GESTION D'UNE CYBERCRISE

Lien : https://innov-systems.com/formation/gestion-dune-cybercrise

DURÉE	RÉFÉRENCE	CATÉGORIE
4 jours (28h)	**SEC329**	**Sécurité du SI**

OBJECTIFS DE LA FORMATION

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

- Comprendre les enjeux et les spécificités d'une cybercrise
- Savoir identifier, déclencher et gérer une cellule de crise cyber
- Être capable de structurer une réponse organisationnelle cohérente
- Mettre en œuvre les bonnes pratiques en communication de crise
- Respecter les obligations juridiques et réglementaires en cas d’incident
- Savoir coopérer avec les partenaires internes et externes
- Connaître les outils et processus pour la continuité et le redémarrage
- Réaliser un retour d’expérience structuré pour améliorer la résilience
- Expérimenter la gestion d’une cybercrise via un exercice immersif
- Développer une posture professionnelle adaptée en situation de stress extrême
- Contribuer à la mise à jour des plans de réponse à incident et PRA/PCA

Innov Systems

POUR QUI ?

- Dirigeants d’entreprise et membres du COMEX
- Responsables de la sécurité des systèmes d’information (RSSI)
- Directeurs des systèmes d’information (DSI)
- Responsables des risques, de la conformité ou du juridique
- Responsables de la communication de crise
- Responsables métiers exposés à la continuité d’activité
- Responsables des ressources humaines impliqués dans la gestion de crise
- Équipes informatiques en charge de la réponse aux incidents
- Responsables des assurances et gestionnaires de sinistres cyber

Innov Systems

Programme détaillé

1 / Comprendre les fondamentaux de la cybersécurité et des cybermenaces

- Identifier les types de menaces : malware, ransomware, phishing
- Comprendre les vulnérabilités internes et externes
- Analyser les principales failles de sécurité dans les systèmes d'information

2 / Définir ce qu'est une cybercrise et ses spécificités

- Distinguer incident, crise et catastrophe numérique
- Identifier les déclencheurs typiques d’une cybercrise
- Comprendre les impacts sur l’organisation

3 / Mettre en place une gouvernance de gestion de crise

- Définir les rôles et responsabilités en situation de crise
- Structurer une cellule de crise cyber
- Mettre en place un processus décisionnel rapide

4 / Évaluer les risques et préparer le plan de réponse

- Réaliser une cartographie des risques cyber
- Élaborer un plan de réponse à incident (PRI)
- Identifier les ressources et outils nécessaires à la réponse

5 / Réagir efficacement aux premiers signaux de crise

- Détecter et qualifier l’incident
- Activer la cellule de crise en temps opportun
- Coordonner les premières mesures d’endiguement

Innov Systems

6 / Organiser la communication de crise

- Communiquer avec les parties prenantes internes
- Gérer la relation avec les médias et le public
- Construire des éléments de langage cohérents et factuels

7 / Gérer les aspects juridiques et réglementaires

- Connaître les obligations légales en cas de cyberattaque
- Gérer les notifications à la CNDP/CNIL ou autres autorités
- Protéger les preuves numériques et assurer la traçabilité

8 / Mobiliser les partenaires externes de la réponse à crise

- Collaborer avec les prestataires techniques et experts forensics
- Engager les assurances cyber et avocats spécialisés
- Coopérer avec les autorités judiciaires et les CERT

9 / Reprendre l'activité et assurer la continuité

- Mettre en œuvre les procédures de PRA/PCA
- Redémarrer les systèmes en environnement sécurisé
- Assurer la continuité métier prioritaire

10 / Réaliser un retour d'expérience (REX) après la crise

- Documenter les événements et décisions
- Identifier les forces et faiblesses de la réponse
- Mettre à jour les procédures et plans

11 / Simuler une cybercrise : exercice de mise en situation

- Mettre en œuvre une cellule de crise fictive
- Gérer une crise en temps contraint avec montée en charge

Inov Systems

- Produire un débriefing collectif et individuel
- Dirigeants d’entreprise et membres du COMEX
- Responsables de la sécurité des systèmes d’information (RSSI)
- Directeurs des systèmes d’information (DSI)
- Responsables des risques, de la conformité ou du juridique
- Responsables de la communication de crise
- Responsables métiers exposés à la continuité d’activité
- Responsables des ressources humaines impliqués dans la gestion de crise
- Équipes informatiques en charge de la réponse aux incidents
- Consultants en cybersécurité et gestion des risques
- Responsables des assurances et gestionnaires de sinistres cyber

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	Présentiel - Casablanca
16 au 19 Fév. 2027	Présentiel - Casablanca
13 au 16 Avr. 2027	Présentiel - Casablanca
08 au 11 Juin 2027	Présentiel - Casablanca
03 au 06 Août 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

Innov Systems