

Implémenter, gouverner et homologuer un projet NIS 2

Réaliser avec succès un objectif de conformité NIS v2

Séminaire de 2 jours - 14h

Réf : NIS - Prix 2024 : 2 090€ HT

La directive NIS v1 avait pour objectif de créer des capacités en matière de cybersécurité dans toute l'Union, d'atténuer les menaces pesant sur les réseaux et les systèmes d'information servant à fournir des services essentiels dans des secteurs clés et d'assurer la continuité de ces services en cas d'incidents, contribuant ainsi à la sécurité de l'Union et au bon fonctionnement de son économie et de sa société. La directive NIS v2 représente une continuité « augmentée » et nécessaire face à l'expansion du paysage des cybermenaces et à l'émergence de nouveaux défis.

OBJECTIFS PÉDAGOGIQUES

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

Comprendre les enjeux sur les risques cyber et les réponses « européennes »

Intégrer le référentiel sécurité défini par l'état Français pour la directive NIS

Appréhender les changements NIS v1 vers NIS v2

Connaitre, au travers de cas concrets, leur implémentation et déploiement

Comprendre le processus d'homologation porté par l'ANSSI

Evaluer les couts de mise en œuvre dans le cadre d'un projet

LE PROGRAMME

dernière mise à jour : 01/2024

1) Introduction : les enjeux de la cyber sécurité européenne

- Données sensibles : cyber vols, espionnage, sabotage, ...
- Nouvelle guerre froide Est/Ouest, USA/Chine Occident / Russie.
- Hackers organisés, rôle des agences de renseignements.
- APT (Advanced Persistent Threat), les ransomware, les risques ciblés.
- L'approche de la cyber menace : vers un « cyber shengen » ?

2) L'essentiel pour le RSSI

- Pour qui ? : Entités essentielles et Entités Importantes, les nouveaux critères d'éligibilité, d'exclusion.
- Pour quels écosystèmes ? Nouveaux secteurs d'activités et ESN enrôlées.
- Quelles règles : des 23 règles de la NIS v1 plus « ce qui lui manquait » ?
- Quand ? à partir de 2024 jusqu'à 2026, ...
- Comment ? avec un processus de gouvernance et d'homologation maîtrisé.
- Quelles sanctions ? gradué sur le CA, sur l'exemple du RGPD.

3) Les mesures de sécurité

- Rappel des règles de gouvernance, protection, défense et résilience de la NIS v1.
- Les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information.
- La gestion des incidents.
- La continuité des activités et la reprise des activités, la gestion des crises.

PARTICIPANTS

RSSI ou référents sécurité, architectes sécurité, directeurs ou responsables informatiques, ingénieurs IT, chefs de projets (MOE, MOA), auditeurs de sécurité ou juristes réglementaires IT.

PRÉREQUIS

Connaissances de base en cybersécurité ou connaissances équivalentes à celles apportées par les séminaires BYR ou SSI.

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.

- La sécurité de la chaîne d'approvisionnement.
- La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information.
- L'évaluation l'efficacité des mesures de gestion des risques en matière de cybersécurité.
- Les pratiques de base en matière de cyber hygiène et la formation à la cybersécurité.
- Les politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement.
- La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs.
- L'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue.

4) La gestion du projet de mise en conformité

- De l'analyse d'écart/état des lieux à la mise en conformité.
- La gouvernance par le risque : pertinence de EBIOS RM dans un projet NIS.
- La reprise des mesures de sécurité existantes, des règles NIS v1 le cas échéant.
- Le processus d'homologation de l'ANSSI adapté à la directive NIS v2.
- Les principaux jalons du projet NIS v2, les ressources nécessaires.

5) Conclusion : en route vers l'homologation

- Une forte inspiration ISO 27K :Lien avec ISO 27001 et nouvelles bonnes pratiques ISO 27002:2022.
- Une Cyber résilience cohérente : lien avec directives et règlements DORA et CER.
- La transposition Française : l'évolution parallèle de la LPM et des OIV.
- Des contrôles étatiques différenciés (régulation « ex-ante » et/ou « ex post »).
- Un processus de sanction comparable RGPD , les règles de la graduation des amendes.
- La sécurité de son écosystème et des parties prenantes critiques.

LES DATES

CLASSE À DISTANCE
2024 : 20 juin, 15 oct., 09 déc.

PARIS
2024 : 20 juin, 08 oct., 14 nov.