

SPLK-USES6.6: Using Splunk Enterprise Security 6.6

Course Code: SPLK-USES6.6

Duration: 3 days

Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

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

SKILLS COVERED

- Please refer to course overview.

WHO SHOULD ATTEND?

Everyone can attend.

PREREQUISITES

- Splunk Fundamentals 1
- Splunk Fundamentals 2

Or the following single-subject courses:

- 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

MODULES

Module 1: Getting Started with ES

- 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 and 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
- 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: Investigations

- 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 5: Using Security Domain Dashboards

- Use ES to inspect events containing information relevant to active or past incident investigations
- Identify security domains in ES
- Use ES security domain dashboards
- Launch security domain dashboards from Incident Review and from action menus in search results

Module 6: Web Intelligence

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

Module 7: User Intelligence

- Evaluate the level of insider threat with the user activity and access anomaly dashboards
- Understand asset and identity concepts
- Use the session center for identity resolution
- Discuss Splunk User Behavior Analytics (UBA) integration

Module 8: 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 Activity dashboard to examine the status of threat

intelligence information in your environment.

Module 9: 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

END OF PAGE