Administering Splunk Enterprise Security

Category: Networking & Security | **Vendor:** Splunk

Duration: 16.00 hours (2 days) **13.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

This course is for ES Administrators and Engineers.

This 13.5-hour instructor-led course enables SOC Engineers to use Splunk’s Enterprise Security SIEM for detection engineering, incident response, automation, asset and identity configuration, and threat intelligence management. Other topics include ES event processing and normalization, managing risk, data models, deployment requirements, technology add-ons, and dashboard dependencies..

This course may be delivered over two or three days, with 13.5 total hours of content.

About This Course

Module 1 - Introduction to Enterprise Security

- Explain the function of a SIEM
- Give an overview of Splunk’s Enterprise Security (ES)
- Describe detections and findings
- Configure ES roles and permissions
- Give an overview of ES navigation

Module 2 - Customizing the Analyst Queue and findings

- Give an overview of the Analyst Queue
- Create and use Analyst Queue Views
- Customize the Analyst Queue
- Modify Urgency
- Create new Status values
- Add fields to Finding attributes
- Create ad hoc Findings
- Suppress Findings

Module 3 - Working with Investigations

- Give an overview of an investigation
- Use and create Response Plans
- Add Splunk events to an investigation
- Use Playbooks and Actions

Module 4 - 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 5 - Data Normalization

- Understand how ES uses accelerated data models
- Verify data is correctly configured for use in ES
- Validate normalization configurations
- Install additional add-ons
- Ingest custom data in ES
- Create an add-on for a custom sourcetype
- Describe add-on troubleshooting

Module 6 - Detection Engineering

- Give an overview of how to create Event-based detections
- Review the Detection Editor
- Give an overview of how to create Finding-based detections

Module 7 - Risk-Based Alerting

- Give an overview of Risk-Based Alerting (RBA)
- Explain risk scores and how they can be changed by detections or manually
- Review the Risk analysis dashboard
- Understand Finding-based detections
- Describe annotations
- View risk information in Analyst Queue findings

Module 8 - Managing Threat Intelligence

- Understand and configure threat intelligence
- Use the Threat Intelligence interface to configure threat lists
- Configure new threat lists

Module 9 - Post-Deployment Configuration

- Give an overview of general ES install requirements
- Explain the different add-ons and where they are installed

- Provide ES pre-installation requirements
- Describe the Splunk_TA_ForIndexers app and where it is installed
- Set general configuration options
- Configure local and cloud domain information
- Work with the Incident Review KV Store
- Customize navigation
- Configure Key Indicator searches

Who Should Attend

- SOC Analyst
- SOC Engineer

Prerequisites & Entry Requirements

General Prerequisites:

To be successful, students must have completed the following Splunk Education course:

- Using Splunk Enterprise Security (USES)

Students should also be familiar with the topics covered in the following courses:

- Intro to Splunk
- Using Fields (SUF)
- Visualizations
- Search Under the Hood
- Intro to Knowledge Objects
- Creating Knowledge Objects (CKO)
- Creating Field Extractions (CFE)
- Enriching Data with Lookups (EDL)
- Data Models (SDM)
- Introduction to Dashboards (ITD)
- Splunk Enterprise System Administration (SESA) AND Splunk Enterprise Data Administration (SEDA) OR Splunk Cloud Administration (SCA)

Frequently Asked Questions

Q: What delivery options are available for Administering Splunk Enterprise Security?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 2-day Administering Splunk Enterprise Security course provides up to 13.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Administering Splunk Enterprise Security training?

The training takes place over 2 day(s), with each day lasting approximately 16.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Administering Splunk Enterprise Security?

Yes, we provide corporate training, dedicated training, and closed classes for Administering Splunk Enterprise Security. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Administering Splunk Enterprise Security, SOC Administrator (Enterprise Security) On-Prem, ASES

Q: Why choose Nexus Human for Administering Splunk Enterprise Security?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Administering Splunk Enterprise Security training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)