ITTcert
BY ORSYS

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

Official course, exam preparation 350-701 SCOR

Practical course - 5d - 35h00 - Ref. PZL
Price : 4350 € E.T.

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.

Teaching objectives

At the end of the training, the participant 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

Intended audience

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).

Practical details

Teaching methods

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

Course schedule

(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.

Options

Certification : 420 € HT

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.

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.

Dates and locations

REMOTE CLASS
2026 : 23 Mar., 15 June, 30 Nov.