Rançongiciels : défense et récupération efficaces

Durée: 1 jour
Public cible: Professionnel TI

À qui s'adresse cette formation ?

- Équipes de sécurité
- Directeurs TI
- RSSI
- Gestionnaires de continuité des affaires

Objectifs de la formation

- Comprendre les méthodes et impacts des rançongiciels
- Mettre en œuvre des stratégies de prévention et de sensibilisation
- Développer des plans de récupération et de continuité
- Tirer des leçons des cas réels pour renforcer la résilience

Description sommaire

Cette formation pratique outille les participantes et participants pour prévenir, détecter et se remettre d'attaques par rançongiciel. À travers des cas concrets, les apprenantes et apprenants développeront des capacités de défense et de résilience.

Contenu du plan de cours

Module 1 : Comprendre les rançongiciels

- Historique et évolution
- Vecteurs et techniques d'attaque
- Impacts opérationnels et financiers

Module 2 : Stratégies de prévention

- Défense des terminaux et réseaux
- Planification des sauvegardes et récupération

- Formation et sensibilisation des utilisateurs

Module 3 : Détection et réponse

- Indicateurs de compromission
- Playbooks de réponse aux incidents
- Considérations légales et forensiques

Module 4 : Récupération et amélioration continue

- Planification de la continuité et reprise après sinistre
- Études de cas : attaques majeures
- Renforcer la résilience organisationnelle

Approche et méthode pédagogique

Études de cas pratiques, simulation d'incidents, discussion collaborative

Prérequis

Connaissances générales en cybersécurité

Recommandations

Réviser : les bases de la cybersécurité les types de menaces informatiques (malwares, phishing)

Se familiariser avec : les environnements TI et leurs vulnérabilités

Identifier vos enjeux : protection contre les rançongiciels continuité des activités récupération après incident