

SCOR- Implementation et exploitation de Cisco Security Core Technologies

- Durée : 5 Jours (35h)
- Tarif en présentiel ou en classe à distance : 3 960 € HT
- Tarif en E-Learning: 500 € HT

A qui s'adresse ce cours ?

Ingénieur sécurité
Ingénieur réseau
Concepteur de réseau
Administrateur réseau
Ingénieur Systèmes
Ingénieur conseil en systèmes
Architecte de solutions techniques
Gestionnaire de réseau
Intégrateurs et partenaires Cisco

Pré-Requis

Compréhension des protocoles de mise en réseau, du routage et de la commutation
Connaissance des produits de commutation Ethernet Cisco
Compréhension de l'architecture du centre de données Cisco
Connaissance des principes fondamentaux de la virtualisation
Voici les offres d'apprentissage Cisco recommandées qui peuvent vous aider à remplir ces conditions préalables: Implémentation et administration des solutions Cisco (CCNA) v1.0
Comprendre les fondations Cisco Data Center (DCFNDU) v1.0 Présentation de Cisco Data Center Networking (DCICN) v6.2 Présentation des technologies Cisco Data Center (DCICT) v6.2 Interconnexion des périphériques réseau Cisco: accélérée (CCNAX) ou interconnexion des périphériques réseau Cisco partie 1 (ICND1) et interconnexion des périphériques réseau Cisco partie 2 (ICND2)

Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation ou espace WebEx "Zoom, Teams....." en classe à distance

Modalité : Formation réalisée en présentiel ou à distance selon la formule retenue

Méthode : Un formateur expert, Labs à distance, Quiz en salle

Documentées : Support en anglais projeté et remis en PDF téléchargeable

Modalités de suivi et d'évaluation

Formulaires d'évaluations de la formation : pré-évaluation avant formation, évaluation de la satisfaction en fin de stage, évaluation des acquis à 90 jours

Feuille de présence émargée par demi-journée par les stagiaires et le formateur

Attestation de fin de formation

Analyse des attentes client

Accessibilité :

La formation est accessible aux personnes à mobilité réduite.

Une étude des conditions d'accès et des moyens de compensation sera réalisé en amont à l'inscription afin d'identifier plus précisément les conditions de réalisation et de faisabilité de la formation.

Vous pouvez trouver toutes les informations nécessaires sur notre site :

<https://bigso.fr/accueil/formations/>

Objectifs

Décrire la Cisco ACI Fabric Infrastructure et les concepts de base de la Cisco ACI

Décrire les constructions logiques du modèle de politique ACI de Cisco

Décrire le transfert de paquets de base Cisco ACI

Décrire la connectivité du réseau externe

Décrire l'intégration VMM

Décrire les intégrations de la couche 4 à la couche 7

Expliquer les fonctionnalités de gestion de Cisco ACI

La mise en œuvre et d'exploitation Cisco Core Security Technologies (SCOR) v1.0 vous aide à vous préparer aux certifications Cisco CCNP Security et CCIE Security et aux rôles de sécurité de niveau supérieur. Dans ce cours, vous maîtriserez les compétences et les technologies dont vous avez besoin pour implémenter les principales solutions de sécurité Cisco afin de fournir une protection avancée contre les menaces contre les attaques de cybersécurité. Vous apprendrez la sécurité des réseaux, du cloud et du contenu, la protection des terminaux, l'accès sécurisé au réseau, la visibilité et les mises en œuvre. Vous bénéficierez d'une expérience pratique approfondie du déploiement du pare-feu Cisco Firepower nouvelle génération et du pare-feu Cisco Adaptive Security Appliance (ASA); configuration des politiques de contrôle d'accès, des politiques de messagerie et de l'authentification 802.1X; et plus. Vous obtiendrez une pratique d'introduction sur les fonctionnalités de détection des menaces Cisco Stealthwatch Enterprise et Cisco Stealthwatch Cloud.

Ce cours vous aidera à :

- **Acquérir une expérience pratique de la mise en œuvre des technologies de sécurité de base et découvrir les meilleures pratiques à l'aide des solutions de sécurité Cisco**
- **Vous préparez à l'examen de mise en œuvre et d'exploitation des technologies de base de sécurité Cisco (350-701 SCOR)**
- **Vous qualifier pour des postes de travail de sécurité de niveau professionnel et expert**

Déroulement du cours

Décrire les concepts de sécurité de l'information *

- Présentation de la sécurité des informations
- Actifs, vulnérabilités et contre-mesures
- Gérer les risques
- Évaluation de la vulnérabilité
- Comprendre le système Common Vulnerability Scoring System (CVSS)

