Enhancing Cisco Security Solutions with Splunk

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

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

The Enhancing Cisco Security Solutions with Data Analytics (ECSS) training covers intermediate-level knowledge of Splunk, including its fundamentals, key components, and architecture so you can detect, investigate, and respond to security threats effectively. You'll learn to utilize various Splunk components, including Cisco XDR, Splunk SIEM, and Splunk SOAR. You'll also discover how to use and troubleshoot the Cisco Security Cloud App, Cisco Legacy Apps, and technology add-ons (TAs) for integrating Cisco security solutions with Splunk for enhancing user, cloud, and breach protections.

How You'll Benefit

This training will help you:

- Aggregate data from all Cisco security products into a single Splunk instance for centralized visibility
- Monitor your security environment in real time to detect and respond to threats faster
- Streamline security workflows by reducing dashboard switching and manual data correlation
- Enhance decision-making with customizable dashboards and comprehensive, accurate insights
- Protect your organization more effectively by integrating Cisco security solutions with Splunk for unified threat detection and response
- Earn 32 CE credits toward recertification

About This Course

The Enhancing Cisco Security Solutions with Data Analytics (ECSS) training covers intermediate-level knowledge of Splunk, including its fundamentals, key components, and architecture so you can detect, investigate, and respond to security threats effectively. You'll learn to utilize various Splunk components, including Cisco XDR, Splunk SIEM, and Splunk SOAR. You'll also discover how to use and troubleshoot the Cisco Security Cloud App, Cisco Legacy Apps, and technology add-ons (TAs) for integrating Cisco security solutions with Splunk for enhancing user, cloud, and breach protections.

How You'll Benefit

This training will help you:

- Aggregate data from all Cisco security products into a single Splunk instance for centralized visibility
- Monitor your security environment in real time to detect and respond to threats faster
- Streamline security workflows by reducing dashboard switching and manual data correlation
- Enhance decision-making with customizable dashboards and comprehensive, accurate insights
- Protect your organization more effectively by integrating Cisco security solutions with Splunk for unified threat detection and response
- Earn 32 CE credits toward recertification

Who Should Attend

- System Engineers
- SOC Engineers
- Network Architects

Prerequisites & Entry Requirements

General Prerequisites:

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- Cisco CCNP Security or equivalent knowledge

These skills can be found in the following Cisco Learning Offering:

- Implementing and Operating Cisco Security Core Technologies (SCOR)

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Explain the Splunk Enterprise/Cloud fundamentals
- Explain the use of XDR, SIEM, SOAR as part of the modern SOC architecture to enhance the SOC’s ability to detect, investigate, and respond to security threats effectively
- Implement Cisco Security Solutions to Splunk Integration using the Cisco Security Cloud App
- Implement Cisco Security Solutions to Splunk Integration using Cisco Legacy Apps and TAs
- Illustrate the value of integrating Cisco security solutions with Splunk using real-world use cases
- Troubleshoot the Cisco Security Cloud App and the Cisco Apps and TAs

Detailed Course Outline

- Overview of Splunk Enterprise and Splunk Cloud
- Splunk Enterprise and Splunk Cloud Components
- Splunk Enterprise Data Ingestion
- Splunk Search Programming Language
- Splunk Dashboards and Reports
- XDR, SIEM, and SOAR Platforms
- Cisco XDR, Splunk SIEM, and Splunk SOAR
- Cisco Security Cloud App
- Cisco Secure Firewall Integration
- Cisco XDR Integration
- Cisco Secure Malware Analytics, Duo, Secure Network Analytics, Email Threat Defense, and Multicloud Defense Integrations
- Cisco Security Legacy Apps and Technology Add-Ons
- Cisco ISE Integration
- Cisco NVM Integration
- Cisco Security Solutions and Splunk Use Case
- Cisco XDR and Splunk Use Case
- Troubleshoot General Splunk Issues

- Troubleshoot Cisco Security Cloud App

- Troubleshoot Cisco Legacy Apps and Add-ons

Skills You Will Learn:

- Explain the Splunk Enterprise/Cloud fundamentals
- Explain the use of XDR, SIEM, SOAR as part of the modern SOC architecture to enhance the SOC’s ability to detect, investigate, and respond to security threats effectively
- Implement Cisco Security Solutions to Splunk Integration using the Cisco Security Cloud App
- Implement Cisco Security Solutions to Splunk Integration using Cisco Legacy Apps and TAs
- Illustrate the value of integrating Cisco security solutions with Splunk using real-world use cases
- Troubleshoot the Cisco Security Cloud App and the Cisco Apps and TAs

Frequently Asked Questions

Q: What delivery options are available for Enhancing Cisco Security Solutions with Splunk?

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 5-day Enhancing Cisco Security Solutions with Splunk course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Enhancing Cisco Security Solutions with Splunk training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Enhancing Cisco Security Solutions with Splunk?

Yes, we provide corporate training, dedicated training, and closed classes for Enhancing Cisco Security Solutions with Splunk. 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: Enhancing Cisco Security Solutions with Splunk, Security Platform, Architecture & Cloud, ECSS

Q: Why choose Nexus Human for Enhancing Cisco Security Solutions with Splunk?

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 Enhancing Cisco Security Solutions with Splunk 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)