

Cyber Threat Intelligence (CTI) : collecte, analyse et exploitation du renseignement sur les menaces

Lien : https://innov-maroc.com/formation/cyber-threat-intelligence-cti-collecte-analyse-et-exploitation-du-renseignement-sur-les-menaces

DURÉE
5 jours (35h)

RÉFÉRENCE
SI94

CATÉGORIE
Cyber Threat Intelligence (CTI)

INNOV MAROC

🎯 OBJECTIFS DE LA FORMATION

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

- ✔ Comprendre les principes fondamentaux du Cyber Threat Intelligence
- ✔ Identifier et exploiter les sources de renseignement sur les menaces
- ✔ Mettre en place un cycle CTI complet en entreprise
- ✔ Analyser et corréler les données de sécurité multi-sources
- ✔ Utiliser les frameworks CTI (MITRE ATT&CK, STIX/TAXII)
- ✔ Améliorer les capacités de détection des menaces
- ✔ Intégrer le CTI dans les opérations SOC
- ✔ Automatiser la collecte et l’enrichissement des données de sécurité
- ✔ Produire des rapports exploitables pour les équipes techniques et direction
- ✔ Anticiper les attaques grâce à l’intelligence proactive
- ✔ Renforcer la posture de cybersécurité globale
- ✔ Étudier des cas concrets de menaces cyber

INNOV MAROC

👥 POUR QUI ?

- ✔ Analystes SOC
- ✔ Cyber Threat Intelligence Analysts
- ✔ Ingénieurs cybersécurité
- ✔ Threat hunters
- ✔ Pentesters et Red Teamers
- ✔ RSSI / CISO
- ✔ Architectes sécurité
- ✔ Consultants cybersécurité
- ✔ Ingénieurs SIEM/SOAR
- ✔ Data analysts sécurité
- ✔ Forces de défense cyber
- ✔ Toute personne impliquée dans la détection et l’analyse des menaces cyber



Programme détaillé

1 / Introduction au Cyber Threat Intelligence (CTI)

- Définition et rôle du renseignement sur les menaces
- Différences entre données, information et intelligence
- Cycle de vie du Threat Intelligence

2 / Typologie des Threat Intelligence

- Strategic, Tactical, Operational et Technical Intelligence
- Cas d’usage selon les niveaux organisationnels
- Alignement avec les besoins métiers et sécurité

3 / Sources de collecte du renseignement

- Open Source Intelligence (OSINT)
- Threat feeds et bases de données de vulnérabilités
- Logs internes, SIEM et données SOC

4 / Techniques de collecte et d’ingestion des données

- Automatisation de la collecte (APIs, scrapers, feeds)
- Normalisation et enrichissement des données
- Stockage et structuration des indicateurs (IoC)

INNOV MAROC

5 / Analyse des menaces et corrélation

- Identification des patterns d’attaque
- Analyse des campagnes cybercriminelles
- Corrélation multi-sources et contextualisation

6 / Frameworks et standards CTI

- MITRE ATT&CK
- STIX/TAXII
- Diamond Model et Kill Chain

7 / Indicateurs de compromission (IoC) et détection

- Hashes, IPs, domaines et signatures
- Intégration des IoC dans les outils de sécurité
- Détection proactive des menaces

8 / Exploitation du renseignement dans le SOC

- Intégration avec SIEM et SOAR
- Amélioration des règles de détection
- Automatisation de la réponse aux incidents

9 / Production de rapports de Threat Intelligence

- Création de rapports stratégiques et techniques
- Communication avec les équipes métiers et direction
- Visualisation des menaces et tableaux de bord

10 / Cas pratiques et mise en situation CTI

- Analyse d’une campagne d’attaque réelle
- Construction d’un pipeline CTI complet

INOV MAROC

- Bonnes pratiques et retour d’expérience

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

12 au 18 Jan. 2027	Présentiel - Casablanca
08 au 12 Mars 2027	Présentiel - Casablanca
03 au 07 Mai 2027	Présentiel - Casablanca
28 Juin au 02 Juil. 2027	Présentiel - Casablanca
23 au 27 Août 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-maroc.com
Web : https//www.innov-maroc.com

INNOV MAROC

INNOV MAROC — Tous droits réservés