Cisco Security Core Technologies : implementing and operating

Lien : https://innov-systems.com/formation/cisco-security-core-technologies-implementing-and-operating

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC188

CATÉGORIE
Cisco

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Apprendre à maîtriser les compétences et les technologies nécessaires pour implémenter les principales solutions de sécurité Cisco
- Acquérir les compétences nécessaires sur la sécurité des réseaux, du cloud et du contenu, la protection des points d'extrémité, l'accès sécurisé au réseau, la visibilité et les mesures d'application
- Se préparer aux certifications Cisco® CCNP® Security et CCIE® Security

POUR QUI ?

- Ingénieur sécurité
- Ingénieur réseau
- Concepteur réseau
- Administrateur réseau
- Ingénieur système
- Ingénieur en systèmes de conseil
- Architecte des solutions techniques
- Intégrateurs/partenaires Cisco
- Gestionnaire de réseau
- Intégrateurs et partenaires de Cisco

Programme détaillé

1 / Concepts de sécurité de l'information

- Vue d'ensemble de la sécurité de l'information
- Gérer les risques
- Évaluation de la vulnérabilité
- Comprendre le CVSS

2 / Les attaques TCP/IP courantes

- Vulnérabilités héritées de TCP/IP
- Vulnérabilités de IP
- Vulnérabilités de ICMP
- Vulnérabilités de TCP
- Vulnérabilités d'UDP
- Surface d'attaque et vecteurs d'attaque
- Attaques de reconnaissance
- Attaques à l'accès
- Attaques Man in the middle
- Déni de service et attaques distribuées de déni de service
- Réflexion et amplification des attaques
- Attaques par usurpation d'identité
- Attaques DHCP

3 / Les attaques des applications de réseau les plus communes

- Attaques de mots de passe
- Attaques basées sur le DNS
- Tunneling DNS
- Attaques sur le web

- HTTP 302 Amortissement
- Injections de commandes
- Injections SQL
- Scripts intersites et falsification de demandes
- Attaques par courrier électronique

4 / Les attaques de points finaux les plus fréquentes

- Débordement de la mémoire tampon
- Malware
- Attaque de reconnaissance
- Obtenir l'accès et le contrôle
- Obtenir l'accès par l'ingénierie sociale
- Obtenir l'accès par le biais d'attaques basées sur le Web
- Kits d'exploitation et Rootkits
- Escalade des privilèges
- Phase de post-exploitation
- Angler Exploit Kit

5 / Les technologies de sécurité des réseaux

- Stratégie de défense en profondeur
- Défendre à travers le continuum des attaques
- Vue d'ensemble de la segmentation des réseaux et de la virtualisation
- Vue d'ensemble du firewall Stateful
- Vue d'ensemble du Security Intelligence
- Normalisation de l'information sur les menaces
- Vue d'ensemble de la protection contre les logiciels malveillants sur les réseaux
- Vue d'ensemble des IPS
- firewall Next Generation
- Vue d'ensemble de la sécurité du contenu du courrier électronique
- Vue d'ensemble de la sécurité du contenu Web

- Vue d'ensemble des systèmes d'analyse des menaces
- Vue d'ensemble de la sécurité du DNS
- Authentification, autorisation et comptabilité
- Vue d'ensemble de la gestion des identités et des accès
- Vue d'ensemble de la technologie des réseaux privés virtuels

6 / Déployer le firewall Cisco ASA

- Types de déploiement
- Niveaux de sécurité de l'interface
- Objets et groupes d'objets
- Translation d'adresse réseau
- Gestion des ACL
- Global ACL
- Politiques d'accès avancé
- Vue d'ensemble de la haute disponibilité

7 / Déployer le firewall Next Generation Cisco Firepower

- Traitement des paquets et politiques de Cisco Firepower
- Objets Cisco Firepower NGFW
- Gestion du NAT sur le Cisco Firepower NGFW
- Politiques du filtrage
- Politiques de contrôle d'accès
- Security Intelligence
- Politiques IPS
- Malware Cisco Firepower NGFW et politiques de fichiers

8 / Déployer la sécurité du contenu des courriels

- Vue d'ensemble de la sécurité du contenu des courriers électroniques Cisco
- Vue d'ensemble du SMTP

