Cyber Crisis Management : exercices de crise, communication et résilience opérationnelle

Lien : https://innov-systems.com/formation/cyber-crisis-management-exercices-de-crise-communication-et-resilience-operationnelle

DURÉE	RÉFÉRENCE	CATÉGORIE
4 jours (28h)	**SI104**	**ISO 22301**

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les mécanismes de gestion d’une crise cyber
- Mettre en place une organisation efficace de réponse aux incidents
- Développer des plans de continuité et de reprise d’activité
- Concevoir et exécuter des exercices de crise réalistes
- Améliorer la communication interne et externe en situation critique
- Renforcer la résilience opérationnelle de l’entreprise
- Structurer les processus de détection et d’escalade des incidents
- Utiliser les outils de gestion de crise et de sécurité
- Réduire l’impact des cyberattaques sur les activités métiers
- Développer une culture de préparation et de résilience
- Optimiser la coordination entre équipes techniques et direction
- Étudier des cas concrets de gestion de crises cyber

POUR QUI ?

- RSSI / CISO
- Responsables IT et infrastructure
- SOC managers et analysts
- Ingénieurs cybersécurité
- Crisis managers et risk managers
- Responsables PCA/PRA
- Consultants en cybersécurité
- Responsables communication de crise
- Architectes sécurité
- DevSecOps engineers
- Direction générale et décideurs IT
- Toute personne impliquée dans la gestion des incidents et crises cyber

Innov Systems

Programme détaillé

1 / Introduction à la gestion de crise cyber

- Définition d’une crise cyber et typologies d’incidents
- Impact sur les opérations, la réputation et la continuité métier
- Rôle de la gestion de crise dans la cybersécurité globale

2 / Organisation d’une cellule de crise (Crisis Management Team)

- Composition et rôles des équipes de crise
- Gouvernance décisionnelle en situation critique
- Coordination entre IT, sécurité, juridique et direction

3 / Détection et qualification des incidents

- Identification des signaux faibles et alertes
- Criticité et classification des incidents
- Escalade et déclenchement du plan de crise

4 / Plans de réponse aux incidents

- Procédures de containment, éradication et récupération
- Gestion des ransomwares et attaques majeures
- Playbooks de réponse automatisés et manuels

5 / Continuité d’activité et résilience opérationnelle

- PCA (Plan de Continuité d’Activité)
- PRA (Plan de Reprise d’Activité)
- Stratégies de résilience multi-sites et cloud

Innov Systems

6 / Exercices de crise et simulations

- Tabletop exercises (exercices sur table)
- Simulation de cyberattaques réalistes
- Tests de coordination inter-équipes

7 / Communication de crise

- Communication interne (direction, employés)
- Communication externe (clients, médias, régulateurs)
- Gestion de la réputation et transparence

8 / Outils et technologies de gestion de crise

- SIEM et SOAR pour la détection et réponse
- Plateformes de gestion d’incidents
- Outils de collaboration en situation de crise

9 / Retour d’expérience et amélioration continue

- Post-mortem et analyse des incidents
- Identification des failles organisationnelles
- Mise à jour des plans de crise et procédures

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

01 au 04 Déc. 2026	Distanciel
12 au 15 Jan. 2027	Présentiel - Casablanca
09 au 12 Mars 2027	Présentiel - Casablanca
04 au 07 Mai 2027	Présentiel - Casablanca
29 Juin au 02 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

Innov Systems