Rapport d'Incident de Menace Interne

Date: 22 octobre 2025

Samuel Gauthier

Contexte:
Purview a déclenché une alerte DLP indiquant un partage potentiel d'un fichier contenant des numéros NAS. J'ai démarré l'investigation avec le module eDiscovery pour analyser l'alerte. Avec DTEX, j'ai vérifié que "user123" s'est connecté depuis une IP externe (ex. : via openvpn.exe). Le fichier sensible "Client_NAS.zip" a été exfiltré à 2h du matin vers une adresse Gmail externe.

Analyse (Splunk):
Les logs "fake_logs.csv" confirment l'exfiltration via Outlook vers une IP externe (172.16.xxx.x, Tokyo). Voir l'activité à 2h, "activity_plot.png". "analyze_logs.py" montre les partages suspects, indiquant où et quand le fichier a été envoyé.

Confirmation (Sentinel):
Requête KQL ("sentinel_query.txt"): OfficeActivity | where FileName == "Client_NAS.zip" and Operation == "SharedExternally" and TimeGenerated >= datetime(2025-10-22T02:00:00Z) and TimeGenerated < datetime(2025-10-22T03:00:00Z) and IPAddress startswith "172.16" | extend UserInfo = tostring(UserId) | project TimeGenerated, IPAddress, UserInfo. Confirme une connexion suspecte à Tokyo. Besoin d'information additionnel de "user123" pour confirmer si l'intention est malveillante ou s'il s'agit d'une erreur.

Impact (Purview):
Le fichier est classé PII (numéros NAS, règle dans "purview_rule.txt"). Une violation DLP est détectée, avec un risque de non-conformité (GDPR/PIPEDA).

Actions Recommandées:

Notification à l'équipe pour valider les étapes suivantes avec un senior qui connais les runbook.

Audit supplémentaire des logs.

Références :

- GitHub: https://github.com/Kurama2/InsiderThreatSimulation
- Fichiers: fake_logs.csv, analyze_logs.py, activity_plot.png.