

Logs and SIEM tools

As a security analyst, one of your responsibilities might include analyzing log data to mitigate and manage threats, risks, and vulnerabilities.

As a reminder, a log is a record of events that occur within an organization's systems and networks.

Security analysts access a variety of logs from different sources.

Three common log sources include firewall logs, network logs, and server logs.

Let's explore each of these log sources in more detail.

A firewall log is a record of attempted or established connections for incoming traffic from the internet.

It also includes outbound requests to the internet from within the network.

A network log is a record of all computers and devices that enter and leave the network.

It also records connections between devices and services on the network.

Finally, a server log is a record of events related to services such as websites, emails, or file shares.

It includes actions such as login, password, and username requests.

By monitoring logs, like the one shown here, security teams can identify vulnerabilities and potential data breaches.

Understanding logs is important because SIEM tools rely on logs to monitor systems and detect security threats.

A security information and event management, or SIEM, tool is an application that collects and analyzes log data to monitor critical activities in an organization.

It provides real-time visibility,
event monitoring and analysis, and automated alerts.
It also stores all log data in a centralized location.

Because SIEM tools index and minimize the number of logs
a security professional must
manually review and analyze,
they increase efficiency and save time.

But, SIEM tools must be configured and customized to
meet each organization's unique security needs.
As new threats and vulnerabilities emerge,
organizations must continually customize
their SIEM tools to ensure that
threats are detected and quickly addressed.

Later in the certificate program,
you'll have a chance to practice using
different SIEM tools to
identify potential security incidents.

Coming up, we'll explore
SIEM dashboards and how cybersecurity
professionals use them to monitor for
threats, risks, and vulnerabilities.

Revision #2

Created 14 June 2023 08:58:29 by naruzkurai

Updated 14 June 2023 08:59:31 by naruzkurai