More Sources, More Use Cases, Equals More Secure

Mature SOCs know it's not just about more data. Data without a use case is just noise. It's about being smart with that data and putting analytics behind the data to drive use cases and actionable response.

"ArcSight ESM provides the best ability to create use cases quickly, easily, and effectively."

KEVIN WHELAN
Chief Technology Officer
ITC Secure Networking

More Sources, More Use Cases = More Secure

As technology advances, so does the fear of potential cyber-attacks. It is important for any company to keep their critical information safe. Last year alone bore witness to one of the largest and most preventable cyber-attacks—the Equifax data breach. Sadly, this was only one example within hundreds[1] of worldwide breaches, which left millions of people's information compromised. Experts agree that security breaches, network hacks, and potential infrastructure vulnerabilities are going to increase[2]. Given this grim outlook, it is important that innovations in cyber-security keep pace with growing business complexities and the modern technologies now being utilized. Research and development must continue to make innovations in technology, but it's also important security teams refine their internal processes and approach to deter cyber-attacks and mitigate threats quickly. Advanced concepts like SecDevOps, agile and having clearly defined security use cases can lead the way to developing an intelligent SOC.

Figure 1. More Sources, More Use Cases = More Secure

Intro to SIEM and Use Cases

Security incident and event management, known as SIEM, centrally collects, aggregates and analyzes event data and logs across an environment to identify threats. Using this powerful correlation technology does not equate to security teams instantly uncovering all bad actors within their network. Network and assets must be defined. Environments and business assets vary, internal policies differ, and risks must be calculated against security controls. Because of all these variables, repeatable and efficient processes should be followed in defining and solving the complex security problems. The most effective approach when building successful SIEM alerts begins with the Use Case.

A use case is simply a formal way to define a security problem, how to alert and respond to that problem and what parameters are necessary for that alert to trigger. When defining the use case, both the security teams and analysts as well as the system owners and stakeholders should be involved. Throwing security problems over the wall asking the security team to "find the bad guys and vulnerabilities"

1 **www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/**
2 **www.businessinsider.com/cyber-attacks-against-our-critical-infrastructure-are-likely-to-increase-2016-5**

> **"The magic here is that we control the amount of false positive by tuning and understanding what works best for us—ArcSight is flexible enough to allow us to do that"**
>
> **DORI FISHER**
> Head Of Managed Cyber Security Services
> BDO Cyber Security Center

Contact us at:
www.microfocus.com

is a recipe for disaster. Micro Focus provides a good SIEM Use Case template for reference on the ArcSight Best Practices page.

ESM 7.0 Is Central to Security

A SIEM sits at the center of an intelligent SOC. It's often the only tool with visibility from an organizations perimeter, down to the internal business applications. Organizations understand that a security tool is only as good as the visibility it provides. The most expensive point solutions, sitting isolated from the data they need to identify malicious activity, are useless. Unfortunately, previous SIEM implementations had to be designed in makeshift hierarchal ways to distribute the event and processing load. Conversely, some organizations chose to limit visibility by selectively choosing which data sources to collect and correlate. Recent technological advancements in collection, like Kafka based open message bus Event Broker, and ESM 7.0's distributed correlation, finally allow ArcSight to scale to meet demand. These two huge advancements together, are a result of the need to collect events from across customer enterprises to apply analytics and correlation around the events occurring.

More Sources + More Use Cases = More Secure

SIEMs can now scale to match the pace of the technology and data volume being generated, thus reestablishing their importance in collecting events from across the enterprise in order to apply correlation and analytics across the enterprise. Security operations and system owners should adopt a SecDevOps cycle where new security use cases are consistently defined. The necessary event feeds for those use cases are then added to SIEMs centralized event collection architecture and alerting and response procedures are structured. Organizations have gone so far as to require a set number of new SIEM use cases to be pushed in to production each month to keep up with the nature evolving cyber threats.

Another impactful change helping SOCs build security content and new use cases is the ArcSight Activate Framework. Developing content around a common attack cycle allows engineers to reuse and share solutions without having to re-invent the wheel each time there is a new threat. Activate includes best practice correlation rule sets, visualization dashboards and event channels for analysts to monitor, all included in easily deployable packages. Review the latest packages being developed by our security subject matter experts here: **https://marketplace.microfocus.com/arcsight** and other community driven solutions on the ArcSight marketplace here: **https://marketplace.microfocus.com/arcsight/category/partner-integrations**

Threats are continuing to evolve and advance. ArcSight ESM 7.0 with ArcSight Data Platform (ADP) and Event Broker gives SOCs the power and scalability to build security controls that keep pace. For help defining more use cases and building an architecture to support the new event sources and data, contact Micro Focus® security professionals.

Learn more at the ArcSight Community page here.