Overview of SIEM technology

Previously, you learned about the SIEM process. In this reading, you'll explore more about this process and why SIEM tools are an important part of incident detection and response. As a refresher, a **security information and event management** (**SIEM**) tool is an application that collects and analyzes log data to monitor critical activities in an organization. You might recall that SIEM tools help security analysts perform **log analysis** which is the process of examining logs to identify events of interest.

SIEM advantages

SIEM tools collect and manage security-relevant data that can be used during investigations. This is important because SIEM tools provide awareness about the activity that occurs between devices on a network. The information SIEM tools provide can help security teams quickly investigate and respond to security incidents. SIEM tools have many advantages that can help security teams effectively respond to and manage incidents. Some of the advantages are:

- **Access to event data:** SIEM tools provide access to the event and activity data that happens on a network, including real-time activity. Networks can be connected to hundreds of different systems and devices. SIEM tools have the ability to ingest all of this data so that it can be accessed.
- **Monitoring, detecting, and alerting:** SIEM tools continuously monitor systems and networks in real-time. They then analyze the collected data using detection rules to detect malicious activity. If an activity matches the rule, an alert is generated and sent out for security teams to assess.
- **Log storage:** SIEM tools can act as a system for data retention, which can provide access to historical data. Data can be kept or deleted after a period depending on an organization's requirements.

The SIEM process

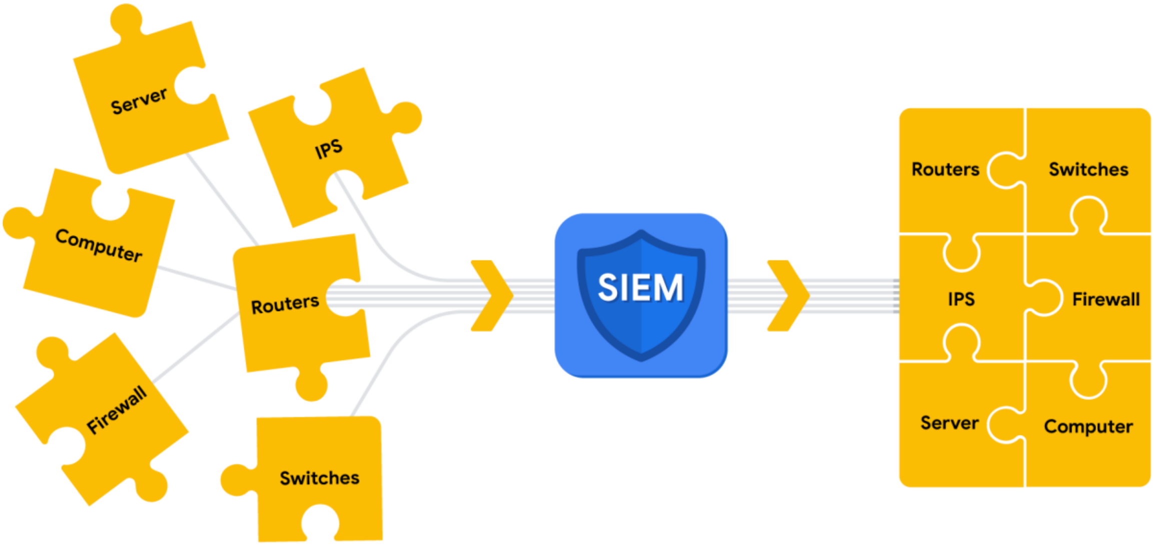
The SIEM process consists of three critical steps:

1. **Collect and aggregate data**
2. **Normalize data**
3. **Analyze data**

By understanding these steps, organizations can utilize the power of SIEM tools to gather, organize, and analyze security event data from different sources. Organizations can later use this information to improve their ability to identify and mitigate potential threats.

Collect and aggregate data

SIEM tools require data for them to be effectively used. During the first step, the SIEM collects event data from various sources like firewalls, servers, routers, and more. This data, also known as logs, contains event details like timestamps, IP addresses, and more. **Logs** are a record of events that occur within an organization’s systems. After all of this log data is collected, it gets aggregated in one location. Aggregation refers to the process of consolidating log data into a centralized place. Through collection and aggregation, SIEM tools eliminate the need for manually reviewing and analyzing event data by accessing individual data sources. Instead, all event data is accessible in one location—the SIEM.



Parsing can occur during the first step of the SIEM process when data is collected and aggregated. *Parsing* maps data according to their fields and their corresponding values. For example, the following log example contains fields with values. At first, it might be difficult to interpret information from this log based on its format:

```
April 3 11:01:21 server sshd[1088]: Failed password for user nuhara from
218.124.14.105 port 5023
```

In a parsed format, the fields and values are extracted and paired making them easier to read and interpret:

- host = **`server`**
- process = **`sshd`**
- source_user = **`nuhara`**
- source ip = **`218.124.14.105`**
- source port = **`5023`**

Normalize data

SIEM tools collect data from many different sources. This data must be transformed into a single format so that it can be easily processed by the SIEM. However, each data source is different and data can be formatted in many different ways. For example, a firewall log can be formatted differently than a server log.

Collected event data should go through the process of normalization. *Normalization* converts data into a standard, structured format that is easily searchable.

Analyze data

After log data has been collected, aggregated, and normalized, the SIEM must do something useful with all of the data to enable security teams to investigate threats. During this final step in the process, SIEM tools analyze the data. Analysis can be done with some type of detection logic such as a set of rules and conditions. SIEM tools then apply these rules to the data, and if any of the log activity matches a rule, alerts are sent out to cybersecurity teams.

Note: A part of the analysis process includes correlation. *Correlation* involves the comparison of multiple log events to identify common patterns that indicate potential security threats.

SIEM tools

There are many SIEM tools. The following are some SIEM tools commonly used in the cybersecurity industry:

- AlienVault® OSSIM™
- Chronicle
- Elastic
- Exabeam
- IBM QRadar® Security Intelligence Platform
- LogRhythm
- Splunk

Key takeaways

SIEM tools collect and organize enormous amounts of data to create meaningful insights for security teams. By understanding how SIEM tools work, what the process includes, and how organizations leverage them, you can contribute to efforts in detecting and responding to security incidents effectively. With this knowledge, you can assist in analyzing log data, identifying threats, and aiding incident response activities to help improve security posture and protect valuable assets from threats.