Network/Internet cybersecurity, summary of IT and corporate communications protection

★★★★★

SII-303 **3 Days (21 Hours)**

Description

This seminar shows you how to meet business security requirements and integrate security into the architecture of an information system. It includes a detailed analysis of threats and means of intrusion as well as an overview of the main security measures available on the market. At the end of this seminar, you will have the technical and legal elements to understand how to ensure and supervise the security of your information system.

Who is this training for ?

For whom

CISO, CIO, architects, developers, project managers, pre-sales salespeople, system & network administrators.

Prerequisites

Aucune

Training objectives

- Know the evolution of cybercrime and its challenges
- Master the security of the Cloud, applications, client workstations
- Understand the principles of cryptography
- Manage IS security supervision processes

Training program

Sécurité de l'information et cybercriminalité

- Security principles: defense in depth, security policy.
- Fundamental notions: risk, asset, threat.
- Risk management methods (ISO 27005 , EBIOS, MEHARI).
- Overview of ISO 2700x standards.
- Evolution of cybercrime.
- Identification of threat agents.
- New threats (APT, spear phishing, watering hole, exploit kit.
-).
- Security flaws in software.
- The progress of a cyberattack (NIST).
- 0day vulnerabilities, 0day Exploit and exploit kit.

Firewall, virtualisation et Cloud computing

- Proxy servers, reverse proxy, address masking.
- Perimeter protection based on firewalls.
- Differences between UTM, enterprise, NG and NG-v2.
- IPS (Intrusion Prevention System) and IPS NG products.
- The implementation of DMZ (demilitarized zone) solutions.
- Vulnerabilities in virtualization.
- The risks associated with Cloud Computing according to ANSSI, ENISA and CSA.
- The Cloud Control Matrix and its use for evaluating cloud providers Cloud.

Sécurité des postes clients

- Understanding client-facing threats.
- The role of the personal firewall and its limits.
- Anti-virus / anti-spyware software.
- How to manage security patches on client workstations? How to secure removable devices.
- Cisco NAC client compliance check, Microsoft NAP.
- Browser and plug-in vulnerabilities.
- Drive-by download.

Fondamentaux de la cryptographie

- Legislation and main usage constraints in France and around the world.
- Cryptographic techniques.
- Public key and symmetric algorithms.
- Hash functions.
- Public key architectures.
- NSA and GCHQ cryptanalysis programs.

Authentification et habilitation des utilisateurs

- Biometric authentication and legal aspects.
- Authentication by challenge/response.
- Password theft techniques, brute force, entropy secrets.
- Strong authentication.
- Smart card authentication and X509 client certificate.
- "3A" architectures: concept of SSO, Kerberos .
- IAM platforms.
- Identity federation via social network APIs.
- Identity federation for enterprise and the Cloud.

La sécurité des flux

- SSL Crypto API and evolutions from SSL v2 to TLS v1.
- 3.
- Attacks on SSL/TLS protocols.
- Attacks on HTTPS flows.
- Hardware key containment, FIPS-140-2 certifications.
- Easily assess the security of an HTTPS server.
- The IPsec standard, AH and ESP modes, IKE and key management.
- Overcoming problems between IPSec and NAT.
- SSL VPNs.
- What is the benefit compared to IPSec? Use of SSH and OpenSSH for secure remote administration.
- Decryption of flows on the fly: legal aspects.

Sécurité Wifi

- Wifi specific attacks.
- How to detect Rogue APs.
- Kiosk security mechanisms.
- WEP vulnerabilities.
- Weakness of the RC4 algorithm.
- Description of the risks.
- The IEEE 802 security standard.
- 11i.
- WLAN architecture.
- Authentication of users and terminals.
- Wifi authentication in the company.
- Audit tools, free software, aircrack-ng, Netstumbler, WifiScanner.

Sécurité des Smartphones

- Threats and attacks on mobility.
- iOS, Android, Windows mobile: strengths and weaknesses.
- Virus and malicious code on mobile.
- MDM and EMM solutions for fleet management.

Sécurité des applications

- Defense in depth.
- Web and mobile applications: what are the differences in security? The main risks according to OWASP.
- Focus on XSS, CSRF, SQL injection and session hijacking attacks.
- The main methods of secure development.
- What security clause in development contracts? The firewall application or WAF.
- Evaluate the security level of an application.

Gestion et supervision active de la sécurité

- Security dashboards.
- Security audits.
- Penetration testing.
- Legal aspects of security testing intrusion.
- IDS probes, VDS scanner, WASS.
- How to respond effectively to attacks? Record the evidence.
- Set up an SIEM solution.
- The ANSSI labels (PASSI, PDIS & PRIS) for outsourcing.
- How to react in the event of an intrusion? Forensic expertise: the role of judicial expert (criminal or civil).
- Private judicial expertise.