Université Lumière Lyon 2

Projet d’application

Livrable 1

Tom Areal et Thomas Lecomte
Automne 2025

Composition de l'équipe, répartition du travail et apports respectifs

Titre temporaire :

EaSIEM (contraction/fusion du mot « Easy » et de l'acronyme « SIEM »)

Présentation :

L'équipe de développement sera composée de **Tom Areal** et de **Thomas Lecomte**. Afin de tirer le meilleur de l'équipe, le travail sera réparti en fonction des compétences de chacun :

- Tom s'occupera principalement de l'**algorithmique** et de la **programmation en C++**.
- Thomas se chargera de la **conception du système** (diagramme de classe) et de son principe de **fonctionnement**.
- L'IA pourra éventuellement être utilisée en cas d'impasse dans le processus de création de l'application ou pour répondre à des questionnements techniques précis. Toute utilisation sera dûment signalée.

Le projet d'application consistera en la création d'un **gestionnaire de journaux de sécurité** (Security Log Manager). L'application **1)** collectera des log, **2)** harmonisera leur format, **3)** analysera leur contenu, **4)** produira des rapports d'événements de sécurité, **5)** archivera les rapports et les logs utilisés.

Afin de mener à bien ce projet, et compte tenu du sujet retenu, l'équipe s'appuiera sur les recommandations formulées dans des référentiels de sécurité comme l'ISO27000 et sur les documentations adressées dans certaines certifications de sécurité[1]. Fait important, nous nous baseront sur la documentation la plus récente en la matière.

Pour valider le fonctionnement de l'application, des jeux de données reproduisant le contenu de logs permettront de tester le gestionnaire de journaux de sécurité. Ces jeux de données offriront une expérience complète de scénarisation.

[1] Daril Gibson et Joe Shelley, 2023, « CompTIA Security+: Get Ahead, Get Certified. SY0-701 Study Guide», Certification Experts LLC.

Fonctionnalités principales

- **Fonctionnalité de collecte des logs :** On veut que le système de logs collecte des logs issus de sources diverses : Windows Logs (security log, system log, application log), Linux Logs (…/var/log/syslog, …/var/log/secure, …/var/log/auth.log, …/var/log/audit.log)[2].
- **Fonctionnalité de reformatage des logs collectés :** On veut que notre système harmonise le format, souvent disparate, des logs. Cette fonctionnalité de reformatage comprend aussi la synchronisation horaire, afin que les logs suivent le même fuseau/format horaire.
- **Fonctionnalité d'ajout, de suppression ou de modification manuelle des logs :** On veut la possibilité de manipuler les données du système. On veut aussi pouvoir ajouter des commentaires sur nos analyses/logs.
- **Fonctionnalité d'import/export de logs :** On veut pouvoir importer ou exporter des données facilement.
- **Fonctionnalité de production automatisée et d'exportation de rapport d'événements :** On veut que notre système produise des rapport clé en main pour retracer des événements de sécurité. Cela implique la création de déclencheur pour identifier automatiquement les événements qui se retrouveront dans les rapports.
- **Fonctionnalité de filtrage et de tri des logs** : On veut pouvoir appliquer un filtre ou un tri sur nos données de logs, afin de rechercher et de sélectionner des éléments spécifiques.
- **Fonctionnalité d'archives simplifiée :** On veut mettre en place un système d'archive adapté à nos capacités de stockage. On doit pouvoir déterminer une date de péremption (longue, moyenne ou courte) pour nos données de logs ET pour nos événements/rapports.

Fonctionnalité et éléments bonus

- **Création d'un Dashboard** (type Excel/tableau croisé dynamique) qui communique les données et l'analyse des logs en temps réel.
- **Création d'une interface graphique** pour rendre l'utilisation de l'application plus intuitive.

[2] Initialement, nous voulions aussi intégrer des Network Logs (firewall logs, IDS/IPS logs, Packet Captures), et des Applications Logs (requêtes server sur le web). Nous avons toutefois revu cette ambition à la baisse, afin que le projet soit réalisable dans les délais imposés.