SECURITY PROFESSIONAL SERVICES

Advanced Security Advisory Services

Helping You Solve Your Toughest Cybersecurity Problems

Overview

The Advanced Security Advisory Services bring in the skills and expertise you need to address your toughest cybersecurity problems and use Splunk to improve your overall security posture.

Advanced Security Advisory Services

The Advanced Security Advisory Services offer you a highly customizable engagement that enables you to apply resources and expertise where you need it most. Bringing vast hands-on experience with Splunk and latest cybersecurity threats, our consultants can help you tune your Splunk deployment to best address your toughest cybersecurity problems.

For example, we can help you leverage Splunk's advanced capabilities to hunt for malware, monitor for fraud or uncover advanced persistent threats. We can help you create custom dashboards and correlation searches; build, migrate (from an MSSP), expand (globally) or optimize your security operations center (SOC); or even conduct tabletop exercises designed to validate your security program is being properly executed by your SOC analysts. With Splunk, you can:

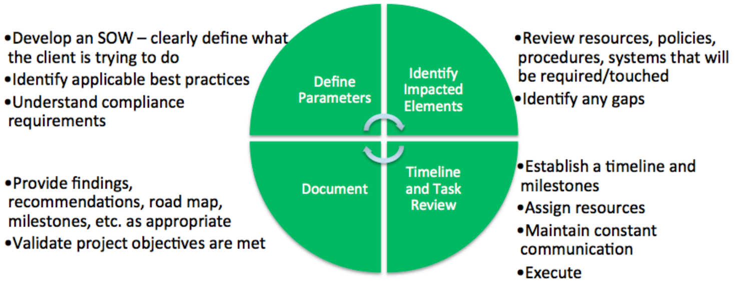
- **Realize the Full Value of Your Splunk Investments:** Building proficiency around Splunk to enable you to take advantage of advanced capabilities to improve the efficiency and effectiveness of your security operations.

- **Mature Your Security Deployment**: Providing prescriptive knowledge on how to implement best practices and deploy data driven security that takes your program to the next level.

- **Improve Your Overall Security**: Maximizing the effectiveness of your security team, while minimizing your risks and enhancing your ability to detect and respond to attacks.

Setting You Up for Success

The Splunk Advanced Security Advisory Services can be tailored to meet your specific cybersecurity needs.


•Develop an SOW – clearly define what the client is trying to do
•Identify applicable best practices
•Understand compliance requirements
Define Parameters
Identify Impacted Elements
•Review resources, policies, procedures, systems that will be required/touched
•Identify any gaps
•Provide findings, recommendations, road map, milestones, etc. as appropriate
•Validate project objectives are met
Document
Timeline and Task Review
•Establish a timeline and milestones
•Assign resources
•Maintain constant communication
•Execute

Splunk Professional Services deliver:

- **Expert Security Guidance:** Assisting your in-house staff with cybersecurity experts who have extensive knowledge on how to build an effective data driven security program.

- **Optimal Security Performance:** Enabling your security practitioners to investigate, respond and remediate threats as quickly as possible.

- **Quick Value:** Helping you avoid pitfalls in planning and implementing key components of your security infrastructure.

- **Increased Understanding:** Helping you get the most of the information you already possess and enhance the visibility you have into your security program, from policies to architecture.

- **Tailored Content:** Enabling your security practitioners to move effortlessly through your system based on your security processes to address your biggest security needs.

Rev. 10.9.15

Engagement

You can work with our Advanced Security Advisory Services consultants to determine the optimal approach for your security requirements. Splunk consultants will assist in everything, from creating and implementing a conversion strategy to the creation of rules and searches, to ensure the Splunk environment meets your success criteria. An engagement may include:

- **Capabilities Assessment**: Review current security use cases, as well as the information sources and data enrichment capabilities in place to identify opportunities to increase the security value of your existing infrastructure.

- **Security Architecture Assessment:** Review the security architecture to help identify areas that could benefit from greater visibility and better monitoring processes.

- **Threat Assessment:** Review threat actors and methodologies targeting your organization, based on broad, cross-industry experience, to better understand and align efforts to protect against the current threat landscape.

- **Guidance and Recommendations:** Work with you to take the findings from the assessments and identify immediate short and long-term enhancements that could improve your organization's operations and overall security posture.

- **Validation Services:** Assess the value obtained at specific milestones to verify the results are exactly what is needed and meet any use case(s) established in the planning phase.

- **Program follow up:** The lead consultant (or project team) will follow up to check on the status of the roadmap, update the gap assessment based on remediation efforts and to offer additional best practices guidance. Note, any additional work identified will be scoped into a new project.

- **Maintenance:** A Splunk consultant can follow up with you, one or two weeks per quarter, over a year and provide ongoing support. They can review the current roadmap and propose revisions, based on changes in technology, the landscape or the organization.

The findings and recommendations will be presented via:

- **Findings Documentation:** Splunk Security Services will deliver documentation on the findings uncovered during the assessments of your current security architecture, processes and program, as well as the threat landscape, any identified gaps, environment roadmaps and milestones.

- **Executive Summary:** As part of the service, the lead consultant will provide a written executive summary and deliver a findings presentation to the project team.

The duration of an Advanced Security Advisory Services engagement often varies, based on the size of the environment, but in general it lasts four to six weeks, spread out over a three to four month period.

Requirements

The Advanced Security Advisory Services offering is designed for customers who want to leverage their Splunk Enterprise and Splunk Enterprise Security (ES) implementations to find the "unknowns" in their networks. It is suitable for customers of all sizes and maturity levels.

To optimize the engagement, customers should have:

- Commitment to end-to-end visibility using Splunk Enterprise and Splunk ES
  - At least a single site instance of Splunk Enterprise in production with clustering or shared searching requirements.
- Full or part time dedicated security team.