Intégrateur sécurité réseaux

Sécuriser les réseaux de l'entreprise - Certification incluse

Présentiel ou en classe à distance

5 jours (35 h) Réf.: CISR1

Dans toute entreprise ou organisation se trouve un système d'information qui est aujourd'hui au coeur de toutes les activités de l'entité. Sans système d'information opérationnel, plus d'activités ! Le protéger des malveillance et assurer son bon fonctionnement tout en préservant ses performances est donc un enjeu crucial. Cette formation certifiante est dédiée aux savoirs fondamentaux nécessaires pour sécuriser les réseaux d'entreprises et organisations. La certification associée à la formation permet de valider des savoirs décrits dans les fiches métiers de l'ANSSI (RSSI, Chef sécurité de projet, Architecte sécurité, Spécialiste sécurité d'un domaine technique, Administrateur de solutions de sécurité, Auditeur de sécurité technique, consultant en cybersécurité, Formateur en cybersécurité).
Cette formation prépare à la certification et inclus le voucher pour passer l'examen.

A qui s'adresse cette formation ?

Pour qui

- Comprendre les menaces qui pèsent sur les réseaux
- Connaitre le rôle des différents équipements de sécurité
- Savoir mettre en oeuvre un réseau sécurisé

Prérequis

- Connaissance du fonctionnement des réseaux informatique
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Introduction SSI

- Le numérique en entreprise
- La convergence des réseaux
- Les outils d'attaques
- Les typologies d'attaques
- Les CVE et CVSS
- Les attaques APT
- The Unified Kill Chain
- Les piliers de la sécurité
- Les principes généraux de la sécurité
- La sécurité dans le cyber-espace
- Les acteurs de la cybersécurité
- La sécurité offensive

2 - Les bases de la cryptographie

- Vocabulaire et objectifs
- Chiffrement de César et chiffrement de Vigenère
- Principe de Kerckhoffs
- Le chiffrement symétrique
- Le chiffrement symétrique

- Les recommandations de sécurité
- Fonction de hash

3 - Virtual Private Network et Accès sécurisé

- Définition
- Les implémentations VPN
- Les protocoles VPN
- IPSEC
- TLS
- Autres protocoles sécurisés : SSH
- TP : Mise en place du VPN IPSec et mise en place de SSH

4 - IAM

- Gestion des identités et des accès
- IAAA
- Les méthodes d'authentification
- Cycle de vie des accès
- Stratégie de gestion des identités
- LDAP
- Les modèles de contrôle des accès
- Les implémentations
- Focus sur Kerberos
- TP : Mise en place de Kerberos

5 - Pare-feu

- Définition
- Place du pare-feu dans le modèle OSI
- Règles de pare-feu
- Pare-feu Stateless et Statefull
- Politique de filtrage
- Les limites des pare-feux traditionnels
- Les pare-feux nouvelles génération
- Méthodologie de la mise en place d'une politique de filtrage
- Bonnes pratiques d'ordre général
- TP : Étude d'une cartographie et mise en place d'une politique de filtrage

6 - Proxy

- Définition
- Pourquoi un serveur mandataire ?
- Le filtrage URL
- Les types de proxy
- Les implémentations de proxy
- TP : Mise en place d'un proxy et de règles de filtrage

7 - Les architectures de passerelle d'interconnexion

- Le concept
- La passerelle d'interconnexion selon les niveaux de sécurité

8 - Sécurité des équipements réseaux

- Administration
- Cloisonnement des réseaux
- Sécurisation des ports
- Mécanismes liés à la disponibilité
- Synchronisation horaire et horodatage
- Journalisation
- TP : Durcissement de commutateurs et routeurs

9 - Examen blanc : préparation examen final

10 - Evaluation et validation

- Partie théorique et pratique
- Le temps destiné au passage de la certification est de 3H.
- L'examen est composé de 3 parties : QCM, mise en situation sur points spécifiques, mise en situation sur cas concrets.
- Il peut se dérouler à distance.
- L'accès au support de cours, aux travaux pratiques est assuré pendant trois semaines à compter du début de session.
- Le passage de la certification doit être réalisé en ce laps de temps.

- En cas d’échec au premier passage de la certification le candidat a la possibilité de réaliser un second passage dans les 15 j suivants le premier passage.

Les objectifs de la formation

- Être capable de comprendre les menaces qui pèsent sur les réseaux
- Pouvoir maîtriser le rôle des équipements de sécurité
- Comprendre comment mettre en oeuvre un réseau sécurisé

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une formation orientée sur la pratique : 70% du temps est consacré à des ateliers.
- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'en faciliter l'assimilation par les participants.
- Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions. Le passage de l'examen est compris dans le prix de la formation.