PECB Certified Lead Cybersecurity Manager

Maîtriser la capacité à mettre en œuvre et à gérer un programme de cybersécurité basé sur les bonnes pratiques du secteur.

Pourquoi devriez-vous y participer ?

De nos jours, les organismes sont affectés par l'évolution constante du paysage numérique et sont constamment confrontés à de nouvelles menaces et à des cyberattaques de plus en plus complexes et perfectionnées. Le besoin en personnel qualifié capable de gérer et de mettre en œuvre efficacement des programmes de cybersécurité robustes pour contrer ces menaces est pressant. La formation « Lead Cybersecurity Manager » que nous proposons a été conçue pour répondre à ce besoin.

Les participants à la formation PECB Certified Lead Cybersecurity Manager acquièrent les concepts, stratégies, méthodologies et techniques fondamentaux de la cybersécurité utilisés pour établir et gérer efficacement un programme de cybersécurité basé sur les directives des normes internationales de cybersécurité, tels que la norme ISO/IEC 27032 et le cadre de cybersécurité du NIST. De plus, cette formation renforce la capacité des participants à améliorer la préparation et la résilience de leur organisme face aux cybermenaces. Les participants sont ainsi mieux préparés à soutenir les efforts continus de leur organisme en matière de cybersécurité et à apporter une contribution précieuse dans le paysage actuel de la cybersécurité, qui est e constante évolution.

À qui s'adresse la formation ?

Cette formation s'adresse :

- Aux responsables et dirigeants impliqués dans la gestion de la cybersécurité
- Aux personnes chargées de la mise en œuvre pratique des stratégies et des mesures de cybersécurité
- Aux professionnels de l'informatique et de la sécurité désireux de booster leur carrière et de contribuer plus efficacement aux efforts de cybersécurité
- Aux professionnels chargés de gérer le risque de cybersécurité et la conformité au sein des organismes
- Aux cadres dirigeants qui ont un rôle crucial dans les processus de prise de décision liés à la cybersécurité

Programme de la formation

Durée : 5 jours

Jour 1 | Introduction to cybersecurity and initiation of a cybersecurity program implementation

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Concepts fondamentaux de la cybersécurité
- Programme de cybersécurité
- L'organisme et son contexte
- Gouvernance de la cybersécurité

Jour 2 | Rôles et responsabilités en matière de cybersécurité, gestion des risques et mécanismes d'attaque

- Rôles et responsabilités en matière de cybersécurité
- Gestion des biens
- Gestion des risques
- Les mécanismes d'attaque

Jour 3 | Mesures de sécurité, communication, sensibilisation et formation en matière de cybersécurité

- Mesures de cybersécurité
- Communication relative à la cybersécurité
- Sensibilisation et formation

Jour 4 | Management des incidents de cybersécurité, surveillance et amélioration continue

- État de préparation des TIC pour la continuité d'activité
- Management des incidents de cybersécurité
- Tests de cybersécurité
- Mesurer et rendre compte des performances et des paramètres en matière de cybersécurité
- Amélioration continue
- Clôture de la formation

Jour 5 | Examen de certification