Security incident 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.

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.
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. Unvetoed 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 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.

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 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**

increasing amount of threats against their corporations. It is a matter of when an attack occurs. It is no longer if an attack will happen. Corporations want more information. SOCs require more information, more awareness, and more intelligence. The implementation of CTI within a security organization’s SIEM provides valuable threat awareness capabilities helping the security posture of a corporation. The intelligence from security engineers and researchers worldwide can help large and small departments with insight from the cybersecurity community. For more information on how CTI can advance your company’s SIEM capabilities, download the Micro Focus® use case outlining ArcSight ESM 7.0 and the utilization of threat intelligence feeds to improve your SOC organization.

Learn More At

www.microfocus.com/arcsightactivate
www.microfocus.com/arcsightesm