Détection d’Intrusion et SOC

Lien : https://innov-systems.com/formation/detection-dintrusion-et-soc

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC40

CATÉGORIE
Test d'Intrusions, Techniques de Hacking, Contre Mesures et Audit

OBJECTIFS DE LA FORMATION

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

- Comprendre les techniques d'analyse et de détection
- Déployer différents outils de détection d'intrusion
- Comprendre, implémenter et manipuler un SOC (Security Operation Center)

POUR QUI ?

- Techniciens et administrateurs systèmes et réseaux

Innov Systems

Programme détaillé

1 / Evolution de la cybersécurité

- Nouveaux acteurs et nouvelles portées de la cybersécurité
- Sécurité et juridique
- CNIL ANSSI
- ENISA
- Les normes

2 / Principes généraux de la sécurité informatique

- Pourquoi la sécurité informatique ?
- Les piliers de la sécurité informatique : confidentialité, intégrité, disponibilité...
- Les composants de la cybersécurité : Que veut-on protéger ? Pourquoi ?
- Défense en profondeur et politique de sécurité
- Méthodes et normes pour l'analyse des risques

3 / Introduction à la cybercriminalité

- L'évolution de la cybercriminalité. Son impact
- Les types d'attaquants (White hat...)
- Qu'est-ce que le hacking ?
- Les principaux groupes de hackers
- Les types d'attaques (Malware, MITM, SE...)
- Les différentes phases d'une attaque (Cyber Kill Chain)
- Sophistication des techniques d'attaques
- Les différentes lois et référentiels

4 / Les protocoles réseaux

Innov Systems

- D’autres aspects des protocoles IP, TCP et UDP
- Focus sur ARP et ICMP
- Le routage forcé de paquets IP
- Problèmes de sécurité de TCP/IP
- Filtrage sérieux : l'utilité
- Sécurisation des serveurs : un impératif
- Routeur filtrant au firewall stateful inspection. du proxy au reverse proxy
- Bref présentation des solutions et des produits

5 / Connaitre les attaques sur TCP/IP

- "Spoofing" IP
- Déni de service
- La technique de la prédiction des numéros de séquence TCP
- Vol de session TCP
- Les attaques sur SNMP
- Attaque par TCP Spoofing (Mitnick)

6 / Intelligence Gathering

- Interrogation des bases Whois, les serveurs DNS, les moteurs de recherche
- Les techniques pour mettre en place l'identification des serveurs
- Analyse des résultats
- Les règles de filtrage

7 / Les trojans et les backdoors - Détection

- Vue d'ensemble des backdoors sous Windows et Unix
- Définition d'un backdoor
- Mettre en place des backdoors et des trojans
- Le téléchargement. Exploitation de bugs des navigateurs
- Les Covert Channels

Innov Systems

8 / Définition et approche stratégique d'un SOC (Security Operation Center)

- Terminologie du monde SOC
- Définition d’un SOC et environnement
- Les objectifs, missions et les bénéfices
- Les services actifs au sein du SOC
- Les processus du SOC
- Les composantes au sein du SOC
- Les rôles et tâches au sein des équipes
- La génération et le traitement des données
- La structuration SOC selon le CLUSIF
- Le SIM (Security Information Management)
- Le SIEM (Security Information and Event Management)
- Le SEM (Security Event Management)

9 / Le métier de l’analyste SOC

- Le métier de l’analyste SOC. Ses compétences
- Surveiller et trier les alertes et les événements
- Prioriser les alertes

10 / Déploiement d'un SOC

- La définition du projet de déploiement
- L'approche constructive entreprise
- La délimitation des besoins
- La phase de "Build"
- La phase de "Run"
- Premier bilan et retour d'expériences
- La poursuite du déploiement

11 / Gestion d'un incident

Inov Systems

- Les signes d'une intrusion réussie dans un SI
- Qu'ont obtenu les hackers ? Jusqu'où sont-ils allés ?
- Comment réagir face à une intrusion réussie ?
- Quels serveurs sont concernés ?
- Savoir retrouver le point d'entrée et le combler
- La boîte à outils Unix/Windows pour la recherche de preuves
- Nettoyage et remise en production de serveurs compromis

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

15 au 19 Fév. 2027	Présentiel - Casablanca
12 au 16 Avr. 2027	Présentiel - Casablanca
07 au 11 Juin 2027	Présentiel - Casablanca
02 au 06 Août 2027	Présentiel - Casablanca
27 Sep. au 01 Oct. 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