

Course : Enhancing Cisco Security Solutions with Splunk (ECSS)

Optimizing Cisco Security Solutions Through Data Analytics

Practical course - 5d - 35h00 - Ref. CI1

Price : 4280 € E.T.

NEW

In this training course, you will learn the fundamentals and advanced features of Splunk for detecting, analyzing, and responding to security threats. You will learn how to integrate Cisco security solutions with Splunk to enhance protection for users, cloud environments, and infrastructure.



INFORMATION

For all registrations for open-enrollment or in-house training, each participant must have a Cisco Learning Space account associated with the email address used when registering for the training. This mandatory step provides access to the official Cisco training materials.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Explain the basics of Splunk Enterprise and Splunk Cloud
- ✓ Understanding the Role of Cisco XDR, Splunk SIEM, and Splunk SOAR in a Modern SOC
- ✓ Implement the integration of Cisco security solutions with Splunk using the Cisco Security Cloud App
- ✓ Implement the integration of Cisco security solutions with Splunk using Cisco Legacy applications and Technology Add-ons (TA)
- ✓ Illustrate the benefits of integrating Cisco security solutions with Splunk through real-world use cases
- ✓ Troubleshooting the Cisco Security Cloud App, as well as Cisco applications and Technology Add-ons (TA)

Intended audience

Systems engineers, SOC engineers.

PARTICIPANTS

Systems engineers, SOC engineers.

PREREQUISITES

Possess a level of knowledge equivalent to the Cisco CCNP Security certification (SCOR training, ref. PZL). Good written English skills.

TRAINER QUALIFICATIONS

The experts who lead the training courses are specialists in the subjects covered. They are approved by the publisher and certified for the course. They have also been validated by our teaching teams in terms of both professional knowledge and teaching skills for each course they teach. They have at least three to ten years of experience in their field and hold or have held positions of responsibility in companies.

ASSESSMENT TERMS

Assessment of targeted skills prior to training.

Assessment by the participant, at the end of the training course, of the skills acquired during the training course.

Validation by the trainer of the participant's learning outcomes, specifying the tools used: multiple-choice questions, role-playing exercises, etc.

At the end of each training course, ITTCERT provides participants with a course evaluation questionnaire, which is then analysed by our teaching teams. Participants also complete an official evaluation of the publisher.

An attendance sheet for each half-day of attendance is provided at the end of the training course, along with a certificate of completion if the participant has attended the entire session.

TEACHING AIDS AND TECHNICAL RESOURCES

The teaching resources used are the publisher's official materials and practical exercises.

Prerequisites

Possess a level of knowledge equivalent to the Cisco CCNP Security certification (SCOR training, ref. PZL). Good written English skills.

Course schedule

1 Official Program

- An Introduction to Splunk Enterprise and Splunk Cloud.
- Components of Splunk Enterprise and Splunk Cloud.
- Data collection and ingestion in Splunk Enterprise.
- Splunk Query Language (SPL).
- Creating dashboards and reports with Splunk.
- Overview of XDR, SIEM, and SOAR platforms.
- Cisco XDR, Splunk SIEM, and Splunk SOAR.
- Integration of Cisco XDR, Splunk SIEM, and Splunk SOAR within a SOC.
- Introduction to the Cisco Security Cloud App.
- Integration of Cisco Secure Firewall with Splunk.
- Integration of Cisco XDR with Splunk.
- Integration with Cisco Secure Malware Analytics, Cisco Duo, Cisco Secure Network Analytics, and Cisco.
- Email Threat Defense and Cisco Multicloud Defense.
- Overview of Cisco Security Legacy Apps and Technology Add-ons (TAS)
- Integration with Cisco Identity Services Engine (ISE)..
- Integration of the Cisco Network Visibility Module (NVM).
- Use Cases for Cisco Security Solutions with Splunk.
- Use Cases for Cisco XDR with Splunk.
- Troubleshooting Common Splunk Issues.
- Troubleshooting the Cisco Security Cloud App.
- Troubleshooting Cisco Legacy Apps and Technology Add-ons.

2 Official Lab Sessions

- Exploring Splunk indices.
- Introduction to Splunk Web and the Command-Line Interface (CLI).
- Verification and testing of data ingestion.
- Analysis of Malware Events Using Splunk Enterprise (Simulation).
- Running search queries with Splunk.
- Creating dashboards and reports.
- An Introduction to Splunk SOAR.
- Exploring Incident Investigation with Cisco XDR.
- Integration of Cisco Secure Firewall with Splunk.
- Simulation of the integration of Cisco XDR with Splunk Enterprise.
- Simulation of the Cisco Duo integration.
- Simulation of the integration of Cisco Secure Malware Analytics (SMA).
- Simulation of the integration of Cisco Secure Network Analytics (SNA).
- Exploring the integration of Cisco ISE with Splunk using the Legacy ISE application and the Technology Add-on.
- Exploring the integration of Cisco NVM with Splunk using the Legacy CESA application and the Technology Add-on.
- Investigating a ransomware attack using Splunk Enterprise and various Cisco Security applications.
- Troubleshooting the Cisco Security Cloud App with Cisco Secure Firewall integration.
- Troubleshooting the integration of Cisco ISE with Splunk.
- Troubleshooting the integration of Cisco NVM with Splunk.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training course.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you have specific accessibility requirements? Contact Ms FOSSE, disability advisor, at the following address: psh-accueil@orsys.fr so that we can assess your request and its feasibility.

This programme is an original creation, developed by the teaching teams at ORSYS Formation. Any reproduction, representation, adaptation or use, in whole or in part, without the prior written authorisation of ORSYS, is strictly prohibited. ORSYS reserves the right to take any action necessary to protect its intellectual property rights.

Dates and locations

REMOTE CLASS

2026 : 30 Nov.

2027 : 8 Mar., 14 June, 6 Sep., 29 Nov.