Public
- Personnels amenés à devoir gérer collectivement une crise suite à une attaque cyber

Prérequis
- Sans objet

Modalités d'admission
- Sur dossier

Durée
- 7 heures

Modalités et méthodes pédagogiques
- Présentiel
- En langue française
- Exposé oral, échange, partage d'expérience, mise-en-commun structurée. Projection de diaporama, d'images et de vidéos, tableau. Mise en situation d'une cyber attaque

Qualité des formateurs
- Formateurs experts métier ayant validé un parcours de qualification pédagogique

Documents remis
- Attestation de formation

Les personnes en situation de handicap sont invitées à contacter le référent Handicap local afin d'étudier les possibilités de suivre la formation

Nous contacter
www.aftral.com
0809 908 908

Gestion de crise cyber au sein de son entreprise : les fondamentaux

Objectifs généraux
- Comprendre en quoi consiste la gestion d'une crise au sein de son organisation suite à une cyberattaque
- Connaître les principales menaces afin de les prévenir et d'en prévenir son entourage professionnel
- Comprendre les effets comportementaux de la crise
- Découvrir l'organisation d'une cellule de crise
- S'approprier les bonnes pratiques essentielles d'animation d'une cellule de crise
- Identifier les fondamentaux de la communication de crise

Les plus de la formation
- Des moyens matériels performants et innovants
- Une formation active et inter active avec des mises en situation pratiques

Mode d'évaluation des acquis
- Évaluation en cours et fin de formation

Validation
- Attestation de formation
- Sans niveau spécifique
- Possibilité de valider un/des blocs de compétences : Sans objet
- Code RNCP/RS : Sans objet
- Certificateur : Sans objet
- Code Certif Info : Sans objet

Agrément
- Sans objet

PROGRAMME

N° SEQUENCE		DUREE
0	**Identifier les objectifs et étapes de la formation**	**/**
▪ Vérification du respect des prérequis ▪ Présentation du centre, de l'équipe pédagogique et des moyens matériels ▪ Présentation de la formation ▪ Modalités pratiques ▪ Tour de table ▪ Test de positionnement		**MOYENS PEDAGOGIQUES ET TECHNIQUES** Salle équipée d'un ensemble multimédia

N° SEQUENCE	OBJECTIF	DUREE
1	**Comprendre en quoi consiste la gestion d'une crise au sein de son organisation suite à une cyberattaque** **Connaître les principales menaces afin de les prévenir et d'en prévenir son entourage professionnel** **Comprendre les effets comportementaux de la crise** **Découvrir l'organisation d'une cellule de crise** **S'approprier les bonnes pratiques essentielles d'animation d'une cellule de crise** **Identifier les fondamentaux de la communication de crise**	**7 h 00**

▪ Avant-propos ▪ Définition ▪ L'anticipation ▪ Effets comportementaux de la crise ▪ Processus de gestion de crise ▪ Méthodologie de gestion de crise ▪ La communication en temps de crise	- Introduction aux cyberattaques : tendances et évolution Exemples récents d'attaques ayant impacté les entreprises Importance de la préparation pour les dirigeants et responsables - Qu'est-ce qu'une cyberattaque ? Différents types d'attaques (ransomware, phishing, DDoS, etc.) Définition d'une crise organisationnelle suite à une cyberattaque Impacts potentiels : financiers, réputationnels, juridiques, opérationnels - Élaboration d'un plan de réponse aux incidents Identification des points critiques dans les systèmes Développement de scénarios de crise et simulations régulières Mise en place de mesures préventives : audits de sécurité, sensibilisation des employés - Les comportements sous stress : panique, déni, paralysie Leadership en situation de crise : maintenir le cap et la confiance Gérer les émotions et la pression dans l'équipe dirigeante Prendre des décisions sous pression - Phases de la gestion de crise : détection, réaction, rétablissement, apprentissage Organigramme de crise : qui fait quoi ? Outils et technologies pour soutenir le processus de gestion (ex : plans de continuité, SIEM) Coordination interne et externe (parties prenantes, fournisseurs, régulateurs)	**MOYENS PEDAGOGIQUES ET TECHNIQUES** Salle de formation équipée d'ordinateurs et vidéoprojecteurs

	- Mise en place d'une cellule de crise Analyse des risques et priorisation des actions Gestion des incidents : techniques et bonnes pratiques Documentation et retour d'expérience - Communication interne : rassurer les employés, donner des instructions claires Communication externe : relation avec les médias, clients, partenaires Utilisation des réseaux sociaux et maîtrise des fuites d'information Préparation de communiqués de presse et points de presse	

N° SEQUENCE		DUREE
2	**Bilan et synthèse de la formation**	**/**
▪ Bilan de la formation ▪ Synthèse du stage ▪ Evaluation de satisfaction de la formation		**MOYENS PEDAGOGIQUES ET TECHNIQUES** Salle équipée d'un ensemble multimédia