TRECCERT

NIS2 Essentials
Formation



TRECCERT NIS2 Essentials est une formation de sensibilisation. Elle donne aux participants une solide compréhension de la directive NIS2 et de sa portée concrète dans le travail. La formation présente la finalité stratégique de la directive, son champ d'application et ses principes clés, ainsi que son évolution depuis la première directive NIS. Les participants apprennent à reconnaître les cybermenaces et vulnérabilités courantes de leurs activités quotidiennes et à y réagir de manière proactive. Ils apprennent aussi à identifier les risques de sécurité liés aux services et aux fournisseurs tiers, pour renforcer la sécurité de toute la chaîne d'approvisionnement.

PUBLIC VISÉ

La formation NIS2 Essentials s'adresse aux personnes qui souhaitent comprendre leur rôle en cybersécurité dans le cadre de la directive NIS2. Elle convient en particulier aux profils suivants.

- Responsables conformité, gestionnaires des risques ou conseillers chargés de la gouvernance de la cybersécurité
- Équipes informatiques et sécurité
- Juristes et délégués à la protection des données
- Chefs d'équipe et managers

OBJECTIFS PÉDAGOGIQUES

- Comprendre la finalité de NIS2 et ses objectifs stratégiques pour renforcer la cybersécurité dans l'UE.
- Décrire la chronologie des directives sur la sécurité des réseaux et des systèmes d'information (NIS) et leur évolution.
- Connaître les principes clés de la directive NIS2.
- Identifier les secteurs clés et les types d'organisations concernés par la directive NIS2.

FICHE DES SUPPORTS DE COURS

Diapositives
200

Questions de quiz
25

Exercice
1

PROGRAMME DE LA FORMATION

1. Introduction à la directive NIS2

- Contexte et objectifs de NIS2
- Champ d'application de NIS2
- Principes clés de NIS2

2. Obligations des organisations selon NIS2

- Exigences de gestion des risques
- Responsabilités de gouvernance et de direction
- Gestion des risques fournisseurs et tiers

3. Signalement des incidents et réponse

- Ce qui constitue un incident
- Obligations et délais de notification
- Procédures d'escalade internes

4. Exigences de sécurité et rôle des collaborateurs

- Facteurs humains en cybersécurité
- Bonnes pratiques des collaborateurs
- Repérer et signaler une activité suspecte

5. Accompagnement de la conformité et amélioration continue

- Comment votre organisation assure sa conformité
- Droits des lanceurs d'alerte et signalement
- Implication des collaborateurs dans une culture de sécurité durable

MODALITÉS DE L'EXAMEN

Nombre de questions
20

Type d'examen
Choix multiples

Durée
60 minutes

Lieu
En ligne

INFORMATIONS PRATIQUES

Durée
Un (1) jour

Langue
Anglais

Crédits CPE
8

Modalité
Présentiel et en ligne

PATH TO RECOGNITION

info@treccert.com | www.treccert.com

TRECCERT