

## Gérer une cyber-crise - Les fondamentaux

Quand une attaque cyber devient virale, voire vitale, pour un organisme

 Présentiel ou en classe à distance



2 jours (14 h)

Prix inter : 2.190,00 € HT

Forfait intra : 5.390,00 € HT

Réf.: MG858

Le **cyber-risque** s'impose aujourd'hui comme une menace critique pour toutes les organisations. Cette formation, appuyée sur les normes **ISO22301** et **ISO27001**, apporte une méthodologie éprouvée pour anticiper, piloter et maîtriser les cybercrises. Exercices pratiques et mises en situation réalistes permettent d'ancrer les bonnes pratiques et de développer les bons réflexes face à une attaque. Au-delà de l'aspect technique, l'accent est mis sur les dimensions **organisationnelles, managériales et communicationnelles**, afin d'impliquer dirigeants, DSI et fonctions support. Les participants repartent avec une vision claire des enjeux, des outils concrets et une meilleure capacité à **renforcer la résilience numérique** de leur structure.

### A qui s'adresse cette formation ?



#### Pour qui

- Responsable du Plan de Continuité Informatique et de la gestion des crises du SI
- Responsable de la Sécurité du Système d'Information (RSSI)
- Manager d'équipe en charge de gérer une cybercrise
- Gestionnaires d'incidents et de problèmes
- Responsable du Plan de Continuité d'Activité (RPCA) et de la gestion de crise
- Dirigeant d'un organisme, membres ou non de la cellule de crise
- Directeur des risques
- Directeur et manager ayant à gérer des crises, y compris cyber



#### Prérequis

- Cette formation s'adresse à des stagiaires ayant déjà des bases en gestion de crise et souhaitant se mettre à niveau pour gérer une cybercrise.
- **Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !**

### Programme

#### 1 - Contexte et enjeux

- Définitions
- Enjeux
- Périmètre Règlementation
- PCA et Gestion de crise

#### 2 - Les risques de cyber-crise

- Les cybermenaces
- Les attaquants
- Analyser les risques
- L'impact de la Directive NIS2
- Vous protéger

### **3 - Se préparer à gérer une cyber-crise**

- Gestion de crise : mieux vaut prévenir que guérir
- Cybercrises : un des nombreux scénarios de crise ... mais le plus prégnant à ce jour
- Se préparer : s'entraîner et déterminer tous les points à traiter
- S'organiser : se donner les moyens de réagir efficacement
- Documenter : apporter un support pour tous

### **4 - Gérer une cyber-crise**

- Organiser : ne pas laisser faire le hasard
- Mobiliser : se donner les chances d'être opérants
- Gérer : être efficace et résilient
- Communiquer : être transparents et respecter les règles
- Documenter : formaliser pour se rappeler et pour les audits

### **5 - Mise en situation**

- Choix du sujet, mise en situation et bilan commun



#### **Les objectifs de la formation**

- Présenter l'environnement des cybermenaces
- Rappeler les bases de la gestion d'une crise et de la continuité d'activité
- Réaliser le lien entre la gestion d'une cyberattaque et la gestion de crise
- Anticiper la cybercrise par la mise en œuvre d'un dispositif efficace
- Prendre de la hauteur et se positionner comme gestionnaire d'une crise cyber
- Donner les clés de la gestion d'une cybercrise, de l'alerte, en passant par la gestion des incidents et des problèmes, jusqu'au bilan
- Permettre de se mettre en situation, grâce à un exercice de gestion d'une cybercrise et à de nombreux échanges pendant la formation



#### **Evaluation**

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.



#### **Les points forts de la formation**

- Les clés pour se préparer et gérer efficacement une cyber-crise
- Les retours d'expériences de l'intervenant permettent de mieux appréhender les diverses dimensions d'une gestion de cyber-crise
- La formation propose une approche largement inspirée de cas réels
- L'étendue du sujet permet de faire le lien entre des systèmes de management de l'organisme (SMCA, SMSI, ...)
- 81% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.



## Dates et villes 2026 - Référence MG858



Dernières places disponibles



Session garantie

### Rennes

du 9 avr. au 10 avr.

du 20 août au 21 août

du 19 nov. au 20 nov.

### Lyon

du 9 avr. au 10 avr.

du 20 août au 21 août

du 19 nov. au 20 nov.

### Bordeaux

du 9 avr. au 10 avr.

du 20 août au 21 août

du 19 nov. au 20 nov.

### A distance

du 9 avr. au 10 avr.

du 20 août au 21 août

du 28 mai au 29 mai

du 19 nov. au 20 nov.

### Nantes

du 9 avr. au 10 avr.

du 20 août au 21 août

du 19 nov. au 20 nov.

### Paris

du 9 avr. au 10 avr.

du 20 août au 21 août

du 28 mai au 29 mai

du 19 nov. au 20 nov.

## Rouen

du 28 mai au 29 mai

du 19 nov. au 20 nov.

## Lille

du 28 mai au 29 mai

du 19 nov. au 20 nov.

## Marseille

du 28 mai au 29 mai

du 19 nov. au 20 nov.

## Sophia Antipolis

du 28 mai au 29 mai

du 19 nov. au 20 nov.

## Strasbourg

du 28 mai au 29 mai

du 19 nov. au 20 nov.

## Aix-en-Provence

du 28 mai au 29 mai

du 19 nov. au 20 nov.

## Toulouse

du 28 mai au 29 mai

du 20 août au 21 août