🔍 Description :

Un utilisateur standard sur un poste client tente d'utiliser **PsExec** pour exécuter des commandes sur un autre hôte du réseau ce qui est typique d'un **mouvement latéral** utilisé dans des attaques de type **post exploitation**.

🗂 Sources de logs :

- Logs Windows (Security)
- Logs de l'Active Directory
- Logs du pare-feu local

📡 Règle d'alerte dans le SIEM :

Détection d'exécution de **PsExec.exe** par un **utilisateur non privilégié** suivie d'une tentative de **connexion SMB/RPC** sur un autre hôte.

🚨 Résultat d'Analyse dans le SIEM :

Alerte :

⚠️ Exécution de PsExec par un utilisateur non administrateur - **possible mouvement latéral**

Détails :

- 🖥 **Hôte source :** PC-JOHNDOE01 (IP: 192.168.1.57)
- **Utilisateur :** Papi
- 📄 **Fichier exécuté :** C:\Temp\PsExec.exe
- 🔗 **Processus parent :** cmd.exe
- 🎯 **Hôte cible :** SRV-FINANCE01 (IP: 192.168.1.42)
- ⏰ **Heure de l'événement :** 23/04/2025 14:26:13

- 🌐 **Type de connexion :** SMB (port 445) RPC (port 135)

🧠 Analyse :

L'utilisateur **Papi**, non administrateur selon les attributs AD, a tenté d'exécuter **PsExec** pour lancer des commandes à distance sur le serveur **SRV-FINANCE01**.

Ce comportement est **anormal pour son profil**, d'autant plus qu'aucune tâche de support ou d'administration ne lui est assignée.

Les logs indiquent que **PsExec a été lancé manuellement** depuis une console CMD et que le **processus parent est lui-même issu d'une session interactive**.

🔥 Risque :

Élevé – Cette action est souvent liée à :

- Des attaques internes
- Des tentatives de prise de contrôle latérale
- Une compromission de compte

🌓 Réponse :

Actions immédiates :

- 📴 **Isolation du poste** PC-JOHNDOE01 via EDR
- ❌ **Désactivation temporaire** du compte AD Papi
- 💾 **Sauvegarde et analyse de la mémoire** de la machine
- 📁 **Export des logs pour forensique** (Windows, EDR, pare-feu)

Actions à venir :

- 🔍 **Analyse complète** du poste avec un outil
- 🔄 **Vérification des autres connexions** initiées par Papi
- 📊 **Audit de l'activité PsExec** sur l'ensemble du parc via le SIEM
- 🔐 **Réinitialisation des crédenciales** de Papi après enquête

Recommandations :

- 🚫 **Restreindre l’accès** aux outils d’administration comme PsExec aux seuls administrateurs
- 📜 **Activer la journalisation avancée** de PowerShell
- 🔒 **Appliquer le principe de moindre privilège** sur les postes utilisateurs
- 🧠 **Sensibilisation des utilisateurs** aux risques de phishing et d’abus de compte