SECURITY PROFESSIONAL SERVICES

SIEM Migration Services

Ensure a Quick & Seamless Transition to Splunk

Overview

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.

SIEM Migration Services

The Splunk Security Incident and Event Management (SIEM) Migration Services help you quickly and easily migrate from a competitive SIEM offering to Splunk. If you have multiple SIEM solutions operating in parallel, the services can also help you get the most out of your Splunk deployment.

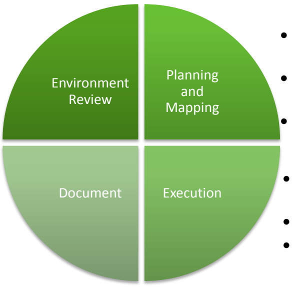
Our seasoned experts have firsthand experience implementing SIEM solutions from many competing vendors, enabling them to guide you on the most efficient and effective way to migrate critical functionality or optimize the deployment of multiple SIEMs in your infrastructure. With Splunk, you can:

- **Realize the Full Value of Your Splunk Investments:** Building proficiency around Splunk that will make it as easy as possible for your team to go from one SIEM platform to another.
- **Maximize Your SIEM Deployment:** Providing guidance on how to implement best practices and make the most of key Splunk functionality to streamline your migration or optimize your cohabitating SIEM solutions.
- **Improve Your Overall Security:** Recommending the best course to migrate to Splunk and leverage its capabilities accelerate attack detection and remediation to minimize the impact of an attack.

Setting You Up for Success

The Splunk SIEM Migration Services offer you a holistic program that makes it as quick and simple as possible to migrate your SIEM solutions and optimize your Splunk deployment.

Review current use cases
Review current reporting
Review current dashboards
Review Log sources
Assess current gaps



- Map current use cases to Splunk use cases
- Document new use cases where none exist
- Create engagement model

Develop mapping document
Develop executive summary
Develop end-state document
Peer review

- Create use cases for 1-to-1 mapping
- Develop new use cases for gaps
- Deploy services, dashboards, reporting, etc.

Splunk Professional Services deliver:

- **Expert SIEM Guidance**: Assisting your in-house staff with cybersecurity experts who have extensive knowledge of the top SIEM solutions in the industry.
- **Fast Migration:** Hastening the deployment of Splunk and the decommissioning of your existing SIEM.
- **Optimal SIEM Usage:** Helping you use Splunk to attain high-quality information in fewer rules than your existing SIEM.
- **Better Vision Into Security:** Delivering a single view into your security environment, as well as providing enhanced intelligence with the inclusion of operational IT data, line data and other information not normally associated with a standard SIEM.
- **Tailored Content:** Ensuring your security practitioners know how to use Splunk within your environment and can move effortlessly through the system to improve the effectiveness of your team and security processes.

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 effectively and efficiently sustain your security environment. The SIEM migration services include:

- **Current SIEM Environment Assessment:** Expert review and recommendations on your current SIEM deployment and security architecture.

- **Analysis of Current SIEM Rules, Reports and Dashboards:** Review of your current SIEM deployment to develop a roadmap for your Splunk implementation.

- **Gap Assessment of Rules and Reports:** Review the current SIEM environment to identify efficiencies you can achieve with Splunk. Additionally, a gap assessment will help you identify new rules, correlation searches or both that can further enhance your SIEM deployment.

- **Industry or Vertical Correlation:** Correlate findings of your environment with industry and vertical best practices and compliance requirements to ensure an optimal deployment.

- **Guidance & Recommendations:** Work with you to determine the optimal approach for your SIEM deployment, including the types of rules and searches you will need to satisfy all your use cases and security requirements.

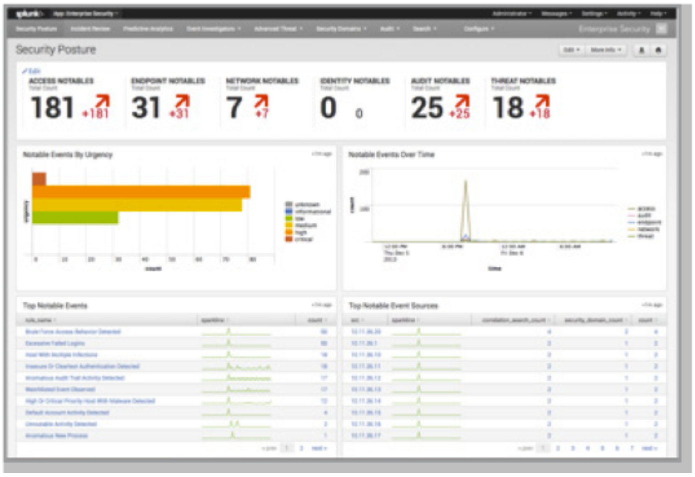
- **Validation Services:** Review the final rules and searches to confirm the output is exactly what is needed and meets the requirements and use case(s) established in the planning phase.

- **Program Follow-Up:** The lead consultant (or project team) will follow up to check on the status of your SIEM deployment, update any gap assessments and offer additional help to implement best practices and streamline your operations. 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 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



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

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

Requirements

The SIEM Migration Services offering is designed around customers who have an existing SIEM and low to medium knowledge of how to use it to effectively monitor their security. Depending on the use case (full replacement or parallel operation), Splunk consultants will assist in everything, from the conversion strategy to the creation of rules and searches, to ensure the final Splunk environment provides the information in a way that best meets the customer's success criteria.

To optimize the engagement, customers should have*:*

- An existing SIEM and processes around it.
- A security program already in place or planned.
- Full or part time dedicated SIEM administrators and users.