Formation Maîtrisez NIS v2 : sécurisez vos infrastructures et respectez les nouvelles normes européennes

Les réglementations NIS, CER, CRA, cybersecurity Act pour la cyber sécurité

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Référence	NIS24
Durée	2 jours (14h)
Tarif	2 197 €HT

SESSIONS PROGRAMMÉES

PARIS

du 28 au 29 novembre 2024

VOIR TOUTES LES DATES

Objectifs

| Expliquer les enjeux sur les risques cyber et les différentes réglementations européennes et françaises à respecter (NIS, LPM, DORA, CER, ...)
| Guider les architectes dans la réalisation des règles NISv2 obligatoires et leurs niveaux d'implémentation EE, EI et écosystèmes dépendants
| Décrire, au travers de cas concrets, les conditions d'implémentation et d'exigences des règles de sécurité incluant le processus de détection/notification des incidents
| Evaluer les couts et délais de mise en oeuvre des moyens de maitrise des risques et les règles de supervision applicables au projet NISv2

Public

| RSSI, architectes de sécurité, DSI ou responsables informatiques, consultants, chefs de projets (MOE, MOA) devant répondre à des exigences de conformité NIS v2 ou équivalent (LPM, NIST-CSF, PIC-DSS, ISO 27001, ...)

Prérequis

| Aucun

Programme de la formation

Introduction : cadrage - acteurs de la cyber sécurité en EU
| Le rôle des agences d'état de l'ANSSI, de l'ENISA, de la commission Européenne
| Les missions en coopération EU - le groupe de coopération
| Les CERTs et CSIRT en France et en Europe
| Les prestataires qualifiés (PDIS, PRIS, PASSI)

Le domaine d'application de NIS 2
| Les Entités Essentielles / Entités Importantes
| Les règles d'inclusion NIS 2 applicables par défaut
| La régulation des administrations publiques et des collectivités territoriales
| L'application de NIS2 aux organismes ayant des activités dans plusieurs pays
| Le processus déclaratif vers l'homologation/conformité des SI NIS2 compliant
| Les exclusions recevables (critères, équivalence et respect autres actes EU »)
| Les éco systèmes numériques ; l'enrôlement des ESN
| Les cas particuliers - les critères spécifiques à la France
| Les exclusions de sauvegarde de sécurité nationale et fonctions essentielles / régaliennes

Les réglementations européennes
| Les directives sur la résilience (CER, DORA, CRA)
| Le cas particulier de la LPM en France - sa révision en cours
| Les interactions possibles, voire obligatoire entre ces directives
| Le projet de loi relatif à la résilience des OIV, à la protection des infrastructures critiques, à la cybersécurité (NIS) et à la résilience DORA
| De la nécessité de technologies / services souverains - l'application du cybersecurity Act

| La directive NISv2 comme socle de « GPRD » pour les activités critiques, essentielles et vitales

Les mesures de sécurité de Gouvernance / Protection
| De l'obligation à analyser les risques cyber et les menaces de type APT
| La sécurité de la chaine d'approvisionnement - les exigences de sécurité sur l'éco système fournisseurs de rang 1 et plus ...
| La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
| La gestion des vulnérabilités et le MCS ; de l'usage d'un référentiel de vulnérabilités EU
| L'évaluation de l'efficacité des mesures de gestion des risques en matière de cybersécurité - la pratiques des audits ; les revues de codes et les tests d'intrusion
| La « cyber hygiène » : sensibilisation et formation à la cybersécurité
| La protection du patrimoine informationnel - les conditions d''utilisation de la cryptographie robuste et des choix algorithmiques
| La sécurité des ressources humaines : le recrutement sécurisé, la gestion des privilèges, le processus disciplinaire
| Les contrôles d'accès logiques et physiques avec authentification MFA et gestion du moindre privilège / besoin d'en connaitre - les revues/ suppressions des droits
| L'application d'un principe de proportionnalité sur la réalisation des mesures de sécurité en fonction du statut EE / EI / ESN, public / privé

La gestion des incidents et des crises (Défense / Résilience)
| La gestion des incidents, de la détection au traitement résilient, - la détection sur base de technologies souveraines FR / EU
| Les critères de classification de gravité d'incident (majeur / mineur)
| Les incidents obligatoires à déclarer auprès des autorités
| La règles de notifications, le processus imposé de notification auprès des CSIRT
| Les délais clé de 24h et 72h, les acteurs concernés, la remise d'un rapport officiel dans le mois
| De la nécessité à des prestataires qualifiés de la cyber sécurité (PDIS, PRIS, ...)
| La coopération en matière de gestion de crise cyber, le réseau CyCLONe
| PCA / PRA et gestion des crises cyber ; les objectifs de résilience nécessaires, les communications d'urgence en cas de crise
| La mise en oeuvre d'un plan de résilience incluant les tiers
| La création d'une base d'incidents anonymisée au niveau de l'ENISA

La supervision
| De la recherche et constatation des manquements
| Les audits de conformité/homologation « ex-ante » et « ex post »
| Les pouvoirs de l'ANSSI : « ce qui doit être présenté à l'autorité compétente »
| Le régime de sanctions applicables si obstacle à la demande de l'autorité
| Les types d'audit et demandes préventives ; leurs couts
| Les mesures consécutives aux contrôles ; actions suite au contrôle mise en demeure
| Les sanctions : principe de la proportionnalité / Chiffre d'affaires
| Les commissions des sanctions, les responsabilités engagées des dirigeants

La gestion d'un projet NIS 2 et des réglementations sur la résilience
| Gouvernance projet - feuille de route
| Analyse des risques cyber - de l'intérêt de EBIOS RM
| La mise en oeuvre des mesures de sécurité (connues par décret)
| Le modèle utilisé par la loi belge : du l'usage référentiel NIST ou ISO 27001
| Les niveaux d'exigences graduées du modèle Cyber Fundamental (basic à Essentiel)
| Gestion des incidents (détection / traitement / notification)
| Audits de sécurité - pen tests - revues
| PCA / PRA - Gestion de crise
| La modèle de communication avec les autorités compétentes et les CSIRT (l'ANSSI en France, le CCB en Belgique, ...)

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.