splunk>

TECH BRIEF

ACCELERATE THE TIME-TO-VALUE OF YOUR SPLUNK ENTERPRISE SECURITY DEPLOYMENT

WORKSHOP HIGHLIGHTS

- **Splunk experts optimizing** our product in your environment
- **Let us help you move quickly** to a mature security monitoring environment
- **Ensure success** by investing in your deployment, training, expert services, and health and updates all in one bundle

Jump start your Splunk Enterprise Security (ES) deployment, with the Splunk Professional Services **Enterprise Security Essentials 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.

The ES Essentials Service Offering includes prescriptive deployment services, training, conference passes and is designed for customers implementing our prescriptive network architecture recommendations, designed to scale your environment up to 1TB.

Installation

- Deploying Splunk Enterprise in your environment
- On-boarding nine essential data sources
- Installing Splunk Enterprise Security
- Deploying and optimizing 18 essential queries (correlation searches) for your environment
- Optimizing out-of-the-box content
- Creating up to four custom dashboards
- Creating one custom glass table visualization
- Implementing four unique adaptive response actions

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
- Providing training credits to get your staff prepared to quickly become proficient with Splunk
- Become part of a larger community of expert users by attending .conf

Conference Passes

A pass/passes to Splunk's annual user conference (.conf) gives you access to the broader Splunk ecosystem. Attendees walk away with fresh ideas and insights into what other companies are doing with Splunk, new use cases that help strengthen your security stance and cool Splunk swag.

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 Essentials Service on-boards nine essential data sources:

- **Mail**
- **DNS**
- **Authentication**
- **Endpoint Anti-Malware**
- **Web Proxy Request**
- **User Activity**
- **Audit Trail**
- **Network Communication**
- **Network Intrusion Detection**

Premium Security Correlation Searches Included

There are certain things you should be looking for that indicate potential threats within your environment. Our team will customize the below 18 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.

- Activity from an 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)

Options to Fit Your Needs

The Splunk ES Essentials Bundle comes in three offerings – Standard, Advanced and Premium – to provide the capabilities to optimize the implementation and decrease the TTV within your environment. Note, all offerings are recommended for customers with up to 1TB in daily data volume. Splunk has included additional services in the Advanced and Premium offerings to continue to deliver value during your first year of deployment.

	Splunk ES Essentials Deployment	Splunk Education Credits	Splunk .Conf Passes	Security Use Case Discovery	ES Health Check	ES Upgrade
Standard	X	16	1			
Advanced	X	48	3	X	X	
Premium	X	100	4	X	X	X

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 12 months of your deployment to optimize your environment, validate any changes you have implemented and work with your staff to increase productivity.

ES Upgrade

With the Premium offering, Splunk Professional Services will upgrade you to the most recent version of Splunk ES and review new features and capabilities with your staff. We will schedule this service with your ES Health Check.

Benefits of a Combined Service Offering

Ensure your vision for a world class security nervous system is realized by including the services your team needs to be successful from the beginning of your journey. Splunk's most successful customers have been pairing our service together to ensure their own success, take advantage of our combined service offering to get your project off to the right start.