Surveiller un système d'information sur des critères de sécurité informatique
Parcours certifiant RS - Code 5020

Titre RNCP de 9 jours - 63h
Réf : ZIX - Prix 2024 : 5 350CHF HT

Ce parcours vous apprend à surveiller un système d'information sur des critères de sécurité informatique. Vous verrez aussi comment gérer le processus de supervision de la sécurité SI, identifier les menaces et sécuriser les applications web ainsi que les fondamentaux de la gestion des risques avec la méthode EBIOS.

Ce cycle est composé de :

- Cybersécurité réseaux/Internet, synthèse (Réf. SRI, 3 jours)
- Sécurité des applications Web, synthèse (Réf. SEW, 2 jours)
- EBIOS Risk Manager, certification PECB (Réf. EBN, 3 jours)
- Certification "Surveiller un système d'information sur des critères de sécurité informatique" (Réf. ZXX, 1 jour)

OBJECTIFS PÉDAGOGIQUES

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

Connaître l'évolution de la cybercriminalité et de ses enjeux

Gérer les processus de supervision de la sécurité SI

Comprendre la méthode EBIOS

Identifier les menaces de sécurité sur les applications web

Comprendre les typologies d'attaque

Sécuriser les applications web

CERTIFICATION

Ce parcours de formation est validé via la rédaction et la présentation orale d'un projet professionnel.

LE PROGRAMME

dernière mise à jour : 07/2022

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, cryptojacking…).
- Les failles de sécurité dans les logiciels.
- Le déroulement d'une cyberattaque (kill chain).
- Les failles zero day, zero day exploit et kit d'exploitation.

2) Gestion et supervision active de la sécurité

- Les audits de sécurité (scope et référentiels : ISO 27001, RGPD….).
- Les tests d'intrusion (black box, gray box et white box).
- Les plateformes de « bug bounty ».

PARTICIPANTS

RSSI, DSI, architectes, développeurs, chefs de projet, commerciaux avant-vente, administrateurs système et réseau.

PRÉREQUIS

Le candidat doit justifier d'une expérience professionnelle d'un an minimum en tant que technicien systèmes et réseaux ou assimilé.

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.

- Comment répondre efficacement aux attaques ?
- Mettre en place une solution de SIEM (Security information and event management).
- Mettre en œuvre ou externaliser son Security Operation Center (SOC) ?
- Les technologies du SOC 2.0 (CASB, UEBA, Deceptive Security, EDR, SOAR, machine learning...).
- Les labels ANSSI (PASSI, PDIS & PRIS) pour l'externalisation.
- Les procédures de réponse à incident (ISO 27035 et NIST SP 800-61 R2).

3) La méthode EBIOS risk manager

- Les fondamentaux de la gestion des risques.
- Zoom sur la cybersécurité (menaces prioritaires).
- Présentation d'EBIOS.
- Principales définitions d'EBIOS risk manager.

4) Menaces, vulnérabilités des applications web

- Risques majeurs des applications web selon IBM X-Force et OWASP.
- Attaques de type cross-site scripting (XSS), injection et sur sessions.
- Propagation de faille avec un web worm.
- Attaques sur les configurations standard.

5) Sécuriser efficacement les applications web

- Durcissement, hardening : sécuriser le système et le serveur HTTP.
- Virtualisation et sécurité des applications web.
- Environnements .NET, PHP et Java. Les 5 phases du SDL.
- Techniques de fuzzing. Qualifier son application avec l'ASVS.
- WAF : quelle efficacité, quelles performances ?

6) Contrôler la sécurité des applications web

- Pentest, audit de sécurité, scanners de vulnérabilité.
- Organiser une veille technologique efficace.
- Déclaration des incidents de sécurité.

Démonstration : Mise en œuvre d'un serveur web avec certificat X509 EV : analyse des échanges protocolaires. Exploitation d'une faille de sécurité critique sur le frontal HTTP. Attaque de type HTTPS stripping.

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
2024 : 18 juin, 09 oct., 04 nov.