# Rapport de détection

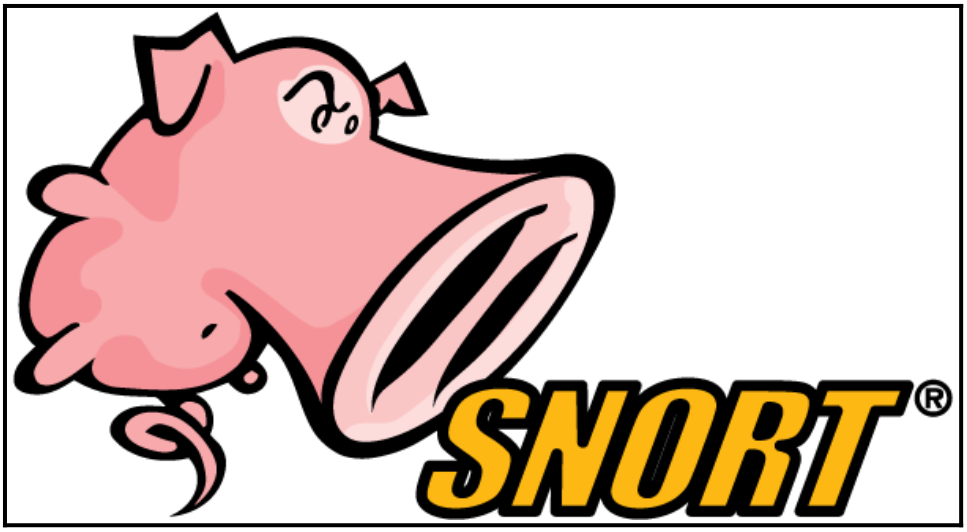

***Sommaire :***



---

## *1./ Outils de détection et prévention d'intrusions*

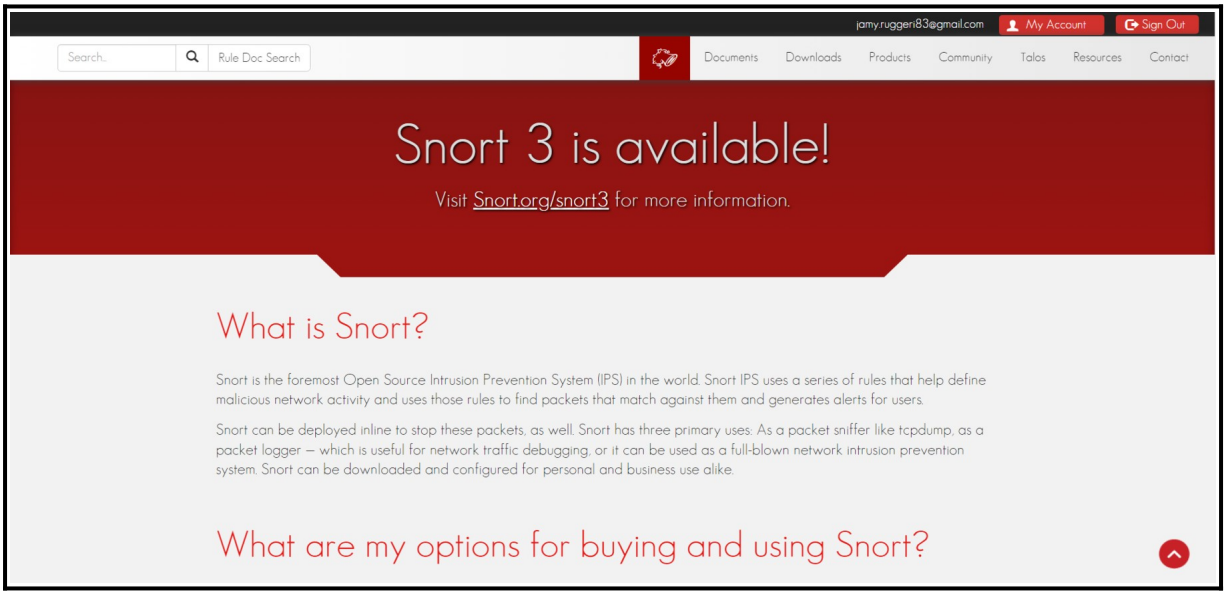
### 1#Snort



Snort est un système de détection d'intrusion et de prévention d'intrusion gratuit et open-source.
Snort a la capacité d'effectuer une analyse du trafic en temps réel et un enregistrement des paquets sur les réseaux IP. Snort effectue l'analyse des protocoles, la recherche et la mise en correspondance des contenus.

