PROJET 2CS SIQ

ÉQUIPE 3 :

Messar Cylia (CE)
Tagzirt Elissa
Sadi Lina
Kedadsa Islam Chakib
Bousba Neda
Bessaha Sofiane

Pourquoi sécuriser son réseau?

Dans notre ère digitale, sécuriser son réseau et ses données sont devenues des enjeux cruciaux. En 2005, Gartner, une entreprise de premier plan spécialisée dans le conseil et la recherche technologique, a introduit la notion de **SIEM** (Security Information and Event Management). Cette innovation marque la convergence des technologies **SEM** (Security Event Management) et **SIM** (Security Information Management), établissant ainsi un nouveau standard essentiel pour la protection continue de l'information.

1

C'est quoi un SIEM?

Le **SIEM** est une solution intégrale qui combine les fonctionnalités des systèmes SIM et SEM. Cet outil collecte, agrège, et normalise les données de sécurité, les analysant selon des règles prédéfinies pour ensuite les présenter dans un format facilement compréhensible par l'utilisateur.

SIM Security Information Management

- Collecte et archivage des données .
- Analyse des données.
- Assurer la conformité et réaliser des revues historiques.

SEM Security Event Management

- Surveillance en temps réel.
- Notification d'événements critiques.
- Orchestration des réponses aux incidents de sécurité.

2

Quelles sont ses fonctionnalités?

3

Ceux-ci sont les fonctionnalités principales (1-5) que l'on trouve dans tous les systèmes :

Collecte :

C'est le processus par lequel il rassemble les données de sécurité , comme les logs de diverses sources réseau comme :

IDS/IPS Firewall Server Router Switch

En utilisant ces méthodes-là :

Push

Les sources transmet périodiquement les données de sécurité, qui peuvent être envoyées soit :

Sans agent Avec agent

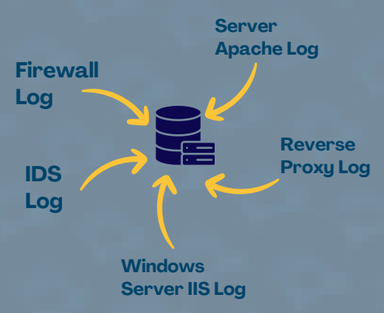
Pull

Les sources envoient automatiquement leurs données de sécurité au SIEM en temps réel.

1

Agrégation :

La consolidation des données collectées en un emplacement centralisé, dans une infrastructure de stockage dédiée .



2

Traitement :

La conversion et l'enrichissement des données pour une analyse précise et efficace.

Parsing :
Transformation des données brutes en un format structuré

Normaliser/Catégoriser :
Uniformisation des données de différentes sources pour les rendre comparables et classifiables selon des critères définis.

Enrichir :
Ajout d'informations complémentaires aux données de sécurité pour améliorer leur pertinence et leur utilité.

3

Corrélation :

Elle utilise des règles et des algorithmes avancés pour associer des événements de sécurité apparentés et identifier des incidents de sécurité potentiels, souvent en réduisant les faux positifs.

4

Visualisation :

Transforme les données de sécurité en tableaux de bord clairs, facilitant le suivi et l'action rapide face aux incidents.

5

Autres fonctionnalités :

Voici quelques fonctionnalités qui ne sont pas entièrement présentes dans tous les SIEM :

- Règles prédéfinies.
- Automatisation intelligente.
- Analyse comportementale .
- Threat Intelligence .
- Rétention .
- Analyse de la posture de système/Réseau.

Quels sont les bénéfices et défis des SIEM dans la gestion de la sécurité IT?

Avantages des SIEM :

- Intégration avec d'autres outils de sécurité.
- Détection accélérée des menaces.
- Gestion des volumes importants de données de sources diverses.
- Amélioration de la visibilité et de la conformité.

Inconvénients des SIEM :

- Coûts et complexité élevés.
- Maintenance et mises à jour constantes.
- Questions de confidentialité.
- Génération de faux positifs.

Limites des technologies SIEM :

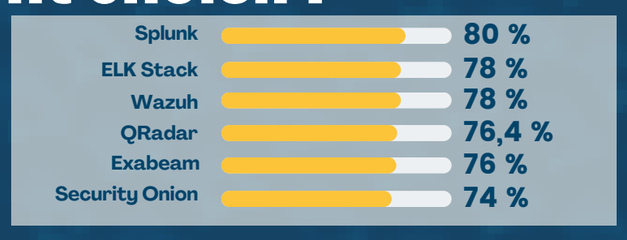
- La détection des menaces inconnues ou avancées.
- Surcharge d'informations.
- Manques d'automatisation et d'orchestration.

4

Quels sont les outils disponibles sur le marché et comment choisir?

5

Selon **Gartner**, nous avons fait notre sélection des six SIEM les plus renommés, incluant trois options open-source(ELK Stack, Security Onion, Wazuh) et trois solutions commerciales(Splunk, QRadar, Exabeam).



Voici une comparaison entre les six SIEM en termes de capacité de traitement des données, conformité réglementaire, sécurité et coût :

	Réponse aux incidents	Génération des alertes en temps réel	Intégration avec des outils de sécurité	Analyse de la posture de sécurité du système	Analyse de la posture de sécurité du réseau	Corrélation sophistiqué et réduction des faux positifs	Performance (Rapidité, Indexation)	Coût	Règles de corrélation prédéfinies et à jour	Documentation	Intégration de la threat intelligence	Complexité	Visualization personnalisé	Génération de rapports	Rétention	Gros volume de donnés	TOTAL /15
Splunk	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	13
QRadar	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	13
Exabeam	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	14
ELK	✗	✓	✓	✗	✗	✗	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	9
Wazuh	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	12
SOS	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	9

Nous avons opté pour quelle solution?

6

WAZUH

Wazuh et **Security Onion** offrent ensemble un SIEM robuste. Toutefois, en raison de la complexité de leur intégration simultanée, nous mettrons en place uniquement Wazuh. Ce dernier assure une surveillance minutieuse des hôtes, détecte les anomalies et maintient la conformité. Pour une sécurité accrue, Wazuh sera intégré avec le **NIDS Suricata** de Security Onion, qui analyse le trafic réseau pour repérer les menaces externes, renforçant ainsi la détection des menaces et la réponse rapide aux incidents.

Conclusion

8

En conclusion, cette étude théorique met en évidence l'importance cruciale de l'intégration de technologies SIEM avancées dans les réseaux traitant des données sensibles. Bien que certains outils commerciaux offrent une facilité de configuration et des fonctionnalités complètes, nous avons préféré adopter une solution open-source. Ce choix, malgré ses défis inhérents, nous permet d'assurer une flexibilité et une personnalisation étendues, parfaitement adaptées aux spécificités de notre environnement réseau.

Quelle est l'architecture de votre solution?

7

1. Wazuh est structuré en trois parties principales :
   - **Le Server** pour la récolte et le traitement de données.
   - **L'Indexer** pour trier les journaux
   - **Le Dashboard** pour présenter et analyser les événements de sécurité.
2. Suricata est configuré au niveau du reverse proxy, qui est le point d'intersection central de notre réseau.
3. Les autres terminaux incluent les serveurs web Apache et IIS, avec le firewall pfSense servant de point d'accès sécurisé au réseau depuis l'extérieur.