Plan d’action

Client : Clinique de Frontignan

Auditeur : DUBRAY Gauthy

I. Plan d'action à court terme

Proposez l'ensemble de vos recommandations réalisables à court terme par le client pour améliorer son niveau de sécurité sur l'environnement Active Directory. Suivez le modèle proposé dans la première case.

- Recommandation R01 : *Mettez en place une politique de mot de passe forte*
- Vulnérabilité corrigée : *Vulnérabilité V01*
- Ordre de priorité : *Priorité 1/5*
- Actions à réaliser : *Modifier la politique de mot de passe avec à minima :*
    - *Exiger des mots de passe d'au moins 12 caractères ;*
    - *Exiger des mots de passe complexes (lettres, chiffres, caractères spéciaux) ;*
    - *.....*
- Ressources : *https://learn.microsoft.com/fr-fr/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide*

- Recommandation R02 : *Activer la pré-authentification Kerberos*
- Vulnérabilité corrigée : *Vulnérabilité V02*
- Ordre de priorité : *Priorité 2/5*
- Actions à réaliser :
    - *Vérifier que l'attribut* **DONT_REQUIRE_PREAUTH** *est désactivé sur tous les comptes.*
    - *Bloquer l'énumération Kerberos permettant de tester la validité d'un compte.*
    - *Mettre en place un monitoring sur les requêtes TGT anormales.*
- *Ressources :* Microsoft Hardening Kerberos : https://learn.microsoft.com/fr-fr/windows-server/security/kerberos/kerberos-authentication-overview

- Recommandation R03 : *Sécuriser le LSA et empêcher le dump de LSASS*
- Vulnérabilité corrigée : *Vulnérabilité V03*
- Ordre de priorité : *Priorité 3/5*
- Actions à réaliser :
    - *Activer* **LSA Protection (`RunAsPPL`).**
    - *Activer* **Windows Defender Credential Guard** *sur les machines du domaine.*
    - *.....*
- *Ressources :* Microsoft Credential Guard :https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/

- Recommandation R04 : *Supprimer les identifiants stockés en clair dans les tâches planifiées et changer le mot de passe compromis*
- Vulnérabilité corrigée : *Vulnérabilité V04*
- Ordre de priorité : *Priorité 4/5*
- Actions à réaliser :
    - *Identifier les Scheduled Tasks utilisant des identifiants explicites.*

    - *Configurer ces tâches pour fonctionner via un compte gMSA ou via un script sécurisé.*
    - *Modifier immédiatement les mots de passe concernés.*
- *Ressources :* Securing Scheduled Tasks :https://support.microsoft.com/fr-fr/windows/gestionnaire-d-informations-d-identification-dans-windows-1b5c916a-6a16-889f-8581-fc16e8165ac0

- Recommandation R05 : *Mettre en place une politique de segmentation réseau*
- Vulnérabilité corrigée : *Vulnérabilité V05*
- Ordre de priorité : *Priorité 5/5*
- Actions à réaliser :
    - *Bloquer l'accès SMB, RDP, WinRM depuis les VLAN utilisateurs vers les serveurs AD.*
    - *Créer des ACL permettant uniquement les flux nécessaires (échange DC ↔ serveurs).*

- *Ressources : https://learn.microsoft.com/fr-fr/azure/well-architected/security/segmentation*

À noter : Vos recommandations devront être hiérarchisées par ordre de priorité. Un lien vers une ou plusieurs ressources est un plus lors de la remontée des recommandations, mais ce n'est pas obligatoire.

Au moins 5 recommandations à court terme sont attendues.

II. Plan d'action à long terme

Proposez des recommandations génériques pour améliorer la sécurité de l'environnement sur le long terme. Suivez le même format que dans l'exemple fourni.

- Recommandation L01 : *Mettre en place un SOC / SIEM pour monitorer AD*
- Vulnérabilité corrigée : *Vulnérabilité V01*
- Ordre de priorité : *Priorité 1/5*
- Actions à réaliser : **:** Détection des comportements suspects (Kerberos anomalies, LSASS, tickets).
    - *Configurer la journalisation avancée AD*
    - *Intégrer Sysmon*
    - *Ajouter des alertes sur attaques Kerberoasting / Pass-the-ticket*

- Ressources : *https://clusif.fr/wp-content/uploads/2017/03/clusif-2017-deploiement-soc_vf.pdf*

- Recommandation L02 : *Passer progressivement sur un modèle Zero Trust*
- Vulnérabilité corrigée : *Vulnérabilité V02*
- Ordre de priorité : *Priorité 2/5*

- Actions à réaliser : Réduire les mouvements latéraux et la propagation d'une compromission.
    - *Limiter les privilèges permanents*
    - *Forcer MFA pour les administrateurs*

- *Ressources : https://www.cloudflare.com/fr-fr/lp/dg/product/zero-trust-security/?&gad_campaignid=22148809594*

- Recommandation L03 :*Mettre en place une politique de durcissement Active Directory*
- Vulnérabilité corrigée : *Vulnérabilité V03*
- Ordre de priorité : *Priorité 3/5*
- Actions à réaliser : Réduire la surface d'attaque.
    - *Appliquer les GPO de durcissement Microsoft*
    - *Auditer régulièrement les ACL et permissions d'objets AD*
    - *Réduire le nombre de comptes privilégiés*

- *Ressources : https://www.it-connect.fr/nis2-active-directory-comptes-mots-de-passe-mfa/*

- Recommandation L04 : *Implémenter LAPS ou LAPS NG*
- Vulnérabilité corrigée : *Vulnérabilité V04*
- Ordre de priorité : *Priorité 4/5*
- Actions à réaliser : Sécuriser les mots de passe des comptes administrateurs locaux.
    - *Déployer LAPS NG sur l'ensemble du parc*
    - *Rotation automatique des mots de passe locaux*
    - *Journalisation des utilisations du compte admin local*

- *Ressources : https://learn.microsoft.com/fr-fr/windows-server/identity/laps/laps-overview*

- Recommandation L05 : *Mettre en place un plan de formation sécurité pour les équipes IT*
- Vulnérabilité corrigée : *Vulnérabilité V05*
- Ordre de priorité : *Priorité 5/5*
- Actions à réaliser : Augmenter la maturité sécurité du SI.
    - *Formation régulière à AD (Kerberos, ACL, gMSA…)*
    - *Sensibilisation aux attaques modernes*
    - *Simulation annuelle de compromission (Purple Team)*

- *Ressources : https://www.bluesecure.fr/nos-formations/?gad_campaignid=20732801402*