

## Mettre en oeuvre et gérer les solutions de sécurité Cisco

Durée: 5 Jours    Réf de cours: SCOR    Version: 2.0

### Résumé:

Le cours Implémentation et exploitation des technologies fondamentales de sécurité de Cisco (SCOR) vous aide à vous préparer aux certifications Cisco® CCNP® Security et CCIE® Security ainsi qu'à des responsabilités de haut niveau dans le domaine de la sécurité. Dans ce cours, vous maîtriserez les compétences et les technologies dont vous avez besoin pour mettre en oeuvre les solutions de sécurité de base de Cisco afin de fournir une protection avancée contre les attaques de cybersécurité.

Vous apprendrez la sécurité pour les réseaux, le cloud et le contenu, la protection des terminaux, l'accès sécurisé au réseau, la visibilité et la mise en oeuvre. Vous obtiendrez une expérience pratique approfondie du déploiement de Cisco Secure Firewall ASA et de Cisco Secure Firewall Threat Defense, de la configuration des politiques de contrôle d'accès, des politiques de messagerie et de l'authentification 802.1X, entre autres. Vous aurez une introduction pratique aux fonctionnalités de Cisco Network Analytics et de Cisco Secure Cloud Analytics.

Veillez noter que ce cours est une combinaison de cours dispensés par un formateur et d'études en autonomie - 5 jours en salle de classe et environ 3 jours d'auto-apprentissage. Le contenu de cette autoformation sera fourni dans le cadre du matériel de cours numérique que vous recevrez au début du cours et devrait faire partie de votre préparation à l'examen.

Ce cours vaut 64 crédits de formation continue (CE).

Mis à jour 14/10/2024

### Public visé:

Ce cours est surtout destiné aux spécialistes chargés de la sécurité qui doivent savoir mettre en oeuvre et exploiter les principales technologies de sécurité, notamment la sécurité des réseaux, la sécurité du cloud, la sécurité du contenu, la protection et la détection des terminaux, l'accès sécurisé au réseau, la visibilité et l'application des règles.

### Objectifs pédagogiques:

- Après avoir suivi ce cours, vous devriez être en mesure de :
- Décrire les concepts et les stratégies de sécurité de l'information dans un réseau
- Décrire les failles de sécurité du protocole de transmission/internet (TCP/IP) et comment elles peuvent être utilisées pour attaquer les réseaux et les hôtes
- Décrire les attaques basées sur les applications réseau
- Décrire comment les différentes technologies de sécurité réseau fonctionnent ensemble pour se prémunir contre les attaques
- Mettre en oeuvre le contrôle d'accès sur Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Déployer les configurations de base de Cisco Secure Firewall Threat Defense, IPS, logiciels malveillants et stratégies d'urgence
- Déployer les configurations de base et les règles de Cisco Secure Email Gateway
- Décrire et mettre en oeuvre les caractéristiques et fonctions de base de sécurité du contenu web fournies par Cisco Secure Web Appliance
- Décrire les différentes techniques d'attaque contre les postes de travail
- Configurer les appareils pour les opérations 802.1X
- Présenter les VPN et décrire les solutions et algorithmes de cryptographie
- Décrire les solutions de connectivité sécurisée de site à site de Cisco
- Déployer des VPN IPsec point à point basés sur Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)
- Configurer les VPN IPsec point à point sur le Cisco Secure Firewall ASA et le Cisco Secure Firewall Threat Defense
- Décrire et déployer les solutions de connectivité d'accès à distance sécurisé de Cisco
- Fournir une vue d'ensemble des contrôles de protection de l'infrastructure du réseau
- Examiner diverses défenses sur les dispositifs Cisco qui protègent le dispositif de contrôle
- Configurer et vérifier les contrôles du dispositif de données (layer 2) du logiciel Cisco IOS, ainsi que les contrôles du dispositif de données (layer 3) du logiciel Cisco IOS et de Cisco ASA
- Examiner diverses défenses sur les appareils Cisco qui protègent le dispositif de gestion
- Décrire les formes de télémétrie de base recommandées pour

- Décrire les capacités de sécurité de Cisco Umbrella®, les modèles de déploiement, la gestion des politiques et la console Investigate
- Fournir une compréhension de base de la sécurité des points finaux et se familiariser avec les technologies courantes de sécurité des postes de travail
- Décrire l'architecture et les fonctions de base de Cisco Secure Endpoint
- Décrire les solutions Cisco Secure Network Access
- Décrire l'authentification 802.1X et le protocole d'authentification extensible (EAP)

l'infrastructure du réseau et les dispositifs de sécurité

- Décrire le déploiement de Cisco Secure Network Analytics
- Décrire les bases du cloud computing, les attaques courantes du cloud, comment sécuriser l'environnement du cloud
- Décrire le déploiement de Cisco Secure Cloud Analytics
- Décrire les bases des réseaux définis par logiciel et de la programmabilité des réseaux

