splunk> turn data into doing

PROFESSIONAL SERVICES

Splunk SOC Modernization and Optimization Workshop

A blueprint to Security Success for your Security Operations Center

Building and running a modern Security Operations Center can be a daunting task, but it doesn't have to be. Utilizing the entire Splunk Security Product suite allows our customers to take advantage of best in class products while utilizing our proprietary approach to Security Operations.

To help our customers take advantage of this approach, the Splunk Professional Services (PS) team has developed an offering that helps teams leverage the power of the entire security suite. This can include Enterprise Security as the detection and investigation platform; Security Analytics for Machine Learning and Artificial Intelligence; Splunk Phantom to provide automation, orchestration and case management all in tandem to defeat modern security threats for businesses and organizations.

Offering Highlights

- Expert guidance on how to integrate whatever Splunk security products your organization uses (ES, Phantom, UBA)
- Strategic Advisory Services
- Develop a plan on how to operationalize each of the products or all of them together
- SOC process guidance and development
- Use case roadmap and response model development
- Leverages the expertise of security professionals who have built and managed security teams and services around the Globe

Speeds the time to value for the each of our security products or all of them together

Modern SOC

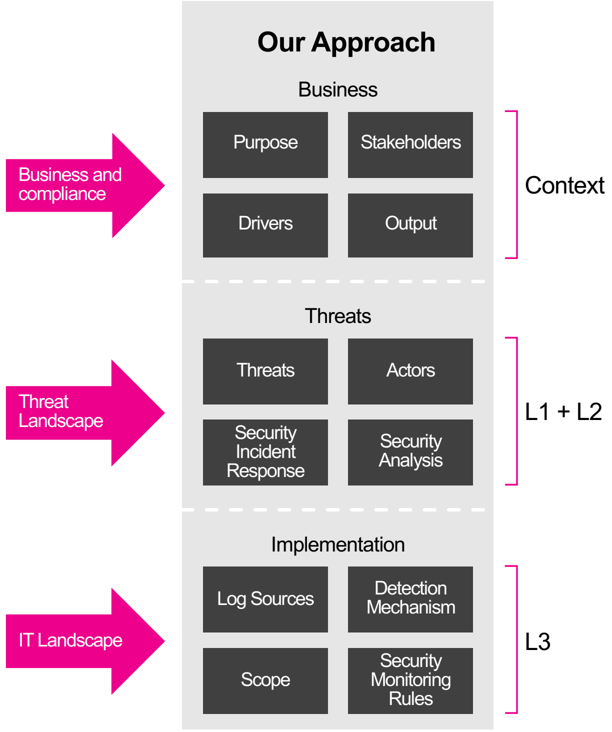
A modern Security Operations Center must be a combination of **People-Process-Technology**. It must have the capability to respond to the ever evolving threatscape as well as highly sophisticated threat actors. In order to build these capabilities, the SOC analysts must be able to respond to incidents in the "golden hour" before exploitation or exfiltration occurs. Post incident analysis will need to be conducted speedily and root cause determined in order to prevent similar incidents in the future.

The goal of this offering is to increase the overall detection and blocking capabilities and thereby reducing the occurrence of major security incidents while at the same time improving the organizations response capabilities. Visibility and transparency are key to success. This is achieved by ensuring that all of the customers security products are properly configured and communicating. So how do we achieve success and prevent failure—by a combination of Scoping--Technology--Implementation.

	Scope	Technology	Implementation
Success	❖ Develop focused requirements for use cases ❖ Set realistic expectations that can be achieved ❖ Define how to appropriately apply the platform (current and future)	❖ Provide high fidelity outputs that are actionable ❖ Ensure that the SIEM meets current and future requirements for in-scope processes ❖ Ensure that analysts have a strong understanding of the platform	❖ Resource/role allocation ❖ Ensure that everyone receives the appropriate training for their role ❖ Understand how knowledge/gaps affects response runbooks
Failure	❖ Wrong focus in wrong areas ❖ Unrealistic expectations ❖ Shallow and narrow coverage	❖ Alert fatigue and noise, too many events ❖ Platform is not operationalized and doesn't deliver ❖ Lack of understanding around the platform and how to perform day to day actions	❖ Resources not allocated correctly ❖ Resources do not receive appropriate training, lacks key skills ❖ No runbook, no process

