EduGroupe
Accompagner pour réussir

Gestion de crise cyber - Les fondamentaux

Référence : **SECCRISEB** Durée : **2 jours (14 heures)** Certification : **Aucune**

Opcommerce

CONNAISSANCES PRÉALABLE

- Aucun prérequis

PROFIL DES STAGIAIRES

- 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

OBJECTIFS

- 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 oeuvre 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

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Pédagogie active et participative : Alternance d'apports théoriques, de démonstrations et d'ateliers pratiques ; Approche learning by doing ; Études de cas et retours d'expérience issus de cyberattaques récentes ; Travaux collaboratifs ; Évaluations formatives
- Formats et adaptation selon le contexte : Présentiel (inter Paris, Lyon, Nantes, Rennes, Toulouse, Pau/ intra partout en France) ; Distanciel synchrone (classe virtuelle) ; Distanciel asynchrone
- Dimension innovante et immersive : Serious game Cyber Crisis Simulation ; Exercice fil rouge ; Tableau de bord interactif ; Auto-diagnostic de préparation à la crise ; Session de retour à froid post-formation (optionnelle)
- Moyens pédagogiques et techniques mobilisés : Plateforme Internet dédiée ; Supports numériques ; Environnement de simulation

FORMATEUR

- Consultant-formateur expert en cyberdéfense et gestion de crise, doté d'une expérience terrain (CERT, SOC, direction sécurité, coordination d'incidents réels)

MÉTHODES D'ÉVALUATION DES ACQUIS

- Avant la formation : test de positionnement ou de validation des prérequis
- Pendant la formation : évluations formatives sous diverses formes
- Fin de formation : évaluation sommative sous forme de quiz général ou étude de cas ; évaluation satisfaction
- Après la formation : Evaluation à froid, un mois après la session de formation
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

1. Matinée (3h30) — Comprendre et anticiper la crise cyber

2. Introduction et cadrage (30 min)

- Présentation des objectifs, attentes des participants, rappel du contexte cyber actuel
- 💡 *Mise en situation d'entrée : un cas récent de cyberattaque (ransomware ou fuite de données)*
- 💡 *Quiz rapide de positionnement*

3. Menace et risque cyber (1h)

- Panorama actualisé de la menace : acteurs, motivations, cibles, typologies d'attaquess
- Comment les attaquants procèdent-ils ? (phishing, exploitation de vulnérabilités, mouvements latéraux)
- Pourquoi les attaques réussissent-elles si souvent ? (facteurs humains, défauts organisationnels, dette technique)
- 💡 *Échange interactif : identification des menaces propres au secteur des participants*

4. Qu'est-ce qu'une crise d'origine cyber ? (1h15)

- Les fondamentaux de la gestion de crise : anticipation, pilotage, communication, retour d'expérience
- Les spécificités d'une crise cyber : vitesse, incertitude, impacts techniques et réputationnels
- Enjeux de coordination entre direction, IT, juridique, communication

5. Anticiper et se préparer à affronter une crise (45 min)

- Les prérequis : plan de continuité, PRA/PCA, chaîne d'alerte, gouvernance
- Construire un dispositif opérationnel : cellule de crise, fiches réflexes, rôles et responsabilités
- 💡 *Mini-exercice : cartographie des acteurs internes à mobiliser en cas de cyberattaque*

6. Après-midi (3h30) — Réagir, piloter et tirer les enseignements

7. Réagir efficacement en adoptant les bonnes pratiques (1h)

- Gérer les seuils d'escalade : du simple incident à la crise majeure
- Premières mesures techniques et organisationnelles de réaction (isolement, communication, coordination)
- Articulation entre réponse à incident (CERT/SOC) et pilotage de la cellule de crise
- 💡 *Cas pratique dirigé : analyse d'une séquence d'incident et décisions à prendre minute par minute*

8. Communiquer efficacement pendant la crise (45 min)

- Élaborer une stratégie de communication de crise : interne, externe, institutionnelle
- Les bons réflexes de communication (timing, transparence, coordination)
- Rôle du porte-parole et gestion des médias / réseaux sociaux
- 💡 *Jeu de rôle : simulation d'un point presse pendant un incident cyber*

9. Mise en situation – Exercice de gestion de crise cyber (1h30)

- 💡 *Exercice sur table : simulation d'une cyberattaque (ex. ransomware ou compromission de données)*
- Pilotage en conditions simulées (alertes, remontées, arbitrages, communication)

10. Débriefing et enseignements (30min)

- 💡 *Retour d'expérience collectif : ce qui a bien fonctionné, les points d'amélioration*
- 💡 *Identification des leviers d'action à court et moyen terme*
- Présentation d'une trame de plan de gestion de crise cyber
- 💡 *Quiz final et évaluation des acquis*

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible .