Reexamine SIEM tools

As a security analyst, you'll need to be able to quickly access the relevant data required to perform your duties.
Whether it's triaging alerts, monitoring systems, or analyzing log data during incident investigations, a SIEM is the tool for this job.
As a quick review, a SIEM is an application that collects and analyzes log data to monitor critical activities in an organization.
It does this by collecting, analyzing, and reporting on security data from multiple sources.
Previously, you learned about the SIEM process for data collection.
Let's revisit this process.
First, SIEM tools COLLECT AND PROCESS enormous amounts of data generated by devices and systems from all over an environment.
Not all data is the same.
As you already know, devices generate data in different formats.
This can be challenging because there is no unified format to represent the data.
SIEM tools make it easy for security analysts to read and analyze data by NORMALIZING it.
Raw data gets processed, so that it's formatted consistently and only relevant event information is included.
Finally, SIEM tools INDEX the data, so it can be accessed through search.
All of the events across all the different sources can be accessed with your fingertips.
Isn't that useful?
SIEM tools make it easy to quickly access and analyze the data flows happening across networks in an environment.
As a security analyst, you may encounter different SIEM tools.
It's important that you're able to adjust and adapt to whichever tool your organization ends up using.
With that in mind, let's explore some SIEM tools currently used in the security industry.
Splunk is a data analysis platform.
Splunk Enterprise Security provides SIEM solutions that let you search, analyze, and visualize security data.
First, it collects data from different sources.
That data gets processed and stored in an index.
Then, it can be accessed in a variety of different ways, like through search.
Chronicle is Google Cloud's SIEM, which stores security data for search, analysis, and visualization.
First, data gets forwarded to Chronicle.
This data then gets normalized, or cleaned up, so it's easier to process and index.
Finally, the data becomes available to be accessed through a search bar.
Next up, we'll explore how to search on these SIEM platforms.

Revision #1
Created 2023-11-04 09:36:15 UTC by naruzkurai
Updated 2023-11-04 09:38:09 UTC by naruzkurai