Cybersécurité opérationnelle : détectez, prévenez et réagissez aux attaques numériques

Lien : https://innov-systems.com/formation/cybersecurite-operationnelle-detectez-prevenez-et-reagissez-aux-attaques-numeriques

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SI13**	**SIEM, SOC et LogPoint**

OBJECTIFS DE LA FORMATION

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

- Comprendre les risques liés à la cybermalveillance
- Identifier les principales menaces numériques
- Adopter les bonnes pratiques de cybersécurité
- Protéger les systèmes et les données
- Détecter et réagir face à une cyberattaque
- Sensibiliser les utilisateurs aux risques
- Respecter les exigences réglementaires
- Mettre en place une stratégie de sécurité efficace

Innov Systems

POUR QUI ?

- Collaborateurs en entreprise
- Responsables informatiques
- Responsables sécurité (RSSI)
- Managers et dirigeants
- Administrateurs systèmes et réseaux
- Toute personne utilisant des outils numériques

Innov Systems

Programme détaillé

1 / Introduction à la cybermalveillance

- Définition et typologie des cybermenaces
- Panorama des attaques (phishing, ransomware, malware)
- Enjeux pour les organisations et les individus

2 / Écosystème des cyberattaques

- Acteurs de la cybercriminalité
- Motivations (financières, espionnage, sabotage)
- Modes opératoires des attaquants

3 / Les principales vulnérabilités

- Failles humaines (ingénierie sociale)
- Vulnérabilités techniques
- Mauvaises pratiques numériques

4 / Sécurité des postes de travail

- Protection des ordinateurs et mobiles
- Antivirus et mises à jour
- Bonnes pratiques d’utilisation

5 / Sécurité des réseaux et des systèmes

- Notions de pare-feu et segmentation réseau
- Accès sécurisé (VPN, authentification)
- Surveillance des systèmes

Innov Systems

6 / Protection des données

- Confidentialité, intégrité, disponibilité (CIA)
- Chiffrement des données
- Sauvegardes et reprise d’activité

7 / Phishing et ingénierie sociale

- Reconnaître les tentatives de fraude
- Techniques utilisées par les attaquants
- Réflexes de sécurité

8 / Gestion des incidents de sécurité

- Détection des incidents
- Procédures de réponse
- Plan de gestion de crise

9 / Sensibilisation et formation des utilisateurs

- Culture cybersécurité
- Campagnes de sensibilisation
- Comportements à adopter

10 / Cadre réglementaire et conformité

- RGPD et protection des données
- Obligations des entreprises
- Normes et référentiels (ISO 27001)

11 / Outils et solutions de cybersécurité

- Solutions de protection (EDR, SIEM)
- Outils de détection des menaces

Innov Systems

- Tableaux de bord de sécurité

12 / Bonnes pratiques et stratégie globale

- Mise en place d’une politique de sécurité
- Amélioration continue
- Anticipation des menaces futures

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.

Innov Systems

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés