

## **Annexe : Etude comparative détaillée**

### **1. Security Onion :**

#### **Description :**

Security Onion est une solution open source complète de détection et de prévention d'intrusions (IDS/IPS) conçue pour garantir la sécurité des réseaux. Basé sur une architecture extensible, il intègre plusieurs outils de renom tels que Snort, Suricata, Bro, Sguil, et Elastic Stack (Elasticsearch, Logstash, Kibana) pour fournir une plateforme robuste de gestion des événements de sécurité.

#### **Avantages :**

- **Gratuit et Open Source** : Security Onion est disponible gratuitement, permettant à l'hôpital de maximiser son budget pour d'autres besoins critiques.
- **Intégration d'Outils Puissants** : En combinant des outils tels que Snort pour la détection d'intrusions et Elasticsearch pour l'indexation et la recherche, Security Onion offre une solution complète.
- **Interface Utilisateur Conviviale** : Son interface utilisateur intuitive facilite la gestion et l'analyse des événements de sécurité, même pour les utilisateurs moins expérimentés.
- **Support de la Communauté Active** : Bénéficie d'une communauté active qui partage des ressources, des conseils et des solutions aux problèmes, assurant ainsi un développement continu.

#### **Inconvénients :**

- **Configuration Nécessitant de l'Expertise** : La mise en place et la configuration de Security Onion peuvent nécessiter une certaine expertise, ce qui pourrait demander une courbe d'apprentissage pour le personnel.
- **Exigences en Ressources Matérielles** : Pour un fonctionnement optimal, Security Onion peut nécessiter des ressources matérielles adéquates, ce qui pourrait constituer un défi en fonction des capacités existantes.
- **Assistance Technique Limitée** : Bien que bénéficiant d'une communauté active, le support technique peut être limité par rapport aux solutions payantes.

## 2. OSSEC :

### **Description :**

OSSEC (Open Source Security Information and Event Management) est une solution de gestion de la sécurité open source conçue pour la détection d'intrusions, la prévention des menaces et la gestion des journaux. OSSEC offre une approche holistique de la sécurité en combinant des fonctionnalités d'IDS, de système de prévention d'intrusion (IPS), et de gestion des événements de sécurité (SIEM). Il est conçu pour fonctionner sur différentes plates-formes, y compris Linux, Windows, et Unix.

### **Avantages :**

- Open Source : OSSEC est une solution open source, ce qui signifie qu'elle est gratuite et que son code source est accessible. Cela offre une flexibilité et une transparence importantes.
- Détection Multiplateforme : OSSEC prend en charge plusieurs plates-formes, ce qui le rend adaptable aux environnements hétérogènes, tels que ceux des hôpitaux avec divers systèmes d'exploitation.
- Corrélation d'Événements : Il propose des fonctionnalités avancées de corrélation d'événements, permettant d'identifier des schémas complexes et de fournir une vision plus approfondie des menaces potentielles.
- Réponse Automatisée : OSSEC offre des fonctionnalités de réponse automatisée pour traiter rapidement les menaces détectées, renforçant ainsi la posture de sécurité globale.

### **Inconvénients :**

- Courbe d'Apprentissage : En raison de sa richesse fonctionnelle, OSSEC peut avoir une courbe d'apprentissage plus prononcée pour les utilisateurs débutants, nécessitant une certaine expertise pour une mise en œuvre optimale.
- Ressources Système : Pour fonctionner efficacement, OSSEC peut nécessiter des ressources système significatives, en particulier dans des environnements réseau à fort trafic.
- Personnalisation Complexe : La personnalisation approfondie peut être complexe, et cela peut nécessiter une compréhension approfondie des règles et des politiques de sécurité.

### 3. Snort :

. Description : Snort est un système de détection d'intrusion (IDS) open source largement utilisé. Il fonctionne en examinant le trafic réseau en temps réel, en analysant les paquets pour identifier les signatures d'attaques ou comportements suspects. Snort prend en charge différents modes, y compris le mode NIDS (Network-based IDS) et le mode NIPS (Network-based IPS).

. Avantages :

- Base de Signatures Étendue : Snort dispose d'une base de signatures étendue qui couvre un large éventail d'attaques connues.
- Flexibilité : Snort est hautement configurable, permettant aux administrateurs de définir des règles personnalisées en fonction des besoins spécifiques du réseau.
- Gratuit et Open Source : Snort est une solution gratuite et open source, ce qui le rend accessible même pour les organisations ayant des contraintes budgétaires.
- Communauté Active : Il bénéficie d'une communauté active qui contribue au développement continu de nouvelles signatures et fonctionnalités.

. Inconvénients :

- Courbe d'Apprentissage : En raison de sa flexibilité, la configuration avancée de Snort peut nécessiter une courbe d'apprentissage pour les administrateurs moins expérimentés.
- Complexité de Configuration : La mise en place de règles personnalisées peut être complexe, en particulier pour des infrastructures réseau complexes.
- Détection Basée sur les Signatures : Snort repose principalement sur la détection basée sur les signatures, ce qui signifie qu'il peut ne pas être aussi efficace contre des attaques inconnues ou des techniques avancées d'évasion.

#### 4. Sagan :

. Description : Sagan est un système IDS/IPS open source conçu pour la détection et la gestion d'incidents de sécurité. Il se distingue par son architecture modulaire qui intègre des fonctionnalités avancées de corrélation d'événements.

. Avantages :

- Corrélation d'Événements : Sagan excelle dans la corrélation d'événements, ce qui lui permet de détecter des attaques complexes en analysant des schémas d'activité.
- Extensibilité : L'architecture modulaire permet l'ajout facile de nouvelles règles et de nouvelles sources de données, offrant ainsi une extensibilité considérable.
- Gestion des Logiciels Malveillants : Intègre des mécanismes avancés pour détecter les logiciels malveillants et les comportements suspects.
- Communauté Active : Bénéficie d'une communauté active qui contribue à son développement continu et à la création de règles de détection.

. Inconvénients :

- Complexité initiale : La configuration initiale peut être complexe pour les utilisateurs novices, nécessitant une certaine expertise pour optimiser les performances.
- Interface Utilisateur : L'interface utilisateur peut être moins conviviale par rapport à d'autres solutions, ce qui peut nécessiter une courbe d'apprentissage pour les administrateurs.
- Ressources Matérielles : Peut nécessiter des ressources matérielles significatives, en particulier pour des environnements réseau étendus.
- Documentation Limitée : Certains utilisateurs ont noté que la documentation peut être limitée dans certaines zones, nécessitant parfois des recherches approfondies pour résoudre des problèmes spécifiques.

**Note :** Cette analyse vise à fournir un aperçu complet de 4 solutions, Security Onion, Snort, OSSEC et Sagan, en mettant en évidence ses atouts tout en reconnaissant les défis potentiels associés à son utilisation dans l'environnement hospitalier. Ces informations aideront à orienter la sélection de la solution IDS/IPS optimale pour l'hôpital.