

NIS2 Directive Lead Implementer (certification comprise)

Référence : **SECNIS2**

Durée : **5 jours**

Certification : **PECB NIS 2 LI**

CONNAISSANCES PREALABLES

- Les principales exigences pour participer à cette formation sont d'avoir une compréhension fondamentale de la cybersécurité.

PROFIL DES STAGIAIRES

- 1-Professionnel de la cybersécurité cherchant à acquérir une compréhension approfondie des exigences de la directive NIS 2 et à apprendre des stratégies pratiques pour mettre en œuvre des mesures de cybersécurité robustes. • 2-Responsables informatiques et professionnels souhaitant acquérir des connaissances sur la mise en œuvre de systèmes sécurisés et améliorer la résilience des systèmes critiques. • 3-Responsables gouvernementaux et réglementaires chargés de faire appliquer la directive NIS 2.

OBJECTIFS

- Expliquer les concepts fondamentaux de la directive NIS 2 et ses exigences. • Acquérir une compréhension approfondie des principes, stratégies, méthodologies et outils nécessaires à la mise en œuvre et à la gestion efficace d'un programme de cybersécurité conformément à la directive NIS 2. • Apprendre à 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 et d'autres bonnes pratiques. • Acquérir les connaissances nécessaires pour soutenir un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un programme de cybersécurité conformément à la directive NIS 2.

CERTIFICATION PREPAREE

PECB Certified NIS 2 Directive Lead Implementer. Cet examen dure 3 heures. Pour connaître tous les détails concernant les prérequis relatifs au passage de l'examen de certification en ligne, nous vous invitons à [cliquer ici](#) pour accéder à la documentation officielle du certificateur.

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Management de la sécurité

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

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

- Objectifs et structure de la formation
- 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

Jour 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

Jour 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

Jour 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
- Clôture de la formation

Jour 5 : Examen de certification

- L'examen « PECB Certified NIS 2 Directive Lead Implementer » répond aux exigences du Programme d'examen et de certification :
 - 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

Notre **référent handicap** se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.