Détection et Réponse Opérationnelle aux Incidents de Cybersécurité

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

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC294

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

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes fondamentaux de la détection et de la réponse aux incidents dans un environnement complexe
- Concevoir et mettre en œuvre une architecture de détection adaptée aux menaces actuelles
- Identifier, analyser et contenir une compromission à travers des scénarios réels
- Exploiter efficacement les outils de surveillance, d'investigation et de remédiation
- Développer une approche proactive de type "Threat Hunting" pour anticiper les attaques

POUR QUI ?

- Membres de SOC, CSIRT, Blue Team ou cellules de réponse à incident
- Administrateurs systèmes, réseaux ou sécurité souhaitant renforcer leur posture de défense
- Responsables sécurité (RSSI, DSSI) souhaitant piloter un dispositif de détection et réponse

Programme détaillé

1 / INTRODUCTION À LA DÉTECTION MODERNE

- Évolution des menaces et limites des approches préventives
- Les nouvelles logiques de défense : Zero Trust, défense adaptative
- Corrélation entre renseignement sur les menaces et détection

2 / MODÈLES DE CYBERDÉFENSE

- Défense en profondeur revisitée
- NIST, MITRE ATT&CK, Cyber Kill Chain
- L'importance de la visibilité et de la traçabilité

3 / STRUCTURATION DE LA VEILLE ET DU RENSEIGNEMENT

- Notions de CTI (Cyber Threat Intelligence)
- Typologie et hiérarchisation des IOC
- Utilisation de plateformes de partage (MISP, OpenCTI)

4 / ANATOMIE D'UNE ATTAQUE

- Objectifs et stratégies des attaquants
- Étude de scénarios : phishing, exploitation AD, ransomware, exfiltration
- Cartographie des tactiques et techniques (MITRE ATT&CK)

5 / CHAMPS DE BATAILLE ET INDICATEURS DE COMPROMISSION

- Réseau : protocoles, flux, et anomalies
- Systèmes d'exploitation : Windows, Linux
- Active Directory et authentification
- Application et utilisateur final : vecteurs et signaux faibles

6 / RECONSTITUER UNE CHAÎNE D’ATTAQUE

- Corrélation temporelle et événementielle
- Outils de traçabilité et timeline d’incident
- Détection comportementale vs. détection par signature

7 / CONCEPTION D’UNE ARCHITECTURE DE SURVEILLANCE

- Structuration d’une architecture SOC moderne
- Sources de logs et priorisation de la collecte
- Schéma d’intégration SIEM – EDR – NDR – SOAR

8 / JOURNALISATION ET ANALYSE DE LOGS

- Bonnes pratiques de logging sous Windows et Linux
- Utilisation de Sysmon, Auditd et Wazuh
- Corrélation et enrichissement des données dans le SIEM

9 / OUTILS DE DÉTECTION ET D’ANALYSE

- IDS/IPS, WAF, honeypots, sandboxing
- Analyse réseau avec Zeek, Wireshark, Suricata
- Détection d’anomalies et chasse aux signaux faibles

10 / ORGANISATION ET PROCESSUS DE RÉPONSE

- Rôles et responsabilités : SOC, CSIRT, DSI
- Gestion du triage et priorisation des alertes
- Documentation, rapport et communication de crise

11 / OUTILS ET TECHNIQUES DE RÉPONSE

- Scripts et automatisation : PowerShell, Bash, Velociraptor

- Outils d’investigation : GRR, Kansa, TheHive, Cortex
- Gestion des artefacts : mémoire, disque, réseau

12 / CONFINEMENT ET RÉTABLISSEMENT

- Isolement, containment et mitigation
- Analyse post-mortem et leçons apprises
- Maintenir la résilience opérationnelle

13 / PRINCIPES DU THREAT HUNTING

- De la détection réactive à la détection proactive
- Définition d’hypothèses de chasse
- Utilisation d’outils et scripts de hunting (KQL, Sigma, Yara)

14 / EXERCICES "BLUE TEAM LAB"

- Simulation d’incidents réels
- Analyse de logs, reconstruction de scénarios, identification d’IOC
- Collaboration SOC – CSIRT – Threat Intel

15 / APPROCHE PURPLE TEAM ET OPTIMISATION

- Validation et test des mécanismes de détection
- Amélioration continue du SOC : indicateurs et KPIs
- Intégrer la culture de la détection dans la gouvernance sécurité

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 au 31 Juil. 2026	Présentiel - Casablanca
21 au 25 Sep. 2026	Distanciel
16 au 20 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