Security Professional Services

Augmenting Security Staff, Addressing Skill Shortages and Optimizing Your Security Operations With Splunk

Overview

Splunk Security Professional Services deliver the unique security insights and services you need to maximize your security investments and strengthen your security posture.

Keeping Up With the Evolving Threat Landscape

It is no secret, enterprises are struggling to keep their sensitive information and resources safe from internal threats and cyberattacks. We are seeing increasingly sophisticated threat actors launch attacks that successfully evade detection – sometimes for days, weeks, months – with costly consequences.

At the same time, there is an overall shortage of skilled cybersecurity professionals available to help enterprises improve their security stance. According to ISACA, 83 percent of enterprises currently lack the right skills and human resources to protect their IT assets, leading many to turn to professional services to fill the gap. Many are turning to Splunk.

Splunk Security Professional Services

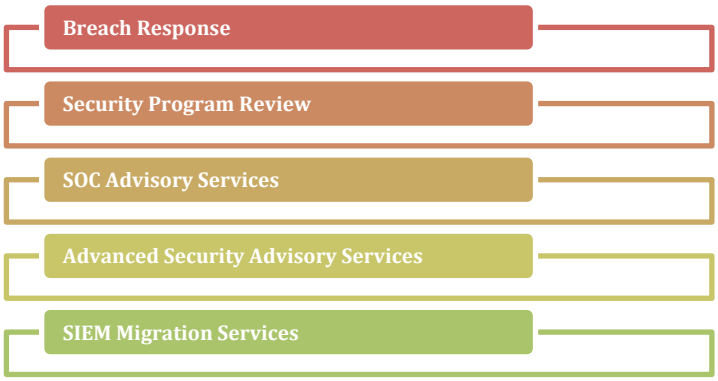
Splunk Security Professional Services are uniquely positioned to help enterprises improve their ability to identify, contain and mitigate the impact of breaches in their environment. As the brains of many enterprises' security operations, Splunk has vast, first-hand experience detecting and remediating the most advanced threats targeting organizations today.

Splunk Security Professional Services give you:

- **Experts in Security AND Splunk**: providing the cybersecurity experience and Splunk skills you need to develop a security program capable of quickly identifying, containing and remediating attacks.
- **Streamlined Operations**: delivering the guidance and tools that enable you to efficiently use resources to effectively remediate the full extent of a breach.
- **Strong Security:** offering a holistic approach to security that helps you improve your overall security stance and maximize the value of all your existing security infrastructure investments.

Splunk Security Professional Services Offerings

There are five security professional services offerings that enterprises can take advantage of:



- **The Splunk Breach Response Services** help you run an investigation to understand the full extent of a breach in your environment and identify the best way to contain and mitigate the impact of the attack.
- **The Security Program Review Service** assesses your security posture to identify gaps and opportunities to maximize the utility of

Rev. 10.9.15

your security infrastructure and improve your overall security stance.

- **The Security Operations Center (SOC) Advisory Services** help you architect/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.

- **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.

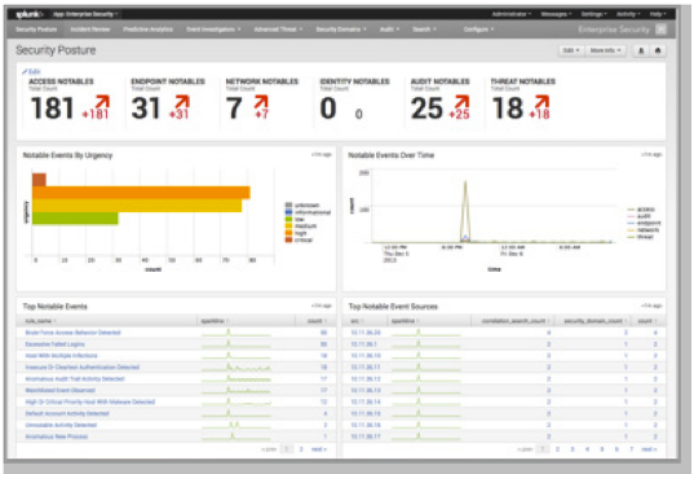
- **The SIEM Migration Services** are designed to help you streamline your migration from an existing SIEM solution to Splunk or optimize your deployment of Splunk with other SIEMs operating in parallel.

Engagement

During the course of the engagement, our seasoned security experts will work with your team to deliver a consistently high quality experience that ensures you can optimize and sustain an effective security environment. Our consultants will work with you to:

- Understand your unique issues and needs.
- Scope out a project, with clear milestones and success criteria.
- Work collaboratively, with frequent touch points and communications, to develop the understanding, systems, processes or tools required to complete the project.
- Deliver documentation and recommendations.
- Provide on-going support, as needed.

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



Splunk Professional Services help you quickly deploy best in class implementations for all your security needs.

Requirements

Splunk's Security Professional Services offerings are designed around customers who have an existing Splunk deployment. 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) or SIEM already in place or planned.
- A full or part-time dedicated security team – with little to intermediate knowledge of security processes, policies and standards.