SÉCURITÉ AD ET VEILLE TECHNIQUE IT

Public	Administrateurs systèmes et réseaux
Durée	3 jours - 21 heures
Pré-requis	Disposer de certaines connaissances en administration système Windows et en réseau
Objectifs	Identifier les différents domaines de la sécurité et de la maîtrise des risques liés aux informations Connaître les principes et les normes de chaque domaine de la SSI Disposer d'informations sur les tendances actuelles au niveau des menaces et des solutions à notre disposition Pouvoir améliorer la communication entre la maitrise d'ouvrage, la maitrise d'oeuvre et la SSI Être en mesure d'effectuer des choix techniques
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

DURCISSEMENT DES DOMAINES WINDOWS

- Stratégies de contrôle d'applications (AppLocker)
- Implémentation de AppLocker via les stratégies de groupe
- Cohérence et défauts de conception de la structure Active Directory (ACL)
- Recommandations de sécurité pour Active Directory (Bonnes pratiques)
- TD / Comment LAPS réduit les chances de réussite de mouvements latéraux
- Implémentation de LAPS pour les clients d'un domaine Windows
- TD / Implémentation d'un contrôle d'accès Radius
- Sécurité des réseaux Wi-Fi
- TD / Implémentation d'un contrôle d'accès Wi-Fi basé sur Radius
- Sécurisation de l'administration du domaine (WinRM, RPC, WMI, RDP)
- Sécurité des services et comptes de services managés (MSA)
- Classification et marquage de l'information pour les systèmes de prévention de pertes de données (DLP)
- Audit et centralisation des journaux d'événements Windows
- Présentation d'une solution d'analyse de menaces avancées (ATA)
- Sécurité des environnements Azure (Identity Protection, RMS, Bonnes pratiques)

DURCISSEMENT DES SERVEURS ET POSTES CLIENTS

- Sécurisation du démarrage (Secure Boot – UEFI)
- Chiffrement des disques durs (Bitlocker, TPM, Agent de récupération)
- Pare-feu Windows (configuration, règles)
- Contrôler l'élévation de privilèges (UAC)
- TD / Élévation de privilèges avec et sans UAC
- Sécurisation des contenus web (Smartscreen)
- Windows Defender
- Fonctionnalités antivirales (Device Guard, Credential Guard, AMSI)
- Augmentation de la maîtrise de Powershell (Scripts signés, Just Enough Administration, Journalisation)

MODÉLISATION DES NIVEAUX DE MATURITÉ DES TECHNOLOGIES SSI

- Les choix structurants et non structurants et positionnements dans la courbe de la pérennité
- La sécurité des accès : filtrage réseau, identification, authentification (faible, moyenne, forte), gestion des identités vs. SSO, habilitation, filtrage applicatif (WAF, CASB et protection du Cloud), détection/protection d'intrusion, journalisation, supervision
- La sécurité des échanges : algorithmes, protocoles, combinaisons symétriques et asymétriques TLS, certificats, IGCP, les recommandations ANSSI
- Infrastructures de clés publiques : autorités de certification et d'enregistrement, révocation
- Le cas du DLP : architecture

NOMADISME

- Sécurité des postes nomades : problèmes de sécurité liés au nomadisme
- Protection d'un poste vs. solutions spécifiques
- Mise en quarantaine
- Accès distants
- VPN : concept et standards de VPN sécurisé, intérêts du VPN, contrôle du point d'accès

LES ARCHITECTURES DE CLOISONNEMENT

- La sécurité des VLAN et hébergements, DMZ et échanges, sécurisation des tunnels, VPN Peer to Peer et télé accès, de la sécurité périphérique à la sécurité en profondeur

LA SÉCURITÉ DES END POINT

- Le durcissement : postes de travail, ordi phones, serveurs
- L'adjonction d'outils : postes de travail, ordi phones, serveurs
- La sécurité des applications : les standards et les bonnes pratiques

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 27/09/2023

PROFIL Formateur : Les formateurs sont recrutés selon plusieurs critères : Expérience, pédagogie, dynamisme et prévoyance.