SPLK-ASES6.6: Administering Splunk Enterprise Security 6.6

Course Code: SPLK-ASES6.6
Duration: 3 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

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.

SKILLS COVERED

- Please refer to course overview.

WHO SHOULD ATTEND?

Everyone can attend.

PREREQUISITES

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

- 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 Subsearches
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards
- Dynamic Dashboards

Students should also have completed the following courses:

- Splunk System Administration
- Splunk Data Administration

MODULES

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

- Give an overview of risk-based alerting
- View Risk Notables and risk information on the Incident Review dashboard
- Explain risk scores and how an ES admin can change an object's risk score
- Review the Risk Analysis dashboard
- Describe annotations

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: Threat Intelligence Framework

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

END OF PAGE