Mis à jour le 17/05/2025

S'inscrire

Formation Directive NIS 2 : nouvelles normes de cybersécurité européennes

2 jours (14 heures)

Présentation

Notre formation directive Network and Information Security 2 (ou NIS 2) vous permettra de vous mettre à niveau sur les dernières directives européennes en matière de sécurité. Cette directive fait suite à NIS 1 créée en 2016 pour renforcer la cybersécurité au sein de l'Union européenne. Elle sera obligatoire à partir de 2024 et vient renforcer les mesures prises par les états membres auxquelles les entreprises devront se plier.

Notre formation NIS 2 vous permettra de prendre de l'avance sur la mise en œuvre de cette directive dans l'espace européen, et ainsi vous assurer que votre entreprise est prête aux prochaines normes européennes.

Dans cette formation, vous apprendrez toutes les changements par rapport à la précédente directive NIS. Vous y aborderez toutes les nouvelles mesures mises en place par l'Union européenne en termes de cybersécurité pour un champ d'application plus large ainsi qu'une collaboration bien plus importante entre les différents États européens.

Objectifs

- Comprendre les nouveautés abordées par NIS 2.
- Pouvoir adapter les processus de son entreprise aux nouvelles réglementations.

Public visé

- CEO
- Responsables en cybersécurité

Pré-requis

Connaissance de NIS 1 est un plus, mais pas indispensable

Programme de notre formation Directive NIS 2

Introduction à la CyberSécurité Européenne

- Enjeux actuels : cybervols, espionnage, sabotage
- Dynamiques géopolitiques : tensions Est/Ouest, USA/Chine, Occident/Russie
- Acteurs de la cybermenace : hackers, agences de renseignement, APT et ransomwares
- Vers une coopération européenne renforcée : l'idée d'un cyber-Schengen

Rôle et Responsabilités du RSSI sous NIS 2

- Ciblage des entités : critères pour les entités essentielles et importantes
- Secteurs affectés et écosystèmes concernés
- Réglementation : évolutions depuis NIS 1 et nouvelles exigences
- Calendrier d'application : de 2024 à 2026
- Mise en œuvre : processus de gouvernance et certification
- Sanctions potentielles : modèle inspiré du RGPD

Implémentation des Mesures de Sécurité

- Revue des politiques de NIS 1 : gouvernance, protection, défense, résilience
- Analyse de risques et sécurité des systèmes d'information
- Gestion des incidents et continuité des opérations
- Sécurité dans la chaîne d'approvisionnement et dans le développement des systèmes
- Évaluation et amélioration continue de la cybersécurité
- Mesures pratiques : cyberhygiène, utilisation de la cryptographie et de l'authentification multi-facteurs

Gestion du Projet de Conformité

- De l'analyse préliminaire à la conformité : intégration des évaluations EBIOS RM
- Adaptation des mesures de sécurité préexistantes et gouvernance par le risque
- Processus d'homologation spécifique à NIS 2 et rôle de l'ANSSI
- Planification et ressources pour le projet de conformité NIS 2

Conclusion : Vers l'Homologation et au-delà

- Intégration des normes ISO 27001 et bonnes pratiques ISO 27002:2022
- Cyberrésilience et alignement avec les directives DORA et CER
- Transposition nationale : évolution de la LPM et régulation des OIV
- Gestion des contrôles et sanctions étatiques : approches et gradation des sanctions
- Sécurisation de l'écosystème et interactions avec les parties prenantes

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.