splunk> turn data into doing

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 PS team has developed an offering that helps teams leverage the power of SOAR to defeat modern threats for businesses and organizations.

Offering Highlights

- Expert guidance on how to integrate Phantom with Splunk and your security tools
- Implementation and Integration Services
- Training for security engineers, architects and security operations teams
- Use case roadmap and response model development
- Leverages the expertise of security professionals who have built and manage security teams and services around the world
- Speeds the time to value for the Phantom platform, realizing the benefits, efficiently and faster

SOAR Maturity

The goal of this offering is to move your security capabilities to a higher level of security maturity and enable the customer to use existing use cases and develop response plans with workbooks that have measurable phases and tasks with automation.

Options to Fit Your Needs

The Splunk Phantom Implementation Success Offering has been packaged to match the needs and maturity of the customer's security program. Additional options to add additional use cases and integrations enabling the usage of additional SOAR use cases.

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 PS will provide the resources to install and configure the Phantom and start the process of integrating the preliminary list of integrations for Phantom to ingest events, lookup information and perform actions. This includes integrating Phantom with Splunk ES.

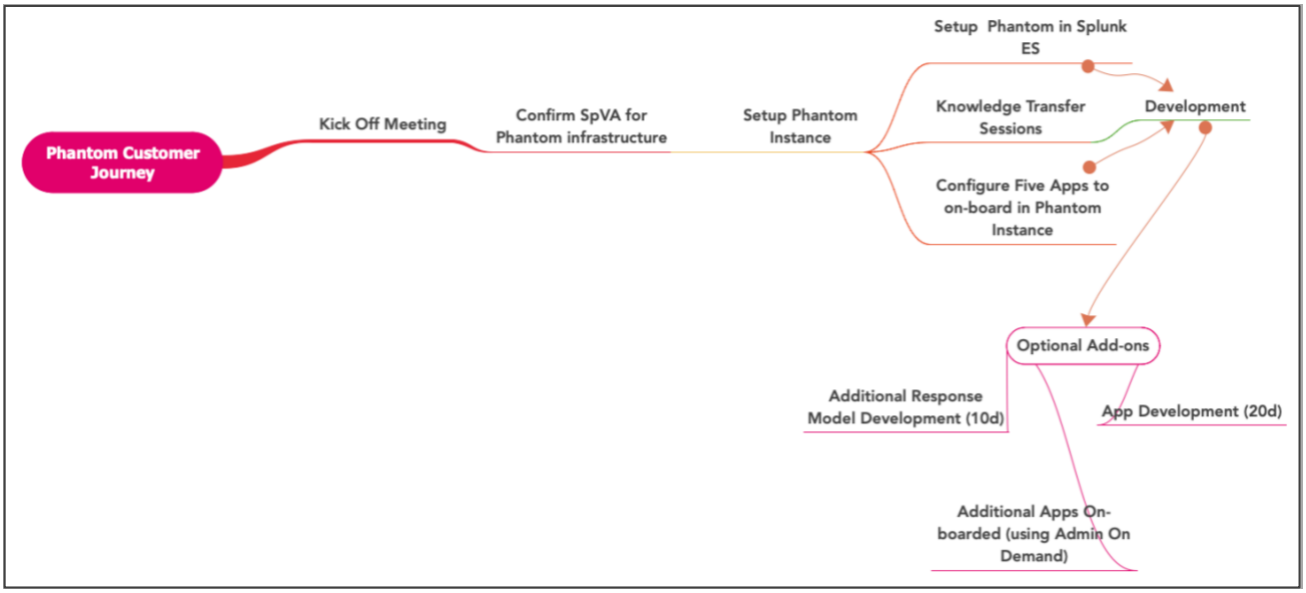
Knowledge Transfer

With years of experience in helping customers develop and mature their Phantom platforms, we know that the key to success is enabling the customer's teams in the identification, design, development and use of the capabilities of the Phantom platform. Our knowledge process achieves the goal of enabling the customer teams to develop new ideas on how to leverage the Phantom platform in new 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 Phantom team will work with you to leverage our library of playbook examples to deliver the security automation and orchestration capabilities to help security teams.

The Phantom Implementation Customer Enjourney



A Proven Delivery to Enable Customers

Every customer is different, so we have a unique sizing model to provide flexibility to your needs. The base service provides the following services:

- Kick Off meeting to align goals, resources and timelines
- An Architecture Review Workshop to identify the right Splunk Phantom Validated Architecture to meet the customer's needs
- The installation, configuration of the Phantom instance
- The integration of the customer's Enterprise or Enterprise Security instance(s) to enable data exchange between the two platforms, and the configuration of up to an initial list of up to 5 app integrations in Phantom
- The delivery of customer specific Knowledge transfer sessions to help with the identification of the right use cases, playbooks and workbooks.
- The co-development of a selected response plan into a set of up to 5 playbooks and/or workbooks

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.

Add-on Options

These are stackable options, i.e. multiple units options can be purchased at one time.

Add Additional Use Cases*

This allows the customer to purchase the services of Splunk PS to develop up to 5 additional playbooks or workbooks to support a response plan.

Improve a Phantom App*

This allows the customer to purchase the services of Splunk PS to develop an action or up to 3 actions for an existing Phantom app. This is typically utilized when the customer has need to add additional actions to an existing Phantom app or improve the functionality of Phantom app.

Develop a custom Phantom App*

This allows the customer to purchase the services of Splunk PS to develop a custom app. This is typically utilized when the customer has an internal app or heavily customized app that they want to use with Phantom to enrich data or take action.

* Please note that these options can be started, once the initial Phantom Implementation service has reached the point where and the Phantom infrastructure Is stood up, the response plan has been identified.

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 ideas are suitable for automation.
- Response plans 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.
- Integrating your response plan on workbooks with playbooks , helps guide the security analyst in understanding all of the attributes of a potential threat, and also can provide a guide to the available response options that an analyst can launch. Response plan workbooks are driven by consolidating the data and expediting the analyst to decide [on the data] and act [on the data] with automation.
- One of the key value attributes of the Phantom Visual Editor is that it 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 300 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, vulnerability management, 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

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 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.**