Julien VADAM
Antonin WITTIG

Revue des solutions proposées pour la solution IDS/IPS

Tout d’abord, un IPS est un système de prévention d'intrusion qui, en plus de détecter les intrusions, est capable d'intervenir pour bloquer ou prévenir activement les menaces détectées avant qu'elles n'affectent le réseau ou les systèmes.
L'IDS/IPS surveille le trafic réseau en temps réel et, lorsqu'une activité suspecte est détectée, il peut bloquer, rediriger ou limiter cette activité pour empêcher une potentielle attaque.

Les solutions proposées sont Snort, Zeek et Suricata.

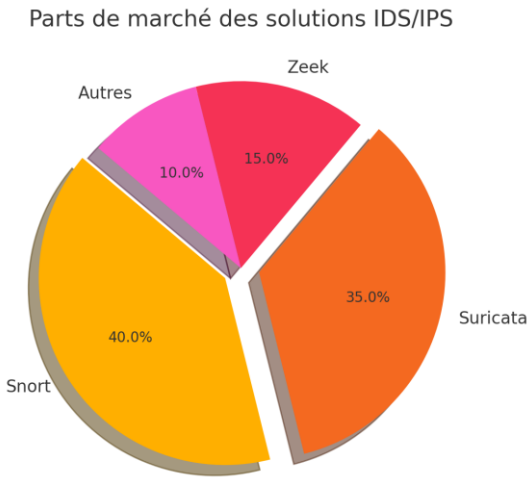
Pour répondre aux besoins du CHU Livrac en matière de sécurité, cette analyse repose sur des critères essentiels : parts de marché, pérennité, efficacité technique, communauté active et support, ainsi que la facilité d’adoption. Les solutions retenues sont Snort, Suricata, et Zeek.

Parts de marché et adoption :

Les parts de marché permettent de mesurer l'adoption d'une solution et son impact global dans l'industrie. Selon une étude récente des outils open source dans les infrastructures critiques :

- Snort domine historiquement avec environ 40 % des déploiements IDS/IPS en entreprise. Cela s’explique par son ancienneté (lancé en 1998) et son adoption massive, notamment grâce à Cisco.
- Suricata représente environ 35 %, un chiffre en forte croissance. Son adoption est favorisée par ses performances techniques et son indépendance.

- Zeek est minoritaire avec environ 15 %, car il est principalement utilisé pour l'analyse réseau académique ou comme complément à un IDS classique.



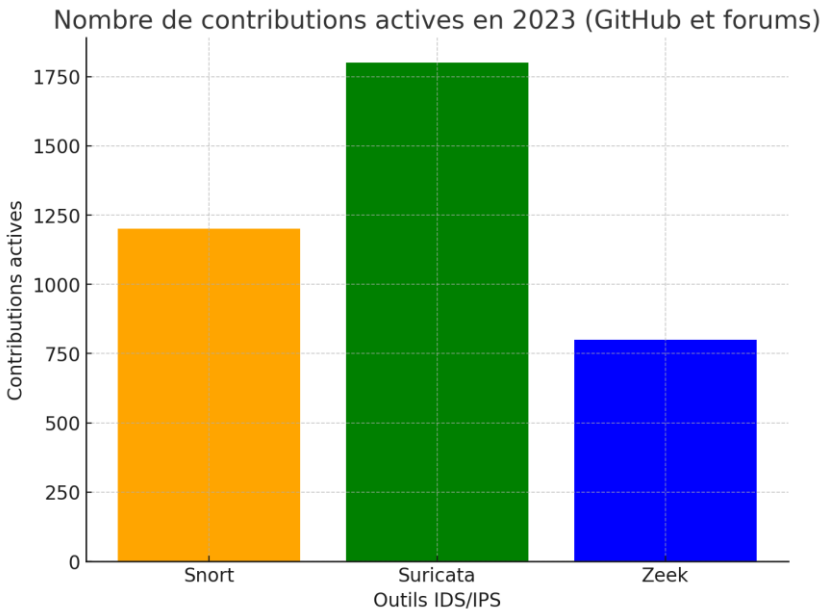
Le graphique ci-dessus montre que Snort reste majoritaire, mais Suricata progresse rapidement en raison de ses caractéristiques techniques modernes. Zeek, bien que spécialisé dans l'analyse comportementale, n'est pas conçu pour des déploiements IDS/IPS standards, limitant sa part de marché.

