# Splunk SOAR Implementation Success

Increase productivity and respond to threats faster with an empowered SOC

Strengthen your Enterprise Resilience

The Splunk SOAR Implementation Success offering is designed for customers looking to build a production-ready SOAR environment, accelerating time-to-value, and leveraging expertise from experts who have real world experience in helping security operations, threat intel teams, and incident responders.

Gain expert guidance on SOAR integrations and best practices
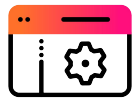
Drive implementation and integration throughout your SOC

Automation of repetitive tasks

Develop a use case roadmap and response model

Uplevel Your Security Capabilities with SOAR

The goal of this offering is to move your security capabilities to a higher level of security maturity and enable you to use existing use cases and develop response plans with workbooks that have measurable phases and tasks with automation. Your team will work with our experts, who have built and managed security teams and services around the world, to help speed up the time-to-value your organization realizes from your SOAR platform.

What We'll Do and Deliver

The mission of this engagement is to enable your team to learn how to develop your own playbooks, based on best practices, and to be able to leverage the power of the SOAR platform with your infrastructure. The Splunk SOAR Implementation Success service provides the following, dependent on what offering level you choose:

- Kickoff meeting to align goals, resources, and timelines
- An Architecture Review Workshop to validate architecture and an ideal state to support SOAR
- Installation & configuration of the SOAR instance
- Integration of your Splunk Enterprise or Enterprise Security instance(s) to enable data exchange between the two platforms, and the configuration of an initial list of up to 5 app integrations in SOAR
- Tailored knowledge transfer sessions to ensure your ongoing success with SOAR, including help with the identification of the right use cases, playbooks, and workbooks
- Co-development of a selected response plan into a set of up to 5 playbooks and/or workbooks

Options to Fit Your Needs

Architectural Guidance	To effectively leverage a security automation and orchestration solution, it should integrate seamlessly to ingest, triage, coordinate, and respond effectively and efficiently. The Splunk PS team works with the customer to choose the right implementation.
Setup	After the appropriate architecture model has been selected, Splunk Professional Services will provide the resources to install and configure the SOAR and start the process of integrating the preliminary list of integrations for SOAR to ingest events, lookup information and perform actions. This includes integrating SOAR with Splunk ES.
Knowledge Transfer	With years of experience in helping customers develop and mature their SOAR platforms, we know that the key to success is enabling your teams in the identification, design, development and use of the capabilities of the SOAR platform. Our knowledge process achieves the goal of enabling the customer teams to develop new ideas on how to leverage the SOAR platform in new and innovative ways.
Development	The Splunk Platform team has identified that there are three categories of playbooks: Enrichment (perform the prep work before presenting to the analysts), Utility (supports the daily tasks with the security teams perform), Autonomous (completely automated response with human decision making if required). The SOAR team will work with you to leverage our library of playbook examples to deliver the security automation and orchestration capabilities to help security teams.

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.