splunk>

PROFESSIONAL SERVICES

Splunk Enterprise Security Implementation Success

Accelerate the Time to Value of Your Splunk Enterprise Security Deployment

Jump start your Splunk Enterprise Security (ES) deployment with the Splunk Professional Services **ES Implementation Success Offering**, which enables you to use our team to help you quickly get up and running and accelerate your time to value (TTV).

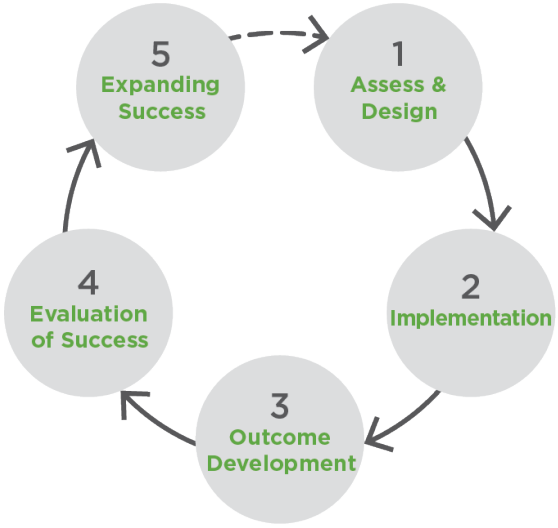
Our experts have created this premium offering to support the rapid implementation of Splunk ES in your environment and increase your overall return on investment (ROI). You benefit from the vast experience of our team, who deploys and works with Splunk every day, and the best practices we have established that ensure ES is quickly optimized for your unique environment.

Offering Highlights

- Solutions Architect designs plan around your needs
- Best-practice based Splunk installation
- Data onboarding of essential data sources
- Installation of Enterprise Security
- Prescriptive use cases implemented

Splunk Success Methodology

Leveraging the experience of thousands of Splunk deployments, the Splunk success methodology will quickly bring you to your desired outcome.



Options to Fit Your Needs

The Splunk ES Implementation Success Offering comes in three sizes – Base, Standard, and Premium – to provide the capabilities that will optimize the implementation and TTV within your environment.

Prescriptive Outcomes

Splunk recommends certain data sources and use cases to get immediate value from Enterprise Security. All levels of this offering have a set of required data sources and a set of recommended use cases they power, to get to those outcomes. The Base offering contains a slimmed-down list of data sources and use cases for base security monitoring outcomes. Standard has a full set of recommended data sources and use cases, while Premium goes beyond and can contain custom analysis and development.

Security Use Case Discovery

Splunk provides workshops designed to help you monitor and increase the effectiveness of your security posture. Our experts will help you identify and customize the security queries (use cases) that will provide the greatest added benefit to your security posture and align with your business needs and risk priorities.

ES Health Check

Splunk Professional Services will come back twice during the first year of deployment to optimize your environment, validate any changes you have implemented, and work with your staff to increase productivity.

ES Upgrade

During the Health Check, Splunk Professional Services will upgrade you to the most recent version of Splunk ES and review new features and capabilities with your staff.

	Splunk Enterprise Deployment	Data Sources	Splunk ES Deployment	Use Cases	Security Use Case Discovery	Future ES Health Check	Future ES Upgrade
Base	X	7	X	7			
Standard	X	9	X	18			
Premium	X	9+	X	18+	X	X	X

Three Sizes to Meet Your Needs

Every customer is different, so we have built three different sizes to provide flexibility to your needs. Each of our offerings includes the alignment of our experts and are surrounded by the support of our talented Delivery Managers.

Base Offering

Base is designed for customers with more internal resources dedicated to the Splunk project. Internal Splunk Admins and Users will receive informal training from the Splunk Accredited Consultant and will complete tasks remaining after Splunk Professional Services finishes their work.

Standard Offering

For customers looking for more support during the initial installation but are confident that ongoing maintenance and optimization of Splunk will be handled well by internal resources, build upon the services offered in Base with our Standard offering.

Premium Offering

This is designed for customers who recognize the opportunity for additional business value beyond the set of initial use cases. With the Premium offering, additional services beyond Standard are included, such as ongoing architectural, workshop, and optimization assistance, plus staff augmentation to meet additional use case and outcome needs.

Included in Every Offering

Planning

- Workshop with a Solutions Architect to develop a plan for implementation

Installation

- Deploy Splunk Enterprise in your environment
- On-board seven or nine essential data sources
- Install Splunk Enterprise Security
- Deploy and optimize 7 or 18 use cases (correlation searches) for your environment
- Optimizing out-of-the-box content

Training

- Providing over-the-shoulder training for your Splunk Admins
- Completing a walk-through of ES functionality for your staff
- Reviewing best practices for on-boarding data
- Reviewing best practices for creating correlation searches

Coordination

- A Delivery Manager tracks your path to success

Data Sources

To ensure Splunk ES can provide the insights you need to make faster and smarter security decisions, you need to ensure Splunk is getting data from critical systems throughout your environment. The ES Implementation Success Offering on-boards seven to nine essential data sources:

Base
- Active Directory
- Exchange
- Windows or Linux servers
- DNS
- Endpoint Anti-Malware
- Network Communication (Firewalls)
- Web Proxy Request

Standard and Premium
- Mail
- DNS
- Authentication
- Endpoint Anti-Malware
- Web Proxy Request
- User Activity
- Audit Trail
- Network Communication (Firewalls)
- Network Intrusion Detection

Setting up Queries

There are certain things you should be looking for that indicate potential threats within your environment. Our team will customize seven to eighteen unique correlation searches (use cases) designed to look for indications of malicious activity on your network. These queries are the foundation of a robust security monitoring program and are recommended, based on the data sources implemented in your environment. For example, they may look for:

Base
- Brute force access detected
- Brute Force Access Detected over One Day
- High Volume Traffic from High/Critical Host Observed
- Host with Recurring Malware Infection
- Host with Multiple Infections
- Host with Old Infection or Potential Re-Infection
- Threat Activity Detected

Standard and Premium
- Activity from expired user identity
- Brute force access detected
- Brute Force Access Detected over One Day
- Expected Host Not Reporting
- High Number of Hosts Not Updating Malware Signatures
- High Number of Infected Hosts
- High/Critical Priority Host w/Malware Detected
- High/Critical Priority Individual Logging into Infected Machine
- High Volume Traffic from High/Critical Host Observed
- Host Sending Excessive Email
- Host with Recurring Malware Infection
- Host with Multiple Infections
- Host with Old Infection or Potential Re-Infection
- Outbreak Detected
- Potential Gap in Data
- Threat Activity Detected
- Vulnerability Scanner Detected (by events)
- Vulnerability Scanner Detected (by targets)

Target Customer Attributes

The Splunk Enterprise Implementation Success offering is designed for customers looking to build a production Splunk infrastructure who are seeking a quick time to value for key business initiatives, from requirements gathering through production deployment.

Splunk Professional Services

Our services are backed by Splunk Accredited Consultants, Solutions Architects, and Delivery Managers. They leverage Splunk best practices and experience from thousands of Splunk deployments.

We only exist to get customers to valuable outcomes with their machine data – faster than they could on their own.

Free Online Sandbox. Get access to a free, personal environment provisioned in the cloud where you can immediately try and experience the power of Splunk IT Service Intelligence. After the initial trial period, or any time before then, you can convert to an Enterprise license by **contacting sales.**

splunk> ps-sales@splunk.com www.splunk.com/