Plan d’action

Client : Clinique de Frontignan

Auditeur : BENE Maël

I. Plan d'action à court terme (0–30 jours)

● Recommandation R01 : Restreindre les droits DCSync ● Ordre de priorité : Priorité 1/8 (Critique) ● Actions à réaliser : Objet domaine / DCs ■ Limiter aux comptes nécessaires ■ journaliser 4662/4742 ■ alertes SIEM ● Ressources : Microsoft – DCSync overview & detection – https://learn.microsoft.com/windows/security/threat-protection/auditing/event-4662
● Recommandation R08 : Rotation mot de passe comptes SPN sensibles + forcer AES (désactiver RC4/etype23) ● Ordre de priorité : Priorité 2/8 (Critique) ● Actions à réaliser : Comptes SPN (incl. tnicolas) ■ Changer le mot de passe ■ n'autoriser qu'AES (etype 17/18) ■ audit des SPN humains ● Ressources : Microsoft – Azure AD Password Protection – https://learn.microsoft.com/azure/active-directory/authentication/concept-password-ban-bad ; Microsoft – Kerberos Encryption Types – https://learn.microsoft.com/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos ; Microsoft – Service Principal Names – https://learn.microsoft.com/windows/win32/ad/service-principal-names ; Harden – Disable RC4 – https://learn.microsoft.com/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain
● Recommandation R02 : Forcer la signature SMB (client & serveur) ● Ordre de priorité : Priorité 3/8 (Élevée) ● Actions à réaliser : FILER01, DESKTOP01 ■ GPO sécurité – Digitally sign communications (always) ● Ressources : Microsoft – SMB signing policy – https://learn.microsoft.com/windows-server/storage/file-server/smb-security#smb-signing
● Recommandation R03 : Supprimer les comptes temporaires / de test ● Ordre de priorité : Priorité 4/8 (Élevée) ● Actions à réaliser : Annuaire AD

■ Revue mensuelle ■ désactivation puis suppression automatisée
● Recommandation R04 : Retirer les secrets en clair des scripts et rotation immédiate ● Ordre de priorité : Priorité 5/8 (Élevée) ● Actions à réaliser : \\FILER01\Configuration ■ Audit des partages ■ coffre à secrets ■ gMSA ● Ressources : Microsoft – Group Managed Service Accounts (gMSA) – https://learn.microsoft.com/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview
● Recommandation R05 : Bannir les mots de passe basés sur l'identifiant ● Ordre de priorité : Priorité 6/8 (Élevée) ● Actions à réaliser : Tous comptes ■ Password filter / AAD Password Protection ■ Smart Lockout ● Ressources : Microsoft – Azure AD Password Protection – https://learn.microsoft.com/azure/active-directory/authentication/concept-password-ban-bad
● Recommandation R06 : Réduire les membres Domain Admins ● Ordre de priorité : Priorité 7/8 (Élevée) ● Actions à réaliser : Groupe DA ■ Comptes DA dédiés ■ JIT/JEA ■ journaux 4728/4729 ● Ressources : Microsoft – Just Enough Administration (JEA) – https://learn.microsoft.com/powershell/jea/overview ; Microsoft – Privileged Access Workstations (PAW) – https://learn.microsoft.com/windows/security/identity-protection/privileged-access-workstations/
● Recommandation R07 : Retirer les SPN des comptes humains à privilèges ; migrer vers un compte de service (gMSA) ● Ordre de priorité : Priorité 8/8 (Élevée) ● Actions à réaliser : Comptes humains membres de groupes à privilèges (ex. tnicolas)

- Déplacer le service (ex. WWW/SHARE02.TRAVERS.IC) vers gMSA
- vérifier qu'aucun DA n'expose de SPN

● Ressources : Microsoft – Group Managed Service Accounts (gMSA) – https://learn.microsoft.com/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview ; Microsoft – Service Principal Names – https://learn.microsoft.com/windows/win32/ad/service-principal-names

II. Plan d'action à long terme (30–180 jours)

● Recommandation L01 : Mettre en place PAM/JIT & tiering admin

● Ordre de priorité : Priorité 1/8 (Haute)

