

Ransomware : comprendre, anticiper et se défendre contre la cybermenace

Lien : https://innov-maroc.com/formation/ransomware-comprendre-anticiper-et-se-defendre-contre-la-cybermenace

DURÉE
5 jours (35h)

RÉFÉRENCE
SI47

CATÉGORIE
Fondamentaux
Sécurité Informatique

INNOV MAROC

🎯 OBJECTIFS DE LA FORMATION

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

- ✔ Comprendre le fonctionnement des ransomwares
- ✔ Identifier les différentes formes de cyberattaques par ransomware
- ✔ Reconnaître les techniques d’infection utilisées par les attaquants
- ✔ Évaluer les risques et impacts pour une organisation
- ✔ Mettre en place des mesures de prévention efficaces
- ✔ Détecter les signes d’une attaque en cours
- ✔ Savoir réagir face à un incident de cybersécurité
- ✔ Protéger les données sensibles et les systèmes d’information
- ✔ Développer une culture de cybersécurité en entreprise
- ✔ Élaborer une stratégie globale de défense contre les ransomwares

👥 POUR QUI ?

- ✔ Responsables informatiques
- ✔ Administrateurs systèmes et réseaux
- ✔ Responsables cybersécurité (RSSI)
- ✔ Techniciens IT
- ✔ Chefs de projet informatique
- ✔ Dirigeants et managers d’entreprise
- ✔ Responsables conformité et risques
- ✔ Toute personne impliquée dans la sécurité des systèmes d’information

INNOV MAROC



Programme détaillé

1 / Introduction aux ransomwares

- Définition et principes de fonctionnement
- Évolution des attaques dans le temps
- Impacts sur les organisations

2 / Typologie des ransomwares

- Ransomware chiffrant (crypto-ransomware)
- Ransomware bloqueur (locker)
- Modèles RaaS (Ransomware as a Service)

3 / Chaîne d’attaque d’un ransomware

- Phases d’intrusion et d’exécution
- Techniques de propagation
- Persistance dans le système

4 / Techniques d’infection utilisées

- Phishing et ingénierie sociale
- Exploitation de failles logicielles
- Téléchargements malveillants et USB infectés

INNOV MAROC

5 / Cibles et motivations des attaquants

- Entreprises et institutions visées
- Secteurs les plus exposés
- Motivations financières et stratégiques

6 / Conséquences d’une attaque ransomware

- Blocage des systèmes d’information
- Perte et vol de données
- Impacts financiers et juridiques

7 / Détection des comportements suspects

- Signaux faibles d’infection
- Outils de détection et monitoring
- Analyse des logs et alertes

8 / Prévention et protection des systèmes

- Bonnes pratiques de cybersécurité
- Gestion des sauvegardes (backup)
- Mise à jour et durcissement des systèmes

9 / Réponse à incident et gestion de crise

- Procédures en cas d’attaque
- Isolement des systèmes infectés
- Communication de crise et coordination

10 / Stratégies globales de cybersécurité

- Mise en place d’une politique de sécurité
- Sensibilisation des utilisateurs

INNOV MAROC

- Plan de continuité d’activité (PCA)

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

07 au 11 Déc. 2026	Présentiel - Casablanca
01 au 05 Fév. 2027	Présentiel - Casablanca
29 Mars au 02 Avr. 2027	Présentiel - Casablanca
24 au 28 Mai 2027	Présentiel - Casablanca
19 au 23 Juil. 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 — Tous droits réservés