**Étude des Solutions IDS/IPS du Marché**

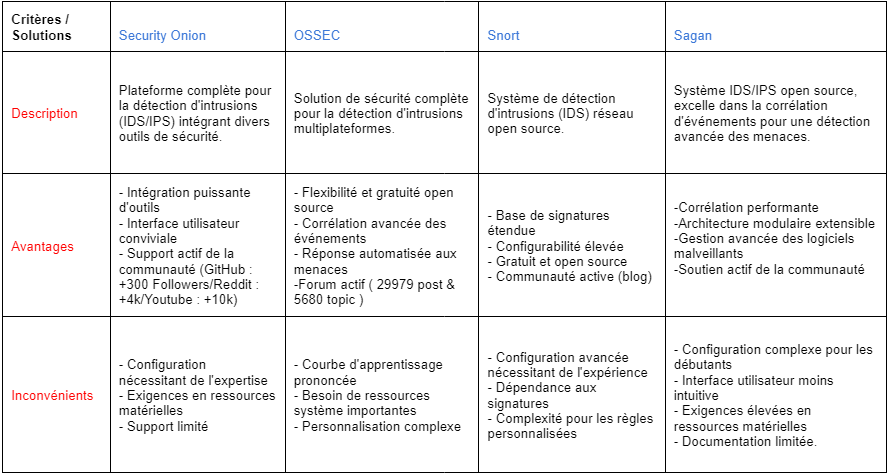
La mise en place d'un système de détection et prévention d'intrusion (IDS/IPS) au sein d'un centre hospitalier commence par une analyse approfondie des solutions disponibles sur le marché. Cette démarche inclut une étude comparative, mettant l'accent sur la sélection d'une solution performante et gratuite.L'objectif principal est d'identifier les avantages et inconvénients de chaque option, en mettant en évidence celle qui répondra le mieux aux besoins spécifiques du centre hospitalier.

Cette étude comparative se déroule en examinant attentivement les fonctionnalités de chaque solution, évaluant leur convivialité, leur flexibilité et leur compatibilité avec l'infrastructure existante. Le processus vise à répondre de manière optimale aux exigences particulières de sécurité du réseau informatique hospitalier tout en tenant compte des contraintes budgétaires. Opter pour une solution gratuite, permet d'optimiser les ressources financières, assurant un équilibre entre la robustesse de la détection et la maîtrise des coûts. L'objectif final est de garantir une intégration harmonieuse de la solution retenue, renforçant ainsi la résilience du réseau informatique face aux cybermenaces, tout en minimisant les perturbations potentielles dans les opérations hospitalières.

*Positionnement de L’IDS/IPS*

L'IDS/IPS est généralement placé de manière à surveiller l'ensemble du réseau, en mettant un accent particulier sur les points sensibles tels que les serveurs de bases de données médicales, les terminaux de contrôle des équipements hospitaliers, et les serveurs d'authentification et de messagerie. Cette approche stratégique offre à l'IDS/IPS une vision globale des flux de données critiques, lui permettant de repérer d'éventuelles tentatives d'intrusion à différents niveaux du réseau. De plus, le positionnement de l'IDS/IPS peut varier en fonction du type choisi, qu'il s'agisse d'une solution logicielle ou d'une appliance physique.

*Étude Comparative*

Bien sûr, voici un tableau comparatif simplifié basé sur les meilleures caractéristiques de chaque solution :

1. Critères d'Évaluation :
   1. Fonctionnalités de Détection → Évalue la capacité de la solution à détecter une variété d'attaques.
   2. Interface Utilisateur → Évalue la convivialité et l'intuitivité de l'interface utilisateur.
   3. Personnalisation → Mesure le degré de personnalisation possible selon les besoins spécifiques.
   4. Compatibilité → Évalue la capacité de la solution à s'adapter à différentes plates-formes et environnements.
   5. Support/Assistance → Indique le niveau de support et d'assistance disponible auprès de la communauté ou des développeurs.
2. Tableau Comparatif :

| **SOLUTION** | Fonctionnalités de détection | Interface Utilisateur | Personnalisation | Compatibilité | Support/Assistance |
| --- | --- | --- | --- | --- | --- |
| Security Onion | Haut | Intuitive | Élevée | Large | ✔️ |
| OSSEC | Élevée | Adaptative | Avancée | Multiplateforme | ✔️ |
| Snort | Étendu | Configurable | Élevée | Large | ✔️ |
| Sagan | Performante | Moins intuitive | Avancée | Large | ✔️ |

*Fonctionnalités de Détection :*

***Security Onion :*** Présente des capacités de détection élevées, couvrant un large spectre d'attaques.

***OSSEC*** : Propose des fonctionnalités de détection élevées, en particulier avec sa corrélation avancée d'événements.

***Snort*** : Dispose d'une base de signatures étendue, couvrant un large éventail d'attaques connues.

***Sagan***: Offre des fonctionnalités avancées de détection, en particulier grâce à sa corrélation sophistiquée d'événements.

*Interface Utilisateur :*

**Security Onion** : Son interface intuitive facilite la gestion et l'analyse des événements de sécurité.

**OSSEC** : Une interface adaptative qui vise à simplifier la visualisation et la gestion des alertes.

**Snort** : Configurable, permettant aux administrateurs d'adapter l'interface à leurs besoins spécifiques.

**Sagan**: Une interface moins intuitive, mais performante pour la navigation et l'interprétation des données.

*Personnalisation :*

**Security Onion** : Permet une personnalisation élevée pour répondre aux besoins spécifiques du réseau.

**OSSEC** : Offre une personnalisation avancée des règles et des politiques de sécurité.

**Snort** : Hautement configurable, permettant aux administrateurs de définir des règles personnalisées.

**Sagan**: Propose une personnalisation avancée des règles pour s'adapter aux exigences spécifiques.

*Compatibilité :*

**Security Onion** : Compatible avec une large gamme d'environnements grâce à son architecture extensible.

**OSSEC** : Multiplateforme, adapté à différents systèmes d'exploitation, Linux, Windows et Unix.

**Snort** : Compatible avec une variété de plates-formes, assurant une large adaptabilité.

**Sagan**: Offre une compatibilité étendue avec différentes configurations réseau.

*Support/Assistance :*

**Security Onion** : Bénéficie d'une communauté active qui offre un support continu et des ressources.

**OSSEC** : Profite d'une communauté active pour le développement continu et le partage de ressources.

**Snort** : Soutenu par une communauté active contribuant à l'évolution constante des signatures et fonctionnalités.

**Sagan**: Bien que moins lié à une solution spécifique, peut bénéficier d'un support communautaire relativement actif.

*Conclusion de la solutions choisie:*

Suite à une analyse approfondie des solutions IDS/IPS disponibles sur le marché, le choix de la solution la plus appropriée pour notre projet au sein du centre hospitalier se porte sur OSSEC. Cette décision résulte de plusieurs considérations alignées sur les besoins spécifiques de l'environnement hospitalier, ainsi que sur les critères de facilité de configuration, de convivialité, et de capacités avancées de détection.

Notre préférence pour OSSEC repose notamment sur sa polyvalence multiplateforme, offrant une compatibilité étendue avec différents systèmes d'exploitation présents dans l'infrastructure hospitalière. Cette caractéristique assure une intégration fluide sans compromettre la stabilité du réseau.

De plus, la corrélation avancée d'événements d'OSSEC constitue un atout majeur pour renforcer notre capacité à détecter de manière proactive les menaces potentielles. Cette fonctionnalité, combinée à la configurabilité élevée, permet aux administrateurs de définir des règles et des politiques de sécurité sur mesure, répondant ainsi aux besoins spécifiques du réseau hospitalier.

Bien que Security Onion soit une solution respectée dans la communauté de la sécurité informatique, son choix n'a pas été privilégié pour notre projet en raison de sa courbe d'apprentissage potentiellement plus abrupte. Malgré sa documentation robuste, la préférence pour OSSEC repose également sur la convivialité de son interface utilisateur, rendant la configuration et la gestion plus accessibles, même pour des utilisateurs moins expérimentés.

En conclusion, le choix d'OSSEC s'aligne avec les impératifs de notre projet en offrant une solution complète, adaptable, et conviviale pour la détection d'intrusion au sein du réseau informatique du centre hospitalier. Cette sélection découle d'une évaluation minutieuse des avantages et inconvénients de chaque solution, avec une priorité accordée à la solution qui répond le mieux aux exigences spécifiques de notre environnement.