Décrire les attaques TCP / IP courantes *

- Vulnérabilités TCP / IP héritées
- Vulnérabilités IP
- Vulnérabilités ICMP (Internet Control Message Protocol)
- Vulnérabilités TCP
- Vulnérabilités du protocole UDP (User Datagram Protocol)
- 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 déni de service distribué
- Attaques de réflexion et d'amplification
- Attaques d'usurpation d'identité
- Attaques DHCP (Dynamic Host Configuration Protocol)

Décrire les attaques d'applications réseau courantes *

- Attaques par mot de passe
- Attaques basées sur le système de noms de domaine (DNS)
- Tunneling DNS
- Attaques basées sur le Web
- Amortissement HTTP 302
- Injections de commandes
- Injections SQL
- Scriptage intersite et falsification de demande
- Attaques par courrier électronique

Décrire les attaques de point de terminaison courantes *

- Débordement de tampon
- Malware
- Attaque de reconnaissance
- Accès et contrôle
- Accès via l'ingénierie sociale
- Accès via des attaques basées sur le Web
- Kits d'exploitation et rootkits
- Escalade de privilèges
- Phase de post-exploitation
- Angler Exploit Kit

Décrire les technologies de sécurité réseau

- Stratégie de défense en profondeur
- Défendre à travers le continuum d'attaque
- Présentation de la segmentation du réseau et de la virtualisation
- Présentation du pare-feu dynamique
- Présentation de Security Intelligence
- Normalisation des informations sur les menaces
- Présentation de la protection contre les logiciels malveillants en réseau
- Présentation du système de prévention des intrusions (IPS)
- Présentation du pare-feu nouvelle génération
- Présentation de la sécurité du contenu des e-mails
- Présentation de la sécurité du contenu Web
- Présentation des systèmes d'analyse des menaces
- Présentation de la sécurité DNS
- Présentation de l'authentification, de l'autorisation et de la comptabilité
- Présentation de la gestion des identités et des accès
- Présentation de la technologie de réseau privé virtuel
- Présentation des facteurs de forme des périphériques de sécurité réseau

Déployer le pare-feu Cisco ASA

- Types de déploiement Cisco ASA
- Niveaux de sécurité de l'interface Cisco ASA
- Objets et groupes d'objets Cisco ASA
- Traduction d'adresses réseau
- Listes de contrôle d'accès à l'interface Cisco ASA (ACL)
- ACL mondiales Cisco ASA
- Stratégies d'accès avancées de Cisco ASA
- Présentation de la haute disponibilité Cisco ASA

Déploiement du pare-feu Cisco Firepower nouvelle génération

- Déploiements Cisco Firepower NGFW
- Traitement et politiques des paquets Cisco Firepower NGFW
- Objets Cisco Firepower NGFW
- Traduction d'adresse réseau (NAT) Cisco Firepower NGFW
- Stratégies de préfiltre Cisco Firepower NGFW
- Stratégies de contrôle d'accès Cisco Firepower NGFW

- Intelligence de sécurité Cisco Firepower NGFW
- Stratégies de découverte de Cisco Firepower NGFW
- Stratégies IPS de Cisco Firepower NGFW
- Stratégies de programmes malveillants et de fichiers Cisco Firepower NGFW

Déploiement de la sécurité du contenu des e-mails

- Présentation de Cisco Email Content Security
- Présentation du protocole SMTP (Simple Mail Transfer Protocol)
- Présentation du pipeline de messagerie
- Auditeurs publics et privés
- Présentation de la table d'accès à l'hôte
- Présentation de la table d'accès des destinataires
- Présentation des stratégies de messagerie
- Protection contre le spam et Graymail
- Protection antivirus et anti-malware
- Filtres anti-épidémies
- Filtres de contenu
- Prévention contre la perte de données
- Cryptage des e-mails

Déployer la sécurité du contenu Web

- Présentation de l'appliance de sécurité Web Cisco (WSA)
- Options de déploiement
- Authentification des utilisateurs du réseau
- Déchiffrement du trafic HTTP sécurisé (HTTPS)
- Stratégies d'accès et profils d'identification
- Paramètres des contrôles d'utilisation acceptable
- Protection anti-malware

Déploiement de Cisco Umbrella *

- Architecture de parapluie Cisco
- Déployer Cisco Umbrella
- Client itinérant Cisco Umbrella
- Gérer Cisco Umbrella
- Présentation et concepts de Cisco Umbrella Investigate

Expliquer les technologies VPN et la cryptographie

- Définition VPN
- Types de VPN
- Communication sécurisée et services cryptographiques
- Clés en cryptographie
- Infrastructure à clé publique

