Date de publication : 23/05/2025

Formation : Big Data, sécurité des données

Formation pratique - 2j - 14h00 - Réf. SBD
Prix : 1680 CHF H.T.

À l'issue de la formation, le participant est capable d'initier une politique de sécurisation des données par une approche technique et légale du sujet. Elle permet de comprendre les enjeux de la sécurité dans les environnements Big Data, d'identifier les risques majeurs et d'y répondre avec des solutions concrètes.

Objectifs pédagogiques

À l'issue de la formation, le participant 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 œuvre une politique de sécurité pour traiter les risques, les menaces, les attaques

Public concerné

Consultants sécurité et SI, administrateurs système.

Prérequis

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

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

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.

Programme de la formation

PARTICIPANTS

Consultants sécurité et SI, administrateurs système.

PRÉREQUIS

Notions d'architectures applicatives. Avoir de bonnes connaissances dans la sécurité réseau et système, connaître 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.

1 Risques et menaces

- Introduction à la sécurité. Les sources d'information externes incontournables (ANSSI, CLUSIF, ENISA, etc.).
- État 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 ?
- Évolution technologique des firewalls (Appliance, VPN, IPS, UTM, etc.).
- 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 ?
- 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.
- Étude 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.

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 formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation 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 participant 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

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

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 ?

Dates et lieux

CLASSE À DISTANCE
2026 : 18 juin, 19 nov.