Cyber Threat Intelligence (CTI) : anticipez et analysez les menaces cyber avancées

Lien : https://innov-systems.com/formation/cyber-threat-intelligence-cti-anticipez-et-analysez-les-menaces-cyber-avancees

DURÉE
5 jours (35h)

RÉFÉRENCE
SI09

CATÉGORIE
Cyber Threat Intelligence (CTI)

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les fondamentaux du Cyber Threat Intelligence
- Maîtriser le cycle du renseignement en cybersécurité
- Identifier et analyser les menaces cyber émergentes
- Exploiter les sources OSINT et autres sources de données
- Utiliser les indicateurs de compromission (IOC)
- Cartographier les acteurs et techniques d’attaque
- Intégrer le CTI dans une stratégie de cybersécurité
- Améliorer la détection et la réponse aux incidents
- Utiliser les outils et plateformes de threat intelligence
- Développer une approche proactive de la cybersécurité

POUR QUI ?

- Analystes SOC
- Responsables cybersécurité (RSSI)
- Ingénieurs sécurité informatique
- Administrateurs systèmes et réseaux
- Experts en cyberdéfense
- Analystes threat intelligence
- Toute personne impliquée dans la protection des systèmes d’information

Innov Systems

Programme détaillé

1 / Introduction au Cyber Threat Intelligence (CTI)

- Définition et principes fondamentaux du CTI
- Rôle du renseignement dans la cybersécurité
- Différence entre CTI, cybersécurité et SOC

2 / Cycle du renseignement en cybersécurité

- Collecte des données (collection)
- Analyse et traitement de l'information
- Diffusion des intelligence reports

3 / Types de Threat Intelligence

- Intelligence stratégique
- Intelligence opérationnelle
- Intelligence tactique et technique

4 / Sources de renseignement (OSINT et autres)

- Open Source Intelligence (OSINT)
- Sources internes et externes
- Dark web et forums spécialisés

5 / Indicateurs de compromission (IOC)

- Définition des IOC
- Types d'indicateurs (IP, hashes, domaines)
- Utilisation dans la détection des attaques

Innov Systems

6 / Analyse des menaces et des acteurs

- Profilage des groupes cybercriminels
- TTP (Tactics, Techniques, Procedures)
- Cartographie des menaces

7 / Outils et plateformes CTI

- SIEM et plateformes de threat intelligence
- Outils d’analyse automatisée
- Bases de données de menaces

8 / Intégration du CTI dans une organisation

- Intégration dans un SOC
- Collaboration entre équipes sécurité
- Automatisation des flux de renseignement

9 / Détection et réponse aux menaces

- Utilisation du CTI pour la détection proactive
- Amélioration des réponses aux incidents
- Réduction du temps de réaction

10 / Cas pratiques et scénarios d’attaque

- Analyse de campagnes de cyberattaques réelles
- Études de cas CTI
- Simulation de réponse à menace avancée

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