Présentation des solutions VPN sécurisées de site à site de Cisco

- Topologies VPN de site à site
- Présentation du VPN IPsec
- Cartes cryptographiques statiques IPsec
- Interface de tunnel virtuel statique IPsec
- VPN multipoint dynamique
- Cisco IOS FlexVPN

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

- VTI Cisco IOS
- Configuration VPN v2 point à point IPsec Internet Key Exchange (IKE) statique

Déploiement de VPN IPsec point à point sur Cisco ASA et Cisco Firepower NGFW

- VPN point à point sur Cisco ASA et Cisco Firepower NGFW
- Configuration VPN point à point Cisco ASA
- Configuration VPN point à point Cisco Firepower NGFW

Présentation des solutions VPN d'accès sécurisé à distance Cisco

- Composants VPN d'accès à distance
- Technologies VPN d'accès à distance
- Présentation de Secure Sockets Layer (SSL)

Déploiement de VPN SSL d'accès à distance sur Cisco ASA et Cisco Firepower NGFW

- Concepts de configuration de l'accès à distance
- Profils de connexion
- Stratégies de groupe
- Configuration VPN d'accès distant Cisco ASA
- Configuration VPN d'accès à distance Cisco Firepower NGFW

Explication des solutions Cisco Secure Network Access

- Accès réseau sécurisé Cisco
- Composants d'accès sécurisé au réseau Cisco
- Rôle AAA dans la solution Cisco Secure Network Access
- Moteur de services d'identité Cisco
- Cisco wisdomec

Décrire l'authentification 802.1X

- 802.1X et EAP (Extensible Authentication Protocol)
- Méthodes EAP
- Rôle du service utilisateur d'accès à distance par authentification à distance (RADIUS) dans les communications 802.1X
- Changement d'autorisation RADIUS

Configuration de l'authentification 802.1X

- Configuration du commutateur Cisco Catalyst® 802.1X
- Configuration du contrôleur LAN sans fil Cisco (WLC) 802.1X
- Configuration de Cisco Identity Services Engine (ISE) 802.1X
- Configuration Supplicant 802.1x
- Authentification Web centrale Cisco

Décrire les technologies Endpoint Security *

- Pare-feu personnel basé sur l'hôte
- Anti-virus basé sur l'hôte
- Système de prévention des intrusions basé sur l'hôte
- Listes blanches et listes noires des applications
- Protection contre les programmes malveillants basés sur l'hôte
- Présentation de Sandboxing
- Vérification de l'intégrité des fichiers

Déploiement de Cisco Advanced Malware Protection (AMP) for Endpoints *

- Cisco AMP for Endpoints Architecture
- Cisco AMP for Endpoints Engines
- Sécurité rétrospective avec Cisco AMP
- Trajectoire des périphériques et fichiers Cisco AMP
- Gestion de Cisco AMP pour les points de terminaison

Présentation de la protection de l'infrastructure réseau *

- Identification des plans des périphériques réseau
- Contrôles de sécurité du plan de contrôle
- Contrôles de sécurité du plan de gestion
- Télémétrie réseau
- Contrôles de sécurité du plan de données de couche 2
- Contrôles de sécurité du plan de données de couche 3

Déploiement des contrôles de sécurité du plan de contrôle *

- ACL d'infrastructure
- Contrôle du plan de contrôle
- Protection du plan de contrôle
- Sécurité du protocole de routage

Déploiement des contrôles de sécurité du plan de données de couche 2 *

- Présentation des contrôles de sécurité du plan de données de couche 2
- Atténuation des attaques basée sur le LAN virtuel (VLAN)
- Atténuation des attaques par le protocole STP (Spanning Tree Protocol)
- Sécurité portuaire
- VLAN privés
- Surveillance du protocole DHCP (Dynamic Host Configuration Protocol)
- Inspection du protocole de résolution d'adresse (ARP)
- Contrôle des tempêtes
- Chiffrement MACsec

Déploiement des contrôles de sécurité du plan de données de couche 3 *

- ACL d'infrastructure antispoofing
- Transfert de chemin inverse unicast
- IP Source Guard

Déploiement des contrôles de sécurité du plan de gestion *

- Accès de gestion sécurisé Cisco
- Protocole de gestion de réseau simple version 3
- Accès sécurisé aux appareils Cisco
- AAA pour l'accès à la gestion

Déploiement des méthodes de télémétrie du trafic *

- Protocole de temps réseau
- Journalisation et exportation des événements de périphérique et de réseau
- Surveillance du trafic réseau à l'aide de NetFlow

