FC9BD05 1 800 € 2 jour(s)

[Formation] Introduction à la sécurité du Big Data

OBJECTIFS

- Identifier les problèmes de sécurité liés au Big Data
- Présenter et mettre en application les techniques de protection des données dans un contexte Big Data
- Mettre en place une architecture de sécurité en environnement Big Data

PROGRAMME

Introduction

Enjeux et problématiques de sécurité dans les systèmes d'information (SI) et les réseaux

- Exemples réels d'attaques et fraudes
- Problématique de confiance à distance dans un monde ouvert
- Contraintes et challenges de la sécurité en entreprise
- Enjeux de sécurité en nomadisme et accès distants
- Motivations et opportunités pour les attaquants
- Écosystème de sécurité, premiers conseils pratiques

Sécurité de l'information et protection des données

- Introduction à la sécurité de l'information
- Données à caractère personnel, gestion des identités
- Réglementation européenne et française (RGPD, CNIL, etc.)
- Conduite à tenir en entreprise
- Techniques d'anonymisation/désanonymisation

Introduction à la cryptographie

- Techniques logiques et cryptographie : systèmes à clé secrète, systèmes à clé publique
- Algorithmes et taille de clés
- Authentification, chiffrement, fonction de hachage, certificats et signature électronique

Infrastructures à clés publiques et applications

RÉALISABLE À DISTANCE

PANORAMA

DATES ET LIEUX

Nous contacter pour les sessions à venir

PUBLIC / PREREQUIS

Cette formation s'adresse plus particulièrement aux personnes souhaitant comprendre la problématique de la sécurité du Big Data, acquérir les bases techniques pour la protection des données et la mise en place de solutions de sécurité adaptées au Big Data.

Des connaissances de base en sécurité des données et des réseaux sont nécessaires pour tirer un meilleur profit de cette formation.

COORDINATEURS

Xavier AGHINA

Responsable de la Sécurité des Systèmes d'Information (RSSI) chez W-HA, avec l'objectif de garantir la sécurité, la disponibilité et l'intégrité du système d'information et des données. Il a développé une expertise en cybersécurité, par la conduite des projets techniques et un programme de recherche sur le paiement mobile et la protection des objets connectés.

MODALITES PEDAGOGIQUES

Des exemples illustrent les concepts théoriques.

sécurisées

- Certificats numériques et infrastructure à clé publique
- Application à la sécurité des Big Data

Sécurité Internet, vulnérabilités et attaques logiques

- Analyse d'une APT (Advanced Persistent Threat)
- Menaces des applications web
- Risques liés aux malwares
- Observation des menaces, écosystème

Architectures de sécurité

- Protocoles de sécurité : SSL, IPSec
- Architecture sécurisée : Firewall, DMZ, VPN
- Appliance IPS/IDS/UTM/DLP
- Politique et audits de sécurité

Sécurité du Cloud et connaissance des risques

- Connaissances des risques du Cloud
  - Environnements virtuels
  - Sécurité de l'hyperviseur
- Contre-mesures, contrôles et monitoring de sécurité
- Security Information Management System (SIEM)
- Security Operating Center (SOC)

Composants de sécurité pour une architecture Big Data

- Briques de sécurité appliquée à un système classique Big Data
- Modèle de sécurité Hadoop
- Usage Big Data pour la sécurité des systèmes d'information

Synthèse et conclusion