- Vue d'ensemble de l'acheminement du courrier électronique
- Auditeurs publics et privés
- Vue d'ensemble des politiques en matière de courrier
- Protection contre le spam et le courrier gris (Graymail)
- Protection antivirus et anti-malware
- Filtres d'épidémie (outbreak)
- Filtres de contenu
- Prévention des pertes de données
- Cryptage des courriers électroniques

9 / Déployer la sécurité du contenu Web

- Vue d'ensemble de Cisco WSA
- Options de déploiement
- Authentification des utilisateurs du réseau
- Décryptage du trafic HTTPS
- Politiques d'accès et profils d'identification
- Paramètres des contrôles d'utilisation acceptables
- Protection contre les logiciels malveillants

10 / Déployer Cisco Umbrella

- Architecture Cisco Umbrella
- Déploiement Cisco Umbrella
- Cisco Umbrella Roaming Client
- Management de Cisco Umbrella
- Introduction à Cisco Umbrella Investigate

11 / Explorer les technologies VPN et la cryptographie

- Définition des VPN
- Types deVPN

- Communications sSecurisées et services de cryptages
- Clés de cryptage
- Infrastructure de clés publiques

12 / Introduire les solutions de VPN Site-to-Site Cisco

- Topologies de VPN Site-to-Site
- Introduction au VPN IPsec
- IPsec Static Crypto Maps
- IPsec Static Virtual Tunnel Interface
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN

13 / Déployer VTI-Based Point-to-Point

- Cisco IOS VTIs
- Configuration de VTI Point-to-Point IPsec statique

14 / Déployer les VPNs IPSEC Point-to-Point sur les Cisco ASA et Cisco Firepower NGFW

- VPN Point-to-Point VPNs sur les Cisco ASA et Cisco Firepower NGFW
- Configuration sur le Cisco ASA
- Configuration sur les Cisco Firepower NGFW

15 / Introduire les solutions d'accès distantes sécurisées VPN Cisco

- Composants d'un VPN d'accès distant
- Technologiesd'un VPN d'accès distant
- Vue d'ensemble du SSL

16 / Déployer les solutions d'accès distantes sécurisées sur les Cisco ASA et Cisco Firepower NGFW

- Vue d'ensemble des concepts

- Connexion Profiles
- Group Policies
- Configuration sur les Cisco ASA
- Configuration sur les Cisco Firepower NGFW

17 / Explorer les solutions Cisco Secure Network Access

- Cisco Secure Network Access
- Composants di Cisco Secure Network Access
- Utilisation du AAA
- Cisco Identity Services Engine
- Cisco TrustSec

18 / L'authentification 802.1X

- 802.1X et EAP
- Méthodes EAP
- Rôle du RADIUS dans les communications 802.1X
- Changements des autorisations sur une serveur RADIUS

19 / Configurer l'authentification 802.1X

- Configuration d'un Cisco Catalyst Switch
- Configuration sur un Cisco WLC
- Configuration sur un Cisco ISE
- Configuration d'un supplicant
- Cisco Central Web Authentication

20 / Les solutions sécurisées sur les endpoints

- Firewalls
- Anti-Virus
- Intrusion Prevention System

- Gestion des listes blanches et listes noires
- Protection contre les malwares
- Vue d'ensemble du bac à sable (Sandboxing)
- Vérification de l'intégraité des fichiers

21 / Déployer Cisco AMP pour les terminaux

- Architecture du Cisco AMP
- Cisco AMP for Endpoints Engines
- Cisco AMP Device and File Trajectory
- Manager Cisco AMP for Endpoints

22 / Introduction de la protection des infrastructures de réseau

- Identification du data plane réseau
- Sécurisation du control plane
- Sécurisation du dataplane
- Télémétrie en réseau
- Contrôle du control plane de la couche 2
- Contrôle du control plane de la couche 2

23 / Déployer la sécurité du control Plane

- Infrastructure des ACLs
- Control Plane Policing
- Protection du Control Plane
- Sécurisation des protocoles de routage

24 / Déployer la sécurité de couche 2 du control Plane

- Vue d'ensemble
- Gestion des attaques basées sur les VLAN
- Gestion des attaques basées sur le STP

- Port Security
- Private VLANs
- DHCP Snooping
- ARP Inspection
- Storm Control
- MACsec Encryption

25 / Déployer la sécurité de couche 3 du control Plane

- Antispoofing ACLs
- Unicast Reverse Path Forwarding
- IP Source Guard

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

28 Sep. au 02 Oct. 2026	Distanciel
23 au 27 Nov. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com