



Normes et méthodes

ISO 27032 - Lead Cybersecurity Manager - Avec certification

5 jours (35h00) | ★★★★★ 4,6/5 | ISO-27032LCM | Certification PECB 27032 Lead Cybersecurity Manager (incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Tarif : 3 600 € ht

Formations Informatique > Cybersécurité > Normes et méthodes

Contenu mis à jour le 12/09/2025. Document téléchargé le 15/05/2026.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts fondamentaux, les stratégies, les méthodologies et les techniques utilisés pour mettre en oeuvre et gérer un programme de cybersécurité
- Expliquer la corrélation entre ISO/IEC 27032, le cadre de cybersécurité du NIST ainsi que d'autres normes et cadres pertinents
- Décrire le fonctionnement d'un programme de cybersécurité et ses composants
- Soutenir un organisme dans l'exploitation, la maintenance et l'amélioration continue de votre programme de cybersécurité.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi



Prérequis

Avoir une compréhension fondamentale des concepts et de la gestion de la cybersécurité. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

L'apprenant s'engage à respecter les prérequis nécessaires ; une déclaration écrite et/ou un CV peut lui être demandé(s). Un QCM réussi de validation des prérequis peut également être nécessaire avant l'entrée en formation.

Public concerné

Responsables et dirigeants impliqués dans la gestion de la cybersécurité, cadres et dirigeants jouant un rôle crucial dans les processus de prise de décision liés à la cybersécurité, professionnels de l'informatique et de la sécurité désireux de booster leur carrière et de contribuer plus efficacement aux efforts de cybersécurité. Professionnels chargés de gérer le risque de cybersécurité et la conformité au sein des organismes et/ou toute personne chargée de la mise en oeuvre pratique des stratégies et des mesures de cybersécurité.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2I Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

Introduction à la cybersécurité et initiation aux programmes d'implémentation cyber

Jour 2

Rôles et responsabilités en matière de cybersécurité, gestion des risques et mécanismes d'attaques

Jour 3

Mesures de sécurité, communication, sensibilisation et formation en matière de cybersécurité

Jour 4

Management des incidents de cybersécurité, surveillance et amélioration continue

Jour 5

Matin : Préparation à la certification

Après-midi : Passage de la certification

- Le prix et le passage de l'examen sont inclus dans la formation

- L'examen (en anglais) a lieu le dernier jour, à l'issue de la formation (sous réserve de place disponible lors d'un passage en distanciel) et s'effectue en ligne ou sur papier, pour une durée moyenne de 3h00
- En cas d'échec à l'examen, le candidat peut le repasser dans les 12 mois qui suivent sans frais supplémentaires

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par une certification éditeur, et/ou un questionnaire d'auto-évaluation

Accessibilité de la formation

Le groupe M2I s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap : les détails de l'accueil des personnes sont consultables sur la page Politique Handicap.

Modalités et délais d'accès à la formation

Les formations M2I sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 12 jours ouvrés.