---

## Pré-requis:

Les participants doivent posséder les prérequis suivants :

- Familiarité avec les réseaux Ethernet et TCP/IP
- Connaissance pratique du système d'exploitation Windows
- Connaissance pratique des réseaux et concepts Cisco IOS
- Familiarité avec les concepts de base de la sécurité des réseaux
- CCNA - Mettre en oeuvre et administrer des solutions réseaux Cisco

## Test et certification

Recommandé comme préparation à l'examen suivant :

350-701 - Implementing and Operating Cisco Security Core Technologies (SCOR 350-701)

Il s'agit de l'examen de base pour la certification CCNP Security de Cisco. Pour obtenir la certification CCNP Security, vous devez également réussir l'un des examens de spécialisation.

---

## Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- SAUI - Implementing Automation for Cisco Security Solutions
- SFWIPF - Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention
- SFWIPA - Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention
- SISE - Mettre en oeuvre et configurer la solution Cisco Identity Services Engine
- SVPN - Implementing Secure Solutions with Virtual Private Networks
- SESA - Sécuriser les emails avec Cisco Email Security Appliance
- SWSA - Sécuriser le Web avec Cisco Web Security Appliance

## Contenu:

### Techniques de sécurité des réseaux

- Stratégie de défense approfondie
- La défense à travers le continuum d'attaque
- Vue d'ensemble de la segmentation et de la virtualisation du réseau
- Pare-feu dynamique (Stateful Firewall)
- Présentation du Cisco IOS Zone-Based Policy Firewall (pare-feu à politique basée sur des zones)
- Aperçu des dispositifs de sécurité
- Classification des informations sur les menaces
- Sécurité contre les logiciels malveillants en réseau
- Présentation de l'IPS
- Présentation du pare-feu de nouvelle génération
- Aperçu de la sécurité du contenu des courriels
- Présentation de la sécurité du contenu Web
- Systèmes d'analyse des menaces
- Présentation de la sécurité DNS
- Présentation de l'authentification, de l'autorisation et de la comptabilisation
- Vue d'ensemble de la gestion des identités et des accès
- Aperçu de la technologie des réseaux privés virtuels (VPN)
- Aperçu des facteurs de forme des dispositifs de sécurité des réseaux

### Déploiement de Cisco Secure Firewall ASA

- Types de déploiement du Cisco Secure Firewall ASA
- Niveaux de sécurité de l'interface du Cisco Secure Firewall ASA
- Objets et groupes d'objets de Cisco Secure Firewall ASA
- Traduction d'adresses réseau
- ACL d'interface du Cisco Secure Firewall ASA
- ACL globales du Cisco Secure Firewall ASA
- Politiques avancées d'accès de Cisco Secure Firewall ASA
- Aperçu de la haute disponibilité de Cisco Secure Firewall ASA

### Principes de base de Cisco Secure Firewall Threat Defense

- Déploiements de Cisco Secure Firewall Threat Defense
- Traitements des paquets et politiques de la défense contre les menaces du pare-feu sécurisé de Cisco
- Objets de Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Threat Defense NAT
- Politiques de préfiltrage de Cisco Secure Firewall Threat Defense
- Politiques de contrôle d'accès de Cisco

Solutions d'accès réseau sécurisé de Cisco (Autoformation)

Description de l'authentification 802.1X (Autoformation)

Configurer l'authentification 802.1X (Autoformation)

Protection de l'infrastructure réseau (Autoformation)

Contrôles de sécurité du plan de contrôle (Autoformation)

Contrôles de sécurité du Plan de Données Layer 2 (Self-Study)

Contrôles de sécurité du Plan de Données Layer 3 (Self-Study)

Contrôles de sécurité du « Management Plane » ( Autoformation)

Méthodes de télémétrie du trafic (Autoformation)

Déploiement de Cisco Secure Network Analytics (Autoformation)

Cloud Computing et sécurité du Cloud (Autoformation)

Sécurité du Cloud (Autoformation)

Déploiement de Cisco Secure Cloud Analytics (Autoformation)

Réseau software defined ( Autoformation)

