ARCUSDATA

206-247-6655 | community@arcusdata.io | arcusdata.io/services

Security Use Case Workshop

Whether you are working on an initial deployment or maturing your security monitoring, the Splunk Enterprise Security Use Case Development Workshop can help.

This Workshop helps you increase the effectiveness of your security monitoring and identify ways to improve your security posture. Our experts aid in identifying and customizing the security queries (use cases) to maximize the opportunities to improve your security posture, align with your business needs and risk priorities.

IMPROVE YOUR SECURITY POSTURE

Our Splunk Enterprise Security Use Case Development Workshop will help you cover three key benefits:

- Development of a roadmap for increasing your visibility into high-risk activity
- Implementing a security monitoring framework will help you reduce noise and help focus your investigations
- Discovery of the most effective monitoring strategy to support your business and processes

The workshops focus on identifying use cases that improve your ability to:

- Monitor your network attack surface
- Conduct advanced threat monitoring on the endpoint
- Conduct advanced threat monitoring in the network
- Monitor cyber key terrain
- Monitor your ability to investigate
- Monitor your policy violations
- Conduct network health monitoring
- Monitor for "first seen" activity
- Monitor user behavior

CATEGORIZATION

Developing a Monitoring Strategy That Aligns with Your Business Priorities

It doesn't matter if you already have a mature Splunk powered security operations center (SOC), are just getting started, or are in the process of migrating from a legacy environment, you can lean on the expertise of our team to accelerate the value you get out of your Splunk deployment. The Security Use Case Development Workshop is designed to help you establish and refine your monitoring strategy to better align with your business priorities.

Based on years of experience implementing security use cases for Splunk's most mature security customers, the Workshop teaches you to categorize your network monitoring. The categorization helps you focus on the activities that pose the greatest risk to your unique environment, so you can take actions to minimize risks and strengthen your security stance. Tactically, the Workshop gives you the tools to identify and implement the monitoring use cases you need. It provides the documentation for each use case identified, including the data sources required to deploy the use case and a plan for implementation.