splunk>

SECURITY PROFESSIONAL SERVICES

SOC Advisory Services

Improve Your Ability to Manage Security Events

Overview

The Splunk Security Operations Center (SOC) Advisory Services help you architect and re-architect your SOC to improve your ability to manage the volume of security events you are facing and mitigate the impact of attacks in your environment.

SOC Advisory Services

The SOC Advisory Services can be customized to meet your unique SOC requirements. Our seasoned security consultants can help you architect your SOC or mature your SOC deployment, so you streamline your operations and better address the threats targeting your environment.

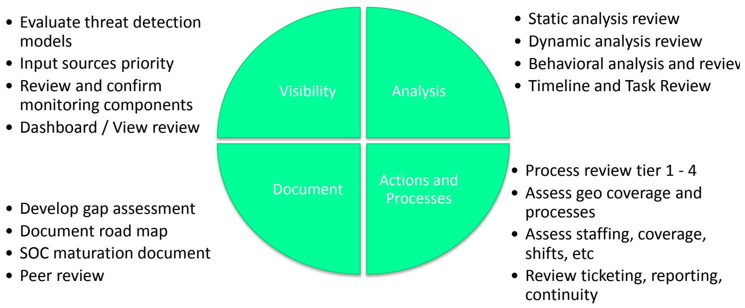
You can use the Splunk SOC Advisory Services to improve your ability to proactively identify intrusions in your environment and coordinate a response to mitigate a breach's impact and prevent attacks. With Splunk, you can:

- **Realize the Full Value of Your Splunk Investments:** Building proficiency around Splunk that will enable your team to streamline and improve the operations of your SOC.
- **Mature Your SOC Deployment**: Providing prescriptive knowledge that helps you implement best practices and take your SOC to the next level.
- **Improve Your Overall Security**: Leveraging advanced capabilities to help you maximize the effectiveness of your security team, policies and standards. Splunk's experts can help you minimize your risks and accelerate incident resolution to prevent attacks before they can be executed.

Setting You Up for Success

The Splunk SOC Security Advisory Services gives you the guidance, experience and training you need to improve and sustain your ability to detect, control and remediate breaches.

Overview of the SOC Advisory Services



- Evaluate threat detection models
- Input sources priority
- Review and confirm monitoring components
- Dashboard / View review

- Static analysis review
- Dynamic analysis review
- Behavioral analysis and reviev
- Timeline and Task Review

- Develop gap assessment
- Document road map
- SOC maturation document
- Peer review

- Process review tier 1 - 4
- Assess geo coverage and processes
- Assess staffing, coverage, shifts, etc
- Review ticketing, reporting, continuity

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 an effective SOC.
- **Faster Program Development:** Providing actionable guidance to help you quickly develop and deploy an effective, successful security program.
- **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 SOC to improve the effectiveness of your security team and processes.

Rev. 10.7.15

Engagement

During the course of the engagement, the SOC Advisory Services will conduct:

- **A Best Practices Assessment:** Review of your information security strategy, infrastructure, technology coverage, compliance and regulatory requirements, and people and processes.

- **A Splunk Deployment and Security Monitoring Assessment:** Evaluation of the current Splunk deployment to understand how best to maximize your ability to monitor and mitigate risks.

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

- **Guidance and Recommendations:** Work with you to identify potential improvements and recommend the architecture and approach that best meets all your security requirements.

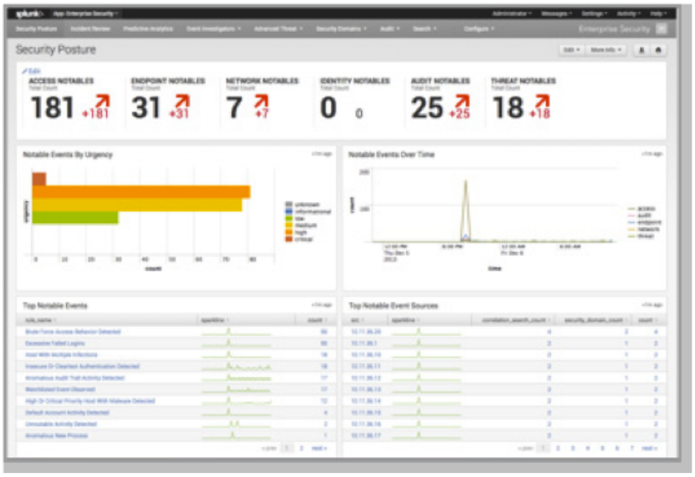
- **Program Follow-Up:** The lead consultant (or project team) can follow up at a later date to review the engagement, check on progress and identify potential opportunities for additional improvements.

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 performed on your current environment.

- **Executive Summary:** The lead consultant will present findings to the project team and provide a written executive summary of the key items uncovered and recommended.

- **Security Program Roadmap:** A visual representation of the maturation of your security program, including important milestones, will enable you to understand how to improve your ability to investigate and respond to intrusions and the overall effectiveness of your SOC.



Splunk Security Professional Services provide best in class SOC implementations that help you improve your security.

The duration of the engagement varies based on the size of your environment, however, the average timeframe is four to six weeks

Requirements

The Splunk SOC Advisory Services are designed for customers who have a relatively new SOC in place or are looking to make changes to the way their SOC operates. As part of that SOC, Splunk should be deployed and used to monitor security events. New and intermediate in-house security analysts will benefit most from the vast knowledge of Splunk's cybersecurity experts.

To optimize the engagement, customers should have:

- At least a single site instance of Splunk Enterprise Security in production, with clustering or shared searching requirements.

- A security program (SOC) already in place or planned.

- A full or part time dedicated security team – with little to intermediate knowledge of security processes, policies and standards.