Sécuriser votre environnement virtualisé

-Réference: **PL-76** -Durée: **2 Jours (14 Heures)**

Les objectifs de la formation

- Identifier les menaces de sécurité sur les environnements virtualisés
-
- Comprendre les typologies d'attaque
-
- Sécuriser le Datacenter virtuel, les VMS serveurs et postes de travail
-
- Evaluer les outils et techniques disponibles
-

A qui s'adesse cette formation ?

POUR QUI :

- Identifier les menaces de sécurité sur les environnements virtualisés Comprendre les typologies d'attaque Sécuriser le Datacenter virtuel, les VMS serveurs et postes de travail Evaluer les outils et techniques disponibles

PRÉREQUIS :

- Connaissances de base en architectures techniques (systèmes et réseaux) et en sécurité informatique.
- .

Programme

- **Introduction à la sécurité**
  - Sécurité : réactive, proactive, prédictive.
  - Les menaces internes et externes.
  - Les champs d'application (serveurs, postes de travail, clients, applications).
- **Les techniques de virtualisation**
  - Isolation de contexte, hyper-virtualisation, para-virtualisation.
  - La virtualisation d'entrées/sorties (I/O), classique et le container.
  - Systèmes unikernels, microviseurs.

Programme

- **La sécurité en milieu industriel**
  - Le modèle de Reason.
  - Organisations et catastrophes.
  - Sauvegardes, réplications, PRA.
  - Tiers de confiance, attaque man in the middle.
- **La sécurité en environnement virtualisé**
  - Avantages industriels, risques.
  - Les couches à surveiller.
  - Le modèle sécurité Zero Trust, nouveau paradigme ? La micro-segmentation.
  - La défense en profondeur.
  - Les domaines sécuritaires : réseau, système, management, applications.
- **La sécurité avec VMware**
  - Les couches de l'OSI.
  - Les VLAN, le routage, les switches virtuels, VSS, VDS, N1KV, VXLAN et switches logiques.
  - Prestataire de Services de Certification, AD, LDAP, Nis, VMware NSX Edge.
  - Les principes de sécurité système : zones de confiance (dmz), politiques de mots de passe.
  - Algorithmes de chiffrement, clés publiques et privées, certificats autosignés, autorité de confiance.
- **La sécurité applicative VMware**
  - Antivirus : VMsafe API, vShield Endpoint.
  - Cartographie applicative, gestion des fluxs.
  - Isolation : application sandboxing, containers.
  - VMware Photon, ieVM.
  - Protection des API.
- **Prédiction, prévention, détection et remediation**
  - Panorama des outils (Nessus, Nmap, kali).
  - Détections et tests d'intrusions.
  - Logs, l'apprentissage automatique.
  - Analyse comportementale.
  - Risques et criticité : vCenter Operations (VMware).
  - Cartographie des risques.
  - Supervision et monitoring, alarmes.

Programme

- **Sécurité du management**
  - ACL, authentification simple, rôles et privilèges.
  - L'ingénierie sociale (ou social engineering).
  - BYOD, Shadow IT (Rogue IT).
  - Plan de durcissement de l'infrastructure virtuelle.
  - Gestion des mises à jour, des backups.

(+212) 5 22 27 99 01 (+212) 6 60 10 42 56 Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7éme étage N° 30
Casablanca 20340, Maroc