L'AKADÉMIE DU DIGITAL · PROGRAMME DE FORMATION Certification Qualiopi en cours de préparation

Cybersécurité pour Managers

FOR-CYBER-M3-A · Cybersécurité & Conformité

Piloter la sécurité numérique de son équipe et de son organisation

DURÉE
7 h

TARIF
450 € HT

PUBLIC
Entreprises & particuliers

DÉLAI D'ACCÈS
Accès sous 2 jours ouvrés après validation du besoin et des prérequis.

Tarifs indiqués « à partir de », hors devis spécifique et promotions. Prix HT, à partir de 2 participants. TVA 20 %.

Objectifs pédagogiques

- Comprendre les enjeux stratégiques et financiers de la cybersécurité pour l'organisation
- Identifier les principaux risques et leur impact métier (interruption d'activité, image, conformité)
- Intégrer la sécurité dans le management : politique, sensibilisation, culture du risque
- Connaître les normes et cadres de référence utiles au pilotage (ISO 27001, NIST, recommandations ANSSI)
- Construire et piloter un plan de réponse aux incidents et un plan de continuité
- Dialoguer efficacement avec les équipes techniques et les prestataires (RSSI, DSI)

Public concerné

- Managers, chefs d'équipe, chefs de service et responsables opérationnels
- Dirigeants de TPE/PME, responsables RH, responsables de site
- Toute personne en position d'encadrement amenée à piloter ou porter la sécurité numérique

Prérequis

- Savoir utiliser un ordinateur et les outils bureautiques courants.
- Occuper une fonction d'encadrement ou de responsabilité (un atout).
- Avoir une sensibilisation de base à la cybersécurité (module Initiation conseillé).
- Disposer d'une motivation à piloter la sécurité numérique de son périmètre.

Programme

THÉORIE Module Théorique — Piloter la cybersécurité à l'échelle de l'organisation

Ce module positionne la cybersécurité comme un enjeu stratégique (risques métier, coûts d'un incident, responsabilité du manager) et apprend à cartographier les risques au-delà du seul volet technique (actifs sensibles, vulnérabilités organisationnelles). Il met l'accent sur le facteur humain (sensibilisation, culture du risque, politique de sécurité, charte informatique), présente les cadres de référence pour piloter (ISO 27001, NIST, recommandations ANSSI) et aborde la gestion de crise cyber (plan de réponse aux incidents, PCA/PRA, communication) ainsi que le dialogue avec les équipes techniques et prestataires.

Objectif : donner aux managers les repères pour piloter la sécurité numérique de leur périmètre, décider et embarquer leurs équipes.

- Angle managérial et stratégique, accessible aux non-techniciens.
- Cartographie des risques orientée impact métier.
- Cadres de pilotage (ISO 27001, NIST, ANSSI) et gestion de crise.

Évaluation : QCM sur les enjeux et les cadres de référence, exercice de cartographie des risques métier.

Accueil & présentation	15 min	Présenter le programme, les objectifs et le déroulé. Présentation orale, support visuel (slides), tour de table.	
La cyber, enjeu stratégique	40 min	Risques métier, coûts d'un incident, responsabilité du manager. Exposé interactif, exemples d'incidents, échanges.	Questions orales de compréhension.
Cartographie des risques	45 min	Actifs sensibles, menaces, vulnérabilités organisationnelles. Méthode de cartographie, gabarit, exercice.	Exercice de cartographie des risques métier.
Facteur humain & politique	45 min	Sensibilisation, culture du risque, politique de sécurité, charte informatique. Exposé, exemples de politiques, discussion de groupe.	QCM intermédiaire.
Cadres & gestion de crise	50 min	ISO 27001, NIST, ANSSI ; plan de réponse aux incidents, PCA/PRA, dialogue RSSI/DSI. Exposé structuré, schéma NIST, exemples de plans.	QCM sur les cadres de référence.
Synthèse	10 min	Résumer les points clés et préparer l'atelier. Récapitulatif, feedback des participants.	QCM rapide de fin de module.

ATELIER **Atelier Pratique — Construire son pilotage de la sécurité**

À partir de leur organisation ou d'un cas fil rouge, les participants cartographient les risques cyber prioritaires et leur impact métier, élaborent les grandes lignes d'une politique de sécurité et d'un plan de sensibilisation des équipes, construisent un plan de réponse aux incidents simplifié (rôles, étapes, communication) et définissent des indicateurs de pilotage ainsi qu'une feuille de route priorisée.

Objectif : repartir avec une cartographie des risques, une ébauche de politique de sécurité, un plan de réponse aux incidents et une feuille de route de pilotage.

- Travail possible directement sur le contexte réel de l'organisation.
- Production d'outils de pilotage : politique, plan de sensibilisation, plan de réponse.
- Définition d'indicateurs de pilotage (KPI sécurité).
- Feuille de route priorisée et orientée décision.

Évaluation : production des livrables (cartographie des risques, ébauche de politique, plan de réponse aux incidents, feuille de route), restitution orale courte et revue collective.

Lancement de l'atelier	15 min	Présenter l'objectif et choisir son organisation ou un cas fil rouge. Présentation, constitution des groupes.	
Cartographie des risques	50 min	Cartographier les risques cyber prioritaires et leur impact métier. TP guidé, gabarit de cartographie, accompagnement.	Livrable : cartographie des risques.
Politique & sensibilisation	50 min	Élaborer les grandes lignes d'une politique de sécurité et d'un plan de sensibilisation. TP collaboratif, modèles, échanges.	Livrable : ébauche de politique + plan de sensibilisation.
Plan de réponse aux incidents	45 min	Construire un plan de réponse simplifié (rôles, étapes, communication). TP guidé, modèle de plan de réponse, jeu de rôle court.	Livrable : plan de réponse aux incidents.
KPI & feuille de route	25 min	Définir des indicateurs de pilotage et une feuille de route ; présenter. Modèle d'indicateurs, présentations courtes, feedback.	Évaluation sommative : feuille de route + QCM final.
Enquête de satisfaction	10 min	Recueillir la satisfaction à chaud. Questionnaire de satisfaction.	Enquête de satisfaction.

Modalités et moyens pédagogiques

Formation en présentiel dans nos locaux ou dans vos locaux, en groupe restreint. Alternance d’apports théoriques, d’ateliers pratiques et de mises en situation.

Matériel requis :

8 Go de Ram

Modalités d’évaluation

Évaluation des acquis en cours et en fin de formation, attestation de fin de formation remise à chaque stagiaire.

Accessibilité

Formation accessible aux personnes en situation de handicap. Contactez-nous avant l’inscription pour étudier les aménagements nécessaires.

Financement

Devis ou convention de formation sur demande. La certification Qualiopi est en cours de préparation : l’éligibilité aux financements OPCO sera ouverte après son obtention.

Audit de certification prévu au T1 2027. Aucune éligibilité OPCO avant l’obtention.