Devenir Lead Cybersecurity Manager ISO/CEI 27032

Ref: PR-CYB-CD-27032LCM

Mettre en œuvre et manager un programme de cybersécurité basé sur la norme ISO/CEI 27032.

DURÉE : **5 Jours** (35H)
Prix : **3 590,00 € HT**

PRÉSENTIEL
FORMATION QUALIFIANTE

Objectifs et compétences visés

- Reconnaître la corrélation entre la norme ISO/CEI 27032, le cadre de cybersécurité du NIST, d'autres normes et cadres d'exploitation puis acquérir des connaissances approfondies sur les éléments et les activités d'un programme de cybersécurité.
- Maîtriser les notions, les approches, les normes, les méthodes et les techniques utilisées pour concevoir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'un organisme.
- Apprendre à interpréter les lignes directrices de la norme ISO/CEI 27032 dans le contexte particulier d'un organisme.
- Acquérir l'expertise nécessaire pour planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité, comme spécifié dans la norme ISO/CEI 27032 et le cadre de cybersécurité du NIST.

À qui s'adresse la formation ?

Profils

- Professionnels de la cybersécurité et experts en sécurité des systèmes d’information
- Professionnels cherchant à gérer un programme de cybersécurité ou responsables d’un programme de cybersécurité.
- Spécialistes en systèmes d’information.
- Conseillers-experts en technologie de l’information.
- Professionnels en systèmes d’information qui cherchent à améliorer leurs compétences et leurs connaissances techniques.

Prérequis

Aucun prérequis n'est nécessaire à cette formation.

Contenu de la formation

Introduction à la cybersécurité et aux notions connexes

- Normes et cadres réglementaires.
- Notions fondamentales de la cybersécurité.
- Construire et lancer un programme de cybersécurité.
- Analyser l’organisme.
- Affirmer son leadership.

Politiques de cybersécurité, management du risque et mécanismes d’attaque

- Politiques de cybersécurité.
- Gestion du risque de la cybersécurité.
- Mécanismes d’attaque.

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.

Gestion des incidents, suivi et amélioration continue

- Continuité des activités et management des incidents de cybersécurité.
- Intervention et récupération en cas d’incident de cybersécurité.
- Tests en cybersécurité et mesure de la performance.
- Amélioration continue.

Révisions et examen de certification

Modalités

Modalités d'évaluation

Passage d'un examen de certification PECB.

Nos plus

Cette formation est animée par un consultant CNPP certifié ISO/CEI 27032 Lead Cybersecurity Manager et ISO/CEI27001 Lead Implementer.
Disponible également en visioconférence.

En bref

21000
stagiaires / an

Des infrastructures pédagogiques uniques

+ de 500
diplômés / an

+ de 400
intervenants

Nos formations complémentaires

Management de la sécurité de l'information
Devenir EBIOS Risk Manager
3 Jours
Présentiel
Maîtriser les principes et les concepts fondamentaux de l’appréciation des risques et de la gestion optimale des risques liés à la sécurité de l’information selon la méthode EBIOS

Management de la sécurité de l'information
Fondamentaux de la directive NIS 2
1 Jour
Présentiel
Découvrir les concepts fondamentaux de la directive NIS 2

Forensic et sécurité opérationnelle
Lead Forensic Examiner
5 Jours
Présentiel
Maîtrisez les concepts et outils d’analyses forensiques dans un contexte judiciaire, ainsi que dans un contexte d’entreprise

Besoin d'informations sur une formation en cybersécurité ?

Nous sommes à votre écoute pour échanger sur votre prochaine formation en cybersécurité.

Contactez-nous !

+33 (0)8 06 00 03 80