Détection des Menaces et Analyse des Incidents de Sécurité

Lien : https://innov-systems.com/formation/detection-des-menaces-et-analyse-des-incidents-de-securite

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC298

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 fondements techniques et organisationnels de la détection des incidents de sécurité
- Concevoir et optimiser une stratégie de détection adaptée à différents environnements (Windows, Linux, Cloud, Réseau)
- Maîtriser la création, la priorisation et l'automatisation des alertes de sécurité
- Développer des compétences d'investigation et de chasse proactive (threat hunting)
- Intégrer la détection dans le cycle complet de la réponse aux incidents

POUR QUI ?

- Analystes SOC de niveau 2 et 3
- Responsables de la détection et de la réponse aux incidents
- Membres d'équipes CSIRT ou Blue Team
- Ingénieurs cybersécurité impliqués dans la supervision et la corrélation des événements

Programme détaillé

1 / INTRODUCTION À LA DÉTECTION ET AUX STRUCTURES SOC

- Rôle de la détection dans le cycle de vie de la cybersécurité
- Organisation type d'un SOC et interactions avec les autres pôles (CSIRT, Threat Intel, Red Team)
- Typologie des menaces et classification des incidents

2 / SOURCES DE DONNÉES ET CHAÎNE DE DÉTECTION

- Identification et catégorisation des sources de logs
- Journalisation et normalisation des événements
- Bonnes pratiques de collecte et d'enrichissement des données

3 / STRUCTURATION DU SYSTÈME DE DÉTECTION

- Conception d'une architecture de détection adaptée à son environnement
- Règles de corrélation et contextualisation des événements
- Métriques de performance et qualité des alertes

4 / CADRES DE RÉFÉRENCE ET MÉTHODOLOGIES

- MITRE ATT&CK, Cyber Kill Chain et Pyramide of Pain
- Détection de menace connue vs inconnue
- Construction d'une base de connaissances de détection (Detection Engineering)

5 / AUTHENTIFICATION ET VOL D'IDENTIFIANTS

- Analyse des journaux d'authentification : AD, Kerberos, NTLM, LSASS
- Techniques de détection des attaques par vol de jetons ou de mots de passe (Mimikatz, Pass-the-Hash)
- Règles Sysmon et Event ID critiques à surveiller

6 / DÉTECTION DES TECHNIQUES DE LATERALISATION

- RDP, SMB, WMI, PSRemoting : mécanismes et indicateurs de compromission
- Détection des déplacements internes et traçabilité réseau
- Corrélation entre logs Windows, réseau et EDR

7 / PERSISTANCE ET ÉLÉVATION DE PRIVILÈGES

- Surveillance des modifications clés du registre, services et tâches planifiées
- Détection des élévations de privilèges : analyse des SIDs, niveaux d'intégrité, tokens
- Étude de cas pratique sur la persistance à l'aide de Sysmon et Sigma

8 / DÉTECTION DES COMPROMISSIONS LINUX

- Outils et logs : auditd, journald, syslog
- Détection des anomalies de comptes, processus, fichiers et permissions
- Exploitation des solutions Wazuh et OSSEC

9 / SURVEILLANCE DU RÉSEAU ET DÉTECTION COMPORTEMENTALE

- Détection de scans, beaconing et flux suspects
- Analyse de trafic HTTP, DNS et HTTPS sortant
- Introduction à la Network Threat Hunting

10 / INDICATEURS DE COMPROMISSION ET AUTOMATISATION

- Structuration des IOC et IOA
- Utilisation des plateformes SIEM/SOAR pour la corrélation automatique
- Enrichissement contextuel avec la Threat Intelligence

11 / DÉTECTION DANS LE CLOUD

- Spécificités de la journalisation sur Azure, AWS et Google Cloud
- Surveillance des API, IAM et comportements anormaux

- Mise en œuvre de détections multi-cloud et gestion des logs centralisés

12 / DÉTECTION DANS LES ENVIRONNEMENTS OT ET IOT

- Particularités des systèmes industriels et objets connectés
- Identification des menaces typiques : sabotage, accès non autorisé, exfiltration
- Bonnes pratiques pour corréler IT et OT dans un SOC hybride

13 / CAS PRATIQUE INTÉGRÉ

- Atelier de création de règles de détection cross-environnement
- Simulation d'un incident multi-système et analyse d'alertes
- Rapport d'investigation et recommandations d'amélioration

14 / PROCESSUS D'INVESTIGATION D'UNE ALERTE

- Méthodologie d'analyse et outils de pivotement
- Analyse de chronologie et reconstruction d'incident
- Validation, priorisation et documentation des résultats

15 / CHASSE PROACTIVE ET THREAT HUNTING

- Élaboration d'hypothèses de chasse
- Utilisation des frameworks (Sigma, YARA, KQL)
- Retours d'expérience et pièges à éviter

16 / AUTOMATISATION ET INDUSTRIALISATION DE LA DÉTECTION

- Intégration avec SOAR : orchestration et playbooks
- Détection pilotée par les données (Machine Learning, Anomaly Detection)
- Bonnes pratiques d'amélioration continue

17 / ÉVALUATION FINALE ET PRÉPARATION À LA CERTIFICATION

- Quiz de validation des acquis
- Étude de cas finale avec investigation complète
- Synthèse, bilan et plan de montée en maturité du SOC

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

03 au 07 Août 2026	Présentiel - Casablanca
28 Sep. au 02 Oct. 2026	Distanciel
23 au 27 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