

Certifiante Sessions garanties disponibles

Formation Mise en œuvre et exploitation des technologies de base de la sécurité Cisco (SCOR)

Réf. SF34589

Développez une expertise complète sur les technologies de sécurité Cisco et préparez-vous à protéger les infrastructures d'entreprise contre les cybermenaces les plus avancées.

5 j
Durée

4 000 € HT
Inter / participant

3
Sessions à venir

Objectifs pédagogiques

- ✓ Déployer et administrer Cisco Secure Firewall ASA et Threat Defense avec ses politiques IPS, anti-malware et de filtrage de fichiers
- ✓ Configurer les passerelles Cisco Secure Email Gateway et les dispositifs de sécurité web Cisco Secure Web Appliance
- ✓ Implémenter les solutions de protection des terminaux avec Cisco Umbrella et Cisco Secure Endpoint
- ✓ Mettre en place les mécanismes de contrôle d'accès réseau via 802.1X et les solutions Cisco Secure Network Access
- ✓ Concevoir et déployer des architectures VPN sécurisées (site à site IPsec et accès distant SSL) sur les différentes plateformes Cisco
- ✓ Renforcer la protection de l'infrastructure réseau à travers les plans de contrôle, de données et de gestion
- ✓ Exploiter la télémétrie réseau, la sécurité cloud et les outils d'analyse Cisco Secure Network Analytics et Cloud Analytics
- ✓ Se préparer efficacement à l'obtention de la certification Cisco Certified Specialist - Security Core (examen 350-701)

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux, Architectes, Responsables de la sécurité des systèmes d'information (RSSI)

Prérequis Bases en Ethernet et TCP/IP, maîtrise de l'environnement Windows, notions de Cisco IOS et des fondamentaux de la sécurité réseau. La certification CCNA constitue un atout recommandé.

Programme détaillé

Fondamentaux de la sécurité de l'information

- Concepts et stratégies de sécurité : cadre de protection des données au sein des infrastructures réseau
- Vulnérabilités TCP/IP : analyse des failles protocolaires et des vecteurs d'attaque ciblant les hôtes et réseaux
- Menaces applicatives : identification des attaques courantes visant les applications réseau
- Synergie des technologies de sécurité : interaction et complémentarité des différentes couches de défense

Cisco Secure Firewall ASA — Déploiement et configuration

- Paramétrage réseau et translation d'adresses : mise en place du NAT sur Cisco Secure Firewall ASA
- Politiques de contrôle d'accès : création et gestion des règles de filtrage du trafic

Activités pratiques :

Configuration des paramètres réseau et NAT, déploiement de politiques de contrôle d'accès sur ASA

Cisco Secure Firewall Threat Defense — Fondamentaux et protection avancée

- Configuration de base : déploiement initial et paramétrage du Threat Defense
- Translation d'adresses : mise en œuvre du NAT sur Threat Defense
- Politiques de contrôle d'accès : définition des règles de filtrage et d'autorisation
- Détection d'intrusion : activation du moteur IPS et des mécanismes de découverte réseau
- Protection anti-malware : déploiement des politiques de fichiers et de détection de logiciels malveillants

Activités pratiques :

Configuration du NAT et des politiques d'accès, activation de l'IPS et de la protection anti-malware sur Threat Defense

Sécurisation de la messagerie avec Cisco Secure Email Gateway

- Fondamentaux de la passerelle : mise en place des listeners, des tables d'accès hôte (HAT) et des tables d'accès destinataire (RAT)
- Politiques de sécurité email : configuration des règles de filtrage, anti-spam et anti-phishing

Activités pratiques :

Déploiement des listeners et paramétrage des politiques de messagerie sécurisée

Protection web avec Cisco Secure Web Appliance

- Services de proxy : paramétrage du proxy web, authentification des utilisateurs et déchiffrement HTTPS
- Contrôle d'utilisation et protection anti-malware : mise en place des politiques d'accès web et de détection de menaces

Activités pratiques :

