Security Information and Event Management

What is a SIEM?

A SIEM (security information and event management) system is a security product that aggregates log data from multiple sources across an enterprise to provide centralized visibility of all activity related to IT security. It collects activity logs from sources such as laptops, servers, intrusion detection systems, domain name servers, and security and network devices. A SIEM combines security information management (SIM) and security event management (SEM) into one security platform/product.

What are the differences between a SIM and a SEM?

A SIM performs log data gathering, offering quick search, reporting and centralized log management. It cannot conduct real-time analysis or correlations, but a SEM handles these more demanding tasks. Paired with a SIM, it enables IT security staff to identify alerts/ incidents requiring response and remediation.

What customer pain points does a SIEM address?

A SIEM is a major upgrade over multiple security products that require IT security staff to view multiple dashboards to get comprehensive visibility. A SIEM can:

- Aggregate logs from multiple sources including devices, laptops, servers, and security products
- Implement a unified dashboard for visibility across the enterprise
- Reduce risks from denial-of-service attacks, brute-force attacks and data breaches
- Simplify regulatory compliance, avoiding exorbitant fines for violations

What technical capabilities does a SIEM bring to the table?

A SIEM gives security teams access to features for centralized log management (with search and reporting), correlation to identify threats needing attention/response, security incident prioritization and compliance with regulatory mandates (e.g., PCI-DSS, HIPAA, SOX, etc.).

Why is it complex and time consuming to deploy and manage a SIEM?

A SIEM can become a never-ending work in progress, requiring constant tuning and updating to keep pace with a rapidly evolving security environment. It requires 24/7 management by security experts, who are capable of triaging alerts. And it needs threat intelligence subscriptions for awareness of the latest threats; it must have established baselines for unusual user behavior (e.g. someone logging in from a different country); and it requires specialized parsers for the different log sources.

What can go wrong with a SIEM?

Misconfigurations are common when deploying a SIEM. The deployment cycle is lengthy, up to six months plus. Ultimately, customers can spend a considerable amount of money, time and effort on SIEM licenses, hardware, maintenance, monitoring and response.

What are the different SIEM deployments?

DIY SIEM

Under this approach, the customer builds and manages its own SIEM, being responsible for proper architecture design and rollout, as well as around-the-clock monitoring. This brings a relatively high total cost of ownership.

Co-managed SIEM

A co-managed SIEM is owned by the customer but managed by an external party like a managed security services provider (MSSP), which handles all administration, monitoring and incident response.

Managed SIEM

This SIEM type entrusts everything to someone else. The customer does not have to worry about the various complexities associated with SIEM ownership and upkeep, while getting all essential benefits.

What is the difference between a SIEM and a SOC?

A SIEM is technology in isolation. It lacks the necessary people and processes for actual operation. A SOC (security operations center) incorporates a SIEM with these additional layers.

What is SOC-as-a-service?

The newest approach to deliver a SOC as a managed service that includes the necessary people, processes and a cloud-based SIEM technology, SOC-as-a-service allows customers to pay a predictable subscription fee for a managed detection and response (MDR) service and more. It's a turnkey solution that deploys quickly (under 60 minutes) and includes threat intelligence at no extra cost.

What is the cost of managing a SIEM vs a SOC?

Building your own SOC on-premises is at least three times more expensive than subscribing to a SOC-as-a-service. The build route requires an initial purchase and deployment of a SIEM, subscribing to threat intelligence feeds, developing processes for incident response, and hiring security experts to manage your SOC. Building your own SOC can take six months to one year to realize value. Whereas a SOC-as-a-service can be deployed quickly and start realizing value in less than one week.

What is AWN CyberSOC™?

Arctic Wolf offers a SOC-as-a-service solution that meets the specific critical security requirements of small-to-midsize enterprises. The AWN CyberSOC™ is affordable and deploys in less than 60 minutes. It provides continuous network monitoring, log aggregation and correlation, incident response and MDR services, as well as personalized security services with a named security engineer to improve each customer's overall security posture.

ARCTIC WOLF

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com