Rapport d'Incident de Menace Interne

Date: 22 octobre 2025

Samuel Gauthier

Contexte:
DTEX a détecté une anomalie avec un score de risque élevé pour l'utilisateur "user123". Il a exporté de manière non autorisée un fichier sensible "Client_NAS.zip" 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.

Confirmation (Sentinel):
Requête KQL ("sentinel_query.txt"): OfficeActivity | where FileName == "Client_NAS.zip" and Operation == "SharedExternally". 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.
- Audit supplémentaire des logs.

Références :

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