Parcours certifiant sécurité des systèmes d'information

Bloc de compétences d'un Titre RNCP

Titre RNCP de 14 jours
Réf : XQN - Prix 2023 : 6 700€ HT

Ce parcours de formation représente le quatrième bloc de compétences du titre RNCP de niveau 7 (Bac +5) "Expert en informatique et systèmes d'information" reconnu par l'État. L'ensemble de ces formations vous permettra de comprendre les impératifs de sécurité des entreprises, les risques et les menaces ainsi que les solutions pour protéger le SI.

Ce cycle est composé de :

- Sécurité des Systèmes d'Information, synthèse (Réf. SSI, 3 jours)
- Cybersécurité réseaux/Internet, synthèse (Réf. SRI, 3 jours)
- ISO 27005:2018 Risk Manager, préparation à la certification (Réf. AIR, 3 jours)
- Plans de continuité des activités et des systèmes d'information (Réf. PDS, 2 jours)
- Sécuriser son environnement virtualisé (Réf. VMW, 2 jours)
- SCADA, la sécurité des systèmes industriels (Réf. DAY, 2 jours)
- Certification responsable cybersécurité (Réf. XYA, ½ journée)

OBJECTIFS PÉDAGOGIQUES

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

Comprendre les impératifs de sécurité des entreprises

Comprendre le concept de risque lié à la sécurité de l'information

Comprendre les enjeux pour l'entreprise d'une stratégie de continuité

Identifier les menaces de sécurité des environnements virtualisés

Analyser les risques d'une architecture SCADA

CERTIFICATION

Chaque bloc de compétences est validé au travers d'un examen écrit sous forme d'étude de cas. Certification déposée par IP-FORMATION. Date de décision du 24/04/2020 portant enregistrement au Répertoire national des certifications professionnelles.

LE PROGRAMME

dernière mise à jour : 12/2022

1) Sécurité de l'information et cybercriminalité

- Principes de sécurité : défense en profondeur, modélisation du risque cyber.
- Les méthodes de gestion de risques (ISO 27005, EBIOS RM).
- Panorama des normes ISO 2700x.
- Évolution de la cybercriminalité.
- Les nouvelles menaces (APT, spear phishing, watering hole, crypto-jacking...).
- Les failles de sécurité dans les logiciels.
- Le déroulement d'une cyberattaque (kill chain).
- Les failles 0day, 0day Exploit et kit d'exploitation.

2) Le management de risques selon l'ISO

- L'appréciation initiale en phase plan de la section 6 : planification.
- La norme 27005:2018 : Information scurity risk management.

FINANCEMENT

Ce cours est éligible au CPF.

PARTICIPANTS

Toute personne souhaitant développer ses connaissances de la sécurité des systèmes d'information (cybersécurité).

PRÉREQUIS

Être titulaire d'un diplôme de niveau 6 (Bac +3) ou d'un niveau 5 (BAC+2) et 3 ans d'expérience, sous réserve de la validation du dossier VAP. Connaissances de base en Python et en statistiques.

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 mise en œuvre d'un processus PDCA de management des risques.
- Le contexte, l'appréciation, le traitement, l'acceptation et la revue des risques.
- Les étapes de l'analyse de risques (identification, analyse et évaluation).
- La préparation de la déclaration d'applicabilité (SoA) et du plan d'action.
- Le partage des risques avec des tiers (cloud, assurance…) ; le domaine 15 de ISO 27002.
- La méthode de la norme 27001:2013 et son processus « gestion des risques ».

3) Pourquoi gérer la continuité ?

- L'évolution des entreprises et de leur stratégie.
- L'importance stratégique de l'information.
- Les enjeux pour l'entreprise d'une stratégie de continuité : lois et réglementations, normes et standards.

4) La sécurité en environnement virtualisé

- Avantages industriels, risques.
- Les couches à surveiller.
- Le modèle sécurité zero trust : nouveau paradigme ?
- La micro-segmentation.
- La défense en profondeur.
- Les domaines sécuritaires : réseau, système, management, applications.

5) Introduction à la sécurité des systèmes SCADA

- La problématique de sécurité dans les systèmes SCADA.
- La cybersécurité des systèmes industriels, les méthodes de classification.
- Les menaces et les vulnérabilités, les intrusions connues, les attaques APT (menaces persistantes avancées).
- Les scénarios d'attaques réelles sur les systèmes SCADA : STUXNET, FLAME.
- L'analyse des attaques : construction de l'arbre d'attaque de STUXNET.
- Authentification/chiffrement.

LES DATES

Ce parcours est composé d'un ensemble de modules. Les dates indiquées ci-dessous correspondent aux premières sessions possibles du parcours.

CLASSE À DISTANCE	PARIS	BRUXELLES
2023 : 27 juin, 27 sept., 27 nov., 18 déc.	2023 : 03 juil., 26 sept., 21 nov., 13 déc.	2023 : 26 sept., 20 nov.