splunk>

SECURITY PROFESSIONAL SERVICES

Security Program Review Services

Improve Your Security Posture

Overview

The Security Program Review Service assesses your security posture to identify gaps and opportunities to maximize the utility of your security infrastructure and improve your overall security stance.

Security Program Review (SPR)

The Splunk Security Program Review Service takes a "10,000 foot view" of your security posture to identify gaps and opportunities to improve your overall stance. The Service is designed to help you use your Splunk deployment to optimize the efficiency and effectiveness of your security program.

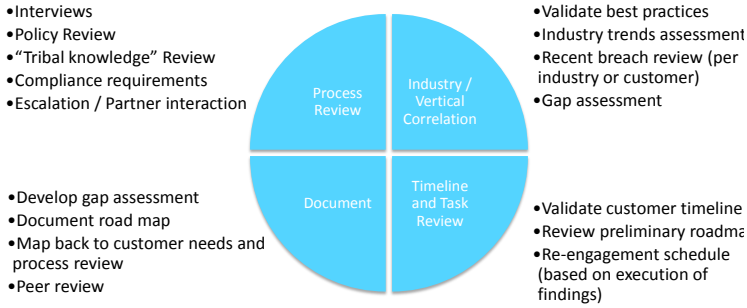
Our seasoned security consultants will assess your program, based on industry best practices and/or relevant compliance requirements. They will leverage their decades of experience to provide you prescriptive guidance that will enable you to maximize the investments you have made in your security infrastructure and strengthen your security posture. With Splunk, you can:

- **Realize the Full Value of Your Splunk Investments:** Building proficiency around Splunk that will enable your team to streamline and improve your security posture.
- **Support Compliance Initiatives**: Providing prescriptive guidance designed to help you implement best practices and address relevant compliance requirements with your security program.
- **Improve Your Overall Security**: Leveraging advanced capabilities to help you maximize the effectiveness of your security program and strengthen your security stance.

Setting You Up for Success

The Splunk Security Program Review Service ensures your security team has the knowledge, experience and capabilities they need to create and sustain a strong security posture for your enterprise.

Overview of the Security Program Review Service



Splunk Professional Services deliver:

- **Expert Security Guidance**: Assisting your in-house staff with cybersecurity experts who have extensive knowledge on how to build and optimize security programs.
- **Faster Program Development:** Providing actionable guidance to help you quickly develop and deploy an effective, successful security program (faster than doing it internally).
- **Optimal Performance for Fast Threat Response:** Enabling your security practitioners to investigate, respond and remediate threats as quickly as possible.
- **Better Vision into Security:** Helping you achieve a single view into your security program, from policies to architecture.
- **Tailored Content:** Ensuring your security practitioners know how to use Splunk within your security program to improve the effectiveness of your security team and operations.

Rev. 10.8.15

Engagement

During the course of the engagement, the Security Program Review Service will conduct:

- **A Security Policy & Architecture Assessment:** Review of your current security architecture and policies, with recommendations on potential improvements.
.
- **A Splunk Deployment and Security Monitoring Assessment:** Evaluation of the current Splunk deployment to understand what it is monitoring and identify possible gaps in system and network vision.

- **A Gap Assessment of Current Environment:** Assess the current state of the security program and Splunk deployment and provide a gap assessment, based on a standard three-tier review of your risks, the ease of remediation, and overall cost.

- **Industry and/or Vertical Baselining:** Correlate findings from your security program with specific industry, vertical and compliance best practices and requirements.

- **Guidance & Recommendations:** Work with you to determine the optimal approach for improving your security program to better align with your security requirements.

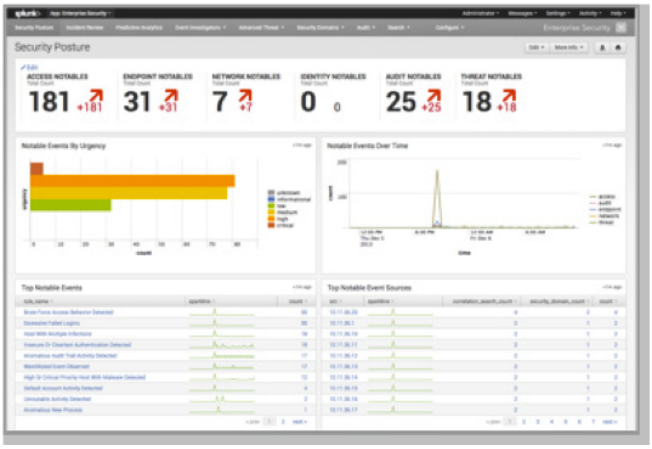
- **Program Follow-Up:** The lead consultant (or project team) will follow up to check on the status of the roadmap, update the gap assessment based on remediation efforts, and offer additional help to further improve your security program. Note, any additional work will be scoped as a new project.

The findings and recommendations will be presented via:

- **Findings Documentation:** Splunk Security Services will deliver documentation on the findings uncovered during the assessments and gap analysis of your current security program.

- **Security Program Roadmap:** Splunk Security Services will create a visual representation of the maturation of your security program, including important milestones.

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



Splunk Professional Services provide best in class implementations to align your security program with your specific compliance and security needs.

The duration of the Security Program Review varies, however, it is designed to be a longer-term engagement. The average timeframe is three to six weeks for the initial review and recommendations, with ongoing touchpoints over a much longer period of time (up to a year).

Requirements

The Splunk Security Program Review is the perfect offering for organizations who want a holistic security review around their Splunk deployment. It is designed for customers who have a new to moderate security program in place and new to intermediate in-house security analysts.

To optimize the engagement, customers should have:

- At least a single site instance of Splunk Enterprise in production with clustering or shared searching requirements.
- A security program already in place or planned, which leverages Splunk to monitor security events.
- Full or part time dedicated security team.