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, aligned with your enterprise needs and risk priorities.

Discover enhanced threat monitoring capabilities

Explore anomaly-based threat detection

Discuss risk-based incident management approach

Create a high-level plan to improve digital resilience

Workshops designed to 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 conduct advanced threat monitoring across your IT environment and improve your security operations in key areas:

- Defending your cyber attack surface
- Monitoring security events and alerts
- Hunting for new threat activity
- Enhancing incident investigation
- Enforcing security policies
- Detecting anomalous user behavior

Developing a security 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.

What we'll do and deliver

During this workshop, customers work with an accredited Splunk Architect to identify the critical use cases and data sources for a successful adoption or enhancement of Splunk Enterprise Security. We leverage Splunk's extensive use case library to map potential best practices to identified priorities and create a customized plan for the implementation of these recommended use cases.

Workshop at a Glance	
Engagement duration	5 days (3 onsite, 2 remote)
Project team	Splunk Architect (5 days)
Activities	Workshop activities ● Understand customer priorities and objectives ● Identify use cases to be implemented aligned to priorities ● Evaluate data sources and map data requirements to use cases
Deliverables	Final documentation package ● Use case and data source recommendations ● Architecture and recommended system specifications ● High-level implementation plan with timelines and estimated levels of effort

Resilience, let's build it together

Splunk Customer Success provides end-to-end success capabilities at every step of your resilience journey to accelerate time to value, optimize your solutions and discover new capabilities. We offer professional services, education and training, success management and technical support, surrounding you with the expertise, guidance and self-service success resources needed to drive the right outcomes for your business. For more information contact us at sales@splunk.com.

Terms and Conditions

This Solution Guide is for informational purposes only. The services described in this solution guide are governed by the applicable fully signed ordering document and any incorporated terms and conditions.

splunk> a CISCO company

Contact us: splunk.com/asksales

splunk.com