The SOC must think in terms of mitigating risk to the organization, this is done by taking a three-pronged approach to everything the SOC team does:

1. **Business Layer (Strategic)** – Defines how the objective is connected to the organizations needs
2. **Threat Layer (Tactical)** – Defines the threat that the objectives are intended to detect
3. **Implementation Layer (Operational)** – Defines what aspects that are relevant for the implementation of the particular objectives



Splunk Consultants will work together with your Security Operations team to customize a plan on how to build this process in order to ensure that all the requirements of the business and organization are being satisfied by the functions of SOC.

Highly experienced Splunk Professional Service consultants who have built world class SOC's across the globe will provide their experience and guidance to provide a set of proven processes for your organization. These integrated processes, along with the Splunk Security Suite, will help guide your organization to success. During this two-week workshop Splunk Expert Consultants will help your organization develop plans for:

- How to properly develop use cases
- How to properly develop Phantom playbooks
- How to create response plans
- Design workflow integrations
- How to manage content lifecycle
- How to conduct threat modeling
- How to conduct Threat Hunts
- How to successfully leverage AI and ML
- How to use Phantom for case management

Options to Fit Your Needs

The Splunk SOC Modernization and Optimization workshop is structured so that we begin by determining the customer's current capabilities and gaps and aligning those with the strategic vision of the security organization. We then work in tandem with the customer's Security Leadership and Operations teams to come up with a set of processes and blueprints that will guide your Security Operations Center to success. This can be done with both existing and new customers. It doesn't matter if the customer's current or future plans for Splunk are to be located in Splunk Cloud, their private cloud or with a more traditional on-premise configuration. The SOC Modernization and Optimization offering has been packaged to help grow the maturity of the customer's security program and operationalize your investment with Splunk. This is ideal for customers purchasing multiple Splunk Security products.

Architectural Guidance

The Splunk PS team works with the customer to choose the right implementation for each of the Security Suite products the customer chooses. This is all based on best practices and Splunk Validated Architectures. This will guide the rest of the deployment or build out.

Knowledge Transfer

With years of experience in helping customers develop and mature their Security Operations, 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 entire Splunk Security Suite. Our knowledge transfer process achieves the goal of enabling the customer's teams to develop new ideas on how to leverage the totality of the Splunk Security Suite and empower their Security Operations team with these tools.

Proven Delivery

Every customer is different, so we have a unique consulting model to provide flexibility to the customer's needs. Each engagement will provide the customer with a customized library of documentation to help ensure their success.

- Kick Off meeting to align goals, resources and timelines
- An Architecture Review Workshop to identify the right Validated Architecture to meet the customer's needs
- Splunk Security Maturity assessment to determine the gaps and goals of the organization
- Tabletop exercises to discuss the current challenges and process improvements required
- Discuss where integration of the customer's Enterprise Security instance(s) to enable data exchange between all the platforms is needed
- The output of this workshop will be a collection of best practices, processes and guidelines to include:
  - Log collection and aggregation best practices
  - Investigation best practices
  - Incident Response best practice methodology
  - Case Management Workflow and best practices
  - Content development and management Workflow (use cases, dashboards, tuning etc.)
  - Playbook development best practices and workflow
  - Threat Modeling workflow and best practices
  - Threat Hunting workflow and best practices
  - Reporting and metrics best practices

.

Target Customer Attributes

The Splunk SOC Modernization and Optimization offering is designed for customers looking to purchase and integrate multiple Security Suite products. The mission of this engagement is to empower the customers Security Operations team to take over these processes and customize them to meet their strategic and tactical requirements, both as a business and a security team. This offering is ideal for existing customers with multiple Splunk Security Suite products who are struggling to integrate and operationalize their various purchases. This set of processes and best practices provides the customer with the blueprint for success as a Security Operations team. Splunk is not only providing products/tools needed by a successful Security Operations team, but it is also providing the customer with a turn-key experience that allows the customer to quickly realize value while leveraging the expertise of Splunk Security Experts.

Splunk Professional Services

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