Mise en œuvre et exploitation des technologies Cisco Security Core (SCOR 350-701)

Date et durée

Code formation : SCOR
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec préparation à la certification

CCNP Security®

Description

Cette formation Cisco SCOR est une **préparation aux certifications Cisco® CCNP Security et CCIE Security**. Son objectif est de vous permettre aussi d'accéder à des responsabilités de haut niveau dans le domaine de la sécurité informatique. En effet, vous développerez des compétences et maitriserez les technologies Cisco nécessaires à la **mise en œuvre de systèmes de sécurité** offrant un niveau de protection supérieur contre les cyberattaques.
Ainsi, le programme aborde la sécurité des réseaux, du cloud et du contenu, la protection des terminaux, l'accès sécurisé au réseau, la visibilité et les processus opérationnels. Des travaux pratiques, tels que le **déploiement du pare-feu Cisco Firepower®** et de Cisco Adaptive Security Appliance (ASA), la configuration des politiques de contrôle d'accès, des politiques de messagerie et de l'authentification 802.1X, et bien d'autres choses encore vous attendent. Pour finir, vous découvrirez les fonctionnalités de **détection des menaces de Cisco Stealthwatch®** Enterprise et de Cisco Stealthwatch Cloud.
Grâce à cette formation de 5 jours qui inclus des supports pédagogiques, vous pourrez vous préparer à l'examen Implementing and Operating Cisco Security Core Technologies (350-701 SCOR). Cet examen permet d'obtenir la certification **Cisco Certified Specialist - Security Core**, ainsi que les prérequis pour les certifications CCNP Security et CCIE Security.

Objectifs

En suivant la **formation Cisco Security SCOR**, vous validerez les objectifs de compétence suivants :

- comprendre et décrire les principes et les stratégies de sécurité de l'information sur un réseau ;
- Identifier les principales attaques du protocole TCP/IP, des applications réseau et des terminaux ;
- expliquer comment les technologies de sécurité des réseaux fonctionnent pour se protéger contre des attaques ;
- mettre en œuvre le contrôle d'accès sur les dispositifs de sécurité Cisco ASA et le pare-feu Cisco Firepower ;
- découvrir et mettre en œuvre les fonctionnalités de base de Cisco Email Security Appliance et de Cisco Web Security Appliance ;
- connaître les fonctions de sécurité de Cisco Umbrella®, les modèles de déploiement, la gestion des politiques et la console Investigate ;
- décrire ce qu'est un réseau privé virtuel (VPN) et présenter les solutions et algorithmes de cryptage ;
- présenter les solutions site à site de connectivité sécurisée de Cisco et décrire les processus de déploiement pour les VPN IPsec point à point basés sur l'interface système Cisco IOS® ainsi que pour Cisco ASA et le

pare-feu Cisco Firepower ;
- connaître et déployer les solutions de connectivité d'accès à distance sécurisé de Cisco, ainsi que la procédure de configuration de l'authentification 802.1X et du protocole EAP ;
- comprendre les bases de la sécurité des terminaux en décrivant l'architecture et les fonctionnalités de base de la protection avancée contre les logiciels malveillants (AMP) pour les terminaux ;
- analyser différentes mesures de protection sur les équipements Cisco pour protéger le plan de contrôle et de gestion ;
- configurer et tester les contrôles du plan de données des couches 2 et 3 de Cisco IOS® ;
- découvrir et expliquer le fonctionnement de Cisco Stealthwatch Enterprise et Stealthwatch Cloud ;
- expliquer les principes de base du cloud, connaître les menaces les plus courantes et savoir sécuriser ce type d'environnement à l'aide des solutions Cisco ;
- être bien préparé à l'examen Cisco 350-701 SCOR afin d'obtenir la certification Cisco Certified Specialist - Security Core et les prérequis pour les certifications Cisco CCNP Security et CCIE Security.

Points forts

Un formateur expert et certifié Cisco, des support de cours officiel avec des labs et une préparation à l'examen Cisco SCOR 350-701.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre la **formation Cisco Security SCOR** nécessite les prérequis suivants :

- une solide connaissance du fonctionnement des réseaux Ethernet et TCP/IP, ainsi que des bases en sécurité réseau ;
- savoir utiliser les systèmes d'exploitation Windows et Cisco IOS.

*Pour obtenir le niveau de compétence requis, il est recommandé de suivre la formation :

Les formations ci-dessous sont recommandées.

Implémentation et administration des solutions Cisco (CCNA 200-301)

Public

Cette formation s'adresse aux publics suivants :

- les intégrateurs et partenaires de Cisco, les consultants en ingénierie de systèmes, les architectes de solutions techniques et tout autre professionnel informatique spécialisé dans les réseaux et la sécurité des systèmes d'information.

