Use SIEM tools to protect organizations

Previously, you were introduced to security information and event management (SIEM) tools and a few SIEM dashboards. You also learned about different threats, risks, and vulnerabilities an organization may experience. In this reading, you will learn more about SIEM dashboard data and how cybersecurity professionals use that data to identify a potential threat, risk, or vulnerability.

Splunk

Splunk offers different SIEM tool options: Splunk® Enterprise and Splunk® Cloud. Both allow you to review an organization's data on dashboards. This helps security professionals manage an organization's internal infrastructure by collecting, searching, monitoring, and analyzing log data from multiple sources to obtain full visibility into an organization’s everyday operations.

Review the following Splunk dashboards and their purposes:

Security posture dashboard

The security posture dashboard is designed for security operations centers (SOCs). It displays the last 24 hours of an organization’s notable security-related events and trends and allows security professionals to determine if security infrastructure and policies are performing as designed. Security analysts can use this dashboard to monitor and investigate potential threats in real time, such as suspicious network activity originating from a specific IP address.

Executive summary dashboard

The executive summary dashboard analyzes and monitors the overall health of the organization over time. This helps security teams improve security measures that reduce risk. Security analysts might use this dashboard to provide high-level insights to stakeholders, such as generating a summary of security incidents and trends over a specific period of time.

Incident review dashboard

The incident review dashboard allows analysts to identify suspicious patterns that can occur in the event of an incident. It assists by highlighting higher risk items that need immediate review by an analyst. This dashboard can be very helpful because it provides a visual timeline of the events

leading up to an incident.

Risk analysis dashboard

The risk analysis dashboard helps analysts identify risk for each risk object (e.g., a specific user, a computer, or an IP address). It shows changes in risk-related activity or behavior, such as a user logging in outside of normal working hours or unusually high network traffic from a specific computer. A security analyst might use this dashboard to analyze the potential impact of vulnerabilities in critical assets, which helps analysts prioritize their risk mitigation efforts.

Chronicle

Chronicle is a cloud-native SIEM tool from Google that retains, analyzes, and searches log data to identify potential security threats, risks, and vulnerabilities. Chronicle allows you to collect and analyze log data according to:

- A specific asset
- A domain name
- A user
- An IP address

Chronicle provides multiple dashboards that help analysts monitor an organization’s logs, create filters and alerts, and track suspicious domain names.

Review the following Chronicle dashboards and their purposes:

Enterprise insights dashboard

The enterprise insights dashboard highlights recent alerts. It identifies suspicious domain names in logs, known as indicators of compromise (IOCs). Each result is labeled with a confidence score to indicate the likelihood of a threat. It also provides a severity level that indicates the significance of each threat to the organization. A security analyst might use this dashboard to monitor login or data access attempts related to a critical asset—like an application or system—from unusual locations or devices.

Data ingestion and health dashboard

The data ingestion and health dashboard shows the number of event logs, log sources, and success rates of data being processed into Chronicle. A security analyst might use this dashboard to ensure that log sources are correctly configured and that logs are received without error. This helps ensure that log related issues are addressed so that the security team has access to the log data they need.

IOC matches dashboard

The IOC matches dashboard indicates the top threats, risks, and vulnerabilities to the organization. Security professionals use this dashboard to observe domain names, IP addresses, and device IOCs over time in order to identify trends. This information is then used to direct the security team’s focus to the highest priority threats. For example, security analysts can use this dashboard to search for additional activity associated with an alert, such as a suspicious user login from an unusual geographic location.

Main dashboard

The main dashboard displays a high-level summary of information related to the organization’s data ingestion, alerting, and event activity over time. Security professionals can use this dashboard to access a timeline of security events—such as a spike in failed login attempts— to identify threat trends across log sources, devices, IP addresses, and physical locations.

Rule detections dashboard

The rule detections dashboard provides statistics related to incidents with the highest occurrences, severities, and detections over time. Security analysts can use this dashboard to access a list of all the alerts triggered by a specific detection rule, such as a rule designed to alert whenever a user opens a known malicious attachment from an email. Analysts then use those statistics to help manage recurring incidents and establish mitigation tactics to reduce an organization's level of risk.

User sign in overview dashboard

The user sign in overview dashboard provides information about user access behavior across the organization. Security analysts can use this dashboard to access a list of all user sign-in events to identify unusual user activity, such as a user signing in from multiple locations at the same time. This information is then used to help mitigate threats, risks, and vulnerabilities to user accounts and the organization’s applications.

Key takeaways

SIEM tools provide dashboards that help security professionals organize and focus their security efforts. This is important because it allows analysts to reduce risk by identifying, analyzing, and remediating the highest priority items in a timely manner. Later in the program, you’ll have an opportunity to practice using various SIEM tool features and commands for search queries.

Revision #1
Created 2023-06-14 09:16:04 UTC by naruzkurai
Updated 2023-06-14 09:16:13 UTC by naruzkurai