MITRE ATT&CK pour les infrastructures réseau threat-informed defense

Lien : https://innov-systems.com/formation/mitre-attck-pour-les-infrastructures-reseau-threat-informed-defense

DURÉE
5 jours (35h)

RÉFÉRENCE
SI61

CATÉGORIE
Cyber Threat Intelligence (CTI)

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre le framework MITRE ATT&CK
- Appliquer une défense basée sur les menaces
- Cartographier les attaques sur les infrastructures réseau
- Améliorer la détection des cyberattaques
- Identifier les techniques adverses en environnement réel
- Structurer une stratégie de cybersécurité défensive
- Intégrer MITRE ATT&CK dans les outils SIEM/SOAR
- Développer des capacités de threat hunting
- Réduire la surface d’attaque réseau
- Améliorer la réponse aux incidents
- Analyser des scénarios d’attaques réels
- Étudier des cas concrets de cybersécurité offensive et défensive

POUR QUI ?

- Ingénieurs cybersécurité
- SOC analysts
- Threat hunters
- RSSI
- Architectes sécurité
- Administrateurs réseaux
- DevSecOps engineers
- Consultants cybersécurité
- Pentesters
- Analystes SOC junior et senior
- Toute personne impliquée dans la défense des infrastructures réseau

Innov Systems

Programme détaillé

1 / Introduction à MITRE ATT&CK et à la threat-informed defense

- Présentation du framework MITRE ATT&CK
- Concept de défense basée sur les menaces (threat-informed)
- Importance pour la cybersécurité moderne

2 / Structure du framework MITRE ATT&CK

- Tactiques, techniques et sous-techniques
- Chaîne d’attaque (kill chain) moderne
- Cartographie des comportements adverses

3 / Application à l’infrastructure réseau

- Surface d’attaque réseau
- Mapping des techniques sur les couches réseau
- Identification des vecteurs d’intrusion

4 / Reconnaissance et accès initial

- Techniques de reconnaissance réseau
- Exploitation des services exposés
- Compromission initiale des systèmes

5 / Exécution et persistance

- Techniques d’exécution à distance
- Maintien de l’accès sur le réseau
- Mécanismes de persistance

Innov Systems

6 / Escalade de privilèges et mouvement latéral

- Techniques d’élévation de privilèges
- Propagation dans le réseau interne
- Exploitation des relations de confiance

7 / Command and Control (C2)

- Communications malveillantes
- Canaux de contrôle réseau
- Techniques d’évasion du trafic

8 / Détection et mitigation des attaques

- Cartographie des techniques de défense
- Détection basée sur MITRE ATT&CK
- Réduction de la surface d’attaque

9 / Intégration dans les outils de sécurité

- SIEM et SOAR compatibles MITRE
- Threat hunting basé sur ATT&CK
- Automatisation de la détection

10 / Études de cas et mise en pratique

- Analyse d’attaques réelles via ATT&CK
- Construction d’un plan de défense réseau
- Bonnes pratiques de threat-informed defense

Inov 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

25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 2027	Présentiel - Casablanca
06 au 10 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