

ECSS

Enhancing Cisco Security Solutions with Splunk

40 horas

Profissional

Cisco

Cisco Continuing Education Credits

32 CE Credits

INTRODUÇÃO

The Enhancing Cisco Security Solutions with Splunk (ECSS) training covers intermediate-level knowledge of Splunk to detect, investigate, and respond to security threats, including Splunk Enterprise, SIEM, SOAR, and Cisco security integrations.

OBJETIVO DO CURSO

Explain Splunk Enterprise/Cloud fundamentals

Explain SIEM and SOAR as part of modern SOC architecture

Implement Cisco Security Solutions to Splunk Integration using 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

Troubleshoot the Cisco Security Cloud App and Cisco Apps and TAs

PÚBLICO-ALVO

System Engineers, SOC Engineers

PRÉ-REQUISITOS

No formal prerequisites. Recommended: Cisco CCNP Security or equivalent knowledge.

CONTEÚDO PROGRAMÁTICO

Course Outline

Overview of Splunk Enterprise and Splunk Cloud
Splunk Enterprise and 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 Integrations
Cisco Security Legacy Apps and TAs
Cisco ISE Integration
Cisco NVM Integration
Cisco Security Solutions and Splunk Use Case
Troubleshoot General Splunk Issues
Troubleshoot Cisco Security Cloud App
Troubleshoot Cisco Legacy Apps and Add-ons

Lab Outline

Explore Splunk Indexes
Verify and Test Data Ingestion
Perform Search Queries
Create Dashboards and Reports
Explore Splunk SOAR
Explore Cisco XDR Incident Investigation
Cisco Secure Firewall Integration with Splunk
Cisco Duo Integration Simulation
Cisco SNA Integration Simulation
Explore Cisco ISE Integration with Splunk
Explore Cisco NVM Integration with Splunk
Investigate Ransomware Using Splunk with Cisco Security Apps
Troubleshoot Cisco Security Cloud App
Troubleshoot Cisco ISE and NVM Integration with Splunk