Parcours certifiant Veille et Sécurité SI
Bloc de compétences d'un Titre RNCP

Titre RNCP de 14 jours - 98h
Réf : ZVS - Prix 2024 : 7 120CHF HT

Ce parcours de formation représente le septième bloc de compétences du titre RNCP de Niveau 6 (bac+3) "Administrateur du système d'information" reconnu par l'État. L'ensemble de ces formations vous permettra d'apprendre les risques et les menaces portant atteinte à la sécurité du système d'information ainsi que les différentes étapes pour mettre en place une veille concurrentielle efficace.

Ce cycle est composé de :

- Sécurité systèmes et réseaux, niveau 1 (Réf. FRW, 4 jours)
- Sécurité systèmes et réseaux, niveau 2 (Réf. SEA, 4 jours)
- Sécurité des applications Web (Réf. SER, 3 jours)
- Mettre en œuvre une veille concurrentielle efficace (Réf. VCU, 2 jours)
- Certification Veille et Sécurité SI (Réf. ZVX, ½ journée)

OBJECTIFS PÉDAGOGIQUES

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

Apprendre les fondamentaux de la sécurité des systèmes d'information

Sécuriser les systèmes d'information en mode avancé

Savoir sécuriser les applications web

Mettre en œuvre une veille concurrentielle efficace

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 : 10/2021

1) Architectures de sécurité

- Quelles architectures pour quels besoins ?
- Plan d'adressage sécurisé : RFC 1918.
- Translation d'adresses (FTP comme exemple).
- Le rôle des zones démilitarisées (DMZ).
- Exemples d'architectures.
- Sécurisation de l'architecture par la virtualisation.
- Firewall : pierre angulaire de la sécurité.
- Actions et limites des firewalls réseaux traditionnels.
- Évolution technologique des firewalls (Appliance, VPN, IPS, UTM...).
- Les firewalls et les environnements virtuels.
- Proxy serveur et relais applicatif.
- Proxy ou firewall : concurrence ou complémentarité ?
- Reverse proxy, filtrage de contenu, cache et authentification.
- Relais SMTP, une obligation ?

Travaux pratiques : Mise en œuvre d'un proxy Cache/Authentification.

PARTICIPANTS

Toute personne souhaitant apprendre la sécurité des systèmes et des réseaux.

PRÉREQUIS

Être titulaire d'un diplôme de niveau 5 (Bac +2). Si ce n'est pas le cas, être titulaire d'un niveau 4 (BAC) et 3 ans d'expérience, sous réserve de la validation du dossier VAP par le certificateur.

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.

2) 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 détaillée de Snort.

Travaux pratiques : Installation, configuration et mise œuvre de SNORT, écriture de signature d'attaques.

3) Les vulnérabilités des applications web

- Pourquoi les applications web sont-elles plus exposées ?
- Les risques majeurs des applications web selon l'OWASP (Top Ten 2017).
- Les attaques "Cross Site Scripting" ou XSS - Pourquoi sont-elles en pleine expansion ? Comment les éviter ?
- Les attaques en injection (commandes injection, SQL injection, LDAP injection...).
- Les attaques sur les sessions (cookie poisonning, session hijacking...).
- Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode...).
- Attaques sur les configurations standard (default password, directory transversal...).

Travaux pratiques : Attaque Cross Site Scripting. Exploitation d'une faille sur le frontal http. Contournement d'une authentification par injection de requête SQL.

4) Les outils documentaires de veille et la surveillance du web

- Les sociétés de piges.
- Les abonnements : presse, newsletters, flux RSS...
- Les types d'informations web recherchées.
- Les modalités, les outils de collecte et d'analyse des contenus.
- La constitution du référentiel (sites web, blogs, forums).
- Les aspirateurs de sites, les logiciels de cartographie de l'information.
- Les logiciels spécialisés de veille globale.

Exercice : Identification de sites Internet pouvant entrer dans la définition d'un référentiel pour une entreprise.

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 : 28 mai, 16 juil., 10 sept., 19 nov.