Parcours certifiant manager la cybersécurité des systèmes, applications et bases de données
Bloc de compétences d'un titre RNCP

Titre RNCP de 24 jours - 168h
Réf : ZCA - Prix 2024 : 12 500€ HT

Ce parcours de formation représente le quatrième bloc de compétences du titre RNCP de niveau 7 (Bac +5) "Expert en informatique et système d'information - cybersécurité" reconnu par l'État. L'ensemble de ces formations vous permettra de maîtriser les actions et les solutions permettant d'assurer la sécurité de votre SI. Vous apprendrez également à manager les risques relatifs à la sécurité de l'information sur les principes et usages de la méthode EBIOS, réaliser des tests de pénétration suite à des attaques, collecter, préserver des preuves et les analyser.

Ce cycle est composé de :

- Sécurité des Systèmes d'Information, synthèse (Réf. SSI, 3 jours)
- Cybersécurité réseaux/Internet, synthèse (Réf. SRI, 3 jours)
- Risk Manager - Méthode EBIOS (Réf. EBU, 2 jours)
- Hacking et sécurité, niveau 1 (Réf. HAC, 5 jours)
- Tests d'intrusion, organiser son audit (Réf. TEI, 4 jours)
- Cybersécurité, tester ses environnements (Réf. CTE, 3 jours)
- Analyse Forensic (Réf. AFB, 3 jours)
- Certification manager la cybersécurité des systèmes, applications et bases de données (Réf. ZAM, 1 jour)

OBJECTIFS PÉDAGOGIQUES

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

Maîtriser le processus de gouvernance de la sécurité

Maîtriser la sécurité du cloud, des applications, des postes clients

Comprendre les principes de la cryptographie

Comprendre les concepts et les principes d'EBIOS (Expression des besoins et identification des objectifs de sécurité)

Cartographier les risques

Réaliser un test de pénétration

Définir l'impact et la portée d'une vulnérabilité

Rédiger un rapport final suite à un test d'intrusion

CERTIFICATION

Chaque bloc de compétences est validé au travers d'un examen écrit sous forme d'étude de cas.

LE PROGRAMME

dernière mise à jour : 04/2024

1) Sécurité des systèmes d'information, synthèse

- Les fondamentaux de la sécurité du système d'information.
- La task force SSI : de multiples profils métiers.
- Les cadres normatifs et réglementaires.
- Le processus d'analyse des risques.

PARTICIPANTS

Toute personne souhaitant manager la cybersécurité des systèmes, applications et bases de données.

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 de Validation des acquis professionnels (VAP). Connaître le guide sécurité de l'ANSSI.

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.

- Les audits de sécurité et la sensibilisation des utilisateurs.
- Le coût de la sécurité et les plans de secours.
- Concevoir des solutions techniques optimales.
- Supervision de la sécurité.
- Les atteintes juridiques au système de traitement automatique des données.
- Recommandations pour une sécurisation "légale" du SI.

2) Cybersécurité réseaux/Internet, synthèse

- Sécurité de l'information et cybercriminalité.
- Firewall, virtualisation et cloud computing.
- Sécurité des postes clients.
- Fondamentaux de la cryptographie.
- Authentification et habilitation des utilisateurs.
- La sécurité des flux réseaux.
- Sécurité WiFi.
- Sécurité des smartphones.
- Gestion et supervision active de la sécurité.

3) Risk manager - Méthode EBIOS

- La méthode EBIOS risk manager.
- Cadrage et socle de sécurité.
- Sources de risques.
- Scénarios stratégiques.
- Scénarios opérationnels.
- Traitement du risque.

4) Hacking et sécurité, niveau 1

- Le hacking et la sécurité.
- Sniffing, interception, analyse, injection réseau.
- La reconnaissance, le scanning et l'énumération.
- Les attaques web.
- Les attaques applicatives et post-exploitation.

5) Tests d'intrusion, organiser son audit

- Les menaces.
- Méthodologie de l'audit.
- Les outils de pentest.
- Rédaction du rapport.
- Mises en situation.

6) Cybersécurité, tester ses environnements

- Les attaques web.
- Détecter les intrusions.
- La collecte des informations.

7) Analyse forensique

- Comment gérer un incident ?
- Analyser les incidents pour mieux se protéger : l'analyse forensique.
- Analyse forensique d'un système d'exploitation Windows.

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
2024 : 04 juin, 09 sept., 17 déc.	2024 : 28 mai, 15 oct., 10 déc.