Explore security information and event management (SIEM) tools

Explore common SIEM tools

Hello again! Previously, we discussed how SIEM tools help security analysts monitor systems and detect security threats.

In this video, we'll cover some industry leading SIEM tools that you'll likely encounter as a security analyst. First, let's discuss the different types of SIEM tools that organizations can choose from, based on their unique security needs.

Self-hosted SIEM tools require organizations to install, operate, and maintain the tool using their own physical infrastructure, such as server capacity. These applications are then managed and maintained by the organization's IT department, rather than a third party vendor. Self-hosted SIEM tools are ideal when an organization is required to maintain physical control over confidential data.

Alternatively, cloud-hosted SIEM tools are maintained and managed by the SIEM providers, making them accessible through the internet. Cloud-hosted SIEM tools are ideal for organizations that don't want to invest in creating and maintaining their own infrastructure.

Or, an organization can choose to use a combination of both self-hosted and cloud-hosted SIEM tools, known as a hybrid solution. Organizations might choose a hybrid SIEM solution to leverage the benefits of the cloud while also maintaining physical control over confidential data.

Splunk Enterprise, Splunk Cloud, and Chronicle are common SIEM tools that many organizations use to help protect their data and systems. Let's begin by discussing Splunk.

Splunk is a data analysis platform and Splunk Enterprise provides SIEM solutions. Splunk Enterprise is a self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time. Splunk Cloud is a cloud-hosted tool used to collect, search, and monitor log data. Splunk Cloud is helpful for organizations running hybrid or cloud-only environments, where some or all of the organization's services are in the cloud.

Finally, there's Google's Chronicle. Chronicle is a cloud-native tool designed to retain, analyze, and search data. Chronicle provides log monitoring, data analysis, and data collection. Like cloud-hosted tools, cloud-native tools are also fully maintained and managed by the vendor. But cloud-native tools are specifically designed to take full advantage of cloud computing capabilities such as availability, flexibility, and scalability.

Because threat actors are frequently improving their strategies to compromise the confidentiality, integrity, and availability of their targets, it's important for organizations to use a variety of security tools to help defend against attacks. The SIEM tools we just discussed are only a few examples of the tools available for security teams to use to help defend their organizations. And later in the certificate program, you'll have the exciting opportunity to practice using Splunk Cloud and

Chronicle.

More about cybersecurity tools

Previously, you learned about several tools that are used by cybersecurity team members to monitor for and identify potential security threats, risks, and vulnerabilities. In this reading, you'll learn more about common open-source and proprietary cybersecurity tools that you may use as a cybersecurity professional.

Open-source tools

Open-source tools are often free to use and can be user friendly. The objective of open-source tools is to provide users with software that is built by the public in a collaborative way, which can result in the software being more secure. Additionally, open-source tools allow for more customization by users, resulting in a variety of new services built from the same open-source software package.

Software engineers create open-source projects to improve software and make it available for anyone to use, as long as the specified license is respected. The source code for open-source projects is readily available to users, as well as the training material that accompanies them. Having these sources readily available allows users to modify and improve project materials.

Proprietary tools

Proprietary tools are developed and owned by a person or company, and users typically pay a fee for usage and training. The owners of proprietary tools are the only ones who can access and modify the source code. This means that users generally need to wait for updates to be made to the software, and at times they might need to pay a fee for those updates. Proprietary software generally allows users to modify a limited number of features to meet individual and organizational needs. Examples of proprietary tools include Splunk® and Chronicle SIEM tools.

Common misconceptions

There is a common misconception that open-source tools are less effective and not as safe to use as proprietary tools. However, developers have been creating open-source materials for years that

have become industry standards. Although it is true that threat actors have attempted to manipulate open-source tools, because these tools are open source it is actually harder for people with malicious intent to successfully cause harm. The wide exposure and immediate access to the source code by well-intentioned and informed users and professionals makes it less likely for issues to occur, because they can fix issues as soon as they're identified.

Examples of open-source tools

In security, there are many tools in use that are open-source and commonly available. Two examples are Linux and Suricata.

Linux

Linux is an open-source operating system that is widely used. It allows you to tailor the operating system to your needs using a command-line interface. An **operating system** is the interface between computer hardware and the user. It's used to communicate with the hardware of a computer and manage software applications.

There are multiple versions of Linux that exist to accomplish specific tasks. Linux and its command-line interface will be discussed in detail, later in the certificate program.

Suricata

Suricata is an open-source network analysis and threat detection software. Network analysis and threat detection software is used to inspect network traffic to identify suspicious behavior and generate network data logs. The detection software finds activity across users, computers, or Internet Protocol (IP) addresses to help uncover potential threats, risks, or vulnerabilities.

Suricata was developed by the Open Information Security Foundation (OISF). OISF is dedicated to maintaining open-source use of the Suricata project to ensure it's free and publicly available. Suricata is widely used in the public and private sector, and it integrates with many SIEM tools and other security tools. Suricata will also be discussed in greater detail later in the program.

Key takeaways

Open-source tools are widely used in the cybersecurity profession. Throughout the certificate program, you will have multiple opportunities to learn about and explore both open-source and proprietary tools in more depth.

Talya: Myths about the cybersecurity field

I'm Talia, and I'm an engineer within privacy, safety and security at Google. So there are a lot of myths in the cybersecurity space. One big one is, you must know how to code, or you must know how to hack, or you must be a math wiz. I don't know how to code, although I have learned how to read code over time. I'm not a hacker. I'm not on the red team site of security, I'm more on like the blue team. I'm not a math wiz. I definitely took the business route, but I'm not a mathematician. That wasn't really the path. A lot of my strength really lies in my ability to build relationships, learn quickly on the job, doing, conducting research, asking all the right questions. I think those have been my strongest strength. Another big myth, is that, you are required to have a cybersecurity degree. I actually went to school for business, an advanced degree is not required. Even though I did later on go back, That was my preference. You do not need to pursue that in order for you to be considered a great candidate for cybersecurity. Another big one is you work in isolation within cybersecurity. It really depends on the path that you choose. But I found that to be one of the most that couldn't be further from the truth. My biggest advice for anyone who's interested in cybersecurity is, be okay with creating your own path. The path looks different for everyone. If you were to talk to five different people, their journeys are all different. So own your journey, and identify people who can support you. Let them know that you're sitting for the certificate, and see what support that you can get as you start your journey.

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.

Wrap-up

Let's quickly review what we covered in this section of the course. We started by discussing the importance of logs and cybersecurity, and we explored different log types, like firewall, network, and server logs. Next, we explored SIEM dashboards and how they use visual representations to provide security teams with quick and clear insights into the security posture of an organization.

Finally, we introduced common SIEM tools used in the cybersecurity industry, including Splunk and Chronicle.

We'll be exploring even more security tools later in the program, and you'll have opportunities to practice using them. Coming up, we'll discuss playbooks and how they help security professionals respond appropriately to identify threats, risks, and vulnerabilities. Meet you there.