Enhancing Cisco Security Solutions with Splunk (ECSS)

Enhancing Cisco Security Solutions with Splunk (ECSS)

In this Enhancing Cisco Security Solutions with Data Analytics course provides a comprehensive introduction to Splunk Enterprise and Splunk Cloud, with a strong focus on integrating Cisco security technologies for centralized monitoring, analytics, and incident response. The curriculum begins by establishing foundational Splunk concepts, including core components, data ingestion methods, the Splunk Search Processing Language, and the creation of dashboards and reports. Learners gain hands-on experience exploring Splunk interfaces, validating data ingestion, and performing effective searches to transform raw security data into actionable intelligence.

The course then expands into security operations, introducing XDR, SIEM, and SOAR concepts and demonstrating how Cisco XDR, Splunk SIEM, and Splunk SOAR work together within the Cisco Security Cloud. Students explore integrations with Cisco Secure Firewall, Cisco Secure Malware Analytics, Duo, Secure Network Analytics, Email Threat Defense, Multicloud Defense, Cisco ISE, and Network Visibility Module, learning how security telemetry from across the enterprise is correlated within Splunk. Both modern Cisco Security Cloud applications and legacy Splunk apps and technology add-ons are examined to provide a complete understanding of integration options and use cases.

Operational skills are reinforced through extensive labs focused on malware and ransomware investigation, incident analysis, dashboard creation, and end-to-end troubleshooting. Students learn how to diagnose data ingestion issues, resolve integration problems with Cisco security platforms, and investigate real-world security incidents using Splunk Enterprise, Cisco XDR, and Splunk SOAR workflows. By the end of the course, learners are equipped to deploy, integrate, analyze, and troubleshoot Splunk-based security monitoring solutions in complex enterprise environments.

How you'll benefit

This class 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 Duration

5 days

Course Price

$4,595.00 or 44 CLCs

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The job roles best suited to the material in this course are:

- System Engineers
- SOC Engineers
- Network Architects

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

OUTLINE

Module 1: Overview of Splunk Enterprise and Splunk Cloud

Module 2: Splunk Enterprise and Splunk Cloud Components

Module 3: Splunk Enterprise Data Ingestion

Module 4: Splunk Search Programming Language

Module 5: Splunk Dashboards and Reports

Module 6: XDR, SIEM, and SOAR Platforms

Module 7: Cisco XDR, Splunk SIEM, and Splunk SOAR

Module 8: Cisco Security Cloud App

Module 9: Cisco Secure Firewall Integration

Module 10: Cisco Splunk Enterprise Integration

Module 11: Cisco Secure Malware Analytics, Duo, Secure Network Analytics, Email Threat Defense, and

Multicloud Defense Integrations

Module 12: Cisco Security Legacy Apps and Technology Add-Ons

Module 13: Cisco ISE Integration

Module 14: Cisco NVM Integration

Module 15: Cisco Security Solutions and Splunk Use Case

Module 16: Cisco Splunk Use Case

Module 17: Troubleshoot General Splunk Issues

Module 18: Troubleshoot Cisco Security Cloud App

Module 19: Troubleshoot Cisco Legacy Apps and Add-ons

Lab Outline

- Lab 1: Explore Splunk Indexes
- Lab 2: Explore Splunk Web and CLI
- Lab 3: Verify and Test Data Ingestion
- Lab 4: Malware Events Analysis Using Splunk Enterprise Simulation
- Lab 5: Perform Search Queries
- Lab 6: Create Dashboards and Reports
- Lab 7: Explore Splunk SOAR
- Lab 8: Explore Cisco XDR Incident Investigation
- Lab 9: Cisco Secure Firewall Integration with Splunk
- Lab 10: Cisco XDR to Splunk Enterprise Integration Simulation
- Lab 11: Cisco Duo Integration Simulation
- Lab 12: Cisco SMA Integration Simulation
- Lab 13: Cisco SNA Integration Simulation
- Lab 14: Explore the Cisco ISE Integration with Splunk Using the Legacy ISE App and TA
- Lab 15: Explore the Cisco NVM Integration with Splunk Using the Legacy CESA App and TA
- Lab 16: Investigate Ransomware Using Splunk Enterprise with the Various Cisco Security Apps
- Lab 17: Troubleshoot Cisco Security Cloud App with Cisco Secure Firewall Integration
- Lab 18: Troubleshooting Cisco ISE Integration with Splunk
- Lab 19: Troubleshooting Cisco NVM Integration with Splunk