Parcours Intégrateur sécurité, le métier

Cycle de 7 jours
Réf : XRY - Prix 2023 : 4 950€ HT

Ce parcours de formation, très pratique, permettra aux candidats de connaître les failles et les menaces des systèmes d'information, maîtriser le rôle des divers équipements de sécurité ainsi que de mettre en œuvre les principaux moyens de sécurisation des réseaux.

Ce cycle est composé de :

- Les bases de la sécurité systèmes et réseaux (Réf. BSR, 3 jours)
- Cisco Firewall ASA, installation et configuration (Réf. CSC, 2 jours)
- Check Point R81, installation et configuration (Réf. CPI, 2 jours)

OBJECTIFS PÉDAGOGIQUES

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

Connaître les failles et les menaces des systèmes d'information

Maîtriser le rôle des divers équipements de sécurité

Savoir mettre en œuvre les principaux moyens de sécurisation des réseaux

LE PROGRAMME

dernière mise à jour : 10/2018

1) Les bases de la sécurité systèmes et réseaux

- Le métier d'intégrateur sécurité.
- Risques et menaces.
- Architectures de sécurité.
- Sécurité des données.

2) Sécurité des échanges

- Sécurité WiFi.
- Risques inhérents aux réseaux sans fil.
- Les limites du WEP. Le protocole WPA et WPA2.
- Les types d'attaques.
- Attaque Man in the Middle avec le rogue AP.
- Le protocole IPSec.
- Modes tunnel et transport. ESP et AH.
- Analyse du protocole et des technologies associées (SA, IKE, ISAKMP, ESP, AH...).

3) Sécuriser un système, le "Hardening"

- Insuffisance des installations par défaut.
- Critères d'évaluation (TCSEC, ITSEC et critères communs).
- Sécurisation de Windows.
- Gestion des comptes et des autorisations.
- Sécurisation de Linux.

4) Introduction Firewall ASA

- Les technologies et caractéristiques des firewalls.

PARTICIPANTS

Techniciens et administrateurs systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances en réseaux et sécurité. Connaître le guide d'hygiène sécurité de l'ANSSI. Avoir suivi le parcours introductif à la cybersécurité.

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.

- Présentation des firewalls. Terminologie et fonctionnalités.
- Exemples d'architecture. La gamme ASA.
- Le démarrage avec un ASA. L'interface utilisateur. Configuration du firewall.
- Paramétrage de NTP. Les niveaux de sécurité ASA.
- Configuration de Syslog.

5) Firewall ASA, installation et configuration

- Introduction.
- ACL et Content Filtering.
- Configuration AAA.
- Failover.

6) Check Point R77, installation et configuration

- Introduction. Les produits Check Point. Les composants. Nouveautés de la version R77.
- Architecture et installation. Le mode distribué et en standalone. Le serveur de management. Le protocole SIC.
- Mettre en place une politique de sécurité. Prise en main de SmartConsole. Démarrer et utiliser SmartDashboard.
- La translation d'adresses (NAT). Les règles de translation d'adresses. Le NAT "static" et le NAT "hide".
- Le VPN site à site. L'architecture du VPN. Bases du chiffrement. Introduction IPSec. L'autorité de certification (CA).

7) Architecture et installation

- L'architecture en mode distribué et en standalone.
- Le serveur de management. Le protocole SIC.
- Présentation du système Gaïa.
- L'interface en ligne de commandes (CLI).
- Les commandes de sauvegarde et de restauration.

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
2023 : 28 août, 27 sept., 08 nov.

PARIS
2023 : 28 août, 27 sept., 08 nov.

LYON
2023 : 16 août, 13 nov.

AIX-EN-PROVENCE
2023 : 16 août, 20 nov.

BORDEAUX
2023 : 31 juil., 25 oct.

GRENOBLE
2023 : 16 août, 13 nov.

LILLE
2023 : 28 août, 08 nov.

MONTPELLIER
2023 : 16 août, 20 nov.

ORLÉANS
2023 : 28 août, 08 nov.

NANTES
2023 : 25 oct.

RENNES
2023 : 25 oct.

SOPHIA-ANTIPOLIS
2023 : 16 août, 20 nov.

STRASBOURG
2023 : 25 oct.

TOULOUSE
2023 : 31 juil., 25 oct.