Analyser les incidents de sécurité détectés
Parcours certifiant RS - Code 5021

Titre RNCP de 11 jours - 77h
Réf : ZIW - Prix 2024 : 5 090CHF HT

Ce parcours de formation vous apprend à analyser les incidents de sécurité informatique détectés dans votre SI. Vous verrez les fondamentaux des réseaux informatiques, comment détecter les attaques et mettre en place les moyens pour se protéger, ainsi que la collecte et l'analyse des logs.

Ce cycle est composé de :

- TCP/IP, mise en œuvre (Réf. INR, 4 jours)
- Sécurité systèmes et réseaux, niveau 1 (Réf. FRW, 4 jours)
- Collecte et analyse des logs, un SIEM pour optimiser la sécurité de votre SI (Réf. LOG, 2 jours)
- Certification "Analyser les incidents de sécurité détectés" (Réf. ZXW, 1 jour)

OBJECTIFS PÉDAGOGIQUES

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

Apprendre à collecter et à analyser les logs

Apprendre les fondamentaux des réseaux informatiques

Connaître les failles et les menaces des systèmes d'information

Concevoir et réaliser une architecture de sécurité adaptée

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) 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.

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

2) Le logiciel Splunk

- L'architecture et le framework MapReduce. Comment collecter et indexer les données ?
- Exploiter les données machine. L'authentification des transactions.
- L'intégration aux annuaires LDAP et aux serveurs Active Directory.
- Les autres logiciels du marché : Syslog, SEC (Simple Event Correlator), ELK (suite Elastic), Graylog, OSSIM, etc.

Travaux pratiques : Installation et configuration d'un logiciel (Splunk, ELK ou autre). Exemple d'analyse et de corrélation des données.

PARTICIPANTS

Techniciens informatiques.

PRÉREQUIS

Les candidats doivent 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.

3) Introduction à TCP/IP

- Notions fondamentales. Architecture et normalisation.
- Services et protocoles. Mécanismes de communication.
- Mode de transfert. Fiable et non fiable, connecté ou non connecté.
- Le modèle client-serveur.
- Les RFC. Rôle de l'IETF, principe de la standardisation.

4) Interconnexion de réseaux IP

- Passerelle. Définition. Translation d'adresses publiques privées via la passerelle Internet (NAT, PAT).
- Répéteur. Interconnexion physique de réseaux.
- Pont. La segmentation du trafic. Le filtrage.
- Le protocole Spanning tree : élection du pont racine, choix des ports passants.
- Le routeur. Protocoles de routage dynamique. Routage à vecteur de distance : RIP, EIGRP.
- Routage à état de liaison : OSPF. Routage à vecteur de chemin : BGP.
- Le switch. Les techniques de commutation. La gestion de la bande passante.
- Les LAN virtuels : VLAN. Principe de fonctionnement.
- Introduction aux réseaux sans fil (802.11x). Les fréquences radio. La sécurité.

Travaux pratiques : Réaliser et valider une interconnexion de réseaux IP différents. Comparer l'utilisation de différents protocoles de routage. Comparer les performances en LAN et en VLAN.

5) Risques et menaces

- Introduction à la sécurité.
- État des lieux de la sécurité informatique.
- Le vocabulaire de la sécurité informatique.
- Attaques « couches basses ».
- Forces et faiblesses du protocole TCP/IP.
- Illustration des attaques de type ARP et IP Spoofing, TCP-SYNflood, smurf, etc.
- Déni de service et déni de service distribué.
- Attaques applicatives.
- Intelligence gathering.
- HTTP, un protocole particulièrement exposé (SQL injection, Cross site scripting, etc.).
- DNS : attaque Dan Kaminsky.

Travaux pratiques tutorés : Installation et utilisation de l'analyseur réseau Wireshark. Mise en œuvre d'une attaque applicative.

6) 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.

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 : 14 mai, 16 juil., 05 nov.