Insider Threat Workshop

Protect your organization against insider threats

While external threats grab most of the news headlines, insider threats, irrespective of whether it is malicious or accidental, are much more costly. Insider threats, in most cases, are hard to detect until it is too late resulting in loss of data, intellectual property and company reputation. Our service is designed to help you detect and mitigate insider threats on your IT systems and stop them in their tracks. We start by assessing your current environment including its architecture, configuration and active insider threat use cases. Leveraging best practices, our Splunk experts will develop recommendations for additional insider threat use cases along with data source requirements and a documented approach to implementing them.

A comprehensive assessment, delivered by Splunk experts, that evaluates your existing insider threat approach and identifies gaps

Recommend specific actions based on industry and Splunk best practices, to supercharge your ability to detect, mitigate and stop insider threats

Provide an actionable plan that can be operationalized to improve the maturity of your insider threat implementation

Accelerator at a Glance	
Designed for	Existing Splunk Enterprise Security customers seeking to strengthen their insider threat protection and expand to cover a comprehensive set of use cases
Duration	5 days
Prerequisites & Assumptions [1]	• A fully functional Splunk Enterprise 8.2+ and Splunk Enterprise Security 6.4+ environment • Splunk ES head with dual forwarding and latest version of both Security Essentials app and Splunk app for Lookup File Editing • Splunk environment with all data sources onboard and CIM compliant, assets and identities implemented and early stages of Risk Based Alerting configuration
Project Team	• Splunk accredited Architect

[1] A complete list of prerequisites and assumptions will be detailed in a Statement of Work document as part of Splunk's transaction process.

What We'll Do & Deliver

Discovery

Splunk experts will conduct an exhaustive evaluation of your current environment, stakeholder requirements, workings of your SOC and its workflows. Following that, our team will drive a discussion around your short and long term monitoring goals, pain points, critical users and assets. These guided conversations span five major areas: access, network, communications, collection and exfiltration, and will cover relevant use cases in the context of frameworks like MITRE, Insider Threat TTP and Splunk best practices.

Assessment & Findings

Our team of experts will analyze the requirements and data collected during the discovery phase and begin to establish a baseline for what is considered normal insider use. The assessment will span areas like daily normal user activity, definition of risky activities, normal system access, privileges and data exfiltration. In addition, our team will assess the state of your assets, identities, and Risk Based Alerting (RBA) risk rules and compare and contrast them to known best practices. Finally, we will present detailed findings that show your current state in relation to your desired state that was gathered during the discovery phase.

Recommendations & Action Plan

In the final phase of this engagement, we will present a RBA maturity roadmap that will clearly lay out an action plan to achieve your desired goals. In addition, we will also present best practice recommendations to help you better protect against insider threats and approaches to operationalizing those recommendations.

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.

1. Outcomes shown were realized by actual Splunk customers and not every customer will realize similar outcomes. Realization of these outcomes are dependent on many factors including state of the customers' environment, skill level of customer personnel, Splunk product(s) being used and many other factors. The figures in this table are used to show examples of the types of outcomes customers can realize and is it not a guarantee for all customers.

Terms and Conditions

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