PROFESSIONAL SERVICES

Enterprise Security Services — Medium

Professional Services Offering

Overview

The Professional Services Enterprise Security offering provides implementation services to completely deploy the Splunk App for Enterprise Security. This offering encapsulates everything necessary to realize your investment in enterprise security, from data onboarding to custom correlation creation.

Professional Services Enterprise Security Offering

These services are backed by Splunk experts, ensuring consistent and quality delivery, architecture, training and ongoing sustainment for Splunk software in your enterprise.

The offering includes:

- **Splunk PS guidance & recommendations:** Splunk Professional Services will work with you to determine the optimal approach for your security requirements.
- **Architecture review:** Expert review and recommendations on the current Splunk environment. Capacity planning, optimal performance and sustained operations will be addressed.
- **Installation and configuration of the Splunk App for Enterprise Security:** Splunk Professional Services will follow documented best practices for the installation and perform knowledge transfer on the process.
- **Configuration of up to 10 standard data sources:** Configuration for data sources based on use case scenarios to support the underlying security requirements.
- **Configuration of up to two (2) custom data sources:** Configuration for custom data sources based on use case scenarios to support the underlying security requirements.
- **Configuration and deployment of standard reports and dashboard content:** Take advantage of pre-generated visualizations and dashboards available through the app.
- **Configuration and deployment of up to two (2) custom views, each with up to four (4) searches per view:** For scenarios not addressed by the out of box content and visualizations, Splunk PS will create custom Dashboard and Report content as required.
- **Reference documentation:** All relevant information and documentation will be made available to you after the implementation is complete.
- **Configuration of three (3) custom event-based correlation searches and proactive alerts:** Provide expert configuration and implementation of three (3) event-based notifications and proactive alerts designed to provide immediate awareness of the anomalies in your environment.
- **Duration:** Four (4) weeks

Targeted Customer Attributes

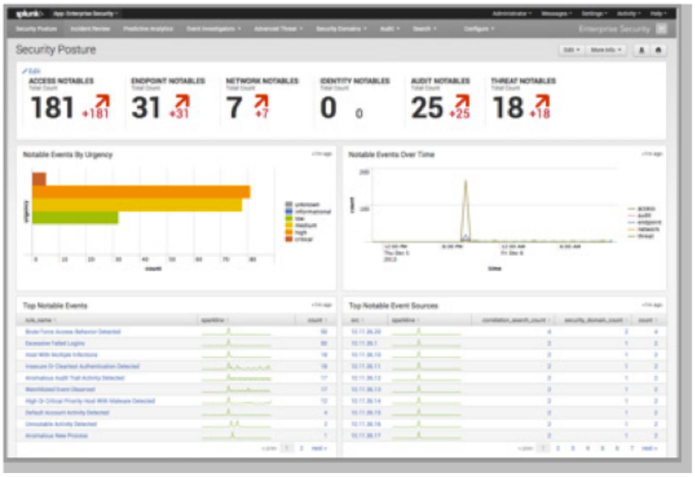
The Splunk Enterprise Security (Medium) offering is designed for customers who have already deployed a functional Splunk infrastructure. This offering can be combined with other service offerings to deploy Splunk Enterprise (Medium) or Splunk Upgrade (Medium) as a complete turnkey solution.

This Professional Services offering is designed for customers with the following prerequisites:

- Single site instance of Splunk Enterprise in production with clustering or shared searching requirements
- Currently using Deployment Server, Puppet or Chef in the production environment for distribution
- Dedicated job server or search head

Benefits

- **Expert guidance for enterprise security**: Learn and understand the best practices and recommendations for getting the most out of your enterprise security investment.
- **Faster innovation:** Leverage Splunk experts to accomplish more in less time.
- **Faster time-to-value:** Using Splunk Professional Services provides the most expedient and efficient method for deploying the enterprise security solution.
- **Optimal performance for fast threat response:** Enable security practitioners to respond to threats as quickly as possible.
- **Custom correlation searches for your data sources:** Create correlation searches across data domains specific to the business systems in use by your company today.
- **Tailor content for your specific security processes:** Enable security practitioners to move effortlessly through the system based on your security processes.



Let Splunk Professional Services provide best in class implementations for your security needs.

Splunk Professional Services

We are here to help customers get the most out of their Splunk deployments. Our services are backed by Splunk experts, who provide consistent and quality service delivery, architecture guidance, training and ongoing support.

Take your Splunk environment to the next level and achieve continual optimization, enhanced processes and active collaboration.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.