Administering ES

This 13.5 hour course prepares architects and systems administrators to install and configure Splunk Enterprise Security (ES). It covers ES event processing and normalization, deployment requirements, technology add-ons, dashboard dependencies, data models, managing risk, and customizing threat intelligence.

Course Topics

- Examine how ES functions including data models, correlation searches, notable events, and dashboards
- Create custom correlation searches
- Customize the Investigation Workbench
- Learn how to install or upgrade ES
- Learn the steps to setting up inputs using technology add-ons
- Fine tune ES Global Settings
- Customize risk and configure threat intelligence

Prerequisite Knowledge

To be successful, students should have a solid understanding of the following:

If on-prem:

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration

If on cloud:

- Splunk Cloud Administration

and

- What is Splunk?
- Intro to Splunk
- Using Fields
- Visualizations
- Search Under the Hood
- Intro to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards

Course Format

Instructor-led lecture with labs. Delivered via virtual classroom or at your site.

Course Objectives

Module 1 – Introduction to ES

- Review how ES functions
- Understand how ES uses data models
- Configure ES roles and permissions

Module 2 – Security Monitoring

- Customize the Security Posture and Incident Review dashboards
- Create ad hoc notable events
- Create notable event suppressions

Module 3 – Risk-Based Alerting

- Explain Risk-Based Alerting
- Explain risk scores
- Review the Risk Analysis dashboard
- Use annotations
- Explain ways to assign risk

Module 4 – Incident Investigation

- Review the Investigations dashboard
- Customize the Investigation Workbench
- Manage investigations

Module 5 – Installation

- Prepare a Splunk environment for installation
- Download and install ES on a search head
- Test a new install
- Post-install configuration tasks

Module 6 – Initial Configuration

- Set general configuration options
- Add external integrations
- Configure local domain information
- Customize navigation
- Configure Key Indicator searches

Module 7 – Validating ES Data

- Verify data is correctly configured for use in ES
- Validate normalization configurations
- Install additional add-ons

Module 8 – Custom Add-ons

- Design a new add-on for custom data
- Use the Add-on Builder to build a new add-on

Module 9 – Tuning Correlation Searches

- Configure correlation search scheduling and sensitivity
- Tune ES correlation searches

Module 10 – Creating Correlation Searches

- Create a custom correlation search
- Manage adaptive responses
- Export/import content

Module 11 – Asset & Identity Management

- Review the Asset and Identity Management interface
- Describe Asset and Identity KV Store collections
- Configure and add asset and identity lookups to the interface
- Configure settings and fields for asset and identity lookups
- Explain the asset and identity merge process
- Describe the process for retrieving LDAP data for an asset or identity lookup

Module 12 – Managing Threat Intelligence

- Understand and configure threat intelligence

- Use the Threat Intelligence Management interface to configure a new threat list

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/education

To contact us, email Education_AMER@splunk.com

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

Contact sales