PROGRAMME DE FORMATION

Gestion de crise cyber : se préparer et réagir à une attaque

Cybersécurité & Protection des données

RÉFÉRENCE	VERSION	ÉDITION	DOMAINE
WF-0466	V2026-005	3 novembre 2026	Cybersécurité & Protection des données

DURÉE	MODALITÉ	PROGRAMME	SANCTION
14 h	Distanciel asynchrone (e-learning)	3 modules 9 leçons	Attestation et certificat de réalisation

Objectifs pédagogiques

- Distinguer un incident d'une crise d'origine cyber et définir les critères de déclenchement de la cellule de crise.
- Organiser la cellule de crise, ses rôles, son annuaire et ses outils de secours, et préparer la continuité des activités critiques.
- Conduire les premières heures d'une attaque : alerter, qualifier, contenir, préserver les preuves et tenir la main courante.
- Prendre et tracer les décisions de crise en respectant les obligations de notification, de plainte et de déclaration.
- Communiquer pendant la crise auprès des collaborateurs, des clients, des partenaires et, le cas échéant, des médias.
- Piloter la reprise d'activité, conduire un retour d'expérience et concevoir un exercice de crise sur table.

L'essentiel de la formation

Public visé

Dirigeants et membres de direction de TPE-PME, responsables informatiques, référents cybersécurité, responsables administratifs, juridiques, qualité ou communication appelés à faire partie d'une cellule de crise en cas d'attaque informatique.

Prérequis

Connaître le fonctionnement général de son organisation (activités, prestataires, outils principaux) ; aucune compétence technique en sécurité n'est exigée.

Notions de base sur les menaces courantes (hameçonnage, rançongiciel) ; à défaut, la formation WF-0459 est conseillée en amont.

Disposer d'un ordinateur avec une connexion internet et d'un traitement de texte ou tableur.

Modalités et déroulement

Formation à distance, en ligne, de 14 h. Le fil rouge suit l'Atelier Brémont, PME fictive frappée par un rançongiciel, depuis la préparation jusqu'au retour d'expérience. L'apprenant prend des décisions chronométrées dans des scénarios à embranchements, rédige les outils de la cellule de crise, joue des échanges difficiles (client, journaliste, assureur) et conçoit un exercice sur table pour son organisation. Environ 60 % du temps est consacré à ces mises en situation corrigées ; les apports courts (vidéos, fiches sourcées) renvoient aux guides publics de l'ANSSI et de Cybermalveillance.gouv.fr. Accompagnement par un formateur par messagerie.

Méthodes pédagogiques

- Positionnement en début de parcours
- Apports en vidéo : explications et démonstrations
- Mises en situation et scénarios à décisions
- Exercices d'application et mises en pratique corrigées
- Production de livrables professionnels
- Atelier de synthèse en fin de module
- Quiz et QCM d'auto-évaluation
- Accompagnement et retours du formateur

Répartition du temps de formation : **16 %** théorique · **58 %** pratique · **26 %** évaluation

Moyens pédagogiques et techniques

- Plateforme de formation en ligne, accès individuel à distance
- Vidéos pédagogiques
- Quiz et exercices interactifs en ligne
- Correction des productions sur grille de critères
- Messagerie avec le formateur

Modalités d'évaluation

Positionnement initial non éliminatoire ; scénarios de décision notés avec explication ; livrables (fiche d'organisation, main courante, messages, rapport de retour d'expérience, scénario d'exercice) vérifiés sur grille critériée ; trois quiz de module ; évaluation finale composée d'une mise en situation de crise chronométrée et d'un questionnaire. Seuil de réussite interne : 70 %. Aucune certification n'est délivrée.

Sanction

Une attestation de fin de formation et un certificat de réalisation sont remis au participant sous réserve de la réalisation du parcours.

Cette formation n'est pas présentée comme préparant à une certification enregistrée : elle ne comprend ni inscription ni présentation à des épreuves de certification, et n'ouvre droit à aucune délivrance de certification ni au financement par le CPF.

Modalités et délais d'accès

La demande d'inscription peut être effectuée par téléphone, par courrier électronique ou au moyen du formulaire en ligne.

Un entretien ou un questionnaire de positionnement permet de vérifier l'adéquation de la formation avec les besoins, le niveau initial et les prérequis du candidat.

L'inscription devient définitive après validation du dossier administratif, acceptation des documents contractuels et, le cas échéant, confirmation du financement.

Les accès à la plateforme sont généralement activés sous 48 à 72 heures ouvrées après validation complète du dossier.

Les formations à distance sont proposées en entrées et sorties permanentes, sous réserve des délais ou dates imposés par le financeur ou le certificateur.

Accessibilité aux personnes en situation de handicap

Vidéos sous-titrées et transcrites, fiches compatibles avec les lecteurs d'écran, navigation au clavier ; le chronométrage des scénarios peut être désactivé sur demande. Référent handicap joignable à handicap@will-formation.com pour étudier toute adaptation (durée, supports, modalités d'évaluation).

Tarif de la formation

Prix : **1 460 €**

Financement : prise en charge possible par les organismes financeurs, selon les critères d'éligibilité applicables.

Qualiopi processus certifié

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION. Certificat QUA25070009. WILL FORMATION — Société par actions simplifiée à associé unique au capital de 30 000 € — NDA 11757059675 (cet enregistrement ne vaut pas agrément de l'État) — SIRET 893 713 180 00014 — 01 85 09 25 99 — info@will-formation.com — www.will-formation.com

Programme détaillé

3 modules, 9 leçons — durée totale 14 h.

01 Se préparer à une crise d'origine cyber

1. Incident ou crise : reconnaître une crise cyber
2. Organiser la cellule de crise et ses outils
3. Préparer la continuité et les appuis externes

02 Réagir et piloter la crise

1. Les premières heures : alerter, qualifier, contenir
2. Décider sous incertitude et respecter les obligations
3. Communiquer pendant la crise

03 Reprendre l'activité, tirer les leçons et s'entraîner

1. Reprendre l'activité de façon maîtrisée
2. Retour d'expérience et plan d'amélioration
3. Concevoir et animer un exercice de crise sur table