Labs

Exercice 1 : Configurer les paramètres réseau et NAT sur Cisco Secure Firewall ASA

Exercice 2 : Configurer les politiques de contrôle d'accès de Cisco Secure Firewall

Exercice 6 : Configurer la politique de protection contre les malwares et les fichiers de Cisco Secure Firewall Threat Defense

Exercice 7 : Configurer Listener, HAT, et RAT sur Cisco Secure Email Gateway

Exercice 8 : Configurer les politiques de Cisco Secure Email

Exercice 9 : Configurer les services proxy, l'authentification et le décodage HTTPS

Exercice 10 : Appliquer le contrôle d'utilisation acceptable et la protection contre les logiciels malveillants

Exercice 11 : Configurer un tunnel VTI statique IPsec IKEv2 point à point

Exercice 12 : Configurer un VPN point à point entre les dispositifs de défense contre les menaces de Cisco Secure Firewall

Exercice 13 : Configurer le VPN d'accès à distance sur le Cisco Secure Firewall Threat Defense

Exercice 14 : Examiner le tableau de bord de Cisco Umbrella et la sécurité DNS

Exercice 15 : Explorer Cisco Umbrella Secure Web Gateway et Cloud-Delivered Firewall

Exercice 16 : Explorer les fonctionnalités de Cisco Umbrella CASB

Exercice 17 : Explorer Cisco Secure Endpoint

Exercice 18 : Effectuer une analyse du terminal à l'aide de la console Cisco Secure Endpoint

Exercice 19 : Découvrez la protection contre les ransomwares par Cisco Secure Endpoint

Exercice 20 : Découvrir Secure Network Analytics v7.4.2



- Cartes cryptographiques statiques IPsec
- Interface de tunnel virtuel statique IPsec
- VPN multipoint dynamique
- Cisco IOS FlexVPN

VPN IPsec point à point basés sur le VTI de Cisco IOS

- VTIs Cisco IOS
- Configuration VPN VTI statique point à point IPsec IKEv2

VPN point à point IPsec dans Cisco Secure Firewall ASA et Cisco Secure Firewall Threat Defense

- VPN point à point dans Cisco Secure Firewall ASA et Cisco Secure Firewall Threat Defense
- Configuration VPN point à point dans Cisco Secure Firewall ASA
- Configuration VPN point à point dans Cisco Secure Firewall Threat Defense

Solutions VPN d'accès à distance sécurisé de Cisco

- Composants d'accès à distance VPN
- Technologies d'accès à distance VPN
- Vue d'ensemble de SSL

Accès à distance aux VPN SSL sur Cisco Secure Firewall ASA et Cisco Secure Firewall Threat Defense

- Concepts de configuration de l'accès à distance
- Profils de connexion
- Stratégies de groupes
- Configuration du VPN d'accès à distance Cisco Secure Firewall ASA
- Configuration du VPN d'accès à distance Cisco Secure Firewall Threat Defense

Description des concepts de sécurité de l'information (autoformation)

- Vue d'ensemble de la sécurité informatique
- Actifs, vulnérabilités et contre-mesures
- Gestion des risques
- Évaluation des vulnérabilités
- Comprendre CVSS

Décrire les attaques courantes contre le protocole TCP/IP (auto-apprentissage)

- Vulnérabilités de l'ancien TCP/IP
- Vulnérabilités IP
- Vulnérabilités ICMP
- Vulnérabilités UDP
- Surface d'attaque et vecteurs d'attaque
- Attaques de reconnaissance
- Attaques d'accès
- Attaques de l'homme du milieu
- Attaques par déni de service et par déni de

<ul style="list-style-type: none"> <li>service distribué</li> <li>■ Attaques par réverbération et amplification</li> <li>■ Attaques d'usurpation d'identité</li> <li>■ Attaques DHCP</li> </ul>	
Décrire les attaques fréquentes d'applications réseau (Self-Study)	
Attaques courantes des terminaux (Self-Study)	
Déploiement de Cisco Umbrella (Autoformation)	
Technologies de sécurité des postes de travail (Autoformation)	
Cisco Secure Endpoint (Autoformation)	

## Méthodes pédagogiques :

Un support de cours officiel sera fourni aux participants.

## Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

### Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via [moncompteformation.gouv.fr](http://moncompteformation.gouv.fr).

### Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur [globalknowledge.fr/handicap](http://globalknowledge.fr/handicap)
- Le Règlement intérieur est disponible sur [globalknowledge.fr/reglement](http://globalknowledge.fr/reglement)