Configuration des services proxy avec authentification et déchiffrement, déploiement du contrôle d'accès web et de la protection contre les programmes malveillants

Technologies VPN et cryptographie

- Principes fondamentaux : présentation des réseaux privés virtuels et des algorithmes de chiffrement
- VPN site à site : conception et déploiement des tunnels IPsec IKEv2 point à point avec interface VTI sur Cisco IOS
- VPN site à site sur Firewall : configuration des tunnels IPsec entre dispositifs Cisco Secure Firewall ASA et Threat Defense
- Accès distant sécurisé : déploiement de VPN SSL sur Cisco Secure Firewall ASA et Threat Defense

Activités pratiques :

Mise en place d'un tunnel IPsec IKEv2 VTI statique, configuration VPN point à point entre dispositifs Threat Defense

Protection des terminaux et sécurité DNS

- Vecteurs d'attaque ciblant les points de terminaison : analyse des techniques courantes utilisées contre les postes de travail et serveurs
- Cisco Umbrella : exploration du tableau de bord, sécurité DNS, passerelle web sécurisée, pare-feu cloud et fonctionnalités CASB
- Technologies de sécurité des terminaux : panorama des solutions de protection des endpoints
- Cisco Secure Endpoint : architecture, fonctionnalités de détection, analyse des comportements et protection anti-ransomware

Activités pratiques :

Exploration de Cisco Umbrella (DNS, passerelle web, CASB), analyse via la console Cisco Secure Endpoint, test de la protection contre les ransomwares

Contrôle d'accès réseau

- Solutions Cisco Secure Network Access : présentation de l'écosystème de contrôle d'accès
- Authentification 802.1X : principes du protocole EAP et mécanismes d'authentification réseau
- Déploiement 802.1X : configuration des équipements pour les opérations d'authentification

Activités pratiques :

Mise en œuvre de l'authentification 802.1X sur les équipements réseau

Renforcement de l'infrastructure réseau

- Protection du plan de contrôle : mise en place des défenses sur les équipements Cisco pour sécuriser le routage et la signalisation
- Sécurité du plan de données couche 2 : contrôles de sécurité au niveau commutation (Cisco IOS)
- Sécurité du plan de données couche 3 : contrôles de filtrage et de protection au niveau routage (Cisco IOS et ASA)
- Sécurité du plan de gestion : défenses pour l'accès d'administration aux équipements réseau

Télémétrie et analyse de sécurité

- Méthodes de télémétrie : collecte et exploitation des données de surveillance réseau
- Cisco Secure Network Analytics : déploiement et utilisation des outils d'analyse comportementale du trafic

Activités pratiques :

Exploration de Secure Network Analytics v7.4.2, analyse des alertes de menaces et audit cryptographique ETA

Sécurité cloud et programmabilité

- Fondamentaux du cloud computing : identification des risques et attaques spécifiques aux environnements cloud
- Sécurisation des environnements cloud : bonnes pratiques et stratégies de protection
- Cisco Secure Cloud Analytics : déploiement des outils de surveillance cloud privé et public
- Réseaux définis par logiciel : introduction à la programmabilité réseau et aux architectures SDN

Activités pratiques :

Exploration du tableau de bord Cloud Analytics, surveillance des environnements cloud privés et publics

Prochaines sessions

DATE	LIEU	STATUT
02/11/2026	à distance	Sur confirmation
18/01/2027	à distance	Sur confirmation
05/04/2027	à distance	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Infrastructures & Réseaux : 4,9/5 — 49 avis

Anthony G. — Formateur à l'écoute, et dans la compréhension sur divers sujets. Prend le temps de bien expliquer les différents thèmes abordés. Merci Fabien.

Aurélien C. — formation excellente

Ils nous font confiance

Cette année notre filière Ingénierie Réseaux & Télécoms a accompagné plus de 28 entreprises dont :

STORMSHIELD ALTEN SA AVEM CEGEDIM CEGEDIM CLOUD CHELA + CONSORT FRANCE CS GROUP CS GROUP FRANCE CTG +18 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com