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.

Revision #1
Created 2023-06-14 09:09:25 UTC by naruzkurai
Updated 2023-06-14 09:09:45 UTC by naruzkurai