Solutions de Sécurité Cisco

Lien : https://innov-systems.com/formation/solutions-de-securite-cisco

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**RST114**	**Cisco Sécurité**

OBJECTIFS DE LA FORMATION

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

- Implémenter les principales solutions de sécurité Cisco afin d'assurer une protection avancée contre les attaques de cybersécurité

POUR QUI ?

- Toute personne chargée de la sécurité

Innov Systems

Programme détaillé

1 / Présentation des concepts de sécurité de l'information

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

2 / Présentation des attaques TCP/IP courantes

- Les vulnérabilités liées aux héritées de TCP/IP
- Les vulnérabilités liées à IP
- Les vulnérabilités liées à ICMP
- Les vulnérabilités liées à TCP
- Les vulnérabilités liées à UDP
- Présentation de la surface d'attaque et vecteurs d'attaque
- Présentation des attaques de reconnaissance
- Présentation des attaques à l'accès
- Présentation des attaques Man in the middle
- Déni de service et attaques distribuées de déni de service
- Réflexion et amplification des attaques
- Présentation des attaques par usurpation d'identité
- Présentation des attaques DHCP

3 / Présentation des attaques des applications de réseau communes

- Les attaques de mots de passe
- Les attaques basées sur le DNS
- Tunneling DNS
- Les attaques sur le web

Innov Systems

- HTTP 302 Amortissement
- Les attaques basées sur l’injection de commandes
- Les attaques basées sur l’injection SQL
- Les scripts intersites et falsification de demandes
- Les attaques par courrier électronique

4 / Présentation des attaques de points terminaux communs

- 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 / Présentation des technologies de sécurité des réseaux

- Stratégie de défense en profondeur
- Défendre à travers le continuum des attaques
- Présentation de la segmentation des réseaux et de la virtualisation
- Vue d'ensemble du pare-feu 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
- Pare-feu Next Generation
- Vue d'ensemble de la sécurité du contenu du courrier électronique
- Vue d'ensemble de la sécurité du contenu Web

Innov Systems

- 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 pare-feu Cisco ASA

- Différents types de déploiement
- Différents niveaux de sécurité de l'interface
- Les objets et groupes d'objets
- Configuration de la translation d'adresse réseau
- Gestion des ACL
- Global ACL
- Politiques d'accès avancé
- Vue d'ensemble de la haute disponibilité

7 / Déployer le pare-feu Next Generation Cisco Firepower

- Traitement des paquets et politiques de Cisco Firepower
- Les objets Cisco Firepower NGFW
- Gestion du NAT sur le Cisco Firepower NGFW
- Vue d'ensemble des politiques du filtrage
- Vue d'ensemble des politiques de contrôle d'accès
- Security Intelligence
- Vue d'ensemble des 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
- Présentation du SMTP

Inov Systems

- Présentation de l'acheminement du courrier électronique
- Auditeurs publics et privés
- Présentation 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

- Présentation de Cisco WSA
- Présentation de différentes options de déploiement
- Gérer l'authentification des utilisateurs du réseau
- Décrypter le trafic HTTPS
- Présentation d politiques d'accès et profils d'identification
- Paramètres des contrôles d'utilisation acceptables
- Protection contre les logiciels malveillants

10 / Déployer Cisco Umbrella

- Présentation de l'architecture Cisco Umbrella
- Déployer Cisco Umbrella
- Cisco Umbrella Roaming Client
- Gestion de Cisco Umbrella
- Présentation de Cisco Umbrella Investigate

11 / Utiliser les technologies VPN et la cryptographie

- Vue d'ensemble des VPN
- Différents types de VPN

Inov Systems

- Communications securisées et services de cryptages
- Les clés de cryptage
- Infrastructure de clés publiques

12 / Introduction aux solutions de VPN Site-to-Site Cisco

- Différents types de VPN Site-to-Site
- Vue d'ensemble de 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
- Configurer VTI Point-to-Point IPsec statique

14 / Déployer des 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 / Introduction aux solutions d'accès distantes sécurisées VPN Cisco

- Présentation des composants d'un VPN d'accès distant
- Présentation des technologies d'un VPN d'accès distant
- Présentation du SSL

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

- Vue d'ensemble des concepts

Inov Systems

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

17 / Utiliser les solutions Cisco Secure Network Access

- Cisco Secure Network Access
- Vue d'ensemble des composants di Cisco Secure Network Access
- Utiliser le modèle AAA
- Cisco Identity Services Engine
- Cisco TrustSec

18 / Présentation de l'authentification 802.1X

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

19 / Configurer l'authentification 802.1X

- Configurer un Cisco Catalyst Switch
- Configurer un Cisco WLC
- Configurer un Cisco ISE
- Configurer un supplicant
- Cisco Central Web Authentication

20 / Présentation des solutions sécurisée sur les endpoints

- Pare-feux
- Anti-Virus
- Intrusion Prevention System

Innov Systems

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

21 / Mettre en oeuvre Cisco AMP pour les terminaux

- Présentation de l'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 / Mettre en oeuvre la sécurité du control Plane

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

24 / Mettre en oeuvre la sécurité de couche 2 du control Plane

- Présentation
- Gestion des attaques basées sur les VLAN
- Gestion des attaques basées sur le STP

Inov Systems

- Port Security
- Private VLANs
- DHCP Snooping
- ARP Inspection
- Contrôle de tempête (storm control)
- MACsec Encryption

25 / Mettre en oeuvre 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

25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 2027	Présentiel - Casablanca
06 au 10 Sep. 2027	Présentiel - Casablanca

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

Innov Systems

Réservation & Renseignements

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

Innov Systems — Tous droits réservés

Innov Systems