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

TABLEAU DE CLASSIFICATION ET TRIAGE DES ALERTES

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

ID Alerte	Horodatage (Timestamp)	Utilisateur	IP Source	Type de Menace	Priorité	Statut	Action Entreprise
AL-001	09:10:14	Bob	172.16.0.3	Ransomware Behavior	Critique	Résolu	Isolation du serveur et coupure des accès réseau.
AL-002	04:19:14	Alice	198.51.100.42	Rootkit Signature	Élevée	En cours	Mise en quarantaine du poste pour réinstallation complète.
AL-003	05:06:14	Bob	203.0.113.77	Worm Infection	Élevée	Résolu	Blocage de l'IP source sur le firewall périmétrique.
AL-004	07:02:14	Alice / David	203.0.113.77	Brute Force (Login Failed)	Moyenne	Clos	Tentatives multiples détectées. IP bannie.
AL-005	07:45:14	Charlie	172.16.0.3	Trojan Detected	Moyenne	En cours	Scan antivirus approfondi (Full Scan) lancé à distance.
AL-006	05:49:14	Charlie	192.168.1.101	Connection Attempt	Faible	Clos	Activité de reconnaissance réseau suspecte mais bloquée.