Sécuriser son environnement virtualisé

Cours Synthèse de 2 jours - 14h
Réf : VMW - Prix 2024 : 1 950€ HT

Ce cours vous présentera une synthèse technique des solutions permettant d'assurer la sécurité de vos environnements virtualisés : des principales faiblesses des architectures virtualisées à la mise en œuvre optimale de solutions de sécurité.

OBJECTIFS PÉDAGOGIQUES

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

Identifier les menaces de sécurité sur les environnements virtualisés

Comprendre les typologies d'attaques

Sécuriser le data center virtuel, les VM, serveurs et postes de travail

Évaluer les outils et techniques disponibles

LE PROGRAMME

dernière mise à jour : 07/2023

1) Introduction à la sécurité

- Sécurité : réactive, proactive, prédictive.
- Les menaces internes et externes.
- Les champs d'application (serveurs, postes de travail, clients, applications).

2) Les techniques de virtualisation

- Isolation de contexte, hypervirtualisation, paravirtualisation.
- La virtualisation d'entrées/sorties (I/O), classique et le conteneur.
- Systèmes unikernels, microviseurs.

3) La sécurité en milieu industriel

- Le modèle de Reason.
- Organisations et catastrophes.
- Sauvegardes, réplications, PRA.
- Tiers de confiance, attaque man-in-the-middle.

4) La sécurité en environnement virtualisé

- Avantages industriels, risques.
- Les couches à surveiller.
- Le modèle sécurité Zero Trust, nouveau paradigme ?
- La microsegmentation.
- La défense en profondeur.
- Les domaines sécuritaires : réseau, système, management, applications.

5) La sécurité avec VMware

- Les couches de l'OSI.
- Les VLAN, le routage, les switchs virtuels, VSS, VDS, N1KV, VXLAN et switchs logiques.
- Prestataire de services de certification, AD, LDAP, Nis, VMware NSX Edge.
- Les principes de sécurité système : zones de confiance (DMZ), politique de mots de passe.

PARTICIPANTS

Directeurs informatiques, directeurs de production/d'exploitation et administrateurs systèmes ou réseaux.

PRÉREQUIS

Connaissances de base en architecture technique (systèmes et réseaux) et en sécurité informatique.

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.

- Algorithmes de chiffrement, clés publiques et privées, certificats autosignés, autorité de confiance.

6) La sécurité applicative VMware

- Antivirus : VMsafe API, vShield Endpoint.
- Cartographie applicative, gestion des flux.
- Isolation : application sandboxing, conteneurs.
- VMware Photon, ieVM.
- Protection des API.

7) Prédiction, prévention, détection et remédiation

- Panorama des outils (Nessus, Nmap, Kali).
- Détections et tests d'intrusions.
- Logs, l'apprentissage automatique.
- Analyse comportementale.
- Risques et criticité : vCenter Operations Manager (VMware).
- Cartographie des risques.
- Supervision et monitoring, alarmes.

8) Sécurité du management

- ACL, authentification simple, rôles et privilèges.
- L'ingénierie sociale (social engineering).
- BYOD, shadow IT (rogue IT).
- Plan de durcissement de l'infrastructure virtuelle.
- Gestion des mises à jour, des backups.

LES DATES

CLASSE À DISTANCE
2024 : 19 sept.