ISO/IEC 27032 – Lead Cybersecurity Manager

Cybersecurity Management

Filière : **DevOps & Infrastructure** Sous-filière : **Cyber Sécurité**

RÉFÉRENCE	DURÉE	PRIX PAR PERSONNE HT
ISO-27032	**4 JOURS (28H)**	**3 550 €**

Description

La formation ISO/IEC 27032 Lead Cybersecurity Manager vous permettra de développer les connaissances et les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et la gestion d'un programme de cybersécurité en conformité avec la norme ISO/IEC 27032 et le Cadre de Cybersécurité NIST.

Cette formation est conçue de manière à vous doter de connaissances approfondies en matière de cybersécurité, et vous permettra de maîtriser la relation entre la cybersécurité et d'autres types de sécurité des technologies de l'information, ainsi que le rôle des parties prenantes dans la cybersécurité.

Objectifs pédagogiques

- Acquérir des connaissances approfondies sur les composantes et les opérations d'un programme de cybersécurité en conformité avec l'ISO/IEC 27032 et le cadre de cybersécurité NIST
- Comprendre la corrélation entre ISO 27032, le cadre de cybersécurité NIST et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, normes, méthodes et techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'un organisme
- Apprendre à interpréter les exigences d'ISO/IEC 27032 dans le contexte spécifique d'un organisme
- Maîtriser l'expertise nécessaire pour planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité tel que spécifié dans ISO/IEC 27032 et le cadre de cybersécurité NIST
- Acquérir les compétences pour conseiller un organisme sur les bonnes pratiques de management de la cybersécurité

Public cible

- Professionnels de la cybersécurité
- Experts en sécurité de l'information

- Professionnels souhaitant gérer un programme de cybersécurité
- Responsables du développement d'un programme de cybersécurité
- Spécialistes des TI
- Conseillers spécialisés dans les TI
- Professionnels des TI souhaitant accroître leurs connaissances et compétences techniques

Pré-requis

Pour tirer pleinement parti de cette formation, les participants doivent avoir une compréhension fondamentale des concepts et de la gestion de la cybersécurité.

Modalités d'évaluation

L'examen de certification « PECB Certified Lead Cybersecurity Manager » répond pleinement aux exigences du programme d'examen et de certification PECB (ECP). L'examen couvre les domaines de compétence suivants :

- Domaine 1 : Principes et concepts fondamentaux de la cybersécurité
- Domaine 2 : Rôles et responsabilités des parties prenantes
- Domaine 3 : Gestion des risques liés à la cybersécurité
- Domaine 4 : Mécanismes d'attaque et contrôles en cybersécurité
- Domaine 5 : Partage de l'information et coordination
- Domaine 6 : Intégrer le programme de cybersécurité dans le management de la continuité des activités
- Domaine 7 : Gestion des incidents de cybersécurité et mesure de la performance.

Date de passage de l'examen au choix :

- dans la continuité de la formation, le 5ème jour
- à programmer à une date ultérieure à la formation

Méthodes pédagogiques

Ce cours couvre les concepts théoriques et les exemples pratiques de la cybersécurité, permettant aux participants de comprendre l'application efficace des stratégies et des technologies de cybersécurité.

La formation comprend diverses évaluations, notamment des exercices de type dissertation et des questions à choix multiples, dont certaines sont basées sur des scénarios pratiques.

Les participants sont encouragés à interagir et à avoir des discussions constructives entre eux tout en travaillant sur les quiz et les exercices, afin de favoriser un environnement d'apprentissage collaboratif. La structure des quiz du cours reflète étroitement celle de l'examen de certification, garantissant ainsi que les participants sont bien préparés pour l'examen.

Programme de la formation

Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032

- Objectifs et structure du cours
- Normes et cadres réglementaires
- Notions fondamentales de la cybersécurité
- Programme de cybersécurité
- Lancer un programme de cybersécurité
- Analyser l'organisme
- Leadership

Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque

- Politiques de cybersécurité
- Gestion du risque de la cybersécurité
- Mécanismes d'attaque

Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information

- Mesures de contrôle de cybersécurité
- Partage et coordination de l'information
- Programme de formation et de sensibilisation

Jour 4 Gestion des incidents, suivi et amélioration continue

- Continuité des activités
- Management des incidents de cybersécurité
- Intervention et récupération en cas d'incident de cybersécurité
- Conclusion de la formation
- Tests en cybersécurité
- Mesure de la performance
- Amélioration continue

Date de passage de l'examen au choix :

- dans la continuité de la formation, le 5ème jour
- à programmer à une date ultérieure à la formation

Qualité

Les frais d'examen et de certification sont inclus avec la formation.

Les participants recevront le matériel de formation contenant plus de 450 pages d'informations explicatives, d'exemples, de bonnes pratiques, d'exercices et de quiz.

En cas d'échec à l'examen, les candidats peuvent le repasser gratuitement dans les 12 mois suivant la tentative initiale.

Programme mis à jour le **23 juillet 2025**