Alert and event management with SIEM and SOAR tools

Our discussion on detection tools may have left you wondering where alerts are sent and how alerts are accessed by security analysts.
This is where security information and event management, or SIEM, tools are used.

SIEM is a tool that collects and analyzes log data to monitor critical activities in an organization.
SIEM provides security professionals with a high-level overview of what goes on in their networks.
How exactly does it do this?

Let's use an example of a car.
Cars have many different parts: tires, lights, and let's not forget all the internal machinery that's under the hood.
There are many different components of a car, but how do you know if one of them has an issue?
Aha, you guessed it! The dashboard warning lights.
The dashboard notifies you about information related to the car's components, whether the tire pressure or battery voltage is low, you need to refuel, or a door hasn't been properly closed.
A car's dashboard notifies you about the status of the car's components, so that you can take action to fix it.

SIEM tools work in a similar way.
Just like cars have many different components, a network can have thousands of different devices and systems, which make monitoring them quite the challenge.

A car's dashboard gives the driver a clear picture of the status of their car, so they don't have to worry about inspecting each component themselves.

Similarly, a SIEM looks at data flows between all the different systems in the network and analyzes them to provide a real-time picture of any potential threats to the network.
It does this by ingesting massive amounts of data and categorizes this data, so that it's easily accessible through a centralized platform similar to a car's dashboard.

Here's what the process looks like.
First, SIEM tools collect and aggregate data.
This data is typically in the form of logs, which are basically a record of all the events that happened on a given source.

Data can come from multiple sources such as IDS or IPS, databases, firewalls, applications, and more.
After all this data gets collected, it gets aggregated.
Aggregation simply means all this data from different data sources gets centralized in one place.

Depending on the number of data sources a SIEM collects from, a huge volume of raw unedited data can get collected.
And not all data that's collected by a SIEM is relevant for security analysis purposes.

Next, SIEM tools normalize data.
Normalization takes the raw data that the SIEM has collected and cleans it up by removing non essential attributes so that only what's relevant is included.
Data normalization also creates consistency in log records, which is helpful when you're searching for specific log information during incident investigation.

Finally, the normalized data gets analyzed according to configured rules.
SIEM analyzes the normalized data against a rule set to detect any possible security incidents, which then get categorized or reported as alerts for security analysts to review.

Now that you've explored the capabilities of SIEM tools, let's examine another security management tool.
Security orchestration, automation, and response, or SOAR, is a collection of applications, tools, and workflows that uses automation to respond to security events.

While SIEM tools collect, analyze, and report on security events for security analysts to review, SOAR automates analysis and response to security events and incidents.
SOAR can also be used to track and manage cases.
Multiple incidents can form a case, and SOAR offers a way to view all of these incidents in one centralized place.

Well, there you have it. You've learned how incident management tools like SIEM and SOAR make it easier for security analysts to see what's happening in a network and to respond to any threats efficiently.

Revision #1
Created 2023-09-06 11:13:24 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai