SAE11:

Sensibilisation a Hygiène Informatique

Projet fait par :

Karcher thibaut

Saleiro david

badreddine iheb

les points à aborder dans ce projet sont:

1)journalisation:

-Présentation de la journalisation .

-importance de la journalisation .

2)les NIDS et les HIDS :

-Présentation des NIDS .

-Information sur l'utilité des NIDS

-Présentation des HIDS .

-Information sur l'utilité des HIDS .

3)LE SIEM :

-Présentation du SIEM .

-Fonctionnement du SIEM .

La sécurité informatique est une préoccupation majeure dans le domaine des réseaux et des télécommunications. Avec la prolifération des attaques cybernétiques sophistiquées, il devient essentiel de mettre en place des mécanismes efficaces de détection d'intrusions pour protéger les systèmes d'information. La détection d'intrusions est un processus visant à identifier et à réagir aux activités suspectes ou malveillantes. Dans cette optique, plusieurs outils et technologies sont utilisés, dont la journalisation, les systèmes de détection d'intrusions réseau (NIDS), les systèmes de détection d'intrusions sur les hôtes (HIDS) et les solutions SIEM (Security Information and Event Management).

Journalisation

-Présentation de la journalisation :

La journalisation, également connue sous le terme de logging, représente un pilier essentiel dans la détection d'intrusions en réseaux et télécommunications. Elle englobe la collecte systématique, le stockage et l'analyse des données relatives aux événements se produisant au sein d'un système informatique. Les journaux, ou logs, peuvent revêtir différentes formes, allant des enregistrements simples des connexions aux informations détaillées sur les modifications de fichiers, les accès aux ressources, et bien plus encore.

importance de la journalisation

L'importance des journaux se manifeste à travers :

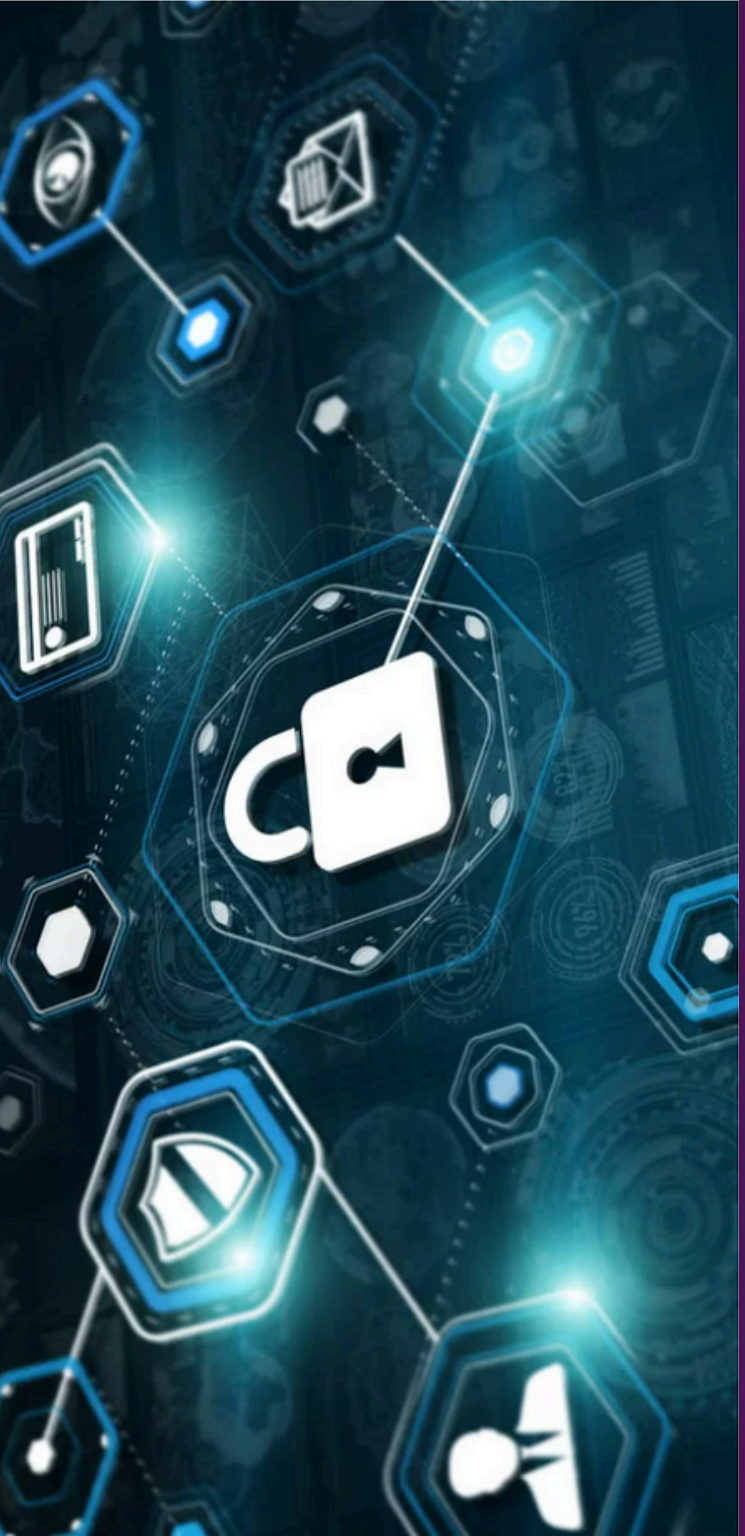
1. Traçabilité : Les journaux permettent une traçabilité complète des actions, facilitant la détection de schémas d'activité suspects.

2. Détection précoce : L'analyse régulière des journaux permet une identification rapide des activités anormales, permettant une réponse proactive aux menaces potentielles.

3. Analyse forensique : En cas d'intrusion, les journaux sont essentiels pour retracer les actions des attaquants, comprendre le mode opératoire, et renforcer la sécurité.

4. Conformité : La conservation des journaux répond aux exigences réglementaires, démontrant la mise en place de mesures de sécurité adéquates.

5. Prévention : L'analyse des journaux identifie les vulnérabilités, permettant la mise en place de contre-mesures préventives.



les NIDS et les HIDS

-Présentation des NIDS et HIDS: .

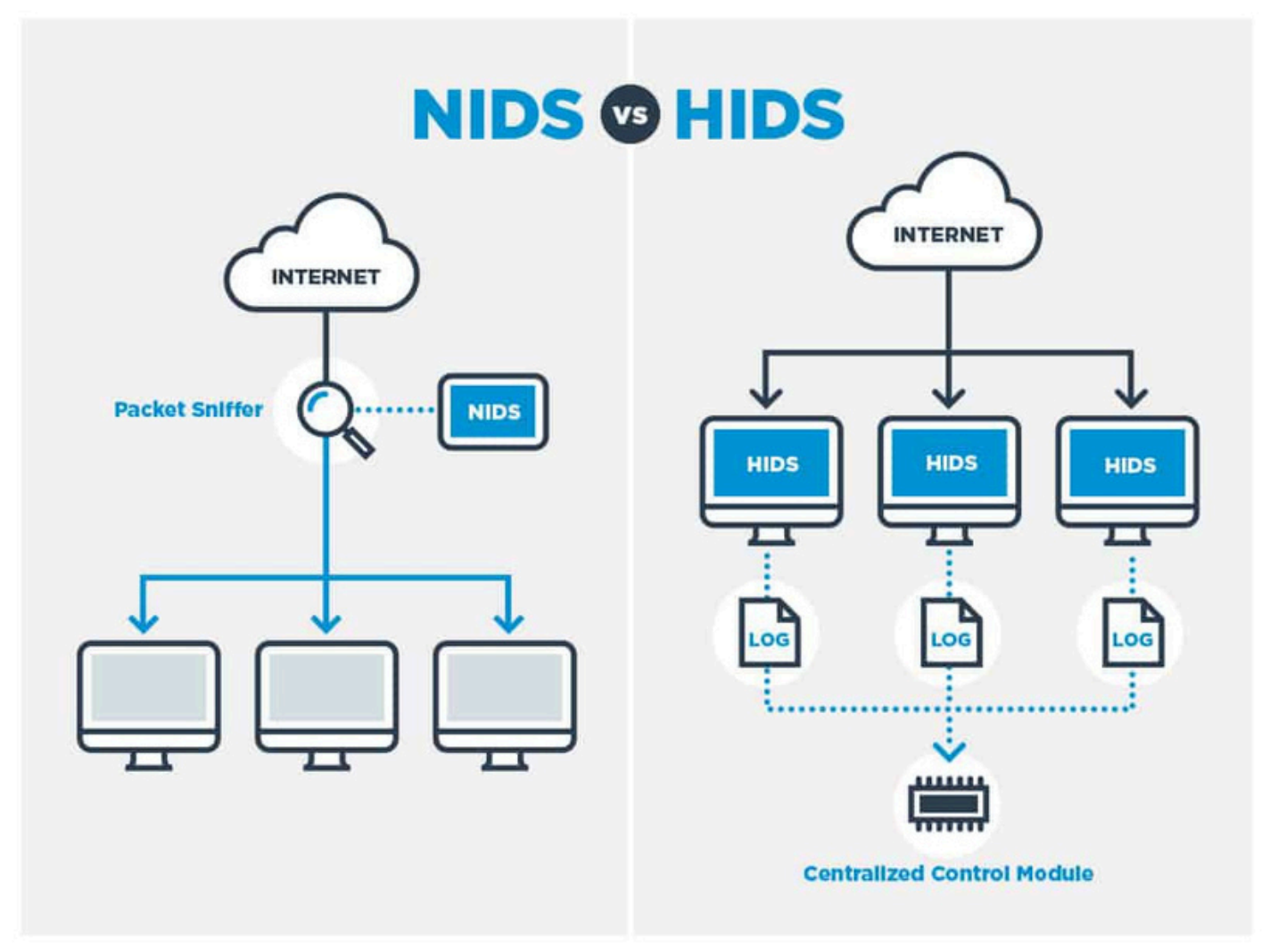
NIDS

Les NIDS ou Network Intrusion Detection System sont des sondes réseaux pour analyser le trafic et essayer de trouver des activités inhabituelles, comme le scanning, les tentatives d'intrusions, les portes dérobées, etc.

HIDS

Sur les systèmes HIDS, des applications de protection, comme les pare-feu, les antivirus et les programmes de détection des logiciels espions, sont installées sur tous les ordinateurs d'un réseau ayant accès à un environnement extérieur, comme Internet.

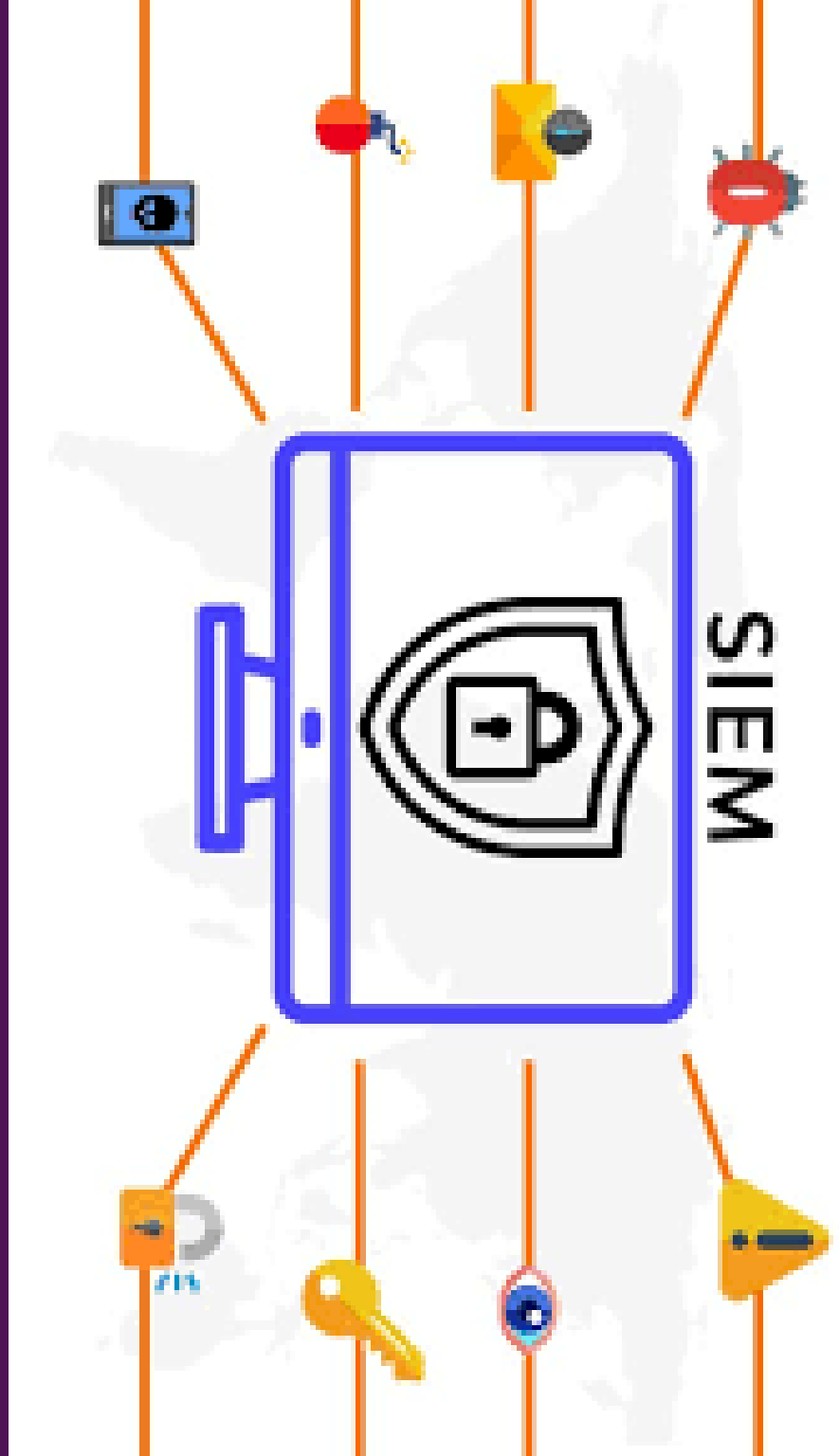
La différence NIDS / HIDS en image



LE SIEM

-Présentation du SIEM :

Un SIEM ou Système de gestion des informations et des événements de sécurité est un systéme qui collecte des logs et des événements afin de normaliser ces données pour une analyse ultérieure pouvant générer des visualisations, des alertes, des recherches, des rapports et bien plus encore.



Fonctionnement d'un SIEM :

Collecte des Données :

Un SIEM collecte des données provenant de diverses sources au sein du réseau, telles que les journaux système, les journaux d'applications, les pare-feu, les dispositifs de détection d'intrusions (NIDS), les systèmes de détection d'intrusions sur hôte (HIDS), et d'autres dispositifs de sécurité.

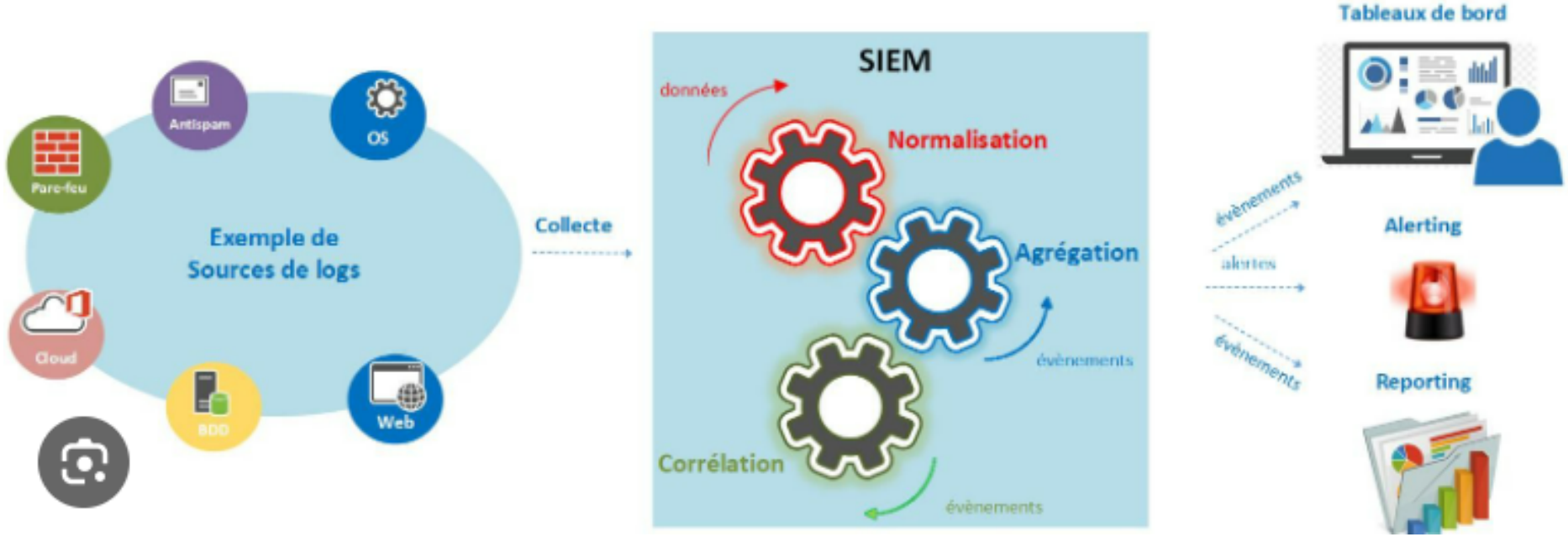
Corrélation des Événements :

Le SIEM utilise des règles de corrélation pour analyser les données en temps réel.
La corrélation permet de détecter des schémas d'activité qui pourraient indiquer une menace.

Génération d'Alertes

Lorsque des événements correspondant à des règles prédéfinies sont détectés, le SIEM génère des alertes en temps réel. Ces alertes sont souvent classées en fonction de leur gravité pour aider les équipes de sécurité à prioriser leurs actions.

Schéma de fonctionnement d'un SIEM



conclusion

En résumé, les SIEM utilisent la journalisation comme source principale de données, collectant des journaux à partir de diverses sources, y compris les NIDS et les HIDS, pour fournir une vue globale des événements de sécurité dans un environnement informatique. Les NIDS se concentrent sur la surveillance du trafic réseau, tandis que les HIDS se concentrent sur les activités au niveau de l'hôte, et les journaux sont essentiels pour l'analyse des incidents et la détection des menaces.

Merci à tous pour votre attention nous attendrons de répondre à vos questions

les sites utilisés :

-https://www.elastic.co/fr/what-is/siem/#/what-is/siem
- https://www.dnsstuff.com/host-based-intrusion-detection-systems
- https://www.comparitech.com/net-admin/nids-tools-software/
- https://www.logpoint.com/fr/c-est-quoi-le-siem/
- https://medium.com/@huglertomgaw/tryhackme-introduction-to-siem-bf1e4d5363f8