Administering Splunk Enterprise Security

(SP-ASES)

COURSE OVERVIEW

This course is part of the following Certifications:

- Splunk Core Certified Power User
- Splunk Core Certified Advanced Power User

PREREQUISITES

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

- How Splunk works
- Creating search queries
- Lookups

WHO SHOULD ATTEND

This 13.5-hour course prepares architects and systems administrators to install and configure Splunk Enterprise Security (ES).

COURSE OBJECTIVES

- Calculate Co-Occurrence Between Fields
- Analyze Multiple Datasets

Administering Splunk Enterprise Security

(SP–ASES)

COURSE OUTLINE

Module 1 – Introduction to ES

- 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