Big Data, sécurité des données

Cours Pratique de 2 jours - 14h
Réf : SBD - Prix 2024 : 1 620€ HT

A l'issue de la formation, le stagiaire sera capable d'initier une politique de sécurisation des données par une approche technique et légale du sujet.

OBJECTIFS PÉDAGOGIQUES

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

Comprendre la qualification complexe des données

Identifier les principaux risques touchant les solutions de traitement des données massives

Maîtriser le cadre juridique (CNIL et PLA (Privacy Level Agreement))

Connaître les principales solutions techniques de base pour se protéger des risques

Mettre en oeuvre une politique de sécurité pour traiter les risques, les menaces, les attaques

LE PROGRAMME

dernière mise à jour : 11/2022

1) Risques et menaces

- Introduction à la sécurité. Les sources d'information externes incontournables (ANSSI, CLUSIF, ENISA, etc.).
- Etat des lieux de la sécurité informatique.
- Le vocabulaire de la sécurité informatique.
- La classification DICT/P : Disponibilité, Intégrité, Confidentialité et Traçabilité/Preuve.
- Attaques "couches basses". La sécurité sur Hadoop. Intelligence gathering.
- Forces et faiblesses du protocole TCP/IP. HTTP : protocole exposé (SQL injection,Cross Site Scripting, etc.).
- Illustration des attaques de type ARP et IP Spoofing, TCPSYNflood, SMURF, etc
- Déni de service et déni de service distribué. DNS : attaque Dan Kaminsky. Attaques applicatives.

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

2) 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, firewalls et environnements virtuels.
- Proxy serveur et relais applicatif. Proxy ou firewall : concurrence ou complémentarité ?
- Evolution technologique des firewalls (Appliance, VPN, IPS,UTM...).
- Reverse proxy, filtrage de contenu, cache et authentification. Relais SMTP : une obligation ?

Travaux pratiques : Mise en œuvre d'un proxy cache/authentification.

3) Vérifier l'intégrité d'un système

- Les principes de fonctionnement.
- Quels sont les produits disponibles ?

PARTICIPANTS

Consultants sécurité et SI, administrateurs système.

PRÉREQUIS

Notions d'architectures applicatives. Avoir de bonnes connaissances dans la sécurité réseau et système, connaitre les plateformes Hadoop.

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 de Tripwire ou AIDE (Advanced Intrusion Detection Environment).
- L'audit de vulnérabilités.
- Principes et méthodes et organismes de gestion des vulnérabilités.
- Site de référence et panorama des outils d'audit.
- Définition d'une politique de sécurité.
- Etude et mise en œuvre de Nessus (état, fonctionnement, évolution).

Travaux pratiques : Audit de vulnérabilités du réseau et serveurs à l'aide de Nessus et Nmap. Audit de vulnérabilités d'un site Web.

4) Les atteintes juridiques au Système de Traitement Automatique des Données

- Rappel, définition du Système de Traitement Automatique des Données (STAD).
- Les risques sur les solutions de traitement des données massives.
- Types d'atteintes, contexte européen, la loi LCEN. Le règlement RGPD, CNIL, PLA.
- Quels risques juridiques pour l'entreprise, ses dirigeants, le RSSI ?

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 15 juil., 17 oct.	2024 : 08 juil., 10 oct.