Security information and event management (SIEM) dashboards

Welcome to week 3

Welcome back! Previously, we discussed security frameworks, controls, and design principles, and how security professionals apply these to security audits.

In this section, we'll continue to explore security tools and how they can help you keep organizations and the people they serve safe. Security professionals often use a variety of tools to address specific security challenges, such as collecting security data, detecting and analyzing threats, or automating tasks. Security tools help organizations achieve a more comprehensive security posture.

We'll begin by covering different types of logs, what they track, and how they're used.

Then we'll explore security information and event management, otherwise known as SIEM, dashboards. Finally, we'll discuss some common SIEM tools used in the security industry. Let's get started!

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.

SIEM dashboards

We've explored how SIEM tools are used to collect and analyze log data. However, this is just one of the many ways SIEM tools are used in cybersecurity.

SIEM tools can also be used to create dashboards. You might have encountered dashboards in an app on your phone or other device. They present information about your account or location in a format that's easy to understand.

For example, weather apps display data like temperature, precipitation, wind speed, and the forecast using charts, graphs, and other visual elements. This format makes it easy to quickly identify weather patterns and trends, so you can stay prepared and plan your day accordingly.

Just like weather apps help people make quick and informed decisions based on data, SIEM dashboards help security analysts quickly and easily access their organization's security information as charts, graphs, or tables.

For example, a security analyst receives an alert about a suspicious login attempt. The analyst accesses their SIEM dashboard to gather information about this alert. Using the dashboard, the analyst discovers that there have been 500 login attempts for Ymara's account in the span of five-minutes. They also discover that the login attempts happened from geographic locations outside of Ymara's usual location and outside of her usual working hours. By using a dashboard, the security analyst was able to quickly review visual representations of the timeline of the login attempts, the location, and the exact time of the activity, then determine that the activity was suspicious.

In addition to providing a comprehensive summary of security-related data, SIEM dashboards also provide stakeholders with different metrics. Metrics are key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application.

SIEM dashboards can be customized to display specific metrics or other data that are relevant to different members in an organization. For example, a security analyst may create a dashboard that displays metrics for monitoring everyday business operations, like the volume of incoming and outgoing network traffic.

We've examined how security analysts use SIEM dashboards to help organizations maintain their security posture. Well done!

Coming up, we'll discuss some common SIEM tools used in the cybersecurity industry. Meet you there.

The future of SIEM tools

Previously, you were introduced to security information and event management (SIEM) tools, along with a few examples of SIEM tools. In this reading, you will learn more about how SIEM tools are used to protect organizational operations. You will also gain insight into how and why SIEM tools are changing to help protect organizations and the people they serve from evolving threat actor tactics and techniques.

Current SIEM solutions

A **SIEM** tool is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools offer real-time monitoring and tracking of security event logs. The data is then used to conduct a thorough analysis of any potential security threat, risk, or vulnerability identified. SIEM tools have many dashboard options. Each dashboard option helps cybersecurity team members manage and monitor organizational data. However, currently, SIEM tools require human interaction for analysis of security events.

The future of SIEM tools

As cybersecurity continues to evolve, the need for cloud functionality has increased. SIEM tools have and continue to evolve to function in cloud-hosted and cloud-native environments. Cloud-hosted SIEM tools are operated by vendors who are responsible for maintaining and managing the infrastructure required to use the tools. Cloud-hosted tools are simply accessed through the internet and are an ideal solution for organizations that don’t want to invest in creating and maintaining their own infrastructure.

Similar to cloud-hosted SIEM tools, cloud-native SIEM tools are also fully maintained and managed by vendors and accessed through the internet. However, cloud-native tools are designed to take full advantage of cloud computing capabilities, such as availability, flexibility, and scalability.

Yet, the evolution of SIEM tools is expected to continue in order to accommodate the changing nature of technology, as well as new threat actor tactics and techniques. For example, consider the current development of interconnected devices with access to the internet, known as the Internet of Things (IoT). The more interconnected devices there are, the larger the cybersecurity attack surface and the amount of data that threat actors can exploit. The diversity of attacks and data that require special attention is expected to grow significantly. Additionally, as artificial intelligence (AI) and machine learning (ML) technology continues to progress, SIEM capabilities will be enhanced to better identify threat-related terminology, dashboard visualization, and data storage

functionality.

The implementation of automation will also help security teams respond faster to possible incidents, performing many actions without waiting for a human response. **Security orchestration, automation, and response (SOAR)** is a collection of applications, tools, and workflows that uses automation to respond to security events. Essentially, this means that handling common security-related incidents with the use of SIEM tools is expected to become a more streamlined process requiring less manual intervention. This frees up security analysts to handle more complex and uncommon incidents that, consequently, can’t be automated with a SOAR. Nevertheless, the expectation is for cybersecurity-related platforms to communicate and interact with one another. Although the technology allowing interconnected systems and devices to communicate with each other exists, it is still a work in progress.

Key takeaways

SIEM tools play a major role in monitoring an organization’s data. As an entry-level security analyst, you might monitor SIEM dashboards as part of your daily tasks. Regularly researching new developments in SIEM technology will help you grow and adapt to the changes in the cybersecurity field. Cloud computing, SIEM-application integration, and automation are only some of the advancements security professionals can expect in the future evolution of SIEM tools.

Parisa: The parallels of accessibility and security

My name is Parisa and I'm a vice president of engineering and lead the Chrome Team. So as General manager of the Chrome Team, I lead a team of engineers and product managers and designers around the world who actually build Chrome and keep all of our users safe. I think accessibility is important to all aspects of technology, and when we think about its relevance for cybersecurity, you know, we ultimately want to keep everybody safe. I think of accessibility as making information, activities, or even environments meaningful, sensible, usable to as many people as possible. And when we're talking about this in a technology standpoint, it's usually about making information or services available to people with disabilities. Decisions we make based on our own abilities to enhance security can actually be ineffective. For example, you'll sometimes see the color red used for indication of a warning. Well, for somebody who's colorblind, like that is going to be ineffective. And so really thinking about accessibility when we're trying to keep people safe is super important for them to be effective. I've worked in the space of security for a really long time. And I do see some parallels between the spaces. I've really been able to see innovation driven when you're trying to solve a very specific security problem or a specific accessibility problem. Closed Captioning was originally designed and built to help people with hearing impairments, but it ends up helping everybody. For people who are new to the field of cybersecurity, it's just really important to remember that there's a range of abilities that you are wanting to serve. It's so important to get user research and feedback and a range of abilities in terms of testing the effectiveness of your security mitigations. I know it was scary for me early on. I didn't look like everybody else. I really struggled with whether I belonged. Finding people who could be mentors, having the courage to ask questions and recognize that you're rarely the only person with that question. And just sort of persevering through, sometimes hard moments can lead to breakthroughs and also just growing confidence. And one of the things I've learned is me having a different background than other people in this space was my own superpower. Instead of focusing on the delta between what I was and what the norm was in the room, I should feel a lot of pride in what made me unique and what unique skills and perspective I brought to the table.