Enhancing Cisco Security Solutions with Data Analytics (ECSS)

What you'll learn in 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 Splunk Enterprise, 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.

This training also earns you 32 Continuing Education (CE) credits toward recertification.

Course duration

Instructor-led training: 5 days in the classroom

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

Course Objectives

- Explain the Splunk Enterprise/Cloud fundamentals
- Explain the use of 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

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 Splunk Enterprise Integration
- Cisco Secure Malware Analytics, Duo, Secure Network Analytics, Email
- Threat Defense and Multiload Defense Integrations
- Cisco Security Legacy Apps and Technology Add-Ons
- Cisco ISE Integration
- Cisco NVM Integration
- Cisco Security Solutions and Splunk Use Case Cisco Splunk Use Case
- Troubleshoot General Splunk Issues
- Troubleshoot Cisco Security Cloud App
- Troubleshoot Cisco Legacy Apps and Add-ons

Lab Outline

- Explore Splunk Indexes Explore Splunk Web and CLI Verify and Test Data Ingestion
- Malware Events Analysis Using Splunk Enterprise Simulation Perform Search Queries
- Create Dashboards and Reports Explore Splunk SOAR
- Explore Cisco XDR Incident Investigation Cisco Secure Firewall Integration with Splunk
- Cisco XDR to Splunk Enterprise Integration Simulation Cisco Duo Integration Simulation
- Cisco SMA Integration Simulation

- Cisco SNA Integration Simulation
- Explore the Cisco ISE Integration with Splunk Using the Legacy ISE App
- Explore the Cisco NVM Integration with Splunk Using the Legacy CESA App and TA
- Investigating Ransomware Using Splunk Enterprise with the Various Cisco Security Apps
- Troubleshoot Cisco Security Cloud App with Cisco Secure Firewall Integration
- Troubleshooting Cisco ISE Integration with Splunk
- Troubleshooting Cisco NVM Integration with Splunk

Course 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

Who should Enroll

- System Engineers
- SOC Engineers
- Network Architect