Enhancing Cisco Security Solutions with Splunk

Duration: 5 Days **Course Code: C-ECSS** **Version: 1.0** **Delivery Method: Company Event**

Overview:

The **Enhancing Cisco Security Solutions with Splunk (ECSS)** course 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 is worth 32 Continuing Education (CE) credits towards recertification.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

System and SOC Engineers needing to integrate Cisco Security Solutions with Splunk.

Objectives:

- **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

Prerequisites:

Attendees should meet the following pre-requisites:

- **Cisco CCNP Security or equivalent knowledge**
- SCOR - Implementing and Operating Cisco Security Core Technologies

Testing and Certification

Recommended as preparation for the following exam:

- There is no exam aligned to this course.

Content:

Overview of Splunk Enterprise and Splunk Cloud

- AI-Powered Data-Driven Analysis
- Reflective Case Study: Optimizing IT and Security Operations
- Splunk Enterprise Platform Overview
- Splunk Cloud Platform Overview
- Splunk Security and Observability Products
- Common Use Cases for Splunk
- Reflective Case Study Debrief: Optimizing IT and Security Operations

Splunk Enterprise and Splunk Cloud Components

- Indexer
- Forwarder
- Search head
- Splunk Enterprise Deployments
- Reflective Case Study: Designing a Distributed Splunk Environment
- Apps and Technology Add-Ons
- Splunk RBAC
- Splunk Web and CLI
- Reflective Case Study Debrief: Designing a Distributed Splunk Environment

Splunk Enterprise Data Ingestion

- Basic Methods to Ingest Data
- Advanced Methods to Ingest Data
- Reflective Case Study: Optimizing Data Ingestion
- Verification Methods for Data Ingestion
- Reflective Case Study Debrief: Optimizing Data Ingestion

Splunk Search Programming Language

- Search Fields
- Search Processing Language
- Search Processing Language 2
- App Dashboard Panel Drill Down

Splunk Dashboards and Reports

- Create, Edit and Schedule Reports
- Create and Edit Dashboards

XDR, SIEM, and SOAR Platforms

- Evolution of SIEM, SOAR, XDR
- Introduction to SIEM
- Introduction to SOAR
- Introduction to XDR
- Advanced Security Operations with SIEM, SOAR and XDR

Cisco XDR, Splunk SIEM, and Splunk SOAR

- Splunk SIEM
- Reflective Case Study: Using Splunk SIEM

Cisco Security Cloud App

- Cisco Security Cloud App Overview
- Cisco Security Cloud App Installation
- Cisco Security Cloud App User Roles and Permissions
- Cisco Security Cloud App Setup Overview
- Cisco Security Cloud App Dashboards
- Scaling from a Standalone Splunk Instance to a Distributed Deployment

Cisco Secure Firewall Integration

- Cisco Secure Firewall Management Center eStreamer
- Secure Firewall Integration
- Cisco Secure Firewall Management Center Configurations
- Cisco Secure Firewall Integration Verification

Cisco XDR Integration

- Cisco XDR API Client Configuration
- Cisco XDR Application in Cisco Security Cloud Configurations
- Cisco XDR Integration Verifications
- Cisco XDR and Splunk Cloud Integration

Cisco Secure Malware Analytics, Duo, Secure Network Analytics, Email Threat Defense, and Multicloud Defense Integrations

- Cisco Duo Integration
- Cisco Secure Malware Analytics Integration
- Cisco Secure Network Analytics Integration
- Cisco Secure Email Threat Defense Integration
- Cisco Multicloud Defense Integration

Cisco Security Legacy Apps and Technology Add-Ons

- Cisco Security Legacy Apps and Add-Ons
- Cisco Security Legacy Apps Transitioning to Cisco Security Cloud App

Cisco ISE Integration

- Cisco ISE App
- Cisco ISE Add-On
- Cisco ISE and ISE App Configuration
- Cisco ISE and ISE App Verification
- Cisco ISE Dashboards Use case
- Cisco Enterprise Networking for Splunk Platform App

Cisco NVM Integration

Cisco Security Solutions and Splunk Use Case

- Cisco Security Suites
- Cisco Security Cloud App Use Case

Cisco XDR and Splunk Use Case

- Cisco XDR and Splunk
- Blind Eagle Use Case

Troubleshoot General Splunk Issues

- Monitor Resource Usage and Verify Configuration
- Troubleshoot Index or Issues
- Troubleshoot Forwarder Issues
- Troubleshoot Search Head Issues
- Splunk Enterprise Log Files

Troubleshoot Cisco Security Cloud App

- Upgrade or Reinstall the Cisco Security Cloud App
- Common Setup and Integration Issues and Solutions
- Splunk Enterprise Log Files Related to Cisco Security Cloud App
- Cisco Security Cloud App Data Integrity and Resource Utilization Dashboards

Troubleshoot Cisco Legacy Apps and Add-ons

- Upgrade or Reinstall Cisco Legacy Apps and Add-ons
- Common Setup Issues and Solutions
- Splunk Enterprise Log Files Related to Cisco Legacy Apps and Add-ons
- Dashboards in the Legacy Apps

Labs:

- Discovery Lab 1: Explore Splunk Indexes
- Discovery Lab 2: Explore Splunk Web and CLI
- Discovery Lab 3: Verify and Test Data Ingestion
- Discovery Lab 4: Malware Events Analysis Using Splunk Enterprise Simulation
- Discovery Lab 5: Perform Search Queries
- Discovery Lab 6: Create Dashboards and Reports
- Discovery Lab 7: Explore Splunk SOAR
- Discovery Lab 8: Explore Cisco XDR Incident Investigation
- Discovery Lab 9: Cisco Secure Firewall Integration with Splunk
- Discovery Lab 10: Cisco XDR to Splunk Enterprise Integration Simulation
- Discovery Lab 11: Cisco Duo Integration Simulation
- Discovery Lab 12: Cisco SMA Integration

in a SOC
- Splunk SOAR
- Cisco XDR
- Reflective Case Study Debrief: Using Splunk SIEM in a SOC

- CESA and NVM App
- CESA and NVM Add-On
- CESA and NVM App Configuration
- CESA and NVM App Verification
- CESA and NVM Dashboards Use Case

Simulation
- Discovery Lab 13: Cisco SNA Integration Simulation
- Discovery Lab 14: Explore the Cisco ISE Integration with Splunk Using the Legacy ISE App and TA
- Discovery Lab 15: Explore the Cisco NVM Integration with Splunk Using the Legacy CESA App and TA
- Discovery Lab 16: Investigate Ransomware Using Splunk Enterprise with the Various Cisco Security Apps
- Discovery Lab 17: Troubleshoot Cisco Security Cloud App with Cisco Secure Firewall Integration
- Discovery Lab 18: Troubleshooting Cisco ISE Integration with Splunk
- Discovery Lab 19: Troubleshooting Cisco NVM Integration with Splunk

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo