Sensibilisation cybersécurité avancée pour dirigeants et membres de COMEX

Lien : https://innov-systems.com/formation/sensibilisation-cybersecurite-avancee-pour-dirigeants-et-membres-de-comex

DURÉE
4 jours (28h)

RÉFÉRENCE
SI106

CATÉGORIE
Sécurité Organisationnelle

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les enjeux stratégiques de la cybersécurité pour les dirigeants
- Identifier les principales menaces ciblant les COMEX
- Appréhender les responsabilités légales et organisationnelles des dirigeants
- Savoir réagir efficacement en cas de crise cyber
- Intégrer la cybersécurité dans la stratégie d’entreprise
- Évaluer les risques business liés aux cyberattaques
- Renforcer la résilience organisationnelle face aux incidents
- Améliorer la prise de décision en situation de crise
- Développer une culture de cybersécurité au niveau exécutif
- Optimiser les investissements en cybersécurité
- Anticiper les risques liés à l’ingénierie sociale avancée
- Étudier des cas concrets de cyberattaques ciblant les dirigeants

POUR QUI ?

- Membres de COMEX
- Directeurs généraux (CEO)
- Directeurs financiers (CFO)
- Directeurs des systèmes d’information (CIO / CTO)
- Directeurs juridiques et conformité
- Responsables risques
- Administrateurs de grandes entreprises
- Membres de comités de direction
- Dirigeants d’ETI et grandes entreprises
- Conseillers exécutifs
- Responsables de la transformation digitale
- Toute personne impliquée dans la prise de décision stratégique en entreprise

Innov Systems

Programme détaillé

1 / Panorama des cybermenaces pour les dirigeants

- Évolution des menaces ciblant les décideurs
- Risques stratégiques, financiers et réputationnels
- Exemples d’attaques contre les COMEX

2 / Comprendre l’économie de la cybercriminalité

- Modèles économiques des attaques (ransomware-as-a-service)
- Cibles prioritaires des cybercriminels
- Impact business des incidents de sécurité

3 / Rôle et responsabilité des dirigeants en cybersécurité

- Gouvernance de la cybersécurité au niveau exécutif
- Responsabilité légale et réglementaire
- Implication du COMEX dans la gestion des risques

4 / Risques humains et ingénierie sociale avancée

- Phishing ciblé (spear phishing, whaling)
- Deepfakes et usurpation d’identité
- Techniques de manipulation des décideurs

5 / Gestion de crise cyber en entreprise

- Organisation d’une cellule de crise
- Prise de décision en situation d’incident majeur
- Communication interne et externe

Innov Systems

6 / Continuité d’activité et résilience organisationnelle

- Plans de continuité et de reprise (PCA/PRA)
- Résilience face aux attaques critiques
- Priorisation des activités essentielles

7 / Investissements et stratégie cybersécurité

- Arbitrage des budgets de sécurité
- ROI des investissements cyber
- Alignement cybersécurité et stratégie d’entreprise

8 / Bonnes pratiques et simulation de crise

- Exercices de simulation de cyberattaque
- Retours d’expérience d’incidents réels
- Construction d’une culture cyber au niveau exécutif

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

Inov Systems

Prochaines dates programmées

01 au 04 Déc. 2026	Distanciel
05 au 08 Jan. 2027	Présentiel - Casablanca
02 au 05 Mars 2027	Présentiel - Casablanca
27 au 30 Avr. 2027	Présentiel - Casablanca
22 au 25 Juin 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