

## Administering Splunk Enterprise Security

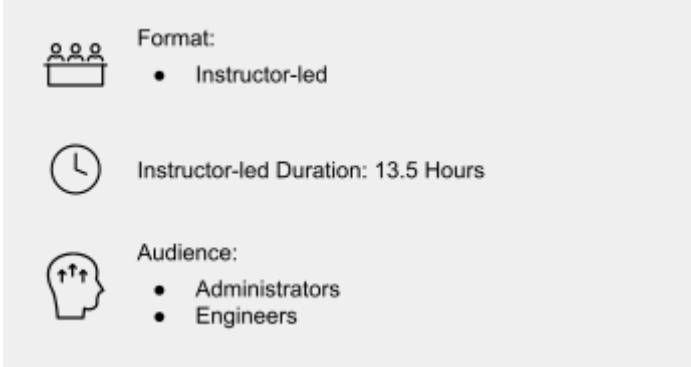
### Summary

This course is for ES Administrators and Engineers.

This 13.5-hour course prepares Security Administrators and Engineers 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.

### Prerequisites

- To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
  - Using Splunk Enterprise Security
  - What is Splunk?
  - Intro to Splunk
  - Using Fields
  - Introduction to Knowledge Objects
  - Creating Knowledge Objects
  - Creating Field Extractions
  - Enriching Data with Lookups
  - Data Models
  - Splunk Enterprise System Administration
  - Splunk Enterprise Data Administration



**Format:**

- Instructor-led

**Instructor-led Duration:** 13.5 Hours

**Audience:**

- Administrators
- Engineers

### Course Outline

#### Module 1 – Introduction to Enterprise Security

- Review how ES functions
- Understand how ES uses data models
- Describe correlation searches, adaptive response actions, and notable events
- 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

- Give an overview of Risk-Based Alerting (RBA)
- Explain risk scores and how they can be changed
- Review the Risk Analysis dashboard
- Describe annotations
- View Risk Notables and risk information

## Module 4 – Incident Investigation

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

## Module 5 – Installation

- Give an overview of general ES install requirements
- Explain the different add-ons and where they are installed
- Provide ES pre-installation requirements
- Identify steps for downloading and installing ES

## Module 6 – General Configuration

- Set general configuration options
- Configure local and cloud domain information
- Work with the Incident Review KV Store
- 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

- Ingest custom data in ES
- Create an add-on for a custom sourcetype
- Describe add-on troubleshooting

## Module 9 – Tuning Correlation Searches

- Describe correlation search operation
- Customize correlation searches
- Describe numeric vs. conceptual thresholds

## 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
- Configure new threat lists

## Module 13 – Supplemental Apps

- Review apps to enhance the capabilities of ES including, Mission Control, SOAR, UBA, Cloud-based Streaming Analytics, PCI Compliance, Fraud Analytics, and Lookup File Editor

### About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit <http://www.splunk.com/education>.

To contact us, email [education@splunk.com](mailto:education@splunk.com).