SIEM dashboards

We've explored how SIEM tools are used to collect and analyze log data. However, this is just one of the many ways SIEM tools are used in cybersecurity.

SIEM tools can also be used to create dashboards. You might have encountered dashboards in an app on your phone or other device. They present information about your account or location in a format that's easy to understand.

For example, weather apps display data like temperature, precipitation, wind speed, and the forecast using charts, graphs, and other visual elements. This format makes it easy to quickly identify weather patterns and trends, so you can stay prepared and plan your day accordingly.

Just like weather apps help people make quick and informed decisions based on data, SIEM dashboards help security analysts quickly and easily access their organization's security information as charts, graphs, or tables.

For example, a security analyst receives an alert about a suspicious login attempt. The analyst accesses their SIEM dashboard to gather information about this alert. Using the dashboard, the analyst discovers that there have been 500 login attempts for Ymara's account in the span of five-minutes. They also discover that the login attempts happened from geographic locations outside of Ymara's usual location and outside of her usual working hours. By using a dashboard, the security analyst was able to quickly review visual representations of the timeline of the login attempts, the location, and the exact time of the activity, then determine that the activity was suspicious.

In addition to providing a comprehensive summary of security-related data, SIEM dashboards also provide stakeholders with different metrics. Metrics are key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application.

SIEM dashboards can be customized to display specific metrics or other data that are relevant to different members in an organization. For example, a security analyst may create a dashboard that displays metrics for monitoring everyday business operations, like the volume of incoming and outgoing network traffic.

We've examined how security analysts use SIEM dashboards to help organizations maintain their security posture. Well done!

Coming up, we'll discuss some common SIEM tools used in the cybersecurity industry. Meet you there.

Revision #1
Created 2023-06-14 08:59:46 UTC by naruzkurai
Updated 2023-06-14 09:00:08 UTC by naruzkurai