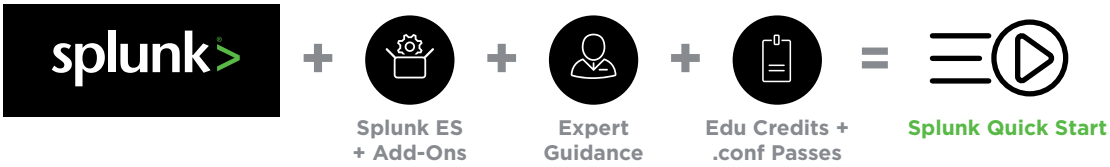
SPLUNK QUICK START FOR SIEM

Quickly Gain Insight Into Threat and Malware Activity

The Splunk Quick Start for SIEM provides a fast approach to get up and running using Splunk Enterprise Security, an analytics-driven SIEM.



Today's enterprise requires big data security solutions that can monitor and investigate advanced threats and attacks, and enable rapid incident response. Simple monitoring of traditional security events is no longer enough. Security practitioners need broader insights from new data sources and all security relevant data generated at massive scale across IT, the business and in the cloud.

Staying ahead of external attacks, threats and malware demands continuous threat activity and security monitoring, fast incident response and the ability to investigate and respond to known, unknown and advanced threats.

To help you see results quickly from your Splunk deployment, the Splunk Quick Start for SIEM gives you everything you need to effectively mitigate risk by collaborating between IT security and IT operations, and to monitor your infrastructure and detect malware in an easy-to-deploy package. Benefits of the Splunk Quick Start include:

- **Fast time-to-value,** determine threat and malware activity within your environment
- **Fully deployed** in three weeks and supported by a project manager
- **Additionally,** you can use the full capability of Splunk Enterprise Security to solve a wide range of SIEM use cases and more
- **Continue learning** by using the education credit and .conf event passes
- **Scalable packages** in medium and large sizes to meet your needs

What's Included

- Splunk Enterprise Security
- Personalized and interactive guidance from Splunk experts to quickly deploy your instance
- Education credits to get your team Splunk Certified
- Passes to our yearly user conference, so you can pick up best practices from other Splunk customers
- Apps and Add-ons related to customer environment

Curated Selection of Splunk Apps and Add-ons

With the Splunk Quick Start for SIEM, you get Splunk experts installing Splunk Enterprise Security, configuring required data sources for the Malware and Threat Activity Dashboards and preselected Splunk-certified apps and add-ons to collect and correlate required data sources for the dashboards.

The supported list of data sources is:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft Windows servers
- Linux servers
- DNS servers on Windows or Linux
- Symantec Endpoint Protection
- Sophos Enterprise Console
- Blue Coat ProxySG
- Cisco WSA
- Cisco ASA
- FortiGate
- Palo Alto Networks firewall

Quick Insight Into Threat and Malware Activity Within Your Organization

The Splunk Quick Start for SIEM also comes complete with a Professional Services implementation:

- Install Splunk Enterprise Security and associated apps and add-ons
- Configure appropriate data sources for the Malware Dashboard
- Configure appropriate data sources for the Threat Activity Dashboard

Seven alert-based use cases will be implemented to supplement dashboard-based investigations including:

- Brute Force Access Behavior Detected
- High Volume of Traffic from High or Critical Host Observed
- Host With a Recurring Malware Infection
- Threat Activity Detected

Personalized Support

Your Quick Start includes a consultation with a project manager to answer your questions, help you gain expertise, and maximizing your insight and ROI from Splunk.

Education Credits

Even after you've deployed your Splunk instance, you can continue to up level your skills. The Quick Start contains credits to get you Splunk Admin Certified or multiple people Power User Certified. You can spread the credits out across the team as you see fit. Additionally, you get passes to .conf, Splunk's annual user conference, where you can meet and learn from the experiences of other Splunk customers.

For More Information:
www.splunk.com/bundles