Parcours introductif à la Cybersécurité

Cycle de 10 jours - 70h
Réf : BCS - Prix 2024 : 6 640CHF HT

A l'issue de la formation, l'apprenant sera capable de mettre en oeuvre de manière opérationnelle les principes fondamentaux, les normes et les outils de la sécurité informatique.

Ce cycle est composé de :

- Introduction à la sécurité informatique (Réf. ISI, 1 jour)
- Les fondamentaux de la sécurité des SI (Réf. FTS, 3 jours)
- La sécurité dans le cyberespace (Réf. SCE, 3 jours)
- Cybersécurité, tester ses environnements (Réf. CTE, 3 jours)

OBJECTIFS PÉDAGOGIQUES

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

Détenir une vision globale de la cybersécurité et son environnement (enjeux, écosystème…)

Connaître les différents référentiels, normes et outils de la cybersécurité

Appréhender les métiers liés à la cybersécurité

Connaître les obligations juridiques liées à la cybersécurité

Comprendre les principaux risques et menaces ainsi que les mesures de protection

Identifier les bonnes pratiques en matière de sécurité informatique

LE PROGRAMME

dernière mise à jour : 07/2022

1) Les menaces et les risques

- Qu'est-ce la sécurité informatique ?
- Comment une négligence peut-elle créer une catastrophe ?
- Les responsabilités de chacun.
- L'architecture d'un SI et ses vulnérabilités potentielles.
- Les réseaux d'entreprise (locaux, distantes, Internet).
- Les réseaux sans fil et mobilité. Les applications à risques : Web, messagerie...
- La base de données et système de fichiers. Menaces et risques.
- La sociologie des pirates. Réseaux souterrains. Motivations.

2) La sécurité du poste de travail

- La confidentialité, la signature et l'intégrité. Les contraintes liées au chiffrement.
- Les différents éléments cryptographiques. Windows, Linux ou MAC OS : quel est le plus sûr ?
- Gestion des données sensibles. La problématique des ordinateurs portables.
- Les différentes menaces sur le poste client ? Comprendre ce qu'est un code malveillant.
- Comment gérer les failles de sécurité ?
- Les ports USB. Le rôle du firewall client.

3) Le processus d'authentification

- Les contrôles d'accès : l'authentification et l'autorisation.

PARTICIPANTS

Toutes personnes souhaitant apprendre les fondamentaux de la sécurité informatique et/ou souhaitant s'orienter vers les métiers de la cybersécurité (techniciens, administrateurs systèmes et réseaux).

PRÉREQUIS

Avoir des connaissances générales dans les systèmes d'information et connaître le guide d'hygiène 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.

- L’importance de l'authentification.
- Le mot de passe traditionnel.
- L’authentification par certificats et par token.
- La connexion à distance via Internet.
- Qu’est-ce qu’un VPN ?
- Pourquoi utiliser une authentification renforcée.

4) Le processus d’un audit de sécurité

- Processus continu et complet.
- Les catégories d’audits, de l’audit organisationnel au test d’intrusion.
- Les bonnes pratiques de la norme 19011 appliquées à la sécurité.
- Comment créer son programme d’audit interne ? Comment qualifier ses auditeurs ?
- Apports comparés, démarche récursive, les implications humaines.
- Sensibilisation à la sécurité : qui ? Quoi ? Comment ?
- Définitions de Morale/Déontologie/Ethique.
- La charte de sécurité, son existence légale, son contenu, sa validation.

5) Le plan de secours et le coût de la sécurité

- La couverture des risques et la stratégie de continuité.
- L'importance des plans de secours, de continuité, de reprise et de gestion de crise, PCA/PRA, PSI, RTO/RPO.
- Développer un plan de continuité, l’insérer dans une démarche qualité.
- Comment définir les budgets sécurité.
- La définition du Return On Security Investment (ROSI).
- Quelles sont les techniques d’évaluation des coûts, les différentes méthodes de calcul, Total Cost of Ownership (TCO).
- La notion anglo-saxonne du “Payback Period”.

6) Le pare-feu, la virtualisation et le Cloud Computing

- Les serveurs proxy, reverse proxy, le masquage d'adresse.
- La protection périmétrique basée sur les pare-feu.
- Les différences entre firewalls UTM, enterprise, NG et NG-v2.
- Les produits d’Intrusion Prevention System (IPS) et les IPS NG.
- Les solutions DMZ (zones démilitarisées).
- Les vulnérabilités dans la virtualisation.
- Les risques associés au Cloud Computing selon l'ANSSI, l'ENISA et la CSA.
- Le Cloud Control Matrix et son utilisation pour l'évaluation des fournisseurs de Cloud.

7) La supervision de la sécurité

- Les tableaux de bord sécurité.
- Les audits de sécurité et les tests d'intrusion.
- Les aspects juridiques des tests d'intrusion.
- Les sondes IDS, scanner VDS, WASS.
- Comment répondre efficacement aux attaques ?
- Consigner les éléments de preuve.
- Mettre en place une solution de SIEM.
- Les labels ANSSI (PASSI, PDIS & PRIS) pour l'externalisation.
- Comment réagir en cas d'intrusion ?
- L'expertise judiciaire : le rôle d'un expert judiciaire (au pénal ou au civil).
- L'expertise judiciaire privée.

8) Les attaques Web

- OWASP : organisation, chapitres, Top10, manuels, outils.
- Découverte de l'infrastructure et des technologies associées, forces et faiblesses.
- Côté client : clickjacking, CSRF, vol de cookies, XSS, composants (flash, java). Nouveaux vecteurs.

- Côté serveur : authentification, vol de sessions, injections (SQL, LDAP, fichiers, commandes).
- Inclusion de fichiers locaux et distants, attaques et vecteurs cryptographiques.
- Evasion et contournement des protections : exemple des techniques de contournement de WAF.
- Outils Burp Suite, ZAP, Sqlmap, BeEF.

Mise en situation : Présentation et prise en main des environnements, outils. Mise en œuvre de différentes attaques Web en conditions réelles côté serveur et côté client.

9) Détecter les intrusions

- Les principes de fonctionnement et méthodes de détection.
- Les acteurs du marché, panorama des systèmes et applications concernés.
- Les scanners réseaux (Nmap) et applicatifs (Web applications).
- Les IDS (Intrusion Detection System).
- Les avantages de ces technologies, leurs limites.
- Comment les placer dans l'architecture d'entreprise ?
- Panorama du marché, étude détaillé de SNORT.

Mise en situation : Présentation et prise en main des environnements, outils. Installation, configuration et mise œuvre de SNORT, écriture de signature d'attaques.

10) La collecte des informations

- L'hétérogénéité des sources. Qu'est-ce qu'un événement de sécurité ?
- Le Security Event Information Management (SIEM). Les événements collectés du SI.
- Les journaux système des équipements (firewalls, routeurs, serveurs, bases de données, etc.).
- La collecte passive en mode écoute et la collecte active.

Mise en situation : Démarche d'une analyse de log. La géolocalisation d'une adresse. La corrélation de logs d'origines différentes, visualiser, trier et chercher les règles.

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 : 17 juin, 30 sept., 25 nov.