Rapport de Projet Cybersécurité - Détection et Analyse d'Incidents

Projet : Détection et Réponse aux Incidents de Sécurité

Auteur : Analyste SOC - Projet de simulation

Date : Juin 2025

1. Introduction

Ce projet vise à simuler un environnement d'analyse de sécurité à travers l'utilisation d'outils tels que auditd, Suricata, Sysmon for Linux, et Splunk. L'objectif est de détecter, visualiser et répondre à différents types d'incidents de sécurité, qu'ils soient liés à l'intégrité des fichiers, au trafic réseau ou aux utilisateurs malveillants.

2. Outils utilisés

- auditd : Audit des accès et modifications des fichiers critiques

- Suricata : IDS pour la détection du trafic réseau anormal

- Sysmon for Linux : Surveillance des activités systèmes (processus, connexions réseau)

- Splunk : Ingestion, corrélation et visualisation des journaux

3. Étape 1 : Surveillance des fichiers sensibles

1. Installation d'auditd sur la machine cible

2. Ajout de règles de surveillance sur /etc/

3. Simulation : création/modification de fichier (/etc/myfirstfile.txt)

4. Analyse via ausearch et Splunk

5. Réaction : identification de l'accès non autorisé

4. Étape 2 : Détection de trafic réseau anormal

1. Installation de Suricata avec les règles Emerging Threats

2. Configuration pour surveiller l'interface réseau

3. Intégration dans Splunk via le forwarder

4. Simulation : Scan Nmap (nmap -sS)

5. Analyse : Alertes Suricata dans Splunk (src_ip détectée)

6. Réaction : Corrélation et réponse possible (blocage IP)

5. Étape 3 : Activité suspecte des comptes utilisateurs

1. Installation de Sysmon for Linux et configuration XML

2. Simulation : ajout d'un utilisateur 'maluser'

3. Visualisation dans /var/log/syslog et Splunk

4. Requêtes Splunk pour identifier l'utilisateur, le processus, et l'action

5. Réaction : suppression du compte malveillant

6. Résultats et visualisation

Les événements collectés ont été correctement ingérés dans Splunk et affichés dans des dashboards. Les alertes ont été générées sur la base de règles personnalisées (ex : adduser détecté).

7. Conclusion et recommandations

Ce projet a permis de démontrer la capacité à :

- Surveiller l'activité système et réseau en temps réel

- Intégrer différents outils de sécurité dans une solution SIEM

- Réagir de manière structurée à des incidents

Recommandations : mettre en place des alertes automatisées, enrichir les règles Suricata, étendre Sysmon avec des règles spécifiques.