+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 27/07/2023

S'inscrire

Formation Sécurité et Réglementation des données

2 jours (14 heures)

Présentation

Pour des raisons juridiques et éthiques, la sécurité des données est devenu un sujet fondamental. De nos jours, les lois encadrant la protection des données personnelles se multiplient. En effet, face aux sanctions de la CNIL, les entreprises peinent à se mettre en conformité. Pourtant, les bénéfices d'un traitement de données conforme et sécurisé sont nombreux. Il permet aux entreprises d'obtenir des données fiables, d'éviter les risques de cyberattaques et d'empêcher toutes atteinte à la protection de la vie privée. Acquérir des connaissances en protection d'infrastructure SI peut être un réel avantage pour contrer l'augmentation du nombre d'attaques cybercriminelles. Notre formation en sécurité et réglementation des données vous démystifiera le RGPD ainsi que le rôle de la CNIL. Vous découvrirez également les techniques permettant de sécuriser et qualifier vos données.

Objectifs

- Comprendre la qualification complexe des données
- Connaître les différents risques concernant les solutions de traitement des données massives
- Maitriser l'environnement juridique (CNIL, PLA et RGPD)
- Connaître les principales solutions techniques de base pour se protéger des risques
- Savoir mettre en œuvre une politique de sécurité pour traiter les risques, les menaces et les attaques

Public visé

- Consultant sécurité
- Consultant SI
- Administrateurs systèmes

Pré-requis

- Bonnes connaissances en sécurité réseau et système
- Connaître les plateformes Hadoop

Programme de notre formation sécurité des données

L'environnement juridique encadrant les traitements des données

- Présentation de la CNIL
- Les actions et le rôle de la CNIL
- Protection des données personnelles
- Privacy Level Agreement (PLA)

La RGPD

- Introduction à la RGPD
- Comment la CNIL intègre la RGPD ?
- Les notions fondamentales
- Les obligations légales définies par la RGPD
- Tenir un registre de traitement de données et le mettre à jour
- Désigner un DPO
- Obligation de sécuriser des données
- Maintenir la conformité de ses sous-traitants
- Les risques encourus en cas de non-respect

Mettre en œuvre une politique de sécurité

- Qu'est-ce qu'une bonne politique de sécurité des données ?
- Établir une politique de qualification des données
- Le processus pour élaborer une politique de qualification efficace
- Exemple de classification des données

Sécuriser son architecture

- Intégrer progressivement les pratiques de sécurité dans votre organisation
- Contrôler les accès
- Isoler les navigateurs
- Gérer les privilèges
- Se protéger du phishing
- Gestion des sessions et de l'authentification pour la totalité de son infrastructure SI
- Mettre en place une stratégie de gestion des risques

Se protéger des logiciels malveillants

- Présentation des différents malwares
- Les bonnes pratiques pour empêcher l'intrusion de virus
- Se protéger contre les botnets
- Introduction à la forensique
- Évaluer sa vulnérabilité

L'usage de la cryptographie

- Cryptage standard et avancé
- Le fonctionnement de la cryptographie (clés publiques, privées, algorithme RSA)
- Les approches modernes pour casser le chiffrement
- Les concepts cryptographiques actuels

Sécurité du navigateur et cross site scripting

- Les principes fondamentaux à connaître pour la sécurité du navigateur
- Hypertext Transfer Protocol
- Rendering Content
- Les cookies
- Frame Busting
- Isoler son code
- Sandbox
- Web worker
- Cross-Origin Ressource Sharing

Sécurité des serveurs

- Présentation des outils de cybersécurité
- Les rôles des serveurs et les protocoles
- Les bonnes pratiques de sécurité réseau
- Auditer et suivre la protection de ses systèmes

Sécuriser ses bases de données

- Appliquer la cryptographie aux bases de données
- L'analyse des privilèges
- Les principales menaces
- Gérer les accès
- Les bonnes pratiques de codage pour sécuriser ses bases de données

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.