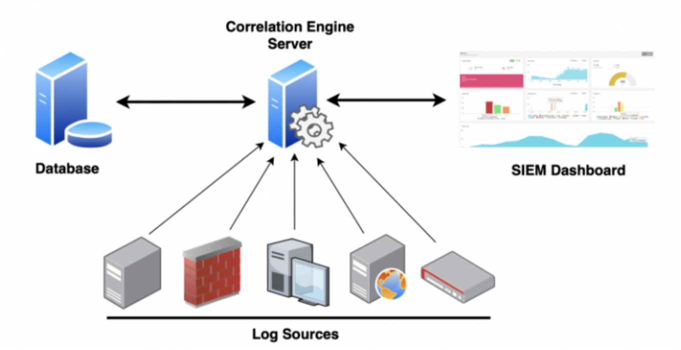
What is a SIEM?

Security Information and Event Management (SIEM) is a software solution that aggregates and analyzes activity from different resources across an organization's entire IT infrastructure. SIEM is a combination of security information management (SIM) and security event management (SEM) that uses rules and statistical correlations to help organizations detect threats and turn log entries, and events from security systems, into actionable information.

SIEM collects security data from network devices, servers, domain controllers, and more. It then stores, normalizes, aggregates, and applies analytics to that data, which can help security teams detect threats, manage incident response and perform a forensic investigation.

Setting up SIEM tools is a complex task for even the most advanced security practitioner, but when done correctly, it can eliminate blind spots across the network. The first step consists of understanding your existing network and security stack and figuring out how to collect log information from those points. You'll also need to consider planning for hardware if a software as a service (SaaS) storage option isn't offered by the vendor. Finally, an ongoing step is to write rules to detect events of interest and create reports to highlight key metrics on overall network risk.



Above is a simple diagram of SIEM architecture, which we will expand on in future lessons. Different devices will be configured to send logs to the correlation engine for analysis, and then stored in the database. The analysis performed by the correlation engine will be displayed on the front-end dashboard that is accessed by security analysts to identify, triage, and respond to security events.

BENEFITS OF A SIEM

Advanced Threat Detection: Malware has evolved in a way that eludes detection by traditional antivirus solutions, firewalls, intrusion detection and prevention systems, and other security solutions. Many organizations have implemented a defense in depth strategy around their network security solutions, hence generating a huge amount of data, which is difficult to monitor. As a result, a new type of security solution called advanced threat detection has emerged. SIEMs are capable of continuous real-time monitoring and correlation across the breadth and depth of the enterprise; therefore can help detect, mitigate, and prevent advanced threats such as malicious insiders and data exfiltration.

Forensics and Incident Response: A forensics investigation can be a long process because a forensics analyst must interpret log data to determine what happened and also preserve the data in a way that makes it admissible in a court of law. SIEMs can help organizations in a forensics investigation by storing and protecting historical logs and providing tools to quickly navigate and correlate the data. SIEMs can help security analysts realize that a security incident is taking place and set immediate steps for remediation.

Compliance Reporting and Auditing: Primarily, SIEM is implemented in response to governmental compliance requirements. Every business is bound by some sort of regulation such as HIPAA, PCI/DSS, SOX, FERPA, and HITECH. SIEMs can help organizations prove auditors and regulators that certain requirements are being met. SIEM aggregates log data from across the organization and presents it in an audit-ready format.

Other reasons why businesses need SIEM include: data storage, gaining and maintaining certifications (such as ISO 27000, ISO 27001, ISO 27002 and ISO 27003), log management and retention, case management or ticketing systems, and policy enforcement validation and policy violations.

‹ Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic ›