La sécurité dans le cyberespace
panorama des solutions de sécurités dans les domaines réseaux, virtualisation et Cloud

Séminaire de 3 jours - 21h
Réf : SCE - Prix 2024 : 2 890CHF HT

La cybercriminalité est une menace grandissante sur la société et les cybercriminels agissent de n'importe où pour s'attaquer aux infrastructures des entreprises au travers du cyberespace. Cette formation vous montrera comment répondre aux impératifs de sécurité des entreprises et intégrer la sécurité dans l'architecture d'un système d'information. Il vous sera présenté une analyse détaillée des menaces et des moyens d'intrusion ainsi qu'un panorama des principales mesures de sécurité disponibles sur le marché.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Connaître l'évolution des criminels dans le cyberespace

Comprendre la sécurité dans le Cloud

Savoir sécuriser les postes clients et les applications

Comprendre les principes de la cryptographie

Apprendre à gérer la supervision de la sécurité SI

LE PROGRAMME

dernière mise à jour : 10/2018

1) Le cyberespace et la sécurité de l'information

- Les principes de la sécurité : défense en profondeur, politique de sécurité.
- Les notions fondamentales : risque, actif, menace...
- Les méthodes de gestion de risques (ISO 27005, EBIOS, MEHARI). Panorama des normes ISO 2700x.
- L'évolution de la cybercriminalité. L'identification des agents de menace.
- Les nouvelles menaces (APT, spear phishing, watering hole, exploit kit...).
- Les failles de sécurité dans les logiciels.
- Le déroulement d'une cyberattaque (NIST).
- Les failles 0day, 0day Exploit et kit d'exploitation.

2) Le pare-feu, la virtualisation et le Cloud Computing

- Les serveurs proxy, reverse proxy, le masquage d'adresse.
- La protection périmétrique basée sur les pare-feu.
- Les différences entre firewalls UTM, enterprise, NG et NG-v2.
- Les produits d'Intrusion Prevention System (IPS) et les IPS NG.
- Les solutions DMZ (zones démilitarisées).
- Les vulnérabilités dans la virtualisation.
- Les risques associés au Cloud Computing selon l'ANSSI, l'ENISA et la CSA.
- Le Cloud Control Matrix et son utilisation pour l'évaluation des fournisseurs de Cloud.

3) La sécurité des postes clients

- Les menaces sur les postes clients.

PARTICIPANTS

Toutes les personnes souhaitant apprendre les fondamentaux de la sécurité SI.

PRÉREQUIS

Avoir suivi la formation "Les fondamentaux de la sécurité des SI".

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.

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 stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage 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 stagiaire 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

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Le rôle du firewall personnel et ses limites.
- Les logiciels anti-virus/anti-spyware.
- Les correctifs de sécurité sur les postes clients.
- Savoir sécuriser les périphériques amovibles.
- Le contrôle de conformité du client Cisco NAC, Microsoft NAP.
- Les vulnérabilités des navigateurs et des plug-ins.

4) Les bases de la cryptographie

- Les principales contraintes d'utilisation et la législation en France et dans le monde.
- Les techniques cryptographiques.
- Les algorithmes à clés publiques et symétriques.
- Les fonctions de hachage.
- Les architectures à clés publiques.
- Programmes de cryptanalyse de la NSA et du GCHQ.

5) Le processus d'authentification des utilisateurs

- L'authentification biométrique et les aspects juridiques.
- L'authentification par challenge/réponse.
- Les techniques de vol de mot de passe, brute force, entropie des secrets.
- L'authentification forte.
- L'authentification carte à puce et certificat client X509.
- L'architecture "3A" : concept de SSO, Kerberos.
- Les plateformes d'IAM.
- La fédération d'identité via les API des réseaux sociaux.
- La fédération d'identité pour l'entreprise et le Cloud.

6) La sécurité des échanges

- Crypto API SSL et évolutions de SSL v2 à TLS v1.3.
- Les attaques sur les protocoles SSL/TLS et les flux HTTPS.
- Le confinement hardware des clés, certifications FIPS-140-2.
- Evaluer facilement la sécurité d'un serveur HTTPS.
- Le standard IPsec, les modes AH et ESP, IKE et la gestion des clés.
- Surmonter les problèmes entre IPSec et NAT.
- Les VPN SSL. Quel intérêt par rapport à IPSec ?
- Utilisation de SSH et OpenSSH pour l'administration distante sécurisée.
- Déchiffrement des flux à la volée : aspects juridiques.

7) La sécurité des réseaux sans fils et des dispositifs mobiles

- Les attaques spécifiques WiFi. Comment détecter les Rogue AP ?
- Les mécanismes de sécurité des bornes.
- Les vulnérabilités WEP. Faiblesse de l'algorithme RC4.
- La description des risques.
- Le standard de sécurité IEEE 802.11i. Architecture des WLAN.
- L'authentification des utilisateurs et des terminaux.
- L'authentification WiFi dans l'entreprise.
- Les outils d'audit, logiciels libres, aircrack-ng, Netstumbler, WifiScanner...
- Les menaces et attaques sur la mobilité.
- iOS, Android, Windows mobile : forces et faiblesses.
- Virus et codes malveillants sur mobile.
- Les solutions de MDM et EMM pour la gestion de flotte.

8) La sécurité des logiciels

- Les applications Web et mobiles : quelles différences en matière de sécurité ?
- Les principaux risques selon l'OWASP.
- Focus sur les attaques XSS, CSRF, SQL injection et session hijacking.
- Les principales méthodes de développement sécurisé.

- Les clauses de sécurité dans les contrats de développement.
- Le pare-feu applicatif ou WAF.
- Comment évaluer le niveau de sécurité d'une application ?

9) Les concepts de Security by Design et Privacy by Design

- La sécurité dans la conception.
- L'approche en matière d'assurance de sécurité de la Security by Design.
- Les 7 principes fondamentaux du Privacy by Design.
- Prise en compte de la vie privée tout au long du processus.

10) La supervision de la sécurité

- Les tableaux de bord Sécurité.
- Les audits de sécurité et les tests d'intrusion.
- Les aspects juridiques des tests d'intrusion.
- Les sondes IDS, scanner VDS, WASS.
- Comment répondre efficacement aux attaques ?
- Consigner les éléments de preuve.
- Mettre en place une solution de SIEM.
- Les labels ANSSI (PASSI, PDIS & PRIS) pour l'externalisation.
- Comment réagir en cas d'intrusion ?
- L'expertise judiciaire : le rôle d'un expert judiciaire (au pénal ou au civil).
- L'expertise judiciaire privée.

LES DATES

CLASSE À DISTANCE
2024 : 01 juil., 14 oct., 09 déc.