Anticiper et gérer une cybercrise pour protéger son organisation

Date et durée

Code formation : ARI003FR
Durée : 2 jours
Nombre d'heures : 14 heures

Description

Une **cyberattaque** n'est plus une question de « si », mais de « quand ». En cas d'incident, chaque minute perdue coûte en données, en image et en euros. Cette formation intensive de 2 jours transforme la panique en **réponse structurée** : vous gérerez une crise avec la même assurance qu'un arrêt planifié.
Au-delà de la technique, vous définirez les rôles clés, validerez le **plan de gestion crise cyber** et entraînerez votre équipe à détecter les signaux faibles avant qu'ils ne deviennent paralysants. Communication interne**, gestion des médias, preuve à conserver** : chaque scénario est simulé en temps réel, sous pression horaire, avec retour filmé.
Vous repartirez ainsi avec un **playbook de crise clé en main**, une procédure de remédiation étape par étape et une méthode de retour d'expérience. Résultat : votre entreprise sera opérationnelle plus vite, votre réputation sera protégée et votre direction disposera d'indicateurs fiables pour justifier les **investissements de sécurité**.

Objectifs

À l'issue de cette formation, vous atteindrez les objectifs de compétences suivants :

- comprendre les spécificités et la dynamique d'une cybercrise ;
- structurer et mettre en place une organisation de gestion de crise efficace ;
- détecter les signaux faibles pour identifier une cyberattaque au plus tôt ;
- activer le Plan de Gestion de Crise (PGC) et le Plan de Continuité d'Activité (PCA) ;
- maîtriser la communication de crise auprès de ses collaborateurs et des médias ;
- capitaliser sur le retour d'expérience (REX) pour renforcer le dispositif.

Points forts

- **Pédagogie immersive** : vous testerez vos réflexes à travers des simulations de crise et des mises en situation réalistes.
- **Approche transverse** : vous traitez la crise sous tous ses angles : technique, juridique, organisationnelle et communicationnelle.
- Livrables opérationnels : vous travaillerez sur l'élaboration concrète de vos plans (PGC, PCA) et repartez avec des guides pratiques exploitables.
- **Expertise terrain** : vous bénéficierez de l'accompagnement d'experts certifiés ayant une expérience réelle de la gestion d'incidents cyber.

Modalités d'évaluation

Travaux Pratiques

Etude de cas

Pré-requis

Suivre cette formation nécessite le prérequis suivant :

- **Connaissances de base :** une familiarité avec les concepts fondamentaux de la cybersécurité et de la gestion de crise est recommandée pour maximiser les bénéfices de la formation.

Public

Cette formation s'adresse aux décideurs et acteurs opérationnels de la résilience. Le public inclut notamment :

- les **RSSI et DSI** qui pilotent la réponse opérationnelle et coordonnent les équipes techniques sous pression ;
- les **dirigeants et membres de la direction** (ComEx) qui portent la responsabilité légale et doivent arbitrer les décisions stratégiques rapides ;
- les **responsables de gestion des risques et de la continuité (RPCA)** chargés d'activer les plans de secours (PCA) pour limiter les impacts métiers ;
- les **équipes fonctionnelles de la cellule de crise** (Communication, Juridique, RH) qui gèrent la réputation, les obligations déclaratives et le climat interne.

Programme

Module 1 : comprendre la mécanique d'une cybercrise

- Les bases et les enjeux spécifiques d'une crise d'origine cyber.
- Le panorama des menaces actuelles et leurs impacts potentiels.

Études de cas

- L'analyse de cas d'incidents majeurs récents.

Module 2 : se préparer et anticiper l'attaque

- La mise en place d'un dispositif de gestion de crise opérationnel.
- L'élaboration et le test des plans de secours (PCA et PGC).
- L'identification des actifs critiques et la cartographie des vulnérabilités.
- La sensibilisation et la formation des collaborateurs aux réflexes de sécurité.

Module 3 : détecter l'incident et activer la cellule de crise

- Le repérage des signaux faibles et des indicateurs de compromission.
- Le processus d'escalade et la mobilisation rapide des équipes.
- L'activation de différentes cellules, comme la technique, la décisionnelle et la communication.
- La coordination avec les autorités et les parties prenantes externes.

Module 4 : piloter la réponse opérationnelle

- Le confinement technique et la remédiation de l'attaque.
- La mobilisation des équipes internes et le pilotage des prestataires spécialisés.
- La gestion de la communication : élaboration des messages clés et relation média.
- Le respect des obligations légales et déclaratives (CNIL, ANSSI, assurances).

Module 5 : organiser le retour à la normale

- La planification de la reprise progressive des activités.
- L'évaluation précise des dommages et le renforcement des systèmes.
- La conduite du retour d'expérience (REX) et le plan d'amélioration continue.
- La mise en œuvre de nouvelles mesures de sécurité pérennes.