Threat Hunting proactif : techniques MITRE ATT&CK et chasse aux menaces persistantes (APT)

Lien : https://innov-systems.com/formation/threat-hunting-proactif-techniques-mitre-attck-et-chasse-aux-menaces-persistantes-apt

DURÉE
5 jours (35h)

RÉFÉRENCE
SI95

CATÉGORIE
Cyber Threat Intelligence (CTI)

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes du threat hunting proactif
- Identifier les comportements associés aux APT
- Exploiter le framework MITRE ATT&CK pour structurer les investigations
- Développer des hypothèses de chasse aux menaces
- Utiliser les données SIEM/EDR pour détecter des activités malveillantes
- Détecter les techniques d’évasion et de persistance
- Améliorer la visibilité sur les environnements IT et cloud
- Réduire le temps de détection des attaques avancées
- Renforcer les capacités de réponse aux incidents
- Développer une approche structurée de la chasse aux menaces
- Corréler intelligence de menace et logs techniques
- Étudier des cas réels d’attaques APT

POUR QUI ?

- Threat hunters
- Analystes SOC
- Ingénieurs cybersécurité
- Blue team engineers
- Incident responders
- Architectes sécurité
- Consultants cybersécurité
- Ingénieurs SIEM/EDR
- Responsables SOC
- RSSI / CISO
- Analysts Threat Intelligence
- Toute personne impliquée dans la détection avancée des menaces et la cybersécurité opérationnelle

Innov Systems

Programme détaillé

1 / Introduction au Threat Hunting proactif

- Définition et rôle du threat hunting dans la cybersécurité moderne
- Différence entre détection réactive et chasse proactive
- Typologie des menaces avancées (APT)

2 / Fondamentaux des APT (Advanced Persistent Threats)

- Cycle de vie d’une attaque APT
- Techniques de persistance et d’évasion
- Objectifs des groupes de menaces avancées

3 / Framework MITRE ATT&CK

- Structure et organisation du framework
- Tactiques, techniques et procédures (TTPs)
- Utilisation pour la modélisation des menaces

4 / Hypothèse de chasse (hypothesis-driven hunting)

- Construction d’hypothèses de compromission
- Identification des comportements suspects
- Méthodologie de priorisation des hunts

5 / Collecte et exploitation des données de sécurité

- Logs endpoints, réseau et cloud
- SIEM, EDR et telemetry data
- Normalisation et corrélation des événements

Innov Systems

6 / Techniques de détection avancées

- Détection comportementale (behavioral analytics)
- Indicators of Compromise (IOC) et Indicators of Attack (IOA)
- Analyse des anomalies et déviations

7 / Analyse des techniques adverses

- Mapping des TTPs sur MITRE ATT&CK
- Détection des mouvements latéraux
- Identification des techniques d’évasion

8 / Outils de Threat Hunting

- SIEM (Splunk, Elastic, Sentinel)
- EDR/XDR (CrowdStrike, Defender for Endpoint)
- Plateformes de threat intelligence

9 / Réponse et remédiation

- Escalade des incidents détectés
- Collaboration avec SOC et Blue Team
- Durcissement des systèmes compromis

10 / Cas pratiques et scénarios APT

- Simulation de compromission avancée
- Chasse aux menaces dans un environnement réel
- Retours d’expérience et amélioration continue

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

08 au 12 Fév. 2027	Présentiel - Casablanca
05 au 09 Avr. 2027	Présentiel - Casablanca
31 Mai au 04 Juin 2027	Présentiel - Casablanca
26 au 30 Juil. 2027	Présentiel - Casablanca
20 au 24 Sep. 2027	Présentiel - Casablanca

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