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

Updated 07/27/2023

Sign up

Data security and regulation training

2 days (14 hours)

Presentation

For legal and ethical reasons, data security has become a fundamental issue. Today, the number of laws governing the protection of personal data is multiplying. Indeed, faced with CNIL sanctions, companies are struggling to comply. Yet the benefits of secure, compliant data processing are numerous. It enables companies to obtain reliable data, avoid the risk of cyber-attacks and prevent any breach of privacy. Acquiring knowledge of IS infrastructure protection can be a real advantage in countering the increasing number of cybercriminal attacks. Our data security and regulation training course will demystify the RGPD and the role of the CNIL. You'll also discover techniques for securing and qualifying your data.

Objectives

- Understanding complex data qualification
- Understanding the various risks associated with massive data processing solutions
- Master the legal environment (CNIL, PLA and RGPD)
- Know the main basic technical solutions to protect against risks
- Implement a security policy to deal with risks, threats and attacks

Target audience

- Security Consultant
- IS Consultant
- System administrators

Prerequisites

- Good knowledge of network and system security
- Understanding Hadoop platforms

Our data security training program

The legal environment for data processing

- Presentation of CNIL
- CNIL's actions and role
- Personal data protection
- Privacy Level Agreement (PLA)

The RGPD

- Introduction to the RGPD
- How does CNIL integrate RGPD?
- Fundamental concepts
- The legal obligations defined by the RGPD
- Maintain and update a data processing register
- Appointing a DPO
- Obligation to secure data
- Maintaining subcontractor compliance
- Risks of non-compliance

Implementing a safety policy

- What is a good data security policy?
- Establish a data qualification policy
- The process for developing an effective qualification policy
- Example of data classification

Securing your architecture

- Gradually integrate safety practices into your organization
- Access control
- Isolate browsers
- Manage privileges
- Protecting yourself against phishing
- Session and authentication management for its entire IS infrastructure
- Implement a risk management strategy

Protecting yourself against malware

- Malware overview
- Best practices to prevent virus intrusion
- Protecting yourself against botnets
- Introduction to forensics
- Assessing your vulnerability

The use of cryptography

- Standard and advanced encryption
- How cryptography works (public and private keys, RSA algorithm)
- Modern approaches to breaking encryption
- Current cryptographic concepts

Browser security and cross-site scripting

- Fundamentals of browser security
- Hypertext Transfer Protocol
- Rendering Content
- Cookies
- Frame Busting
- Isolating your code
- Sandbox
- Web worker
- Cross-Origin Resource Sharing

Server security

- Presentation of cybersecurity tools
- Server roles and protocols
- Network security best practices
- Auditing and monitoring system protection

Securing your databases

- Applying cryptography to databases
- Privilege analysis
- The main threats
- Manage access
- Best coding practices for secure databases

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.