WHAT IS SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)?

In the myriad of IT systems designed to protect an enterprise's sensitive data, it's the Security Information and Event Management (SIEM) software that assembles all the security logs and event data into a central location for meaningful analysis of past breach events, detection of security weaknesses, and validation of audit records for compliance regulations. SIEM software built on strong data management procedures is becoming to enterprise security professionals what Houston is to the astronauts.

SIEM (pronounced "sim") software has been around for over a decade and in its most basic form is designed to do four things:

- Accept relevant data from multiple sources
- Normalize and analyze the data
- Identify potential security issues
- Take action by generating alerts or instructing other security controls to shut down the offending activity

These are not small tasks and an organization's SIEM system is only as good as the data on which it's built.

Making Sense of Log Data

Today's data security ecosystems span across host systems, network devices, servers, domain controllers, firewalls, antivirus filters, intrusion prevention systems, and so on. Each of these networked components generates their own log and event data which are text-based files that are produced automatically every time certain events occur in the system. Log files are usually time-stamped and may record practically anything that is happening behind the scenes in operating systems or software applications, including when users log in or attempt to log in.

Not only are numerous log files created any time an activity happens, to complicate things a bit more, not all log data is created the same -- literally. There are audit logs, transaction logs, event logs, error logs, and message logs that all serve different purposes and can come in a variety of extensions like .log .txt or even proprietary extensions. Some logs can be read by using a standard text editor while others require particular applications to view and extract useful data from them. Some logs can be read by a human while others that are kept for auditing purposes that are not even human-readable.

Over time, the number of logs grows exponentially, especially in larger enterprises that can generate hundreds of gigabytes of log data per day. This immense amount of disparate data creates the need for a systematic approach to maintaining security logs. Log management is the discipline of developing processes to collect, centralize, parse, transmit, store, archive, and dispose of massive amounts of computer-generated log data, especially for the purposes of security, performance enhancements, auditing, or troubleshooting. A good log management system is key to getting the information aggregated and unified in one location, but it is still only one piece of a holistic system that utilizes the information in these logs for real-time security monitoring.

Why SIEM is Important

The management of all this data is an expensive, time, and resource-consuming process that requires a lot of customization and planning. However, the value of these logs is not in the logging itself. It's in the analysis of the logs to address three important aspects of a comprehensive security strategy.

Incident Detection

A well-run SIEM system can detect security incidents that would go unnoticed without it by logging security events, analyzing the log entries for signs of attack or malicious activity from sources across the network. A SEIM can use this data to reconstruct the events and determine the nature of the attack and if it did or did not succeed.

Regulatory Compliance

Regulated industries rely heavily on SIEM because failing a compliance audit could mean loss of business, damage to reputation, and hefty fines. SIEM is a method for companies to protect their most sensitive data and establish proof they are doing so, which allows requirements to be met.

Incident Management

SIEM solutions can significantly increase the efficiency of incident handling with the real-time monitoring and customized alerts and protocols security teams establish. This ultimately increases the speed of incident containment, which can reduce the extent of damage a breach can cause.

Evolution of SIEM

SIEM evolved out of the log management discipline by combining SIM (Security Information Management) and SEM (Security Event Management), which both have specific focuses concerning the observance of abnormal behavior and potential breaches within log and event data.

- SIM primarily focuses on storing, analyzing, manipulating, and reporting on logs and security records
- SEM primarily focuses on real-time monitoring and correlating events, and providing console views with custom notifications

Combining these techniques into SIEM software and tools creates a birds-eye-view of all security data. This approach blends all SIM and SEM functions into a single source of truth for an enterprise's security management team to monitor for abnormal behavior and potential cyberattacks across their network by filtering massive amounts of security data while prioritizing the security alerts the software generates.

SIEM Software Today

As the market for SIEM expands into a $2 billion industry, so do the capabilities of what newer products offer companies who want to leverage SIEM to set up a security operations center. SIEM technologies are now bringing in threat intelligence feeds in addition to log data while other products have security analytics which are able to look at network behavior and how it coincides with user behavior to give more intelligence around whether an activity is indicative of maliciousness. AI and machine learning are also being incorporated into SIEM software with the ultimate goal of providing more accurate threat detection rates at a faster pace.

Most companies continue to use SIEM software primarily for tracking and investigating the events surrounding a breach which is driven by the fallout impacting an organization if a breach does occur. As more and more security breaches impact companies of all sizes, SIEM advancements are focusing on speed of detection and near real-time response.

BMC: Your Security Information and Event Management Partner

BMC AMI Command Center for Security is an affordable Security Information & Event Management system especially designed and preconfigured for use by z/OS security administrators and system programmers.

Benefits:

- Point-and-click functionality from a standard web browser
- Dashboard views
- Event message correlation

- Text messages as alerts of security events generated from z/OS
- Integrates RACF, CICS, DFSMS, and Db2 accesses/failed access attempts in real-time
- Handles massive throughput of event messages—up to bursts of 20,000 per second
- Provides reporting by type of compliance mandate: GDPR, FISMA, GLBA, PCI DSS, HIPAA, SOX, IRS Pub. 1075, ISO 27001, and other data security standards

BMC AMI Command Center for Security provides a central view of security, auditing, and compliance efforts in real-time.

To get a personal tour of BMC AMI Command Center for Security and a free two-week trial, **click here**.