Cette formation s'adresse aux profils suivants

Administrateur système
Administrateur réseaux - télécoms
Ingénieur système
Ingénieur réseaux - télécoms
Architecte informatique / SI

Programme

Domaine 1 : les concepts de sécurité

- Compréhension sur les menaces les plus courantes :
    - Sur site : les virus (cheval de Troie, etc.), les attaques DoS/DDoS, le phishing, les rootkits, les attaques man-in-the-middle, l'injection SQL, les scripts intersites et les logiciels espions ;
    - Dans le cloud : les violations de données, les API non sécurisées, les attaques DoS/DDoS et les informations d'identification falsifiées.
- Comparaison des vulnérabilités communes en matière de sécurité, notamment les bogues logiciels, les mots de passe faibles ou codés en dur, l'injection SQL, l'absence de chiffrement, le dépassement de mémoire tampon, la rupture de chemin, les scripts intersites et la falsification.
- Présentation des fonctions des composants cryptographiques tels que le hachage, le cryptage, l'ICP, le SSL, l'IPsec, le NAT-T IPv4 pour l'IPsec, la clé pré-partagée et l'autorisation basée sur un certificat.
- Comparaison des types de déploiement de VPN de site à site et de VPN d'accès à distance tels que sVTI, IPsec, Cryptomap, DMVPN, FLEXVPN, incluant les aspects de haute disponibilité et AnyConnect.
- Création, partage et utilisation des informations relatives à la sécurité.
- Explication des fonctions du terminal pour la protection contre les attaques d'hameçonnage et d'ingénierie sociale.
- Compréhension des interfaces de programmation North Bound et South Bound dans une architecture SDN.
- Compréhension des interfaces de programmation DNAC pour l'approvisionnement, l'optimisation, la surveillance et le dépannage du réseau.
- Interprétation des scripts Python de base servant à appeler des API d'appareils de sécurité Cisco.

Domaine 2 : la sécurité réseau

- Comparaison des solutions de sécurité réseau dotées de fonctionnalités anti-intrusion et d'un pare-feu.
- Présentation des modèles de déploiement pour les solutions de sécurité réseau ainsi que des architectures intégrant des fonctionnalités anti-intrusion et d'un pare-feu.
- Description des composants, des caractéristiques et des avantages de NetFlow et de l'enregistrement flexible.
- Configuration et contrôle des méthodes de sécurité de l'infrastructure du réseau (routeur, commutateur et réseau sans fil).
- Implémentation de la segmentation, des politiques de contrôle d'accès, de l'AVC, du filtrage d'URL et de la protection contre les logiciels malveillants.
- Implémentation des fonctions de gestion pour les solutions de sécurité réseau tels que la prévention des intrusions et la sécurité périmétrique.
- Configuration de l'AAA pour l'accès aux appareils et au réseau (authentification, autorisation, TACACS+, RADIUS, etc.).
- Configuration de la gestion réseau sécurisée des dispositifs de sécurité du périmètre et de l'infrastructure (gestion sécurisée des dispositifs, SNMPv3, vues, groupes, utilisateurs, authentification et cryptage, journalisation sécurisée et NTP avec authentification).
- Configuration et audit d'un VPN site à site et d'un VPN d'accès à distance avec Cisco IOS et Cisco AnyConnect Secure Mobility.

Domaine 3 : la sécurité du Cloud

- Identification des solutions de sécurité dans les environnements cloud (types de cloud et modèles de services).
- Comparaison des responsabilités du client et du fournisseur en matière de sécurité selon les différents modèles de services cloud.
- Présentation du concept de DevSecOps (pipeline CI/CD, orchestration de conteneurs et sécurité)
- Implémentation de la sécurité des applications et des données dans le cloud.
- Identification des capacités de sécurité, des modèles de déploiement et de la gestion des politiques pour sécuriser le cloud.

- Configuration des protocoles de journalisation et de surveillance dans le cloud
- Explication des concepts de sécurité des applications et de la charge de travail.

