Les impacts de la Directive NIS2 sur votre organisation

Animé en partenariat avec KYRON

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Pilotage de la sécurité organisationnelle

Rubrique : Management de la CyberSecurité : Certifications

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

- Comprendre les enjeux stratégiques de la cybersécurité et les réponses Européennes.
- Intégrer les lignes directrices de sécurité spécifiques à la NIS2, selon les référentiels nationaux.
- Analyser les différences entre les directives NIS1 et NIS2.
- Appliquer les concepts et procédures par des études de cas pratiques.
- Appréhender le processus d'homologation encadré par l'ANSSI.
- Évaluer les implications budgétaires d'un projet de conformité NIS2.

Public visé

- Responsables et référents en sécurité des systèmes d'information (RSSI), architectes sécurité.
- Directeurs et responsables informatiques, ingénieurs IT, chefs de projet (MOE/MOA).
- Auditeurs en cybersécurité et juristes spécialisés en réglementation IT.

Pré-requis

Des connaissances de base en cybersécurité sont nécessaires.

PROGRAMME

Contexte

La directive NIS2 marque une étape décisive dans la réponse de l'Union européenne aux cybermenaces croissantes, renforçant la directive NIS1 pour faire face à l'évolution rapide des risques et à l'augmentation des attaques. Elle vise à sécuriser les infrastructures essentielles dans des secteurs critiques, tout en assurant une continuité des services, ce qui soutient la stabilité de l'économie et de la société européennes. Cette formation approfondit les nouvelles exigences de la directive et son application concrète.

Programme de la formation

1. Introduction : Enjeux et contexte de la cybersécurité européenne

- Données sensibles et menaces associées : Vols, espionnage, sabotage, etc.
- Nouveaux enjeux géopolitiques : La montée des tensions (Est/Ouest, USA/Chine, Occident/Russie).
- Cybercriminalité organisée : Rôle des groupes de hackers, APT (Advanced Persistent Threats), ransomwares.
- Vers une harmonisation européenne : L'idée d'un "Cyber Schengen" et son implica**tion.**

2. Conformité NIS2 pour les RSSI

Code de formation : NIS2-01

€ Tarifs

Prix public : 2090 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Campus : Ensemble des sites

Durée : 14 heures

Délai d'accès :
Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Distanciel possible : Oui

Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

- 18 / 09 / 2025
  : Ensemble des sites
  ✓ : Distanciel possible
  : 14 heures
  : 2 jours
- 25 / 09 / 2025
  : Ensemble des sites
  ✓ : Distanciel possible
  : 14 heures
  : 2 jours
- 18 / 12 / 2025
  : Ensemble des sites
  ✓ : Distanciel possible
  : 14 heures
  : 2 jours

○ Identification des entités visées : Entités essentielles (EE) et importantes (EI) ; critères d'éligibilité.
○ Écosystèmes concernés : Inclusion de nouveaux secteurs et entreprises de services numériques (ESN).
○ Cadre de gouvernance : Répartition des 23 règles NIS1 et nouveaux ajouts.
○ Calendrier de mise en œuvre : Exigences progressives de 2024 à 2026.
○ Sanctions financières : Barème des sanctions, inspiré du RGPD, en fonction du chiffre d'affaires.

3. Mesures de sécurité de la directive NIS2

○ Gouvernance et politiques de sécurité : Rappels des principes de NIS1 (protection, résilience).
○ Analyse des risques et gestion des SI : Méthodologies pour une évaluation efficace des risques.
○ Gestion des incidents : Mise en place de protocoles pour une réponse rapide.
○ Continuité d'activité et gestion de crise : Plans de continuité (PCA) et de reprise d'activité (PRA).
○ Chaîne d'approvisionnement sécurisée : Suivi des risques associés aux fournisseurs critiques.
○ Acquisition et maintenance des systèmes : Sécurité dans les phases de développement et maintenance.
○ Cyberhygiène et formation : Meilleures pratiques et éducation continue en cybersécurité.
○ Cryptographie : Normes de chiffrement et gestion des clés.
○ Sécurité RH et contrôle d'accès : Gestion des accès, authentification multi-facteur (MFA).

4. Conduite d'un projet de mise en conformité NIS2

○ Analyse d'écart : État des lieux par rapport aux exigences de NIS2.
○ Approche gouvernance par le risque : Importance d'EBIOS RM pour les projets NIS.
○ Reprise des mesures de sécurité existantes : Adaptation des règles NIS1.
○ Homologation ANSSI : Processus d'accréditation et étapes spécifiques à la directive NIS2.
○ Ressources et jalons projet : Allocation des ressources nécessaires et gestion de l'échéancier.

5. Conclusion : Vers une gouvernance renforcée

○ Alignement avec les normes ISO : Lien avec les standards ISO 27001 et ISO 27002:2022.
○ Synergies réglementaires : Interactions avec les directives DORA et la Loi de Programmation Militaire (LPM).
○ Contrôles étatiques : selon le profil de risque.
○ Règles de sanctions : Mécanismes de sanction inspirés du RGPD.
○ Sécurisation de l'écosystème : Collaboration avec les partenaires critiques et harmonisation de la cybersécurité.

MODALITÉS

Modalités

Méthodes pédagogiques :

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de format