Anticiper et gérer la crise cyber

Rançongiciel & fuite de données

Formation pour les décideurs

Taux de satisfaction	N/A
Durée	7 heures
Certification	Aucune
Référence	2401
Prix inter-entreprise	1.300 euros H.T. par stagiaire
Prix intra-entreprise	Nous consulter

Les attaques cyber qui touchent les PME / ETI ne sont pas des crises techniques : elles sont des enjeux business, humains, juridiques et réputationnel

Cette formation donne aux dirigeants une compréhension claire des menaces (dont l'IA), et surtout des réflexes de décision pour réduire l'impact et tenir le cap en situation dégradée.

Pré-requis	• Aucun
Public concerné	• Dirigeants et membres de direction de PME/ETI : DG, DAF, DRH, DCOO/Directeur Exploitation, Directeur Industriel, Directeur Commercial, Direction Juridique/Conformité, responsable communication, responsables métiers.
Nombre de stagiaires	• Minimum 5
Délai d'accès au public	• 2 semaines à compter de la demande de formation • Pour les formations 'sur-mesure', deux entretiens préliminiaires sont proposés pour définir ensemble la session de formation souhaitée.
Objectifs pédagogiques A la fin du cours l'apprenant sera en mesure de	• Permettre aux décideurs de comprendre le risque réel et de s'entraîner à piloter une crise cyber (rançongiciel + fuite de données), avec un plan d'action simple, réaliste et immédiatement applicable.
Compétences visées	• Comprendre les principales menaces PME/ETI, les acteurs et leurs modes opératoires (dont usages de l'IA). • Etre à même d'identifier leurs impacts critiques en cas de rançongiciel (arrêt d'activité, production, trésorerie, fournisseurs, etc.). • Etre à même de pouvoir anticiper les impacts critiques en cas d'intrusion/fuite de données (clients, RH, PI, obligations, image).

	• Pouvoir décider des priorités et arbitrages dans les premières heures d'une crise (continuité d'activité, communication, preuves, partenaires). • Pouvoir mettre en place des mesures d'anticipation simples et réalistes pour réduire probabilité et impacts. • Anticiper le dispositif de gestion de crise : rôles, responsabilités, check-lists, messages clés, numéros utiles, et plan d'action.
Méthode d'évaluation	• Evaluation sous la forme d'un questionnaire. Ce questionnaire permettra de confirmer les acquis des participants sur les thèmes des modules vus durant la formation.
Certificat de stage	• Attestation de fin de stage
Références bibliographiques & sitographiques utilisés pour ce module de formation	• 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
Méthodes pédagogiques	• En français ou en anglais • Remise d'une documentation pédagogique numérique pendant le stage • La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience • Les échanges seront encouragés autour de retours d'expériences, témoignages des participants.
Débouché et suite du parcours	• 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
Lieu	• Dans nos locaux, sur site ou à distance
Nom de l'intervenant	• Un consultant formateur expérimenté à même de partager de
Eléments de biographie de l'intervenant	• Sa devise 'La cybersécurité est l'affaire de tous, notamment celle des dirigeants et des comités de direction' • Anne est co-auteur d'une Méthode de gestion de crise cyber écrite avec le soutien de l'ANSSI et l'Ecole de Guerre Economique.
Modalités d'accès	• 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
Accessibilité	• Nous vous invitons à préciser dans le formulaire d'inscription si vous avez besoin d'un accompagnement particulier.

	• Nous nous tenons à votre disposition par mail contact@adhel.fr pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.

Contenu de la formation – 7H

Ouverture & cadrage – 30 min

- Tour de table : "Qui a déjà vécu un incident ?" (même mineur)
- Objectifs de la journée, règles du jeu, cadre de confiance
  Livrable : attentes & priorités des dirigeants

Comprendre la menace & le rôle de l'IA - 50 min

- Menaces principales PME/ETI : rançongiciel, fuite de données, blocage outil métier, fraude, usurpation, deepfake…
- Qui sont les attaquants / ce qu'ils cherchent
- IA & cyber : côté attaquants (phishing crédible, deepfake), côté entreprise (assistants, automatisations, exposition des données)
- 2–3 cas concrets adaptés au secteur
  Livrable : fiche "Ce que je risque vraiment (dont IA)"

Pause – 15 min

Exercice de crise #1 : rançongiciel (mise en situation) – 1H30

- Déclenchement : "vos équipes ne peuvent plus travailler"
- Décisions des premières heures : priorités, arbitrages, continuité, preuves, partenaires, communication interne
- Organisation : qui décide quoi ? comment éviter la panique ?
  Debrief à chaud : réflexes clés & erreurs fréquentes

Anticiper le rançongiciel : mesures simples & réalistes – 35 min

- Réduire l'impact : continuité, sauvegardes, dépendances critiques, prestataires, procédures "mode dégradé"
- Réduire le risque : habitudes et contrôles essentiels (sans technique)
  Livrable : mini check-list "anti-chaos" rançongiciel

Déjeuner – 60 min

Ce que les crises apprennent vraiment – 20 min

- Respiration / décompression guidée
- "Ce que les crises apprennent vraiment" : décisions, charge émotionnelle, communication, fatigue, coordination

Exercice de crise #2 : intrusion + fuite / vol de données - 75 min

- Déclenchement : suspicion d'accès non autorisé + données sensibles concernées
- Décisions : clients, RH, juridique, preuves, communication, partenaires, assurances, priorisation business
- Spécificités : rumeurs, pression médiatique, risques de "double peine"
  Debrief : réflexes et points de vigilance

Pause – 15 min

Anticiper la fuite de données & le risque IA – 30 min

- Réduire l'exposition : cartographie des données sensibles, accès, partage, prestataires
- Prévenir les erreurs humaines : pratiques simples, règles "dirigeants & COMEX", cas IA (données dans outils, prompts, usages, prestataires)
  Livrable : "règles simples de protection des données (dont IA)"

Plan d'action & outils de préparation (prêt à l'emploi) – 45 min

- Répartition des rôles & tâches (direction, métiers, RH, communication, IT, partenaires)
- Fiche réflexe dirigeant : les premières heures
- Check-list de préparation + numéros utiles + circuit de décision
- Communication de crise : messages clés, erreurs à éviter, qui parle et quand
  Livrables :
- Fiche réflexe "Premières heures"

Conclusion – 20 min

FIN DU DOCUMENT