Course : Securing Email with Cisco Email Security Appliance (SESA) v3.2

Official course, exam preparation 300-720 SESA

Practical course - 4d - 28h00 - Ref. LQN
Price : 3640 € E.T.

With this training course, you deploy and use Cisco Email Security Appliance to protect your e-mails against phishing, ransomware and compromise. You'll learn how to manage security policies and implement the main functions: anti-spam, anti-virus, threat filtering, encryption, quarantines and data loss prevention. You will develop your skills in deploying, troubleshooting and administering the solution.

Teaching objectives

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

- Describe, administer and configure the Cisco Email Security Appliance (ESA)
- Control sender and recipient domains
- Fighting e-mail threats with Talos SenderBase
- Apply email security policies
- Prevent data loss (DLP) and secure data exchanges
- Authenticate users and e-mails
- Manage message delivery and quarantines
- Centralized management using clusters
- Test, diagnose and troubleshoot messaging flows

Intended audience

Network and security engineers, administrators, architects and technicians, as well as Cisco integrators, partners, system designers and IT managers.

Prerequisites

Solid grounding in cybersecurity, network protocols (DNS, SSH, FTP...) and Cisco, CompTIA, (ISC)² certification or equivalent experience.

PARTICIPANTS

Network and security engineers, administrators, architects and technicians, as well as Cisco integrators, partners, system designers and IT managers.

PREREQUISITES

Solid grounding in cybersecurity, network protocols (DNS, SSH, FTP...) and Cisco, CompTIA, (ISC)² certification or equivalent experience.

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.

Practical details

Teaching methods

Training in French. Official course material in English.

Course schedule

1 Official program

- Introducing the Cisco Email Security Appliance.
- Control of sender and recipient domains.
- Fighting spam with Talos SenderBase and anti-spam.
- Use of antivirus and epidemic filters.
- Use of messaging policies.
- Using content filters.
- Using message filters.
- Data loss prevention.
- Using LDAP.
- Overview of SMTP session authentication.
- Using e-mail authentication
- Using e-mail encryption.
- Cisco Email Security Appliance administration.
- Use of quarantines and delivery methods.
- Centralized management with clusters.
- Testing and troubleshooting.

2 Official practical work

- Check and test Cisco ESA configuration.
- Advanced detection of malware in attachments (macros).
- Protection against malicious or unwanted URLs hidden behind shortened URLs.
- Protection against malicious or unwanted URLs in attachments.
- Intelligent management of non-analyzable messages.
- Leverage AMP cloud intelligence via pre-classification enhancement.
- Integrate Cisco ESA with the AMP console.
- Prevent threats with antivirus protection.
- Application of epidemic filters.
- Configure attachment analysis.
- Configure output data loss prevention.
- Integrate Cisco ESA with LDAP and activate the LDAP acceptance request.
- Domain Keys Identified Mail (DKIM).
- Sender Policy Framework (SPF).
- Detection of forged e-mails.
- Perform basic administration.
- Configure Cisco Secure Email and Web Manager for tracking and reporting.

Options

Certification : 320 € HT

To obtain Cisco Certified Network Professional Security (CCNP Security) certification, you need to pass exam 350-701 SCOR and one of the following exams (your choice): 300-710 SNCF, 300-715 SISE, 300-720 SESA, 300-725 SWSA, 300-730 SVPN, 300-740 SCAZT or 300-745 SDSI.
Comment passer votre examen ?

The certification option comes in the form of a voucher or invitation that will allow you to take the exam at the end of the training course.

TEACHING AIDS AND TECHNICAL RESOURCES

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

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.

Dates and locations

REMOTE CLASS
2026 : 23 June, 8 Dec.

PARIS LA DÉFENSE
2026 : 23 June, 8 Dec.