NIS 2 Directive Lead Implementer, certification PECB

Cours Pratique de 5 jours - 35h
Réf : NI2 - Prix 2024 : 3 960CHF HT

Cette formation vous permettra d'acquérir une connaissance approfondie des exigences de la directive NIS 2, des stratégies de mise en œuvre et des bonnes pratiques qui protègent les infrastructures critiques contre les cybermenaces. Vous apprendrez à évaluer les risques de cybersécurité d'un organisme, à élaborer des plans robustes de réponse aux incidents et à mettre en œuvre des mesures de sécurité efficaces pour répondre aux exigences de la directive NIS 2.

OBJECTIFS PÉDAGOGIQUES

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

Expliquer les concepts fondamentaux de la directive NIS 2 et ses exigences.

Compréhension des principes, stratégies, et outils nécessaires à la mise en œuvre d'un programme de cybersécurité

Interpréter et à mettre en œuvre les exigences de la directive NIS 2 dans le contexte spécifique d'un organisme.

Initier et planifier la mise en œuvre des exigences de la directive NIS 2, en utilisant la méthodologie de PECB.

Planifier, mettre en œuvre, surveiller et maintenir un programme de cybersécurité conformément à la directive NIS 2.

LE PROGRAMME

dernière mise à jour : 10/2024

1) Introduction à la directive NIS 2 et lancement de la mise en œuvre de la directive NIS 2

- Introduction à la directive NIS 2 et lancement de la mise en œuvre de la directive NIS 2
- Normes et cadres réglementaires.
- Directive NIS 2.
- Exigences de la directive NIS 2.
- Initiation de la mise en œuvre de la directive NIS 2.
- L'organisme et son contexte.

2) Analyse du programme de conformité à la directive NIS 2, de la gestion des actifs et de la gestion des risques

- Gouvernance de la cybersécurité.
- Rôles et responsabilités de cybersécurité.
- Gestion des actifs.
- Gestion des risques.

3) Contrôles de cybersécurité, gestion des incidents et gestion des crises

- Contrôles de cybersécurité.
- Sécurité de la chaîne d'approvisionnement.
- Gestion des incidents.
- Gestion des crises.

PARTICIPANTS

Professionnel de la cybersécurité, responsables informatiques souhaitant acquérir des connaissances sur la mise en œuvre de systèmes sécurisés, responsables gouvernementaux et réglementaires

PRÉREQUIS

Avoir une compréhension fondamentale de la cybersécurité.

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.

4) Communication, tests, surveillance et amélioration continue de la cybersécurité

- Continuité d'activité.
- Sensibilisation et formation.
- Communication.
- Tests en cybersécurité.
- Audit interne.
- Mesurer, surveiller et rendre compte des performances et des indicateurs.
- Amélioration continue.

5) Certification

- Domaines de compétences couverts par l'examen :
- Domaine 1 : Concepts fondamentaux et définitions de la directive NIS 2.
- Domaine 2 : Planification de la mise en œuvre des exigences de la directive NIS 2.
- Domaine 3 : Rôles et responsabilités en matière de cybersécurité et gestion des risques.
- Domaine 4 : Contrôles de cybersécurité, gestion des incidents et gestion des crises.
- Domaine 5 : Communication et sensibilisation.
- Domaine 6 : Test et surveillance d'un programme de cybersécurité.

LES DATES

CLASSE À DISTANCE
2025 : 24 mars, 28 juil., 06 oct.,
15 déc.