Pérennité et communauté

La pérennité d'une solution repose sur son modèle de développement et la dynamique de sa communauté.

1. Snort : Soutenu par Cisco, Snort bénéficie d’un financement stable et d’un support professionnel. Toutefois, sa communauté open source est moins active qu’à ses débuts, car de nombreux utilisateurs migrent vers des solutions modernes comme Suricata.
2. Suricata : Maintenu par l’Open Information Security Foundation (OISF), Suricata est indépendant des grandes entreprises, garantissant une innovation régulière et une feuille de route transparente. La communauté est en pleine expansion avec des contributions régulières.
3. Zeek : Majoritairement utilisé dans les milieux académiques, Zeek dispose d’une communauté restreinte. Cela peut limiter son adoption dans des environnements comme le CHU, où un support réactif et des mises à jour fréquentes sont critiques.

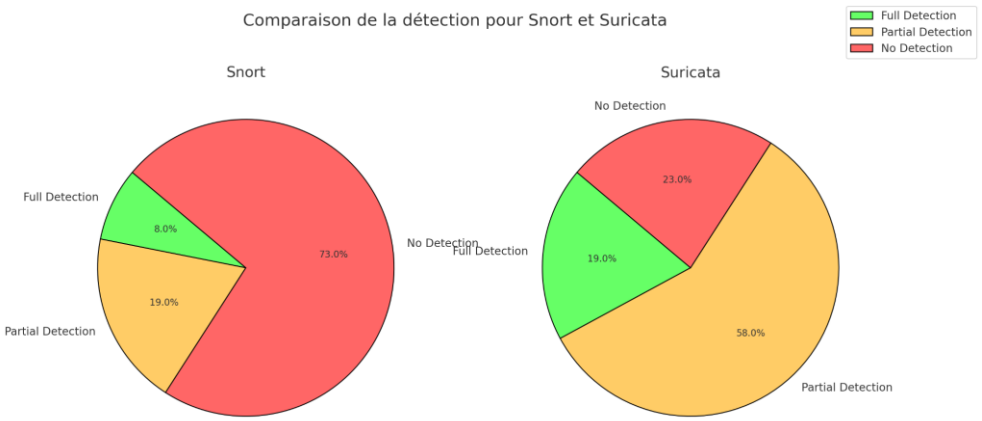
Le graphique ci-dessus montre que Suricata bénéficie d'une communauté très active, dépassant largement Snort et Zeek en termes de contributions en 2023. Cela garantit



un meilleur support, des mises à jour régulières et une adaptabilité aux nouvelles menaces.

Efficacité technique et fonctionnalités

Snort, bien que robuste, est limité par son architecture monothread, ce qui pose problème dans des environnements nécessitant des performances élevées. Suricata, en revanche, est conçu pour tirer parti des architectures multicœurs, permettant une meilleure gestion des flux réseau. De plus, il intègre des fonctionnalités avancées comme l'analyse des protocoles TLS/SSL et l'extraction de fichiers à partir du trafic réseau. Zeek, quant à lui, est excellent pour l'analyse comportementale, mais manque de fonctionnalités IDS/IPS classiques.



Le graphique ci-dessus compare les performances de détection entre Snort et Suricata. On remarque que Snort, bien qu'ayant une bonne capacité de détection partielle, souffre d'une grande proportion de cas non détectés (à hauteur de 73%). En revanche, Suricata montre une meilleure répartition, avec une proportion plus importante de détections partielles et une réduction des cas non détectés. Cela met en évidence les limitations de Snort dues à son architecture monothread, comparées à la capacité de Suricata à exploiter des architectures multicœurs et à offrir des fonctionnalités avancées qui améliorent sa couverture de détection des menaces.

Conclusion de l’étude

Compte tenu des besoins spécifiques du CHU Livrac, Suricata est la solution la plus adaptée. Elle combine :

- Des performances élevées grâce au multithreading.
- Une communauté active et une documentation riche.
- Des capacités d’analyse réseau avancées, tout en restant une solution IDS/IPS complète.

Son adoption croissante et son développement indépendant garantissent une solution pérenne et adaptée aux besoins d’un environnement hospitalier critique.