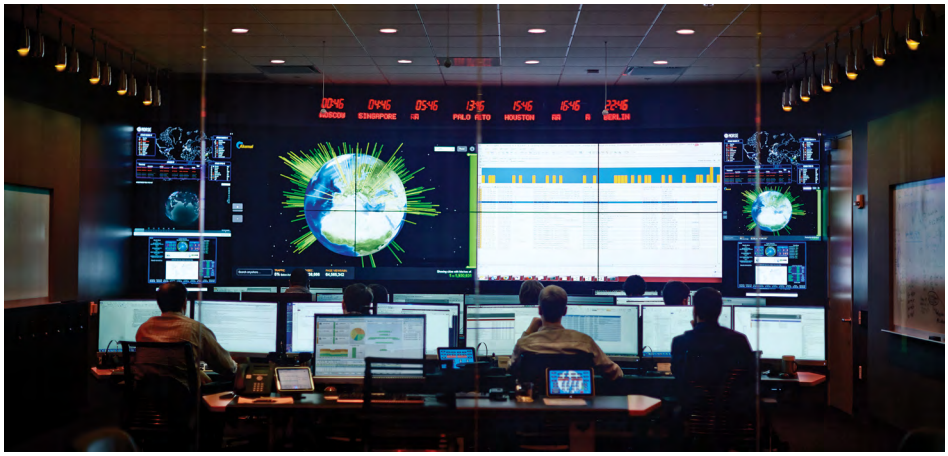
Security information and event management (SIEM) systems are a key component for security operations. Learn to incorporate cyber threat intelligence (CTI) to get more value from your SIEM.

Security information and event management (SIEM) software and appliances are a central piece of any security operations center (SOC) for enterprises and corporations. SIEM provides a core capability for SOCs to collect logs and data from multiple sources within their networks to evaluate, analyze, and correlate network events. The events once correlated are analyzed by the SIEM to detect known threats. This is extremely valuable for SOC organizations, but a primary challenge is the continued evolution of cyber threats and device vulnerabilities. SOCs are not only challenged with maintaining their current environment, but also learning and understanding new threats across the cyber landscape that affect their network and environments. How can SIEMs be improved to better protect networks, endpoints, environments, and global corporations and increase their threat awareness?

Threat intelligence feeds are one solution to this challenge.

Cyber Threat Intelligence (CTI)

Cyber threat intelligence feeds are sources of information, indicators, and artifacts gathered from security researchers and analysts to provide information to security organizations to better improve their cybersecurity methods. These third-party streams of information and data allow security analysts to have the ability to leverage intelligence and experience from other enterprises that are aware of the cyber landscape. This information is valuable for SOCs with limited resources and also for SOCs with unlimited budgets. The shared information within the security community from



verified and knowledgeable security engineers is useful to all.

The primary data sources are malware processing, custom telemetry, honeypots and darknets, scan and crawling, open source, and human intelligence.

There are two types of cyber threat intelligence (CTI) with data sources that security engineers can access: Open Source and Subscription Based. Most intelligence feeds are in a standard format, which allows for data to be shared between organizations and their security tools. ArcSight ESM, with their free Activate Threat Intelligence package, now supports both the CIF and STIXX CTI formats. Micro Focus has partnerships with leading CTI vendors, like Anomali, Infoblox, EclectIQ and ThreatConnect. These packages allow security analysts and engineers to get more value out of their SIEM by adding new correlation and alerting, evaluating the CTI data against the telemetry and data feeds they are already ingesting. Threat Intelligence is now considered so valuable, that the Department of Homeland Security now allows both US government and private industries to subscribe to their Automated Indicator Sharing (AIS) program.

The Cybersecurity Information Sharing Act of 2015 (CISA) creates a framework for United States federal agencies to voluntarily share data amongst themselves. Security analysts and engineers must continue to review feeds, provide feedback, and evaluate the information received to see if it is pertinent for their environment.

There are some challenges with CTI to be aware of. Open Source feeds are free and contain large data sets contributed by diverse participants.

ArcSight ESM incorporates CTI within the Activate Framework and RepSM+.

Contact us at:
www.microfocus.com

Like what you read? Share it.

However, contributors and indicators are not always well vetted. They often put emphasis on velocity and volume, letting the consumers vet the indicators they receive. Unvetted feeds however, can waste analyst's time responding to the high number of false positives.

Fee-Based or Subscription-Based CTI includes curated intelligence; moreover, it is more focused, and produces fewer false positives. Paid intelligence feeds are validated and reviewed by security engineers and by organizations with researchers and analysts. These organizations focus resources on collecting data, reviewing information, reverse engineering threats, and providing insight into the malicious nature of threats. The alerts and warnings from these feeds provide the most immediate value to SOCs.

Threat Intelligence Is Useful for All Security Organizations

Corporations face an increasing amount of threats. It is no longer a matter of *if* an attack will happen, it is a matter of *when*. Corporations and their SOCs require more information, more awareness, and more intelligence. The implementation of CTI within a security organization's SIEM provides insight from the global cybersecurity community and supplies valuable threat awareness capabilities that can improve the security posture of any corporation.

Learn more at

www.microfocus.com/arcsightactivate

www.microfocus.com/arcsightesm

www.microfocus.com/media/data-sheet/repsm_plus_threat_intelligence_ds.pdf

161-000440-001 | H | 01/20 | © 2020 Micro Focus or one of its affiliates. Micro Focus and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.