Security Assessment

Security Monitoring

Security monitoring is the process of collecting and analyzing information to detect suspicious behavior or unauthorized changes on your network and connected systems.

Early SIEM devices focused on the collection of the information needed processes.

Later SIEMs advanced into managing the event data associated with the detected events.

Today, security, orchestration, automation, and response (SOAR) systems complete the move to full cycle automation of security

Security orchestration, automation, and response (SOAR) systems take SIEM data as well as data from other sources and assist in the creation of runbooks and playbooks.

Security Orchestration, Automation, and Response (SOAR)

Exam Tips

SOAR systems combine data and alarms from integrated platforms throughout the enterprise and place them in a single location where automated responses can then address threats and vulnerabilities.

Sentiment analysis is used to identify and track patterns in human emotions, opinions, or attitudes that may be present in data.

Common Vulnerabilities and Exposures (CVE) is a list of known vulnerabilities, each with an identification number, description, and reference.

The Common Vulnerability Scoring System (CVSS) determines how risky a vulnerability can be to a system. The CVSS score ranges from 0 to 10. As it increases, so does the severity of risk from the vulnerability.

Remember that syslog can be used for log aggregation on network devices and Linux operating systems. A syslog server listens for and logs messages from syslog clients. SIEM systems collect, aggregate, and apply pattern matching to the volumes of data to produce human readable information.

Packet Capture

Diagnosing and understanding network communication problems is easier when one can observe how packets flow through a network.

Most security alerting occurs after the fact. Something happens, a rule fires, and data is generated, causing an investigation into the rule. Although this can be done quickly with automation, the packets involved are long since gone.

Enter continuous packet captures. In key areas of a network, where the ability to play back traffic from a previous period of time is important, a continuous collection of the packets can provide that opportunity.

This typically will consume significant storage, so the placement and duration of collection can be very important.

Using a SIEM, coupled with smart appliances like next-generation firewalls, when a rule is fired, the network capture appliance can automatically collect and ship off a predetermined amount of traffic for later analysis.

User Behavior Analysis

Advances in user behavioral analysis has provided another interesting use of the SIEM: monitoring what people do with their systems and how they do it.

Many modern SIEMs have modules that analyze end-user behaviors, looking for anomalous behavior patterns that indicate a need for analysis.

Sentiment Analysis

The same systems that are used to pattern-match security issues can be adapted to match patterns of data indicating specific sentiments.

Approximations of sentiment can be determined by using inputs such as emails, chats, feedback collection mechanisms, and social media communications, coupled with AI systems that can interpret text communications.

Syslog/Security Information and Event Management (SIEM)

Syslog stands for System Logging Protocol and is a standard protocol used in Linux systems to send system log or event messages to a specific server, called a syslog server

The value in syslog is the separation of a system from error reports, allowing both for the security functions of logging to be separate from the system being monitored and for the aggregation of multiple log streams on a common server.

A syslog server listens on either UDP port 514 or TCP port 6514.

Security Information and Event Management (SIEM)

To make the logs easier to use security information and event management (SIEM) is employed to collect, aggregate, and apply pattern matching to the volumes of data.

This turns tables of data into meaningful actionable information based on rules established by an organization.

Working Process

The first step o collect data int tables.
This allows diff different data e work together.

These data tabl lookups and ot provide greater has been collec

The system can time related da that can be use response actio

Reviewing Reports

The primary means of providing output from a SIEM is either an alert or a report.

These are predetermined conditions that trigger a specific output of information based on rules in the system.

These reports can then be reviewed to determine whether an incident exists or is a false alarm.

Log Collectors

Log collectors are pieces of software that function to gather data from multiple independent sources and feed it into a unified source such as a SIEM.

Data Inputs

The data inputs to a SIEM are as varied as the systems they are used to protect.

What is important in a SIEM is to determine what information is needed to support what decisions.

A SIEM is tuned by the security personnel to answer the questions relative to their environment and their risks.

Log Aggregation

Log aggregation is the process of combining logs together.

This is done to allow different formats from different systems to work together.