TACHE 2 : SURVEILLANCE DES ALERTES DE SÉCURITÉ ET SIMULATION DE RÉPONSE AUX INCIDENTS

BROUILLON DE COMMUNICATION (EMAIL)

Période d'analyse : 03 Juillet 2025

Outil utilisé : Elastic Stack (ELK)

Objectif : Identifier, catégoriser et prioriser les incidents détectés dans les journaux système.

AUTEUR : BARIKI Wilson

Date du rapport : 9 Janvier 2026

Objet : [ALERTE SÉCURITÉ CRITIQUE] Rapport d'incident et mesures de remédiation - Incident INC-2025-07-03

Bonjour,

Je vous informe qu'une activité malveillante critique a été détectée sur notre réseau aujourd'hui, le 03 juillet 2025, par notre système de surveillance SIEM.

Détails de l'incident :
L'alerte principale concerne un comportement de type **Ransomware** identifié sur le serveur de fichiers (172.16.0.3) via le compte de l'utilisateur **Bob**. D'autres menaces (Rootkit et Ver informatique) ont également été détectées sur les postes des utilisateurs Bob et Alice.

Actions immédiates effectuées :

- Les postes et serveurs compromis ont été isolés du réseau pour empêcher toute propagation.
- Les adresses IP externes malveillantes (203.0.113.77 et 198.51.100.42) ont été bannies au niveau du pare-feu.
- Les comptes utilisateurs concernés ont été temporairement désactivés.

Situation actuelle :
La menace est sous contrôle et aucune perte de données définitive n'est à déplorer pour le moment. Nous procédons actuellement au nettoyage des systèmes et à la réinitialisation sécurisée des accès.

Vous trouverez en pièce jointe le rapport détaillé ainsi que nos recommandations pour renforcer la sécurité de nos accès distants.

Je reste à votre disposition pour tout complément d'information.

Cordialement,

BARIKI Wilson
Analyste SOC Junior