splunk>

PROFESSIONAL SERVICES

Splunk Phantom Implementation Success

Work Smarter, Respond Faster, Strengthen Your Defenses

Security Automation, Orchestration and Response (SOAR) is changing the world of security operations, incident response, governance, and threat intelligence enablement. Work smarter, respond faster, and leverage the true capability of your security infrastructure, at machine speed.

To help our customers take advantage of this approach, the Splunk Phantom team has developed an offering that helps security teams get there faster.

OFFERING HIGHLIGHTS

- ·Guidance on how to integrate Phantom across your infrastructure
- ·Implementation and Integration Support
- ·Training to enable security engineers, architects and security operations teams
- ·Use case roadmap and playbook development
- ·Leverages the expertise of security professionals who have built and manage security teams and services around the world
- ·Speeds the operationalization of the Phantom platform, realizing the benefits, efficiently and faster

SOAR Maturity

The goal of this offering is to help move your security capabilities to higher level of SOAR maturity.

Options to Fit Your Needs

The Splunk Phantom Implementation Success Offering has been packaged into three levels – Base, Standard, and Premium. These offerings are designed to match the needs and maturity of the customer's security program.

Architectural Guidance

To effectively leverage a security automation and orchestration solution, it should be designed to integrate with all the necessary tools to ingest, triage, coordinate and respond effectively and efficiently. This powerful solution can touch all parts of an IT's infrastructure. The Splunk Phantom team works with the team to identify the right integration, determining the best approach based on the customer's specific environment, including backup, recovery, administration, and playbook development.

Security Use Case Road Mapping

After years of experience in helping customer develop and mature their Phantom platform, we know that the key to success to the development of a methodology and the continuous improvement in their usage of playbooks to enable their security response capabilities. The Splunk Phantom team will work with the customer to help them develop their own roadmap identification capabilities, leveraging our experience of working with hundreds of security teams.

Playbook Development

The Splunk Platform team has identified that there are three categories of playbooks: Autonomous (completely automated response with human decision making if required), Utility (supports the daily tasks with the security teams perform), Enrichment (perform the prep work before presenting to the analysts). The Phantom team will work with you to leverage our library of over 150 playbook examples to deliver the security automation and orchestration capabilities to help security teams across the world.

DESIGNED FOR	
STANDARD	Organizations who are starting their journey into the world of security automation and orchestration and that want to start with a single use case.
PREMIUM	Organizations who want to develop multiple playbooks to enable their security teams.

Two Sizes to Meet Your Needs

Every customer is different, so we have built three different sizes to provide flexibility to your needs. Each of our offerings includes the alignment of our expert SOAR Architects and Engineers based on the customer needs, and are supported by our talented Project Managers and Success Managers.

The mission of these engagements is to enable the customer to learn how to develop their own playbooks, based on best practices, and to be able to leverage the power of the Phantom Security Automation Orchestration and Response platform, with their infrastructure, and people.

Standard Offering

This offering is designed to help organizations that are looking for guidance on how to design, implement, and operationalize their Phantom security automation and orchestration platform. The Splunk Phantom team will train the customer's teams and work with them on a customer specific user case and to co-develop up to eight playbooks that the customer can start using in production and can be used as a reference model for future playbooks.

Premium Offering

The Premium Offer is an extended version of the Standard offering but delivers additional production ready playbooks based on an addition use case or an app for the customer.

Included in Every Offering

Architecture and Implementation Guidance

- The Splunk Phantom Security Solution Architects work with the customer to design, document and support the implementation of the Phantom environment

Installation Support

- The Splunk Phantom team will provide support during the implementation process
- Help the customer integrate the Phantoms apps with their infrastructure
- Provide guidance on how to monitor and maintain the Phantom platform
- Conduct workshops on administration, backup and BCP/DR best practices

Training

- Training is customized according to the customer requirements and focus and can include:
  - Phantom Administration and Usage Training
  - Use Case Development Methodology Training
  - Introduction to Playbook Development
  - Introduction to App Development
  - Advanced Playbook Development Workshops

Playbook Development Best Practices

Identifying the right use cases that can leverage the full potential of a security automation and orchestration platform is an important aspect of achieving success. Some of the lessons we have learnt:

- ·Not all use cases are suitable for automation.
- ·Use cases can be broken up into modular playbooks that can be leveraged across multiple playbooks.
- ·Translating a manual process to leverage the power of a machine augmented requires the security automation and orchestration architect / developer to think differently. It is not effective to just replicate the manual processes.
- ·One of the key value attributes of the Phantom Visual Editor is that has the flexibility to support the beginner playbook developer and as well as the advanced playbook developer who wants to leverage the deep power of Python and the integrations with over 220 integrations with other security tools and solutions.

The Splunk Phantom team has the experience of working with, developing and implementing a wide range of playbooks, ranging from automated phishing response, threat intelligence handling, incident management, and event enrichment.

Target Customer Attributes

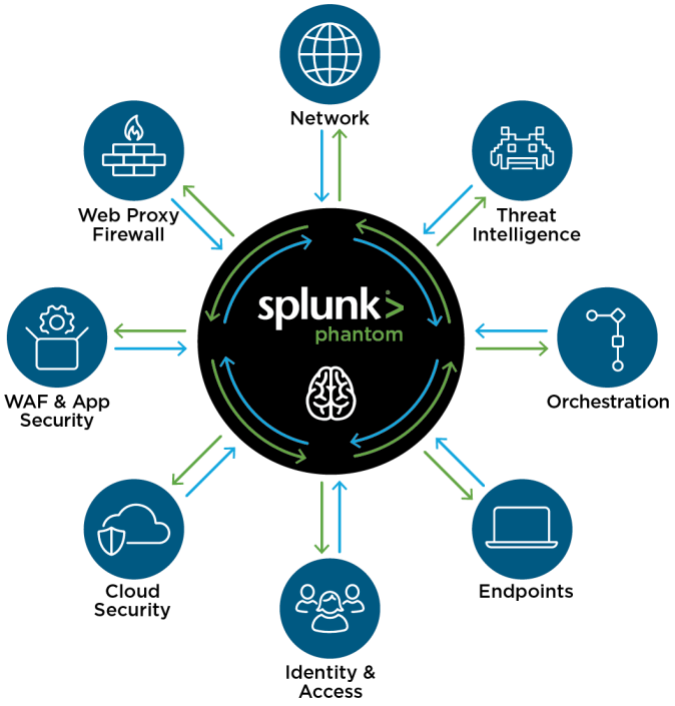
The Splunk Phantom Implementation Success offering is designed for customers looking to build a production Phantom Security Automation and Orchestration, quickly, leveraging expertise to learn from experts who have real world experience in helping security operations, threat intel teams, and incident responders. They are seeking a quick time to value for key security initiatives, from implementation planning through production deployment.

Splunk Professional Services

Our services are backed by Splunk Accredited Consultants, Solutions Architects, and Delivery Managers. They leverage Splunk best practices and experience from thousands of Splunk deployments.

We only exist to get customers to valuable outcomes with their machine data – faster than they could on their own.

Security Nerve Center



Free Online Sandbox. Get access to a free, personal environment provisioned in the cloud where you can immediately try and experience the power of Splunk IT Service Intelligence. After the initial trial period, or any time before then, you can convert to an Enterprise license by **contacting sales.**

splunk>

ps-sales@splunk.com

www.splunk.com