



Exercice sur table de gestion de crise

Mise en situation d'une crise avec une ou plusieurs cellules de crise - Réf. 2409

Formation intra entreprise <u>uniquement</u>	
Taux de satisfaction :	N/A
Durée	A préciser
Certification	Aucune
Prix	Nous contacter

Cette formation permet au bénéficiaire de la formation d'appréhender les spécificités et les modalités de gestion d'une crise cybersécurité et de s'exercer à la gestion de crise cyber.

Pré-requis	<ul style="list-style-type: none"> • Aucun • Toutefois la maitrise des fondamentaux de la gestion de crise est plus. • Avoir une connaissance de l'organisation de la gestion et du guide de gestion de crise de l'organsation est un plus.
Public concerné	<ul style="list-style-type: none"> • Dirigeants • Cadres supérieurs des administrations publiques, fonctionnaires titulaires (administrateurs civils, ingénieurs, coprs équivalents) our contractuels. • Membres du CODIR ou COMEX • Responsable de CODIR ou COMEX • Responsable du Plan de Continuité d'Activité (RPCA – BCM) • Chargé de gestion de crise • Responsables opérationnels • Responsable de la sécurité des Systèmes d'Information – RSSI - CISO
Nombre de stagiaires	<ul style="list-style-type: none"> • Minimum 5
Délai d'accès au public	<ul style="list-style-type: none"> • 2 semaines à compter de la demande de formation • Pour les formations 'sur-mesure', deux entretiens préliminaires sont proposés pour définir ensemble la session de formation souhaitée



<p>Objectifs pédagogiques</p> <p>A la fin du cours l'apprenant sera en mesure de :</p>	<ul style="list-style-type: none"> • Acquérir une compréhension approfondie des principes de gestion de crise pour évaluer une situation et identifier les actions à mener • Développer les compétences en prise de décision rapide et efficace dans des situations dégradées ou d'urgence. • Renforcer la capacité à communiquer de manière claire et efficace en période de crise • Pratiquer la coordination et la collaboration entre les différents intervenants impliqués dans la gestion de crise pour établir des stratégies d'actions concertées. • Identifier les lacunes et les points forts dans les plans de réponse à la crise et proposer des axes d'amélioration.
<p>Compétences visées</p>	<ul style="list-style-type: none"> • Etre prêt à gérer une crise cyber • Etre à même d'avoir des reflexes ou s'appuyer sur des bonnes pratiques en matière de gestion de crise • Apprendre à mettre en place une organisation adaptée pour répondre efficacement aux situations de crise
<p>Méthode d'évaluation</p>	<ul style="list-style-type: none"> • Phase d'évaluation : questionnaire sous la forme d'un QCM. Ce questionnaire permettra de confirmer les acquis des participants sur les thèmes des modules vus durant la formation.
<p>Certificat de stage</p>	<ul style="list-style-type: none"> • Attestation de fin de stage
<p>Tests de certification</p>	<ul style="list-style-type: none"> • Aucun
<p>Références bibliographiques & sitographiques utilisés pour ce module de formation</p>	<ul style="list-style-type: none"> • https://www.ssi.gouv.fr/ • https://www.cybermalveillance.gouv.fr/ • https://cyber.gouv.fr/publications/crise-cyber-les-cles-dune-gestion-operationnelle-et-strategique • https://www.ege.fr/actualites/louvrage-cybersecurite-methode-de-gestion-de-crise-est-disponible-en-librairie • https://www.alliancy.fr/chroniques/dirigeants-et-cybersecurite
<p>Méthodes pédagogiques</p>	<ul style="list-style-type: none"> • En français ou en anglais • Remise d'une documentation pédagogique numérique à la fin du stage • La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience



	<ul style="list-style-type: none">• Les échanges seront encouragés autour de retours d'expériences, témoignages des participants.
Débouché et suite du parcours	<ul style="list-style-type: none">• Compétence permettant la mise en place et la gestion du pilotage de gestion de crise au sein de son organisation.• Réaliser des exercices de gestion de crise Approfondissement des connaissances acquises sur les métiers et les compétences cyber
Lieu	<ul style="list-style-type: none">• Paris centre, en région, sur site ou à distance
Nom et prénom de l'intervenant	<ul style="list-style-type: none">• Anne Doré ou autre formateur expert en cybersécurité
Éléments de biographie de l'intervenant	<ul style="list-style-type: none">• Anne Doré - Anne possède une solide expérience dans le conseil pour CSC Peat Marwick puis chez IBM, un des leaders mondiaux de la cyber sécurité.• Elle a accompagné de nombreux dirigeants dans la mise en œuvre de projets stratégiques intégrant de nouvelles technologies (cloud, AI, big data) et la transformation des organisations.• Sa devise 'La cybersécurité est l'affaire de tous, notamment celle des dirigeants et des comités de direction'• Autre formateur : à préciser selon le calendrier et les modalités d'intervention
Modalités d'accès	<ul style="list-style-type: none">• Pour vous inscrire vous pouvez nous contacter à l'adresse suivante : contact@adhel.fr• Ou remplir le questionnaire ci-joint• Nous nous engageons à vous répondre dans les 48H

Contenu de la formation

- Présenter les conventions d'exercice du scénario de crise aux participants,
- Expliquer les objectifs de l'exercice et des règles de participation.
- Simuler la crise : les participants réagissent au scénario en temps réel, prenant des décisions et mettant en œuvre les plans de gestion de crise.
- Débriefing : une réunion est organisée avec tous les participants pour discuter des performances individuelles et collectives, des points forts et des points faibles, et des recommandations pour améliorer la préparation à la gestion de crise.

FIN DU DOCUMENT



CONTACT :

Mél: contact@adhel.fr
Tél. +33 6 60 26 27 48
<https://adhel.fr>

ADHEL – 63 rue Nationale - 92100 Boulogne Billancourt
Siret : 88274050900014 – NDA : 11922660392
Organisme de formation Qualiopi au titre des actions de formation continue



Tous droits réservés