Enhancing Cisco Security Solutions with Splunk (ECSS)

ID ECSS   **Price** on request   **Duration** 5 days

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

Who should 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 Cisco Learning Offering:

- [Implementing and Operating Cisco Security Core Technologies (SCOR)](#)

Course Objectives

- 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

About Fast Lane

Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

Fast Lane Services
✓ High End Technology Training
✓ Business & Soft Skill Training
✓ Consulting Services
✓ Managed Training Services
✓ Digital Learning Solutions
✓ Content Development
✓ Remote Labs
✓ Talent Programs
✓ Event Management Services

Training Methods
✓ Classroom Training
✓ Instructor-Led Online Training
✓ FLEX Classroom – Classroom & Online Hybrid
✓ Onsite & Customized Training
✓ E-Learning
✓ Blended & Hybrid Learning
✓ Mobile Learning

Technologies & Solutions
✓ Digital Transformation
✓ Artificial Intelligence
✓ Cloud
✓ Networking
✓ Cyber Security
✓ Wireless & Mobility
✓ Modern Workplace
✓ Data Center
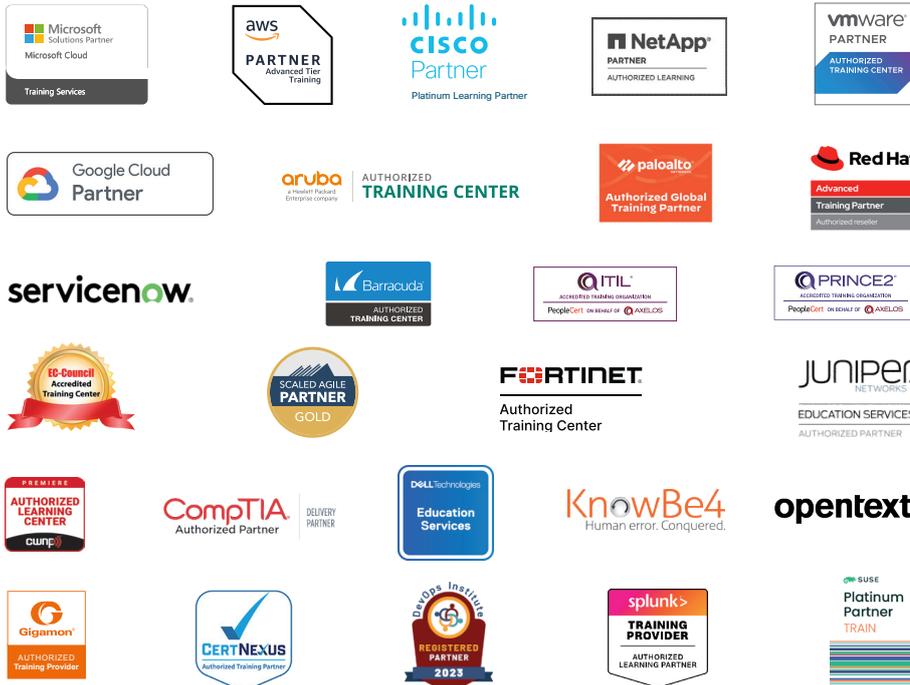
Worldwide Presence
with high-end training centers around the globe

Multiple Awards
from vendors such as AWS, Microsoft, Cisco, Google, NetApp, VMware

Experienced SMEs
with over 19.000 combined certifications