NIS 2, NIST CSF 2, ISO 27001:2022
Panorama des normes et des référentiels en cybersécurité

Séminaire de 2 jours - 14h
Réf : NST - Prix 2024 : 2 090CHF HT

Composante incontournable dans la maîtrise de son SI, la lutte contre la cybercriminalité a vu exploser la publication de référentiels de bonnes pratiques et d'exigences. Face à cette multiplicité d'outils, l'objectif de ce séminaire est d'apporter une vision large des référentiels disponibles, d'en préciser leur portée ou leur spécificité afin de guider le choix des acteurs chargés de la cybersécurité. Vous verrez quelles sont les bonnes questions à vous poser à l'heure des choix et de la confrontation à l'augmentation de la menace cyber.

OBJECTIFS PÉDAGOGIQUES

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

Comprendre les enjeux liés aux risques cyber et les réponses État de l'art

Connaître les principaux référentiels internationaux de cybersécurité

Intégrer un référentiel sécurité aux bonnes pratiques IT

Connaître, au travers de cas concrets, l'implémentation et déploiement des référentiels

Comparer et choisir le plus efficace pour atteindre ses objectifs de sécurité

Comprendre les processus de certification/mise en conformité, d'homologation

Évaluer les coûts de mise en œuvre dans le cadre d'un système d'information global

LE PROGRAMME

dernière mise à jour : 04/2024

1) Le modèle européen : Network Information Security 2 (NIS 2)

- Nouvelle guerre froide Est/Ouest, USA/Chine Occident/Russie.
- Hackers organisés, rôle des agences de renseignements.
- APT (Advanced Persistent Threat), les ransomwares, les risques ciblés.
- Cartographie des référentiels : du spécialiste au généraliste.
- Les enjeux européens de la cybersécurité.
- Domaines d'application EE, EI, OSE, FSN, les nouveaux critères d'éligibilité.
- Pour quels écosystèmes - Nouveaux secteurs d'activité et ESN/IT enrôlées.
- Les principales mesures de sécurité : à partir des 23 règles de la NIS 1 et bien plus…
- Le processus de gouvernance par le risque et d'homologation maîtrisée.
- Le système de sanctions gradué sur le CA, comme le RGPD.

Etude de cas : Déployer un projet NIS 2, à partir de NIS v1, avec pour objectif son homologation.

2) Le modèle américain : NIST CSF 2.0

- Le core avec son ensemble de catégories et sous-catégories.
- La nouvelle fonction GOVERN et son intérêt pour une gouvernance stratégique cyber.
- Les guides de mises en œuvre de la série 800 et 1800 en support du CSF.
- Les niveaux de mise en œuvre du cadre : tiers 1 à 4.
- Apprendre à graduer sa sécurité en fonction de ses objectifs et de la criticité des activités.

PARTICIPANTS

RSSI ou correspondants sécurité, architectes sécurité, directeurs ou responsables informatiques, ingénieurs, chefs de projet (MOE, MOA), auditeurs devant intégrer des exigences de sécurité.

PRÉREQUIS

Connaissances de base en cybersécurité, ou connaissances équivalentes à celles apportées par les stages 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.

- Intégrer le développement sécurisé avec le framework complémentaire SSDF.
- Créer son profil à partir des objectifs de sécurité des métiers ainsi que des exigences de parties prenantes.
- Construire un profil en rapport aux menaces cyber sur l'écosystème.

Etude de cas : Déployer un profil de gouvernance avec le nouveau NIST CSF 2.0

3) Le modèle universel ISO 27001:2022

- La norme ISO 27001 dans une démarche système de management (roue de Deming/PDCA).
- La gouvernance par le risque de l'ISO : ISO 31000/ISO 27005.
- L'élaboration du plan de traitement des risques et de la déclaration d'applicabilité.
- Les bonnes pratiques universelles de la norme ISO 27002:2022.
- Les domaines de la sécurité et les attributs associés aux 93 mesures.
- Construire une gestion documentaire et une base de preuves.
- Appréhender le processus d'audit du SMSI (première partie et tierce partie).

Etude de cas : Déployer une dynamique d'amélioration continue avec l'ISO 27001.

4) Un modèle IT cloud SecNumCloud

- La vision de l'informatique sécurisée en mode cloud par l'ANSSI et ses dernières évolutions 2023.
- Les principales bonnes pratiques de protection/défense des hébergements de confiance.
- Un label de sécurité englobant l'ISO 27001 et l'ISO 27017/27018 pour un cloud souverain.
- Les critères de protection vis-à-vis des lois extra-européennes.
- Vers une qualification européenne de prestataires de services informatiques en nuage EUCS ?

5) Un modèle pour la santé : HDS (hébergeurs de données de santé)

- Le référentiel HDS : l'ISO 27001 comme socle.
- Les données de santé : exigences de protection et lien avec le RGPD.
- Les exigences complémentaires.
- Cadre de la certification des hébergeurs.

6) Un modèle pour la finance/paiement : PCI DSS v4

- L'industrie du paiement par carte PCI et ses référentiels d'exigences.
- Les principaux acteurs du secteur : marques, banques, marchands, PSP.
- L'écosystème des acteurs PCI : QSA, ASV, éditeurs certifiés…
- Les cybermenaces spécifiques sur les données CB : vol, skimming.
- La gestion d'un projet jusqu'à sa mise en conformité, premiers pas avec le SAQ.

7) La sécurité selon COBIT®, ITIL®

- COBIT®: un cadre pour aligner la gouvernance IT avec les objectifs de l'entreprise.
- Les processus de maîtrise des risques selon COBIT®.
- Les modèles organisationnels et RH.
- Les principes de sécurité selon COBIT®.
- Les templates de contrôle de la sécurité.
- ITIL® : un cadre de travail pour la délivrance des services IT.
- Les processus ITIL®.
- Le processus Information Security Management.
- ITIL® et ses liens avec l'ISO 27001.

8) Quels choix de stratégie ?

- Avantages et inconvénients de chacun des référentiels.
- Comparatifs et critères de choix.
- Les approches hybrides et complémentaires.
- Les coûts comparés et les alignements multiréférentiels.

LES DATES

CLASSE À DISTANCE
2024 : 30 sept., 02 déc.