Déploiement de Cisco Stealthwatch Enterprise

- Présentation des offres Cisco Stealthwatch
- Composants requis pour Cisco Stealthwatch Enterprise
- Assemblage de flux et déduplication
- Composants facultatifs de Stealthwatch Enterprise
- Stealthwatch Enterprise et intégration ISE
- Cisco Stealthwatch avec Cognitive Analytics
- Analyse du trafic crypté Cisco
- Groupes hôtes
- Événements et alarmes de sécurité
- Hôte, rôle et stratégies par défaut

Décrire les attaques Cloud et Common Cloud *

- Evolution du cloud computing
- Modèles de service cloud
- Responsabilités de sécurité dans le cloud
- Modèles de déploiement cloud
- Menaces de sécurité courantes dans le cloud
- Gestion des correctifs dans le cloud
- Évaluation de la sécurité dans le cloud

Sécuriser le cloud *

- Approche centrée sur les menaces de Cisco en matière de sécurité réseau
- Sécurité de l'environnement physique du cloud
- Sécurité des applications et de la charge de travail
- Gestion du cloud et sécurité des API
- Virtualisation de la fonction réseau (NFV) et fonctions de réseau virtuel (VNF)
- Exemples Cisco NFV
- Rapports et visibilité des menaces dans le cloud
- Courtier de sécurité d'accès au cloud
- Cisco CloudLock®
- Attaques OAuth et OAuth

Déploiement de Cisco Stealthwatch Cloud *

- Cisco Stealthwatch Cloud pour la surveillance du cloud public
- Cisco Stealthwatch Cloud pour la surveillance de réseaux privés
- Opérations dans le cloud de Cisco Stealthwatch

Décrire le réseau défini par logiciel (SDN *)

- Concepts de mise en réseau définis par logiciel
- Programmabilité et automatisation du réseau
- Plateformes et API Cisco
- Scripts de base Python pour l'automatisation

* Cette section est du matériel d'autoformation qui peut être fait à votre propre rythme si vous suivez la version dirigée par un instructeur de ce cours.

Aperçu du lab

- Configurer les paramètres réseau et NAT sur Cisco ASA
- Configurer les stratégies de contrôle d'accès de Cisco ASA
- Configurer le Cisco Firepower NGFW NAT
- Configurer la stratégie de contrôle d'accès de Cisco Firepower NGFW
- Configurer Cisco Firepower NGFW Discovery et IPS Policy
- Configurer la politique de malware et de dossier de Cisco NGFW
- Configurer l'écouteur, la table d'accès d'hôte (HAT) et la table d'accès de destinataire (RAT) sur l'appliance de sécurité du courrier électronique de Cisco (ESA)
- Configurer les politiques de messagerie
- Configurer les services proxy, l'authentification et le déchiffrement HTTPS
- Appliquer le contrôle d'utilisation acceptable et la protection contre les logiciels malveillants
- Examinez le tableau de bord du parapluie
- Examiner Cisco Umbrella Investigate
- Explorez la protection DNS contre les ransomwares par Cisco Umbrella
- Configurer un tunnel IKEv2 IPsec point à point VTI statique
- Configurez le VPN point à point entre Cisco ASA et Cisco Firepower NGFW
- Configurez le VPN d'accès à distance sur le Cisco Firepower NGFW
- Explorez Cisco AMP for Endpoints
- Effectuer une analyse des points de terminaison à l'aide d'AMP pour la console des points de terminaison
- Explorez File Ransomware Protection par Cisco AMP pour Endpoints Console
- Découvrez Cisco Stealthwatch Enterprise v6.9.3
- Explorez Cognitive Threat Analytics (CTA) dans Stealthwatch Enterprise v7.0
- Explorez le tableau de bord Cisco Cloudlock et la sécurité des utilisateurs
- Explorez Cisco Cloudlock Application and Data Security
- Explorez Cisco Stealthwatch Cloud
- Explorez les paramètres d'alerte, les listes de surveillance et les capteurs Stealthwatch Cloud

ALLEZ PLUS LOIN

Ce cours vous aidera à vous préparer à passer l'examen de **mise en œuvre et d'exploitation des technologies de base de sécurité Cisco (350-701 SCOR)**. Cet examen teste les connaissances d'un candidat sur la mise en œuvre et l'exploitation des technologies de sécurité de base.

Après avoir passé 350-701 SCOR :

- Vous gagnez le **spécialiste Cisco Certified – Security Core** certification
- Vous répondez aux exigences essentielles de sécurité CCNP et de sécurité CCIE.

Pour terminer votre certification de **sécurité CCNP**, passez l'un des examens de concentration de sécurité.

Pour compléter votre certification **CCIE Security**, passez l'examen **CCIE Security v6.0 Lab**.