400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE

SÉCURITÉ DES INFRASTRUCTURES WINDOWS

CODE STAGE : SIW

OBJECTIFS

La écurité des infrastructures Microsoft Windows est indispensable à la protection des systèmes d'information. Cette formation aborde la configuration des services Windows pour la sécurité et les différentes bonnes pratiques à adopter.

DURÉE

4 jours

PUBLIC

consultant en cybersécurité, administrateur système, ingénieur en informatique, développeur.

PRÉ-REQUIS

avoir des bases de la sécurité des systèmes dcode2utf('8217',0)information. Connaître le fonctionnement dcode2utf('8217',0)un des systèmes Windows et Linux ainsi que les langages Shell.

PROGRAMME

Jour 1 matin

Section 1 – Introduction sur l'écosystème actuel

L'évolution des systèmes d'information et de leurs menaces

Segmentation et études des phases d'un attaquant (CyberKill Chain code2utf('038',0) MITRE ATTcode2utf('038',0)CK)

Chronologie et évolutions majeures des systèmes d'exploitation Windows

Les attaques courantes dans un domaine Windows

TP 1 / Mener une étude Cyber Kill-Chain

Jours 1 Après-midi

Section 2 – Durcissement des domaines Windows

Cohérence et défauts de conception Active Directory (AGDLP, GPO, Relations approbations, délégation)

Sécurité des droits d'administrations (ACL, Red Forest ESAE, Silo, Bastion, délégation)

Sécurité des comptes à privilèges (AdminSDHolder, LAPS, PAM)

Utilisation d'une infrastructure de clés publiques PKI (NPS, Radius, WIFI, carte à puce, ...)

Sécurisation des protocoles d'administration (RPC, WMI, WinRM)

Sécurité des services et comptes de services managés

TP 2 / Implémenter LAPS

Jour 2 matin

Système de prévention de perte de données (Classification, Marquage, DLP)

Surveillance et journaux d'événements (Surveillance en profondeur, Sysmon)

Microsoft ATA et Threat Intelligence

TP 3 /Appliquer les règles de classification et de surveillance sur des données confidentielles

TP 4 / Renforcer la journalisation (Sysmon + Journalisation WMI pivoting)

Jour 2 après-midi

Section 3 – Durcissement des serveurs et postes clients

Sécurisation du démarrage (UEFI, Bitlocker, ...)

Sécurité des applications (Applocker, Device Guard)

Sécurité de l'authentification (SSP, credential guard)

Contrôler l'élévation de privilèges (UAC)

Fonctionnalité antivirale (Defender, AMSI, SmartScreen)

Sécurité de Powershell (Politique de restriction, JEA, Journalisation)

Réduction de la surface d'attaque (Serveur Core / Nano)

TP 5 / Déployer Bitlocker

TP 6 / Configurer powershell JEA

Jours 3 Matin

Section 4 – Durcissement des protocoles réseaux

L'authentification Microsoft (NTLM, NET-NTLM, Kerberos)

Les protocoles microsoft (WPAD, SMB, RDP, LLMNR, ..)

Etude et recherche de vulnérabilités protocolaires

TP 7 / Sécuriser LLMNR code2utf('038',0) SMB

Jours 3 Après-midi

Section 5 – Mécanisme de défense avancé

Détection des attaques avancées

Auditer son architecture

TP 8 / Auditer son architecture et préparer un plan de contre mesure

Jours 4 (Matin / après-midi)

Section 6 – Durcissement des domaines Azure

Rappel sur Azure et IAM

Authentification et autorisation Azure

Zoom sur les attaques Azure

Renforcement des défenses Azure

Auditer son architecture cloud