6 STEPS TO Build the Best SIEM Use Cases for Your Business

1

Frame Your Security Use Cases

Once you've considered the threat landscape and better understand your business-specific security risks, it's time to define your use cases based on risk-driven insights.

Pro Tip: By building use cases that are relevant to your environment, security teams can avoid scope creep (i.e., use cases that end up expanding beyond their management or monitoring capabilities) and ensure they stay on track.

2

Identify Specific Data Sources

There are a lot of different data sources out there and you need to make sure that the information is relevant for your top priority risks. The sooner you identify which data sources are most appropriate for your needs, the better.

Pro Tip: It's important to focus on your prioritized objectives first. If you have the license and capability, then data from "just in case" data sources may be brought in–additional context will always come in handy during an investigation!

3

Apply Data-Powered Analytics

Choosing the right data analytics can help identify anomalies quickly. This will also help ensure your SIEM is aligned with your objectives.

Pro Tip: Don’t get caught up in the moment. Before you try to perform complex analytics, make sure that the simpler SIEM use case analytics can be managed first before you advance further.

4

Catalog Your Use Case Set

SIEMs can be expensive to implement and maintain. Organizing your use cases into families and subfamilies will help you maximize efficiency while also ensuring optimal return on investment.

Pro Tip: If you leverage Splunk Enterprise Security, you will want to use Analytic Stories. This capability provides contextual and actionable guidance to help you better define your use cases and organize your content.

If you need any help, Hurricane Labs specializes in providing custom Splunk SIEM capabilities for our customers!

5

Prioritize Your Use Cases

Again, there are many ways that deploying use cases that have not been built for your business requirements may decrease the effectiveness of a SIEM. This is especially true for security teams that do not have the advanced skill sets to handle the complexity of their use case deployments.

Pro Tip: Determine which use cases should take priority before deploying them.

6

Understand the Use Case Life Cycle

Security use cases go through multiple stages–including planning, deployment, and evaluation–that need to be managed to ensure their effectiveness.

Pro Tip: You should review your use cases at regular intervals, such as once a year or more often if necessary, to make sure they still align with the originally intended goal. During your review, include any new data ingested into your SIEM, or that are still relevant to your organization and current level of defensive measures.

We're here to ensure that your SIEM is up and running with the right partner for success.

Let us know if you would like to schedule a consultation to learn more about our services!

Hurricane Labs