splunk>

PROFESSIONAL SERVICES

Splunk Phantom Adoption Success – Use Cases

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.

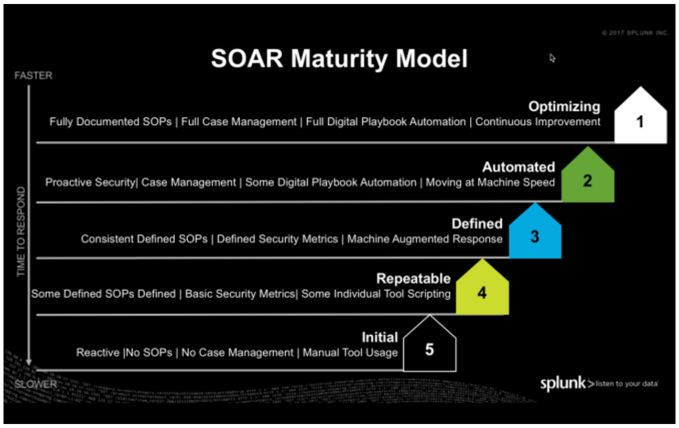
To help our customers take advantage of this approach, the Splunk Phantom team has developed an offering that helps security teams get there faster.

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 customers move their security capabilities to higher level of SOAR maturity.


© 2017 SPLUNK INC.
SOAR Maturity Model
FASTER
TIME TO RESPOND
SLOWER
Optimizing
Fully Documented SOPs | Full Case Management | Full Digital Playbook Automation | Continuous Improvement
1
Automated
Proactive Security| Case Management | Some Digital Playbook Automation | Moving at Machine Speed
2
Defined
Consistent Defined SOPs | Defined Security Metrics | Machine Augmented Response
3
Repeatable
Some Defined SOPs Defined | Basic Security Metrics| Some Individual Tool Scripting
4
Initial
Reactive |No SOPs | No Case Management | Manual Tool Usage
5
splunk> listen to your data

Expands Your Use Case Portfolio

The Splunk Phantom Playbook Adoption Success Offering has been designed for a customer who already has setup and integrated the Phantom platform into the environment. They are looking to extend the usage and capabilities of the SOAR platform in their environment.

Strategic 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 a customer's infrastructure. The Splunk Phantom team works with the customers to identify the right workflows that deliver on the goals of the use case, determining the best approach based on the customer's specific environment, security organization structure, maturity, and key business security influencers.

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. The Splunk Phantom team will work with the customer to identify playbooks that not only deliver the required orchestration, automation, and response, but that also be used in other use cases.

	Designed For
Standard	Customers who have already setup and integrated the Phantom platform into the environment and that are looking to extend the usage and capabilities of the SOAR platform in their environment, to meet existing security demands and new requirements or integration possibilities.

The Phantom Adoption Success provides the skilled resources to design and develop effective playbooks that deliver the results required to solve a use case problem. This leverages a team with multiple years of experience in SOAR, combined with years of real-world security experience in building SOCs, running threat intelligence teams and incident response.

Included in Every Offering

Use Case Review and Design

- A Splunk Phantom Security Solution Architect and Engineer will work with the customer to identify and design the work flow required and the playbook designs.

Playbook Development

- Trained Splunk Phantom Engineers will develop the playbook leverage our knowledge and experience of developing complex SOAR response capabilities, solving advanced security challenges.

Testing Support

- As part of the offering, a Splunk Phantom Engineer will be on-site to help test the playbooks. This provides an opportunity to fine tune and to provide the customer’s engineering and operation teams with insight and guidance into how the playbooks were developed.

Promotion to Production Support

- The Splunk Phantom Engineer will also be available to help as the customer moves the playbooks into production.

Knowledge Transfer

- A core tenant of our Phantom Delivery methodology is to ensure that customer is enabled to continue adding and enhancing playbooks. As the team works with the customer’s architects, engineers, and operations teams, we share our knowledge and experience.

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 200 integrations with other security tools and solutions.

The Splunk Phantom team have the experience of working with, developing and implementing a wide range of playbooks, ranging from automated phishing response, event enrichment,

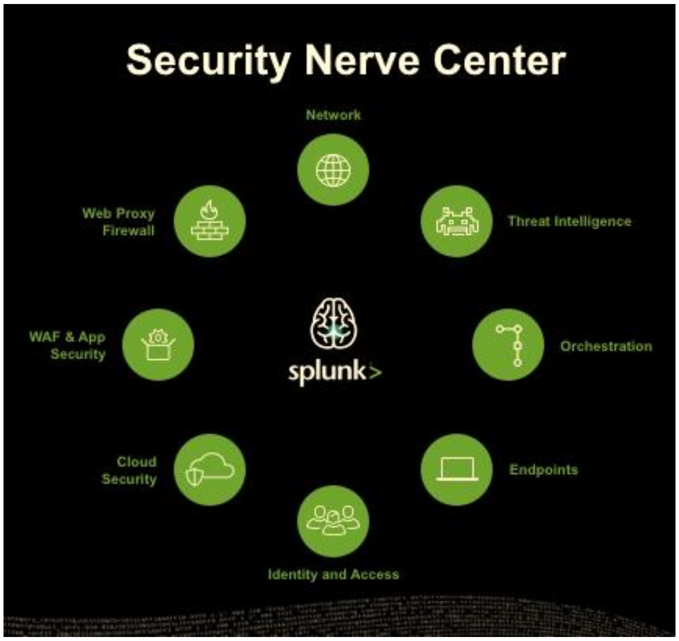
Target Customer Attributes

The Splunk Phantom Adoption Success offerings are designed for customers looking to extend their 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.



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**