

Asset and Identity Workshop and Implementation

Speed up security event detection, triage and resolution by integrating asset and identity data into Splunk ES

Asset and Identity information in an IT environment represents valuable data that can be used to enrich existing event data to accelerate detection and resolution of security events. The new Splunk Asset and Risk Intelligence (ARI) application combined with the powerful features of Splunk Enterprise Security(ES) provides comprehensive asset visibility, accelerates investigation, reduces risk and compliance exposure. Our service enables you to rapidly realize the benefits of the two Splunk products by quickly installing and configuring asset and identity data into your existing Splunk ES environments with or without Splunk ARI.



Comprehensive risk assessments and notable enrichment with asset and identity data



Continuously discover assets, enrich and accelerate investigations and uncover compliance gaps with Splunk Asset and Risk Intelligence



Delivered by certified Splunk security architects and consultants with many years of experience delivering customer solutions

Accelerator at a Glance

Designed for	Splunk Enterprise Security customers that want to integrate asset and identity data to provide richer context that enables faster detection, triage and enables them to make better security decisions. This service supports Splunk ES with or without the Splunk Asset and Risk Intelligence application.
Duration	5 days
Prerequisites & Assumptions	<ul style="list-style-type: none"> • Healthy Splunk Enterprise and Enterprise Security environment <ul style="list-style-type: none"> ◦ Splunk Enterprise 8.2+ ◦ Splunk Enterprise Security Version 6.4+ minimum • Data Sources onboarded and CIM compliant • Accessible and Splunk supported Add-on available for applicable data sources not currently in Splunk • Splunk Asset Risk Intelligence app installed on the ES search head, if applicable.
Project Team	Splunk Security Accredited Architect and Consultant

What We'll Do

Discovery & Design Workshop

Our experts will conduct a structured workshop to understand your requirements, discuss prerequisites and to confirm technical readiness of your environment. Following this, our team will review in-scope data sources, onboarding status, and details of your asset and identity data all of which is mapped to your requirements.

Build & Configure

In this phase, our experts normalize your asset and identity data to conform to the Splunk Common Information Model (CIM) and validate it. Once that is complete, the data will be configured to populate the ES Asset and Identity framework according to the requirements that were discussed during the discovery and design workshop.

Knowledge Transfer

Our experts will wrap up the engagement with a review of the new implemented Asset and Identity framework. Necessary enablement and handoffs will be delivered, so that when we are finished with the configuration of the framework, you will be confident to operate and grow its functionality to support your security program.

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.



Contact us: splunk.com/asksales

splunk.com

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2024 Splunk Inc. All rights reserved.