Skillsoft global knowledge™

ECSS - ENHANCING CISCO SECURITY SOLUTIONS WITH DATA ANALYTICS V1.0

Course Code: 860043

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.

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

What You'll Learn

After completing this course, you should 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

Who Needs to Attend

- 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

These skills can be found in the following offering:

ECSS - ENHANCING CISCO SECURITY SOLUTIONS WITH DATA ANALYTICS V1.0

Course Code: 860043

VIRTUAL CLASSROOM LIVE	$4,395 USD	5 Day

Virtual Classroom Live 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

Virtual Classroom Live Labs

- 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 and TA
- Explore the Cisco NVM Integration with Splunk Using the Legacy CESA App and TA
- Investigate 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

ECSS - ENHANCING CISCO SECURITY SOLUTIONS WITH DATA ANALYTICS V1.0

Course Code: 860043

ON-DEMAND	$900 USD

On-Demand Outline

Skills You'll Learn

- Learn how to utilize Splunk to detect, investigate, and respond to security threats effectively
- Explore key components of Splunk, including Cisco XDR, Splunk SIEM, and Splunk SOAR
- Discover how to use the Cisco Security Cloud App, Cisco Legacy Apps, and TAs for Splunk integration

Learning Objectives

1. Basics of Observability: Outline the value, functionalities, and key components (forwarder, indexer, search head, Splunk Search Processing Language (SPL), Apps and Add-Ons, Dashboards and Reports) of Splunk Enterprise and Splunk Cloud.
2. Cisco XDR, Splunk SIEM, Splunk SOAR: Explain the use of XDR, SIEM, and SOAR as part of the modern SOC architecture to enhance the SOC's ability to detect, investigate, and respond to security threats effectively. Describe the functionality and use case of Cisco XDR, Splunk SIEM, and Splunk SOAR.
3. Cisco Security Cloud App: Implement Cisco security solutions to Splunk integration using the Cisco Security Cloud App.
4. Cisco Security Legacy Apps and Technology Add-Ons: Implement Cisco Security Solutions to Splunk Integration using Cisco Legacy Apps and TAs.
5. Cisco Security with Splunk Use Cases: Demonstrate the value of integrating Cisco security solutions with Splunk for enhancing user, cloud, and breach protections.
6. Cisco Apps Troubleshooting and Tuning: Troubleshoot the Cisco Security Cloud App and the Cisco Legacy Apps and TAs.

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 4/2/2026 10:07:37 AM