● Actions à réaliser : Comptes à privilèges

- SAE/SAJ
- bastion
- sessions privilégiées contrôlées

● Ressources : Microsoft – Just Enough Administration (JEA) – https://learn.microsoft.com/powershell/jea/overview ; Microsoft – Privileged Access Workstations (PAW) – https://learn.microsoft.com/windows/security/identity-protection/privileged-access-workstations/ ; Microsoft – Tiered Administrative Model – https://learn.microsoft.com/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material ; Microsoft – Privileged Access Management – https://learn.microsoft.com/microsoft-365/compliance/privileged-access-management-overview

● Recommandation L02 : Durcissement Kerberos & NTLM

● Ordre de priorité : Priorité 2/8 (Haute)

● Actions à réaliser : Tout AD

- Désactiver NTLMv1
- auditing NTLM
- sign/seal LDAP
- channel binding

● Ressources : Microsoft – Kerberos Encryption Types – https://learn.microsoft.com/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos ; Microsoft – Service Principal Names – https://learn.microsoft.com/windows/win32/ad/service-principal-names ; Harden – Disable RC4 – https://learn.microsoft.com/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain ; Microsoft – Network security: LDAP signing –

https://learn.microsoft.com/windows-server/security/kerberos/ldap-signing ; Microsoft – NTLM Auditing and Restriction – https://learn.microsoft.com/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain
● Recommandation L03 : MFA obligatoire pour les comptes à privilèges ● Ordre de priorité : Priorité 3/8 (Haute) ● Actions à réaliser : Admins ■ MFA robuste + stratégie d'accès conditionnel ● Ressources : ANSSI – Authentification multifacteur – https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe
● Recommandation L04 : Gestion des comptes de service (gMSA) ● Ordre de priorité : Priorité 4/8 (Haute) ● Actions à réaliser : Services applicatifs ■ gMSA/groupe restreint ■ mots de passe longs ● Ressources : Microsoft – Group Managed Service Accounts (gMSA) – https://learn.microsoft.com/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview
● Recommandation L08 : Segmenter le réseau ● Ordre de priorité : Priorité 5/8 (Haute) ● Actions à réaliser : AD/Postes/Serveurs ■ Sous-réseaux/VLAN distincts par service (postes utilisateurs / serveurs de fichiers / contrôleurs de domaine), filtrage inter-VLAN, règles moindres privilèges ● Ressources : ANSSI – Segmentation réseau – https://cyber.gouv.fr/sites/default/files/2021/09/anssi-guide-recommandations_architectures_systemes_information_sensibles_ou_diffusion_restreinte-v1.2.pdf ; Microsoft – Securing Active Directory Admin Tier Model (Network) – https://learn.microsoft.com/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material
● Recommandation L05 : Supervision & centralisation des logs ● Ordre de priorité : Priorité 6/8 (Moyenne) ● Actions à réaliser : AD/Serveurs ■ Collecte 4624/4768/4769/4662/4728/4729 ■ détections BloodHound-like

● Ressources : Microsoft – Advanced Security Auditing (Event IDs) – https://learn.microsoft.com/windows/security/threat-protection/auditing/security-auditing-overview ; ANSSI – Supervision des SI – https://cyber.gouv.fr/sites/default/files/2018/04/anssi-guide-admin_securisee_si_v3-0.pdf
● Recommandation L06 : Hygiène GPO & LAPS ● Ordre de priorité : Priorité 7/8 (Moyenne) ● Actions à réaliser : Postes/Serveurs ■ LAPS sur locaux admin ■ revue GPO ■ durcissement baseline ● Ressources : Microsoft – Windows LAPS – https://learn.microsoft.com/windows/security/identity-protection/windows-laps/windows-laps-overview
● Recommandation L07 : Patch management & durcissement hôte ● Ordre de priorité : Priorité 8/8 (Moyenne) ● Actions à réaliser : Postes/Serveurs ■ WSUS/Intune ■ CIS baselines ■ SMB signing partout ● Ressources : Microsoft – SMB signing policy – https://learn.microsoft.com/windows-server/storage/file-server/smb-security#smb-signing ; Microsoft – WSUS Documentation – https://learn.microsoft.com/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus