Cycle Analyste SOC (Security Operation Center)

Lien : https://innov-systems.com/formation/cycle-analyste-soc-security-operation-center

DURÉE
8 jours (56h)

RÉFÉRENCE
SEC03

CATÉGORIE
Cycles Métiers Sécurité Informatique

OBJECTIFS DE LA FORMATION

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

- Identifier et comprendre les techniques d'analyse et de détection
- Déployer différents outils de détection d'intrusion
- Implémenter des solutions de prévention et de détection d'intrusions
- Assimiler les concepts et l’environnement d’un SOC
- Savoir utiliser les outils d’analyse

POUR QUI ?

- Techniciens et administrateurs systèmes et réseaux

Programme détaillé

1 / Bien Comprendre les protocoles réseaux

- D’autres aspects des protocoles IP, TCP et UDP
- Focus sur ARP et ICMP
- Source routing
- La fragmentation IP et les règles de réassemblage
- Filtrage sérieux
- Sécurité des serveurs
- Panorama des solutions et des produits

2 / Les attaques sur TCP/IP

- Comment les pirates informatique mettent en oeuvre le "Spoofing" IP
- Les attaques par déni de service
- La technique de la prédiction des numéros de séquence TCP
- Vol de session TCP
- Comprendre comment les pirates arrivent à réaliser des attaques sur SNMP
- Attaque par TCP Spoofing (Mitnick)

3 / 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

4 / Détection des trojans et des backdoors

- Vue d'ensemble des backdoors sous Windows et Unix

- Définition d'un backdoor
- Mettre en place des backdoors et des trojans
- Le téléchargement de scripts sur les clients, exploitation de bugs des navigateurs
- Les "Covert Channels" : application client-serveur utilisant ICMP
- Exemple de communication avec les Agents de Déni de Service distribués
- Analyse de Loki, client-serveur utilisant ICMP
- Accéder à des informations privées avec son navigateur

5 / Attaques et exploitation des failles

- Prendre contrôle d'un serveur : recherche et exploitation de vulnérabilités
- Exemples de mise en place de "backdoors" et suppression des traces
- Contourner un firewall (netcat et rebonds)
- Les techniques pour effectuer la recherche du déni de service
- Le déni de service distribué (DDoS)
- Comment les pirates s'organisent pour effectuer une telle attaque ?
- Les attaques par débordement (buffer overflow)
- Exploitation de failles dans le code source
- "Format String", "Heap Overflow"
- Les vulnérabilités dans les applications Web : Comment les détecter et se protéger ?
- Comment les personnes malveillantes arrivent à voler les informations dans une base de données
- Les RootKits

6 / Le SOC (Security Operation Center)

- Définition d’un SOC. L'utilité
- Les fonctions du SOC : Logging, Monitoring, Reporting audit et sécurité, analyses post incidents
- Les bénéfices d’un SOC
- Les solutions pour un SOC
- Le SIM (Security Information Management)
- Le SIEM (Security Information and Event Management)
- Le SEM (Security Event Management)

7 / Le métier de l’analyste SOC

- En quoi consiste le métier de l’analyste SOC ?
- Quelles sont ses compétences ?
- Monitorer et trier les alertes et les événements
- Savoir prioriser les alertes

8 / Gestion d'un incident

- 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

9 / Collecte et analyse des logs

- Vue d'ensemble de la collecte et l'analyse des logs
- La collecte des informations
- Syslog
- Le programme SEC
- Le logiciel Splunk

10 / Gestion des logs

- La sécurité SI
- Les problématiques de la supervision et des logs
- Les différentes possibilités de normalisation
- Les avantages d’une supervision centralisée
- Panorma des solutions du marché

11 / La collecte des informations

- L’hétérogénéité des sources. Evénement de sécurité
- SIEM. Les événements collectés du SI
- Les journaux système des équipements
- La collecte passive en mode écoute et la collecte active

12 / Analyse forensic

- L’analyse forensic d’un système
- La cybercriminalité moderne
- La preuve numérique
- Inforensique Windows
- Inforensique Linux

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

27 Juil. au 05 Août 2026	Présentiel - Casablanca
21 au 30 Sep. 2026	Distanciel
16 au 25 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