Détecter et réagir aux cyberattaques : maîtrisez la réponse aux incidents de cybersécurité

Lien : https://innov-systems.com/formation/detecter-et-reagir-aux-cyberattaques-maitrisez-la-reponse-aux-incidents-de-cybersecurite

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SI14**	**SIEM, SOC et LogPoint**

OBJECTIFS DE LA FORMATION

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

- Comprendre les principaux types de cyberattaques
- Identifier les signes d’une compromission informatique
- Maîtriser les outils de détection des menaces
- Réagir efficacement face à un incident de cybersécurité
- Mettre en œuvre des procédures de réponse aux attaques
- Sécuriser les systèmes et infrastructures informatiques
- Analyser les incidents de sécurité après une attaque
- Renforcer la résilience des systèmes d’information
- Élaborer des plans de continuité et de reprise d’activité

Innov Systems

POUR QUI ?

- Analystes SOC (Security Operations Center)
- Administrateurs systèmes et réseaux
- Ingénieurs cybersécurité
- Responsables IT et RSSI
- Techniciens support informatique
- Responsables infrastructures IT
- Toute personne impliquée dans la sécurité des systèmes d’information

Innov Systems

Programme détaillé

1 / Introduction aux cyberattaques modernes

- Types de menaces (malware, phishing, ransomware)
- Acteurs de la menace (hackers, groupes organisés)
- Enjeux de la cybersécurité

2 / Principes fondamentaux de la cybersécurité

- Confidentialité, intégrité, disponibilité (CIA)
- Surface d’attaque et vulnérabilités
- Notions de risque cyber

3 / Techniques de détection des cyberattaques

- Surveillance des systèmes
- Logs et événements de sécurité
- Outils SIEM et IDS/IPS

4 / Analyse des comportements suspects

- Détection d’anomalies
- Indicateurs de compromission (IOC)
- Corrélation des événements

5 / Réponse aux incidents de sécurité

- Procédures de gestion d’incident
- Isolation des systèmes compromis
- Communication de crise

Innov Systems

6 / Gestion des ransomwares et malware

- Modes d’infection
- Techniques de propagation
- Plans de réponse rapide

7 / Sécurisation des systèmes et réseaux

- Durcissement des systèmes (hardening)
- Segmentation réseau
- Contrôle des accès

8 / Outils et technologies de cybersécurité

- Firewalls et EDR
- Solutions de monitoring
- Outils d’analyse forensic

9 / Analyse post-incident

- Investigation numérique (forensic)
- Identification des causes racines
- Rapport d’incident

10 / Plan de continuité et amélioration

- PCA/PRA (plan de continuité et reprise)
- Retours d’expérience
- Renforcement des défenses

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

07 au 11 Déc. 2026	Présentiel - Casablanca
25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 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-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés