Administering Splunk Enterprise Security (ASES)

Price	Duration	Delivery Methods
$1,500.00	2 Days	VILT, Private Group

It covers ES event processing and normalization, deployment requirements, technology add-ons, dashboard dependencies, data models, managing risk, and customizing threat intelligence.

Who Should Attend

This course prepares architects and systems administrators to install and configure Splunk Enterprise Security (ES).

Course Objectives

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

Agenda

1 - INTRODUCTION TO ES

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

2 - SECURITY MONITORING

- Customize the Security Posture and Incident Review dashboards

- Create ad hoc notable events
- Create notable event suppressions

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

4 - INCIDENT INVESTIGATION

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

5 - INSTALLATION

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

6 - INITIAL CONFIGURATION

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

7 - VALIDATING ES DATA

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

8 - CUSTOM ADD-ONS

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

9 - TUNING CORRELATION SEARCHES

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

10 - CREATING CORRELATION SEARCHES

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

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

12 - THREAT INTELLIGENCE FRAMEWORK

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