Détection et Réponse aux Incidents de Cybersécurité - Niveau avancé

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

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC295

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 :

- Concevoir, renforcer et opérer une architecture de détection proactive et résiliente
- Identifier, qualifier et contenir des compromissions à large échelle
- Maîtriser les techniques de traque et d'analyse de compromission (Threat Hunting & DFIR)
- Automatiser les processus de détection et de réponse dans des environnements complexes
- Intégrer la prévention détective dans une approche globale de défense en profondeur

POUR QUI ?

- Analystes SOC et membres de CSIRT
- Administrateurs systèmes et réseaux
- Architectes sécurité
- Responsables sécurité opérationnelle (RSO / RSSI technique)

Programme détaillé

1 / PRINCIPES AVANCÉS DE LA DÉTECTION ET DE LA PRÉVENTION DÉTECTIVE

- Rappel des concepts SOC, CSIRT et DFIR
- Défense en profondeur et approche proactive de détection
- Notion de prévention détective et corrélation avec le renseignement sur la menace

2 / CONSTRUCTION D'UNE INFRASTRUCTURE DE DÉTECTION EFFICACE

- Architecture type d'un SOC moderne : collecteurs, SIEM, EDR, NDR
- Hiérarchisation et corrélation des logs
- Bonnes pratiques de normalisation et d'enrichissement des données (Sysmon, Sigma, YARA)

3 / AUTOMATISATION ET OUTILLAGE DE SUPERVISION

- Introduction à SOAR et intégration dans la chaîne de détection
- Automatisation des alertes et réponse basique
- Gestion des faux positifs et priorisation des incidents

4 / MÉCANISMES DE COMPROMISSION SUR LES SYSTÈMES WINDOWS ET LINUX

- Typologie des persistances (services, tâches planifiées, DLL hijacking, rootkits)
- Analyse des artefacts système et registres
- Utilisation d'outils de détection avancée (Autoruns, WinPrefetchView, Velociraptor)

5 / ANALYSE DES DONNÉES ANTI-VIRUS ET OUTILS D'ENDPOINT

- Exploitation des quarantaines et des journaux d'analyse
- Identification d'activités suspectes malgré la neutralisation
- Corrélation entre événements EDR et indicateurs de compromission (IoC)

6 / DÉTECTION D'EXFILTRATION ET DE MOUVEMENTS LATÉRAUX

- Scénarios de détection de DLP (USB, mail, Cloud)
- Signaux faibles d'un mouvement latéral (RDP, PSExec, WMI, SMB)
- Cas pratique : identification d'un scénario de propagation interne

7 / VISIBILITÉ ET SUPERVISION RÉSEAU

- Captures réseau et analyse avec Zeek, Suricata et Wireshark
- Détection de tunnels et canaux de communication cachés
- Corrélation entre trafic réseau et activité sur les endpoints

8 / CHASSE AUX COMPROMISSIONS (THREAT HUNTING)

- Méthodologie et cycle de la chasse
- Formulation d'hypothèses et recherche d'indices faibles
- Scénario pratique de hunting sur logs EDR et SIEM

9 / INDICATEURS DE COMPROMISSION ET DE COMPORTEMENT

- Construction d'IoC et IoB pertinents
- Validation et intégration dans les outils de détection
- Partage d'information via STIX/TAXII et MITRE ATT&CK

10 / PROCESSUS OPÉRATIONNEL DE RÉPONSE À INCIDENT

- Étapes du cycle DFIR : détection, confinement, éradication, restauration
- Coordination entre équipes SOC, IT et métiers
- Journalisation et traçabilité de la réponse

11 / COLLECTE ET ANALYSE FORENSIQUE À LARGE PARC

- Introduction et mise en œuvre de DFIR-ORC, Velociraptor et GRR Rapid Response
- Déploiement et configuration sur un parc hétérogène

- Analyse des résultats et priorisation des anomalies

12 / GESTION DE CRISE TECHNIQUE ET COMMUNICATION

- Évaluation de l’impact et cartographie des machines compromises
- Gestion de la communication interne/externe en situation de crise
- Retour d’expérience et plan d’amélioration continue

13 / LAB COMPLET : DE LA DÉTECTION À LA RÉPONSE

- Simulation d’un incident complexe (attaque interne + exfiltration)
- Investigation, confinement et remédiation en temps limité
- Débrief collectif et analyse du déroulement

14 / AMÉLIORATION CONTINUE DU SOC ET AUTOMATISATION

- Intégration des retours d’expérience dans la supervision
- Définition des KPI de détection et réponse
- Automatisation avancée via scripts et playbooks SOAR

15 / SYNTHÈSE ET ÉVALUATION FINALE

- Validation des acquis techniques et méthodologiques
- Échanges sur les bonnes pratiques observées
- Élaboration d’un plan d’action individuel post-formation

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