

Using Splunk Enterprise Security

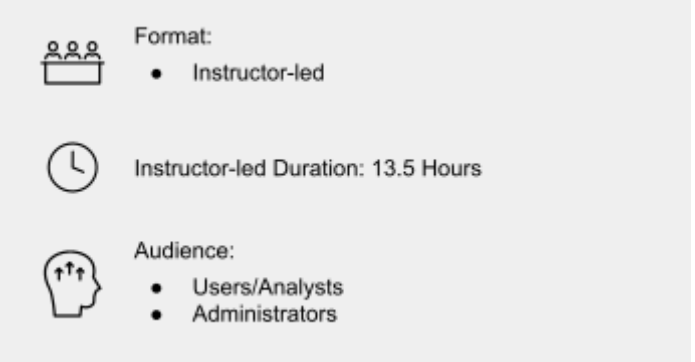
Summary

This course is for Security Analysts and Administrators.

This 13.5-hour course prepares Security Analysts and Administrators to use Splunk Enterprise Security (ES). Students identify and track incidents, analyze security risks, use predictive analytics, and discover threats.

Prerequisites

- To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
 - Splunk Fundamentals 1
 - Splunk Fundamentals 2
- Additional courses and/or knowledge in these areas are also highly recommended:
 - What is Splunk?
 - Intro to Splunk
 - Using Fields
 - Scheduling Reports and Alerts
 - Visualizations
 - Leveraging Lookups and Sub-searches
 - Search Under the Hood
 - Introduction to Knowledge Objects
 - Enriching Data with Lookups
 - Data Models
 - Introduction to Dashboards



Format:

- Instructor-led

Instructor-led Duration: 13.5 Hours

Audience:

- Users/Analysts
- Administrators

Course Outline

Module 1 – Introduction to Enterprise Security

- Describe the features and capabilities of Splunk Enterprise Security (ES)
- Explain how ES helps security practitioners prevent, detect, and respond to threats
- Describe correlation searches, data models, and notable events
- Describe user roles in ES
- Log into Splunk Web and access Splunk for Enterprise Security

Module 2 – Security Monitoring & Incident Investigation

- Use the Security Posture dashboard to monitor ES status
- Use the Incident Review dashboard to investigate notable events
- Take ownership of an incident and move it through the investigation workflow
- Create notable events
- Suppress notable events

Module 3 – Risk-Based Alerting

- Give an overview of Risk-Based Alerting (RBA)

- View Risk Notables and risk information on the Incident Review dashboard
- Explain risk scores and how to change an object's risk score
- Review the Risk Analysis dashboard
- Describe annotations
- Describe the process for retrieving LDAP data for an asset or identity lookup

Module 4 – Assets & Identities

- Give an overview of the ES Assets and Identities framework
- Show examples where asset or identity data is missing from ES dashboards or notable events
- View the Asset & Identity Management Interface
- View the contents of an asset or identity lookup table

Module 5 – Investigation

- Use investigations to manage incident response activity
- Use the Investigation Workbench to manage, visualize and coordinate incident investigations
- Add various items to investigations (notes, action history, collaborators, events, assets, identities, files and URLs)
- Use investigation timelines, lists and summaries to document and review breach analysis and mitigation efforts

Module 6 – Security Domain Dashboards

- Describe the ES security domains
- Use the Security Domain dashboards to troubleshoot various security threats
- Learn how to launch the Security Domain dashboards from a notable event in Incident Review

Module 7 – User Intelligence

- Understand and use user activity analysis
- Use investigators to analyze events related to an asset or identity
- Use access anomalies to detect suspicious access patterns

Module 8 – Web Intelligence

- Use the web intelligence dashboards to analyze your network environment
- Filter and highlight events

Module 9 – Threat Intelligence

- Give an overview of the Threat Intelligence framework and how threat intel is configured in ES
- Use the Threat Activity dashboard to see which threat sources are interacting with your environment
- Use the Threat Artifacts dashboard to examine the status of threat intelligence information in your environment

Module 10 – Protocol Intelligence

- Explain how network data is input into Splunk events
- Describe stream events
- Give an overview of the Protocol Intelligence dashboards and how they can be used to analyze network data

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.