Log sources and log ingestion

In this reading, you'll explore more on the importance of log ingestion. You may recall that **security information and event management** (**SIEM**) tools collect and analyze log data to monitor critical activities in an organization. You also learned about **log analysis,** which is the process of examining logs to identify events of interest. Understanding how log sources are ingested into SIEM tools is important because it helps security analysts understand the types of data that are being collected, and can help analysts identify and prioritize security incidents.

SIEM process overview

Previously, you covered the SIEM process. As a refresher, the process consists of three steps:

1. **Collect and aggregate data**: SIEM tools collect event data from various data sources.
2. **Normalize data**: Event data that's been collected becomes normalized. Normalization converts data into a standard format so that data is structured in a consistent way and becomes easier to read and search. While data normalization is a common feature in many SIEM tools, it's important to note that SIEM tools vary in their data normalization capabilities.
3. **Analyze data**: After the data is collected and normalized, SIEM tools analyze and correlate the data to identify common patterns that indicate unusual activity.

This reading focuses on the first step of this process, the collection and aggregation of data.

Log ingestion

> A SIEM tool collects data from various sources.

Data is required for SIEM tools to work effectively. SIEM tools must first collect data using log ingestion. Log ingestion is the process of collecting and importing data from log sources into a SIEM tool. Data comes from any source that generates log data, like a server.

In log ingestion, the SIEM creates a copy of the event data it receives and retains it within its own storage. This copy allows the SIEM to analyze and process the data without directly modifying the original source logs. The collection of event data provides a centralized platform for security analysts to analyze the data and respond to incidents. This event data includes authentication attempts, network activity, and more.

Log forwarders

There are many ways SIEM tools can ingest log data. For instance, you can manually upload data or use software to help collect data for log ingestion. Manually uploading data may be inefficient and time-consuming because networks can contain thousands of systems and devices. Hence, it's easier to use software that helps collect data.

A common way that organizations collect log data is to use log forwarders. Log forwarders are software that automate the process of collecting and sending log data. Some operating systems have native log forwarders. If you are using an operating system that does not have a native log forwarder, you would need to install a third-party log forwarding software on a device. After installing it, you'd configure the software to specify which logs to forward and where to send them. For example, you can configure the logs to be sent to a SIEM tool. The SIEM tool would then process and normalize the data. This allows the data to be easily searched, explored, correlated, and analyzed.

Note: Many SIEM tools utilize their own proprietary log forwarders. SIEM tools can also integrate with open-source log forwarders. Choosing the right log forwarder depends on many factors such as the specific requirements of your system or organization, compatibility with your existing infrastructure, and more.

Key takeaways

SIEM tools require data to be effective. As a security analyst, you will utilize SIEM tools to access events and analyze logs when you're investigating an incident. In your security career, you may even be tasked with configuring a SIEM to collect log data. It's important that you understand how data is ingested into SIEM tools because this enables you to understand where log sources come from which can help you identify the source of a security incident.

Resources

Here are some resources if you’d like to learn more about the log ingestion process for Splunk and Chronicle:

- Guide on getting data into Splunk
-
- Guide on data ingestion into Chronicle

Revision #1
Created 2023-11-04 09:43:43 UTC by naruzkurai
Updated 2023-11-04 09:44:22 UTC by naruzkurai