Certified Lead Cybersecurity Manager, certification PECB
ISO 27032:2023 / NIST

Cours Pratique de 5 jours - 35h
Réf : CYB - Prix 2024 : 3 990CHF HT

Cette formation vous permettra d'acquérir 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 renforcera votre capacité à améliorer la préparation et la résilience de votre organisme face aux cybermenaces.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Expliquer concepts, stratégies, méthodologies et techniques pour mettre en œuvre et gérer un programme de cybersécurité

Expliquer la corrélation entre la norme ISO 27032, le cadre du NIST ainsi que d'autres normes et cadres pertinents

Comprendre le fonctionnement d'un programme de cybersécurité et ses composantes

Soutenir un organisme dans l'exploitation, la maintenance et l'amélioration continue de son programme de cybersécurité

MÉTHODES PÉDAGOGIQUES

Cours magistral soutenu par une présentation illustrée d'exemples concrets, ponctuée d'échanges, de questions et d'aller-retours théorie-pratique.

ETUDE DE CAS

Anatomie d'une attaque d'une entreprise internationale. Exercices pour identifier les écarts et manipuler les concepts-clés.

CERTIFICATION

Examen papier composé de 12 questions ouvertes, à traiter en 3h, en français. Déroulement à « livre ouvert » (autorisé avec support et notes personnelles prises durant la session). La certification PECB « Certified Lead Cybersecurity Manager » est obtenue en cas de réussite de l'examen de certification.

PARTICIPANTS

Responsables et dirigeants impliqués dans la gestion de la cybersécurité, professionnels de la cybersécurité, experts en sécurité de l'information, chefs de projet et consultants en sécurité IT.

PRÉREQUIS

Bonnes connaissances en sécurité de l'information.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 01/2024

1) Initiation à l'implémentation d'un programme de cybersécurité

- 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.

2) Rôles et responsabilités en matière de cybersécurité

- Rôles et responsabilités en matière de cybersécurité.
- Gestion des biens.

3) Gestion des risques et mécanismes d'attaque

- Gestion des risques.
- Les mécanismes d’attaque.

4) Mesures de sécurité, communication, sensibilisation et formation

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

5) Management des incidents, 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.

6) Examen de certification

- Domaine 1 : concepts fondamentaux de la cybersécurité.
- Domaine 2 : lancement du programme de cybersécurité et de la gouvernance en matière de cybersécurité.
- Domaine 3 : définition des rôles et responsabilités en matière de cybersécurité et gestion des risques.
- Domaine 4 : sélection des mesures de cybersécurité.
- Domaine 5 : mise en place de programmes de communication et de formation en matière de cybersécurité.
- Domaine 6 : intégration du programme de cybersécurité dans la gestion de la continuité d'activités et des incidents.
- Domaine 7 : évaluation des performances du programme de cybersécurité et amélioration continue de celui-ci.

LES DATES

CLASSE À DISTANCE
2024 : 13 mai, 08 juil., 04 nov.