splunk>

SECURITY PROFESSIONAL SERVICES

Breach Response Services

Accelerate the Investigation & Remediation of Breaches in Your Environment

Overview

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.

Breach Response Services

The Splunk Breach Response Services give you access to seasoned security consultants, who have vast experience with advanced security incidents, to help you improve your ability to investigate, contain and remediate a breach in your environment.

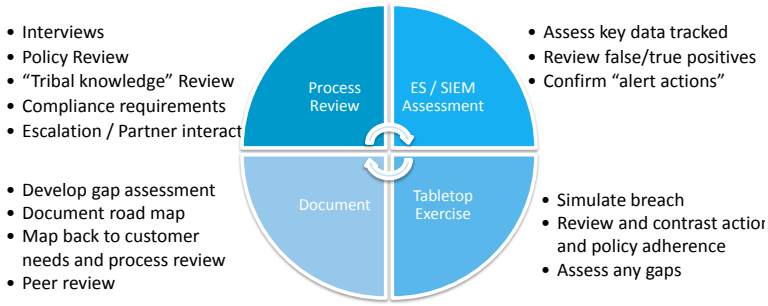
You can use the Breach Response Services to help you **proactively** address a security incident within your infrastructure or **reactively** assess your investigation and remediation capabilities. With Splunk, you can:

- **Realize the Full Value of Your Splunk Investments:** Building the knowledge and skills to help your team use Splunk to run an efficient, effective investigation that uncovers the full extent of a breach.
- **Adopt Best Practices:** Providing guidance on how to implement best practices throughout the course of an investigation to enhance your ability to quickly identify and remediate breaches.
- **Accelerate the Remediation of a Breach:** Recommending the best course of action to contain and remediate a breach to minimize the impact of the attack.

Setting You Up for Success

The Splunk Breach Response Services help you use Splunk to run an efficient, effective investigation capable of uncovering all the components of an attack and identifying all impacted systems. The services also recommend appropriate containment and remediation actions designed to mitigate the full extent of the breach.

Overview of the Breach Response Services



Splunk Professional Services deliver:

- **Expert Security Guidance**: Assisting your in-house staff with cybersecurity experts who have extensive knowledge of how to investigate and mitigate the impact of today's modern, advanced attacks.
- **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 of your security program, from policies to architecture.
- **Tailored Content:** Ensuring your security practitioners know how to use Splunk within your environment to improve the effectiveness of your security team and processes.

Rev. 3.6.14

Engagement

During the course of the engagement, the Breach Response Services will conduct:

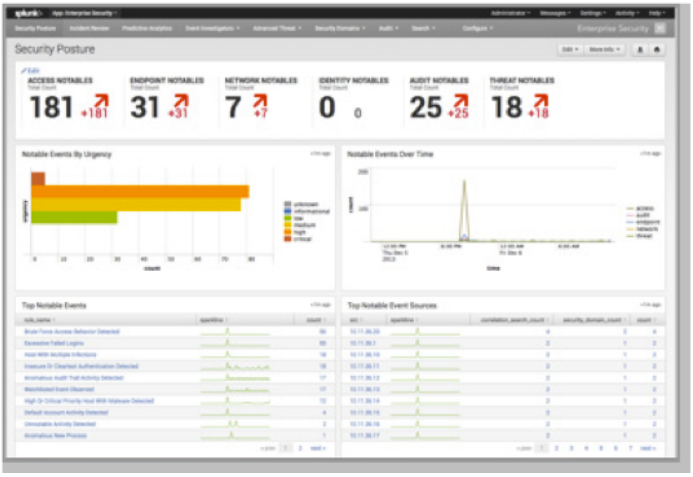
- **An Assessment of Current Operations:** Assess the current state of the incident response capabilities and Splunk deployment.
- **Guidance and Recommendations:** Work with you to determine the optimal approach for improving your security program to better align with your security requirements.
- **Program Follow Up:** The lead consultant (or project team) will follow up at a later date to check in on the status of alert investigations and breach remediation.

The findings and recommendations will be presented via:

Findings Documentation: Documentation of the findings uncovered during the investigation, including:

- Compromised hosts
- Malicious payload research and inspection
- Gap analysis
- Recommendations

- **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.



Splunk Security Professional Services will recommend best in class implementations to accelerate investigations and improve the effectiveness of remediation activities.

The duration of the engagement varies based on the extent of the breach, however, the average timeframe is two to four weeks.

Requirements

The Splunk Breach Response Services are designed for customers who have a new Splunk deployment or are looking to optimize their Splunk investment. New and intermediate in-house security analysts will benefit most from the vast knowledge of the Splunk cybersecurity experts.

To optimize the engagement, customers should have:

- At least a single site instance of the 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.