Domaine 4 : la sécurité du contenu

- Application de méthodes de redirection et de capture du trafic.
- Description de l'identité et de l'authentification du proxy Web, dont l'identification transparente de l'utilisateur.
- Comparaison des composants, des capacités et des avantages des solutions de messagerie et Web en local et dans le cloud (ESA, CES, WSA).
- Configuration et validation des méthodes de déploiement de la sécurité du Web et des e-mails pour protéger les utilisateurs locaux et distants (contrôles entrants et sortants et gestion des politiques).
- Configuration et validation des fonctions de sécurité de la messagerie électronique telles que le filtrage des spams, le filtrage des logiciels malveillants, le DLP, la mise en liste noire et le cryptage des messages.
- Configuration et contrôle des fonctions de sécurité de la passerelle Internet sécurisée et du web, tels que la mise en liste noire, le filtrage des URL, l'analyse des logiciels malveillants, la catégorisation des URL, le filtrage des applications web et le décryptage TLS.
- Présentation des composants, des caractéristiques et des avantages de Cisco Umbrella.
- Configuration et audit des contrôles de sécurité Web sur Cisco Umbrella (identités, paramètres de contenu d'URL, listes de destination et rapports).

Domaine 5 : la protection et la détection des terminaux

- Comparaison des plates-formes de protection des terminaux (EPP) et des solutions de détection et de réponse des terminaux (EDR).
- Explication des logiciels anti-malware, de la sécurité rétrospective, de l'indication de compromission (IOC), de l'antivirus, de l'analyse dynamique des fichiers et de la télémétrie des terminaux.
- Configuration et audit du système de contrôle des intrusions et des mises en quarantaine.
- Description des principes de base de la sécurité des postes de travail.
- Présentation des avantages d'une gestion des points d'accès et de l'inventaire des actifs, notamment par le biais d'un système de gestion des données (MDM).
- Présentation des usages et de l'importance d'une stratégie d'authentification multi-facteurs (MFA).
- Présentation des solutions d'évaluation du comportement des terminaux pour assurer un niveau de sécurité élevé.
- Explication sur l'importance d'une stratégie de remédiation pour les terminaux.

Domaine 6 : l'accès au réseau, la visibilité et le contrôle des applications

- Compréhension des concepts de gestion des identités et d'accès sécurisé au réseau (services d'accueil, profilage, évaluation de la posture et utilisation BYOD).
- Configuration et contrôle des fonctions des dispositifs d'accès au réseau telles que 802.1X, MAB et WebAuth.
- Description de l'accès au réseau avec un certificat d'authenticité (CoA).
- Présentation des avantages de la conformité des dispositifs et du contrôle des applications.
- Compréhension des techniques d'exfiltration (tunnel DNS, HTTPS, e-mail, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, NTP)
- Présentation des avantages de la télémétrie réseau.
- Présentation des composants, des caractéristiques et des avantages des produits et des solutions de sécurité Cisco :
    - Cisco Stealthwatch ;
    - Cisco Stealthwatch Cloud ;
    - Cisco pxGrid ;
    - Cisco Umbrella survey ;
    - Cisco Cognitive Threat Analysis ;

- Cisco Encrypted Traffic Analysis ;
- Cisco AnyConnect Network Visibility Module.

Labs

- Configurer le NAT et les politiques de contrôle d'accès sur Cisco ASA.
- Configurer le NAT et les politiques de contrôle d'accès sur le pare-feu Cisco Firepower.
- Configurer les politiques de découverte, de contrôle IPS de Cisco Firepower.
- Configurer une politique anti-malware et une stratégie de gestion des fichiers sur Cisco Firepower.
- Configurer des listes d'écoute, des tables d'accès aux hôtes (HAT) et des tables d'accès aux destinataires (RAT) sur Cisco Email Security Appliance (ESA).
- Configurer des politiques de messagerie électronique.
- Configurer des services proxys, l'authentification et le décryptage HTTPS.
- Mettre en place un contrôle d'utilisation acceptable et une protection contre les programmes malveillants.
- Analyser le tableau de bord et le système de recherche de Cisco Umbrella.
- Configurer la protection DNS contre les ransomwares avec Cisco Umbrella.
- Configurer le tunnel VTI statique IKEv2 IPsec point à point.
- Configurer un VPN point à point entre Cisco ASA et Cisco Firepower .
- Configurer un VPN d'accès à distance sur Cisco Firepower.
- Utiliser Cisco AMP pour définir des points de terminaison.
- Effectuer une analyse des terminaux à l'aide de la console AMP pour définir les points de terminaison.
- Utiliser la fonction de protection des fichiers contre les ransomwares à l'aide de la console Cisco AMP for Endpoints.
- Explorer Cisco Stealthwatch Enterprise et utiliser l'analyse cognitive des menaces (CTA) dans la version 7.0.
- Explorer le tableau de bord de Cisco Cloudlock et utiliser le système de sécurité de l'utilisateur, la sécurité des applications et les données de Cisco Cloudlock.
- Découvrir et paramétrer des alertes, des listes de surveillance et des capteurs dans Stealthwatch Cloud.