Surveillance, Détection et Réponse aux Incidents de Sécurité

Lien : https://innov-systems.com/formation/surveillance-detection-et-reponse-aux-incidents-de-securite

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC255

CATÉGORIE
Analyse Apres Incident : Analyse Forensique, Investigation Numérique et Plan de Continuité

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les menaces et attaques sur les réseaux et systèmes
- Identifier les indicateurs de compromission (IOC)
- Mettre en œuvre les différents moyens de surveillance et de détection
- Anticiper et limiter l'impact des attaques
- Maîtriser les différentes étapes de gestion des incidents de sécurité

POUR QUI ?

- Membres d'un SOC ou d'un CSIRT
- Administrateurs
- Responsables sécurité

Programme détaillé

1 / Introduction

- Pourquoi la détection ?
- Défense en profondeur
- Évolution de la menace
- Principes de défense
- CTI et renseignement : IOC, Yara, MISP

2 / Comprendre l'attaque

- Objectifs de l'attaquant
- Familles d'attaques
- Phases d'une attaque
- Plusieurs champs de bataille :
- Réseau
- Applications
- Active Directory
- La dimension métier
- Portrait d'une attaque réussie

3 / Architecture de détection

- Architecture sécurisée
- Détections : les classiques
- Parefeu
- IDS/IPS
- SIEM
- SandBox
- Capture réseau

Innov Systems

- WAF
- Valoriser les « endpoints » :
- Whitelisting
- Sysmon
- Protections mémoire
- Mesures complémentaires de Windows 10
- Les outsiders
- « Self-defense » applicative
- Honey-*
- Données DNS
- Focus : Journalisation
- Les IOC : Yara, MISP

4 / **Blue Team vs Attaquant**

- Gérer les priorités
- Outils & techniques
- Wireshark / Tshark
- Bro / Zeek
- Recherche d’entropie
- Analyse longue traîne

5 / **Reconnaissance**

- Reconnaissance passive
- Etude : récupération de données publiques
- Reconnaissance active
- Fuites d'informations
- Reconnaissance réseau
- Etude : Scanning
- Détection/réponse
- Pare-feux

Innov Systems

- IDS/IPS / "Pots de miel"
- Prévention
- Maîtrise de l'information
- Attaquer pour mieux se defender

6 / Exploitation

- Vulnérabilités
- Les failles web
- Etude : Injection SQL
- Défaut de mise à jour
- Etude : OS obsolète
- Mauvaise configuration
- Etude : Rétro-compatibilité et MitM (Responder)
- Le facteur humain
- Détection/réponse
- WAF
- IDS/IPS
- Automatisation
- Prévention
- Supervision sécurité continue (CSM)
- Développement sécurisé
- Sécurisation active
- Moindre privilege

Innov Systems

7 / Post-exploitation

- Objectifs de l'attaquant
- Exfiltration des données
- Ransomware
- Déni de service
- Focus : C&C

- Rebonds et mouvements latéraux
- Pass the hash
- Cassage de mots de passe
- Etude : Du point d'entrée à la cible finale
- Elévations de privilège
- Étude : Objectif Domain Admin
- Détection/réponse
- Prévention

8 / Persistance

- Nettoyer une infrastructure Windows
- "Ticket d'argent et ticket d'or"
- Les dessous d'Active Directory
- Persistance UNIX/Linux
- Autres moyens employés
- Examen de certification

9 / Réponse à incident et Hunting

- Le SOC
- Outils de réponse :
- Linux
- Windows
- Kansa
- Partons à la chasse :
- Principes de base
- Attaquer pour mieux se défendre :
- Audit « Purple Team »
- Focus : Bloodhound
- ISO 27035
- Aspects légaux

Innov Systems

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

29 Juin au 03 Juil. 2026	Présentiel - Casablanca
24 au 28 Août 2026	Distanciel
19 au 23 Oct. 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

Innov Systems — Tous droits réservés