Durcissement d’un SIEM

Encadré par :
Mme.ABBAS WISSAM

2025-2026

Réalisé par :
-FAJRI Abdeljalil
-BAGGY Oussama
-AOUINATI Zakaria
-AIT OURAJLI Mohamed
-AIT ZIDAN Salma
-OUZANZOUL Bouchra

INTRODUCTION

Face à l’augmentation des cybermenaces, la surveillance et l’analyse des événements de sécurité sont essentielles.

Ce projet consiste à mettre en place et durcir un système SIEM pour renforcer la détection des incidents et la sécurité globale de l’infrastructure.

OBJECTIFS

Ce projet vise à :

- Déployer un SIEM sécurisé .
- Protéger et centraliser les logs.
- Appliquer des mesures de durcissement.
- Détecter et corréler des événements de sécurité réels.

Contexte et problématique

Un SIEM centralise les logs pour détecter les activités suspectes, mais il peut devenir une cible s’il n’est pas correctement sécurisé. Le défi est donc de protéger toute la chaîne de collecte, de transmission et d’analyse des journaux afin de garantir leur intégrité et leur disponibilité.

État de l’art des SIEM

- Splunk : solution commerciale puissante mais coûteuse.
- ELK Stack : open source, modulable et extensible.
- Wazuh : dérivé d’OSSEC, combine IDS, gestion des logs et conformité.

Notre choix

Nous avons choisi Wazuh car il est open source, facile à utiliser et couvre la sécurité et la gestion des logs.

Architecture proposée :

Stratégies de durcissement :

Résultats et validation :

Conclusion :

Le durcissement du SIEM a permis de démontrer qu’un système de journalisation bien configuré peut offrir une visibilité complète sur les événements de sécurité tout en restant résistant aux attaques. Cette expérience a renforcé nos compétences techniques en administration système, sécurité réseau et automatisation.

Perspectives :

Les améliorations possibles incluent :

- Intégration d’alertes par e-mail et Slack.
- Ajout d’un module de Threat Intelligence.
- Audit de conformité automatique (CIS Benchmark, ISO 27001).
- Déploiement sur un cloud sécurisé (Azure, AWS) avec gestion centralisée des logs.

MERCI POUR VOTRE ATTENTION