

Die Schulung **Enhancing Cisco Security Solutions with Data Analytics (ECSS)** vermittelt Kenntnisse auf mittlerem Niveau über Splunk, einschließlich seiner Grundlagen, Schlüsselkomponenten und Architektur, damit Sie Sicherheitsbedrohungen effektiv erkennen, untersuchen und auf sie reagieren können. Sie lernen, verschiedene Splunk-Komponenten zu nutzen, darunter Cisco XDR, Splunk SIEM und Splunk SOAR. Darüber hinaus erfahren Sie, wie Sie die Cisco Security Cloud App, Cisco Legacy Apps und Technologie-Add-Ons (TAs) zur Integration von Cisco Sicherheitslösungen mit Splunk nutzen und beheben können, um den Schutz von Benutzern, der Cloud und von Sicherheitsverletzungen zu verbessern.

Kursinhalt

- Erläutern Sie die Grundlagen von Splunk Enterprise/Cloud
- Erläutern Sie die Verwendung von XDR, SIEM, SOAR als Teil der modernen SOC-Architektur, um die Fähigkeit des SOC zu verbessern, Sicherheitsbedrohungen effektiv zu erkennen, zu untersuchen und darauf zu reagieren
- Implementieren Sie die Integration von Cisco-Sicherheitslösungen mit Splunk unter Verwendung der Cisco Security Cloud App
- Implementieren Sie die Integration von Cisco-Sicherheitslösungen mit Splunk unter Verwendung von Cisco Legacy Apps und TAs
- Veranschaulichen Sie den Wert der Integration von Cisco-Sicherheitslösungen mit Splunk anhand von realen Anwendungsfällen
- Beheben Sie Probleme mit der Cisco Security Cloud App und den Cisco Apps und TAs

E-Book Sie erhalten die englischen Original-Unterlagen als Cisco E-Book.

Zielgruppe

- System Engineers
- SOC Engineers
- Network Architects

Voraussetzungen

Für diese Schulung gibt es keine Voraussetzungen. Es wird jedoch empfohlen, dass Sie über folgende Kenntnisse und Fähigkeiten verfügen, bevor Sie an dieser Schulung teilnehmen:

Cisco CCNP Security oder gleichwertige Kenntnisse. Diese Fähigkeiten finden Sie in den folgenden Cisco-Lernangeboten:

SCOR - Implementieren und Betreiben von Cisco Security Core Technologies

Kursziel

Diese Schulung wird Ihnen helfen:

Daten von allen Cisco-Sicherheitsprodukten in einer einzigen Splunk-Instanz zusammenzufassen, um einen zentralen Überblick zu erhalten. Ihre Sicherheitsumgebung in Echtzeit zu überwachen, um Bedrohungen schneller zu erkennen und darauf zu reagieren. Sicherheits-Workflows zu rationalisieren, indem Sie den Wechsel zwischen Dashboards und die manuelle Datenkorrelation reduzieren. Die Entscheidungsfindung mit anpassbaren Dashboards und umfassenden, genauen Einblicken zu verbessern. Ihr Unternehmen effektiver zu schützen, indem Sie Cisco-Sicherheitslösungen mit Splunk integrieren, um Bedrohungen einheitlich zu erkennen und darauf zu reagieren.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/ECSS

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in der Schweiz	5 Tage
Online Training	5 Tage
Termine auf Anfrage	



Inhaltsverzeichnis

ECSS – Enhancing Cisco Security Solutions with Data Analytics

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

Troubleshooting Cisco ISE Integration with Splunk
Troubleshooting Cisco NVM Integration with Splunk

Lab Outline

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

