Using 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 13.5-hour instructor-led course prepares SOC Analysts to use Splunk Enterprise Security (ES).Students identify and track incidents, analyze security risks, use predictive analytics, and discover threats.

Please note that this course may run over three days, with 4.5 hour sessions each day.

About This Course

Module 1 - ES Fundamentals

- Explain the function of a SIEM
- Give an overview of Splunk Enterprise Security (ES)
- Understand how ES uses data models
- Describe detections and findings
- Identify ES roles and permissions
- Give an overview of ES navigation

Module 2 - Exploring the Analyst Queue

- Explore the Analyst Queue
- Filtering
- Triage Findings and Finding Groups
- Create ad hoc Findings
- Suppress Findings from the Analyst Queue

Module 3 - Working with Investigations

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

Module 4 - Risk-based Alerting

- Give an overview of risk and Risk-Based Alerting (RBA)
- Explain risk scores and how to change an entity's risk score
- Review the Risk Analysis dashboard
- Describe annotations
- View risk information in Analyst Queue findings

Module 5 - Assets & Identities

- Give an overview of the ES Assets and Identities (A&I) framework
- Show where asset or identity data is missing from ES findings or dashboards
- View the A&I Management Interface
- View the contents of an asset or identity lookup table
- Identify A&I field matching criteria

Module 6 - Adaptive Responses

- Describe Adaptive Responses
- Identify the default ES Adaptive Responses
- Discuss Adaptive Response invocation methods
- Troubleshoot Adaptive Response issues

Module 7 - Security Domain Dashboards

- Use ES to inspect events containing information relevant to active or past incident investigation
- Identify ES Security Domains
- Use the Security Domain dashboards
- Launch Security Domain dashboards from the Analyst Queue and from field action menus in search results

Module 8 - Intelligence Dashboards

- Use the Web Intelligence dashboards to analyze your network environment
- Filter and highlight events
- Understand and use User Intelligence dashboards
- Use Investigators to analyze events related to an asset or identity
- Use Access Anomalies to detect suspicious access patterns

Module 9 - Threat Intelligence

- Give an overview of the Threat Intelligence framework
- Identify where Threat Intelligence is configured
- Observe Threat Findings
- View downloaded Threat Indicators
- Troubleshooting Threat Intelligence

Module 10 - 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

Who Should Attend

SOC Analysts.

Prerequisites & Entry Requirements

General Prerequisites:

To be successful, students should have a working understanding of the topics covered in the following Splunk courses:

- Intro to Splunk (eLearning)
- Using Fields (SUF)
- Visualizations
- Search Under the Hood
- Intro to Knowledge Objects
- Introduction to Dashboards (ITD)

Frequently Asked Questions

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

Yes, we provide corporate training, dedicated training, and closed classes for Using 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: Using Splunk Enterprise Security, SOC Analyst (Enterprise Security), USES

Q: Why choose Nexus Human for Using 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 Using 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)