



<b>Objectifs</b>	Comprendre les enjeux d'une crise cyber - identifier les rôles clés au sein de la cellule de crise - se préparer à gérer efficacement une attaque informatique - apprendre à réagir, à communiquer et à coordonner les actions de réponse face à une cyberattaque
<b>Participants</b>	Dirigeants et membres de comité de direction - RSSI - DPO - Responsables communication de crise - Responsables IT / infrastructure - Chefs de projets ou responsables métier - Juristes / responsables conformité - Responsables continuité d'activité (PCA/PRA)
<b>Prérequis</b>	Connaissance du fonctionnement d'une organisation - notions de cybersécurité - communication en situation de stress - prise de décision rapide - leadership - esprit collaboratif.
<b>Moyens pédagogiques</b>	1 poste par participant - 1 vidéo projecteur - Support de cours fourni à chaque participant - Ateliers individuels - Modalités d'évaluation : Ateliers (TP) pendant tout au long de la formation et évaluation des acquis tout au long de la formation.
<b>Méthodes pédagogiques</b>	Exposés interactifs et démonstrations – Simulations en groupe (tabletop) – Débriefings collectifs – Partage d'expériences et bonnes pratiques
<b>Type de formation</b>	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
<b>Tarif inter-entreprise</b>	2250 € HT
<b>Durée</b>	3 jour(s) - 21 heure(s)

**Code :** NCI\_87QL44H3

## Programme :

### Introduction à la gestion de crise cyber

Définition d'une crise cyber : quand un incident devient critique  
 Typologies d'attaques : ransomware, fuite de données, sabotage  
 Impacts : techniques, réglementaires, réputationnels, business  
 Rôles de la cellule de crise et articulation DSI-Communication-Direction

Recommandations pour renforcer la préparation réelle

### Conclusion

Maturité organisationnelle face à une cybercrise  
 Intégration des enseignements dans la documentation existante  
 Outils et référentiels utiles (CERT-FR, ENISA, NIST, ANSSI)

### Plan de réponse à incident

Identification et catégorisation des incidents  
 Procédures d'escalade et déclenchement de la cellule de crise  
 Outils de communication et gestion des canaux alternatifs  
 Coordination interne et externe (prestataires, ANSSI, CNIL, police)

### Simulation – Phase 1 : Préparer l'organisation

Revue du PCA/PRA et du plan de réponse à incident  
 Définition des responsabilités individuelles pendant une crise  
 Préparation à l'activation d'une cellule de crise ad hoc  
 Exercices de positionnement des rôles clés

### Simulation – Phase 2 : Exercice Tabletop (jeu de rôle)

Déclenchement d'une attaque simulée (ex. ransomware)  
 Réactions en temps réel simulé : détection, isolement, communication  
 Dialogue avec les parties prenantes fictives (presse, clients, autorités)  
 Prise de décisions en contexte incertain

### Simulation – Phase 3 : Débriefing de la gestion de crise

Retour d'expérience collectif (forces, faiblesses, axes d'amélioration)  
 Analyse du comportement des équipes et de la coordination  
 Synthèse des décisions prises et communication interne/externe