Implementing and Operating Cisco Security Core Technologies (SCOR) v2.0

Official course, exam preparation 350-701 SCOR

Hands-on course of 5 days - 35h
Ref.: PZL - Price 2026: CHF4 350 (excl. taxes)

Cette formation, combinant 5 jours en classe et 3 jours d'auto-apprentissage, vous apporte les compétences essentielles pour déployer efficacement les solutions de sécurité Cisco. Vous apprendrez à mettre en œuvre des mécanismes de protection avancés contre les cybermenaces et à améliorer la posture de sécurité des infrastructures réseau. Ce parcours constitue une étape stratégique pour accéder à des fonctions techniques de niveau avancé dans le domaine de la cybersécurité.

EDUCATIONAL OBJECTIVES

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

Describe key network security concepts and TCP/IP protocol vulnerabilities

Identify attacks on network applications and client workstations

Explain the role of Cisco technologies in countering threats (firewall, IPS, antivirus, etc.).

Configuring security policies on Cisco Secure Firewall ASA and Threat Defense

Deploying e-mail protection with Cisco Secure Email Gateway

Implement web security with Cisco Secure Web Appliance

Explain cloud security solutions with Cisco Umbrella and Secure Cloud Analytics

Deploy site-to-site and remote access IPsec VPNs (ASA, IOS, Threat Defense)

Implement secure network access (802.1X, Cisco Secure Network Access)

Understand infrastructure security, telemetry, and data and management plan controls

TEACHING METHODS

Training in French. Official course material in English. Training duration: 5 days in class and 3 days self-study.

CERTIFICATION

To obtain Cisco Certified Network Professional Security (CCNP Security) certification, you need to pass exam 350-701 SCOR, as well as 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.

PARTICIPANTS

Network and security engineers and administrators, technical architects, Cisco integrators, project managers and IT managers.

PREREQUISITES

Aucune condition préalable n'est requise, mais une connaissance de base en réseau, en sécurité, en Cisco IOS et en Windows est recommandée (niveau CCNA).

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

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

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@ORSYS.fr to review your request and its feasibility.

THE PROGRAMME

last updated: 11/2025

1) Official program

- Cybersecurity fundamentals.
- Network and perimeter security technologies.
- Cisco Secure Firewall (ASA and Threat Defense).
- E-mail security.
- Web security.
- Cisco VPN technologies.
- Workstation safety.

- Network access control and authentication.
- Supervision, telemetry and analytics.
- Cloud security and SDN environments.

2) Official practical work

- Risk analysis and simulation of network attacks.
- Cisco firewall implementation and traffic inspection.
- Deploying a Cisco secure e-mail gateway.
- Deploying Cisco Secure Web Appliance.
- Site-to-site VPN and remote access deployment with Cisco solutions.
- Protect and monitor workstations with Cisco Secure Endpoint.
- Implementing network access control with 802.1X.
- Application of best practices for securing network equipment.
- Traffic analysis and threat detection via Cisco Secure Network Analytics.
- Implementing Cisco cloud security solutions.

DATES

Contact us