12.3.3 SIEM and Log Management Facts

A security information and event management (SIEM) system combines security information management (SIM) and security event management (SEM) functions into one security management system.

This lesson covers the topic of security information and event management.

Security Information and Event Management

Security information and event management tools compile and examine multiple data points gathered from across a network. The following table describes SIEM components.

Component	Description
Vulnerability scan output	Monitoring a network requires experience and solid tools. One tool common to network security is a scanner that can identify vulnerabilities and recommend remediation steps. This tool scans servers, firewalls, switches, software programs, security cameras, and wireless access points. The scan delivers the output to IT admins via the SIEM dashboard. The interval between scans is set by the IT department.
SIEM dashboards	The dashboard is a common component of all SIEM systems. The dashboard consists of customizable information screens that show real-time security and network information. The information in real time allows the IT security team to effectively monitor and respond to events on the network.
Sensors	Sensors are a vital part of monitoring and securing a network. Sensors are set-up at critical endpoints, services, and other vulnerable locations. These sensors are programmed to send customized alerts to the SEIM if certain parameters are not within the acceptable range.
Sensitivity	When the sensors are deployed, the sensitivity level is set by the IT security team. The benefit of variable sensitivity settings is the ability to customize the data that is sent to the SIEM. Not every organization will have the same needs in network monitoring.
Trends	Trends are patterns of activity discovered and reported to the SEIM. This is how baselines are established. Trends help security analysts decide if reported activity is normal or outside of the baseline. Trends that do not fit previously recorded information can be investigated by the security group. As the IT security team investigates and documents these trends it becomes easier for the team to quickly spot a trend that may signal a security event.
Alerts	Alerts are the SIEM's way of letting the IT team know that a pre-established parameter is not within the acceptable range. The alert is intended to get the attention of the IT person, or persons, monitoring the network. A best practice in this area is 24-hour monitoring.
Correlation	Event correlation is a critical SIEM component. The software gathers data from log files, system applications, network appliances, etc., and analyzes it. This work is tedious; people are inefficient at it. That's why the event correlation feature is valuable. Not only does it gather the data, but it analyzes and compares known malicious behavior against the aggregated data, increasing the chances of the discovery of security events.