Date de publication : 01/08/2025

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

Cours officiel, préparation à l'examen 350-701 SCOR

Formation pratique - 5j - 35h00 - Réf. PZL
Prix : 4350 € H.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.

INFORMATIONS

Pour toute inscription en inter ou en intra-entreprise, chaque participant doit disposer d'un compte Cisco Learning Space associé à l'adresse e-mail utilisée lors de son inscription à la formation. Cette démarche obligatoire permet d'accéder au support de formation officiel Cisco.

PARTICIPANTS

Ingénieurs et administrateurs réseaux et sécurité, architectes techniques, intégrateurs Cisco, chefs de projet et responsables IT.

PRÉREQUIS

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).

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Décrire les concepts clés de la sécurité réseau et les vulnérabilités du protocole TCP/IP
- Identifier les attaques sur les applications réseau et les postes clients
- Expliquer le rôle des technologies Cisco pour contrer les menaces (pare-feu, IPS, antivirus, etc.)
- Configurer les politiques de sécurité sur Cisco Secure Firewall ASA et Threat Defense
- Déployer les protections e-mail avec Cisco Secure Email Gateway
- Mettre en œuvre la sécurité web avec Cisco Secure Web Appliance
- Expliquer les solutions de sécurité cloud avec Cisco Umbrella et Secure Cloud Analytics
- Déployer des VPN IPsec site-à-site et d'accès distant (ASA, IOS, Threat Defense)
- Mettre en œuvre l'accès réseau sécurisé (802.1X, Cisco Secure Network Access)
- Comprendre la sécurité des infrastructures, la télémétrie, et les contrôles des plans de données et de gestion

Public concerné

Ingénieurs et administrateurs réseaux et sécurité, architectes techniques, intégrateurs Cisco, chefs de projet et responsables IT.

Prérequis

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).

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français. Support de cours officiel en anglais. Durée de la formation : 5 jours en classe et 3 jours d'auto-apprentissage.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

Programme de la formation

1 Programme officiel

- Fondamentaux de la cybersécurité.
- Technologies de sécurité réseau et périmétrique.
- Cisco Secure Firewall (ASA et Threat Defense).
- Sécurité des e-mails.
- Sécurité Web.
- Technologies VPN Cisco.
- Sécurité des postes de travail.
- Contrôle d'accès réseau et authentification.
- Supervision, télémétrie et analytics.
- Sécurité cloud et environnements SDN.

2 Travaux pratiques officiels

- Analyse des risques et simulation d'attaques réseau.
- Mise en œuvre de pare-feux Cisco et inspection du trafic.
- Déploiement d'une passerelle e-mail sécurisée Cisco.
- Déploiement de Cisco Secure Web Appliance.
- Déploiement de VPN site-à-site et d'accès distant avec les solutions Cisco.
- Protection et surveillance des postes avec Cisco Secure Endpoint.
- Mise en œuvre d'un contrôle d'accès réseau avec 802.1X.
- Application des bonnes pratiques de sécurisation des équipements réseau.
- Analyse du trafic et détection des menaces via Cisco Secure Network Analytics.
- Mise en œuvre des solutions de sécurité cloud Cisco.

Options

Certification : 420 € H.T.

Pour l'obtention de la certification Cisco Certified Network Professional Security (CCNP Security), la réussite de l'examen 350-701 SCOR est requise ainsi que la réussite de l'un des examens suivants (au choix) : 300-710 SNCF, 300-715 SISE, 300-720 SESA, 300-725 SWSA, 300-730 SVPN, 300-740 SCAZT ou 300-745 SDSI.

Comment passer votre examen ?

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.

Ce programme est une création originale, conçu par les équipes pédagogiques d'ORSYS Formation. Toute reproduction, représentation, adaptation ou exploitation, totale ou partielle, sans autorisation préalable écrite d'ORSYS, est strictement interdite. ORSYS se réserve le droit d'engager toute action nécessaire à la protection de ses droits de propriété intellectuelle.

Dates et lieux

CLASSE À DISTANCE
2026 : 30 nov.

2027 : 27 sep., 27 sep.