BTS SIO

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

[TP] Rapport- Gestion des utilisateurs : Analyse des évènements de connexion (AD & RDP)

Candidat : Alenzo Wauters

Spécialité : SISR (Solutions d'infrastructure, systèmes et réseaux)

Réalisation professionnelle : Audit de sécurité des accès et analyse des journaux d'événements Windows Server.

SOMMAIRE

Table des matières

1. Tableau des événements détectés

Événement	ID	Explication technique	Diagnostic (IP Source)
Succès	4624	Connexion réussie (Console ou Réseau)	192.168.x.x (Poste Client)
Échec	4625	Tentative de connexion échouée (Mauvais MDP)	IP Suspecte ou erreur saisie
RDP	4624	Connexion à distance (LogonType 10)	Identifiée via script PowerShell
Reset	4724	Réinitialisation d'un mot de passe par un admin	Action sur le compte cible

2. Schéma du cycle de traitement

Tentative (Log généré) $\rightarrow$ **Analyse** (Filtrage Event Viewer / PowerShell) $\rightarrow$ **Diagnostic** (Identification de l'IP et de la cause) $\rightarrow$ **Remédiation** (Blocage IP, changement MDP ou alerte).

3. Conclusion de l'audit

L'analyse automatisée via le script Audit-Connexions.ps1 a permis de réduire le temps de diagnostic des erreurs de connexion. Cette démarche garantit la traçabilité des accès et permet de détecter rapidement des tentatives de force brute sur le protocole RDP, assurant ainsi la sécurité du contrôleur de domaine sisr.local"..