

Security Use Case Development Workshop

Professional Services

Discover New Security Capabilities

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, identify ways to improve your security posture, and refine your monitoring strategy to better align with your business priorities. Our experts aid in identifying and customizing the security queries (use cases) to maximize the opportunities to improve your security posture, align with your enterprise needs and risk priorities.

Workshops that Enhance Your Digital Resilience

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 workshop is designed to help your organization's ability to conduct advanced threat monitoring on endpoints and your network as well as help with monitoring across key areas:

- Your network attack surface
- Cyber key terrain
- Your ability to investigate
- Policy violations
- For "first seen" activity
- User behavior

Developing a Monitoring Strategy

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.

Guidance at Every Step of Your Splunk Journey

Splunk has developed a wide range of Service offerings to be responsive to dynamic challenges, requirements, and urgent needs. As your organization is focused on achieving accelerated time-to-value, as well as the need to optimize workflows, you may need help to maximize your use of Splunk in driving enterprise resilience for better outcomes.

For more information visit [Splunk.com/services](https://splunk.com/services), or email us at cs-sales@splunk.com to connect.