Le programme peut également être utilisé pour détecter des sondes ou des attaques, y compris, mais sans s'y limiter, les prise d'empreinte de la pile TCP/IP, les attaques d'URL sémantiques, les dépassements de tampon, les attaques sur SMB et les balayages de ports.

Snort peut également être utilisé avec d'autres projets open sources tels que SnortSnarf, ACID, sguil et BASE (qui utilise ACID) afin de fournir une représentation visuelle des données concernant les éventuelles intrusions.



## 2#Zeek

Ce logiciel est programmé de façon totalement différente de Snort, il s'appuie sur les mêmes bases théoriques (filtrage par motif, formatage aux normes RFC, etc.), mais il intègre un atout majeur : l'analyse de flux réseau. Cette analyse permet de concevoir une cartographie du réseau et d'en générer un modèle. Ce modèle est comparé en temps réel au flux de données et toute déviance lève une alerte.

Le principal problème du logiciel par rapport à Snort est son caractère universitaire. En effet, il n'existe aucun *plug-in* ni interface graphique pour paramétrer l'outil. Le système étant produit par des chercheurs, les mises à jour et les communautés d'utilisateurs sont elles aussi parfois insuffisantes.

Le gros avantage du logiciel est son analyse réseau en temps réel qui permet de garantir encore mieux la pérennité du réseau.

# 3#Suricata

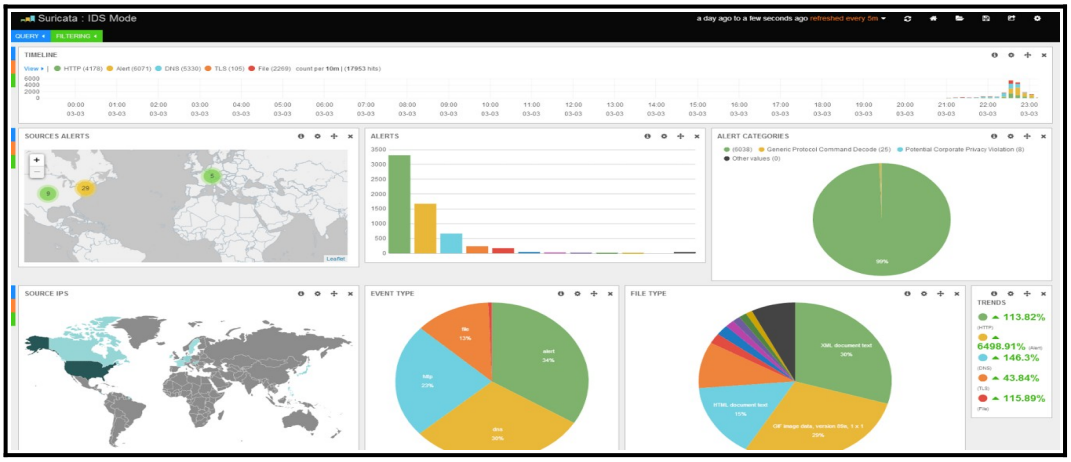
**Suricata** est un logiciel open source de détection d'intrusion (IDS), de prévention d'intrusion (IPS), et de supervision de sécurité réseau (NSM). Il est développé par la fondation OISF (Open Information Security Foundation.

Suricata permet l'inspection des Paquets en Profondeur (DPI). De nombreux cas d'utilisations déontologiques peuvent être mis en place permettant notamment la remontée d'informations qualitatives et quantitatives.

Scirius est une interface web sous licence GPLv3 écrite avec Django destinée à l'édition des règles Suricata. La version mono-serveur est open source et libre tandis que la version multi-serveur Scirius Enterprise est commercialisée, elles sont toutes deux éditées par la société Stamus Networ.

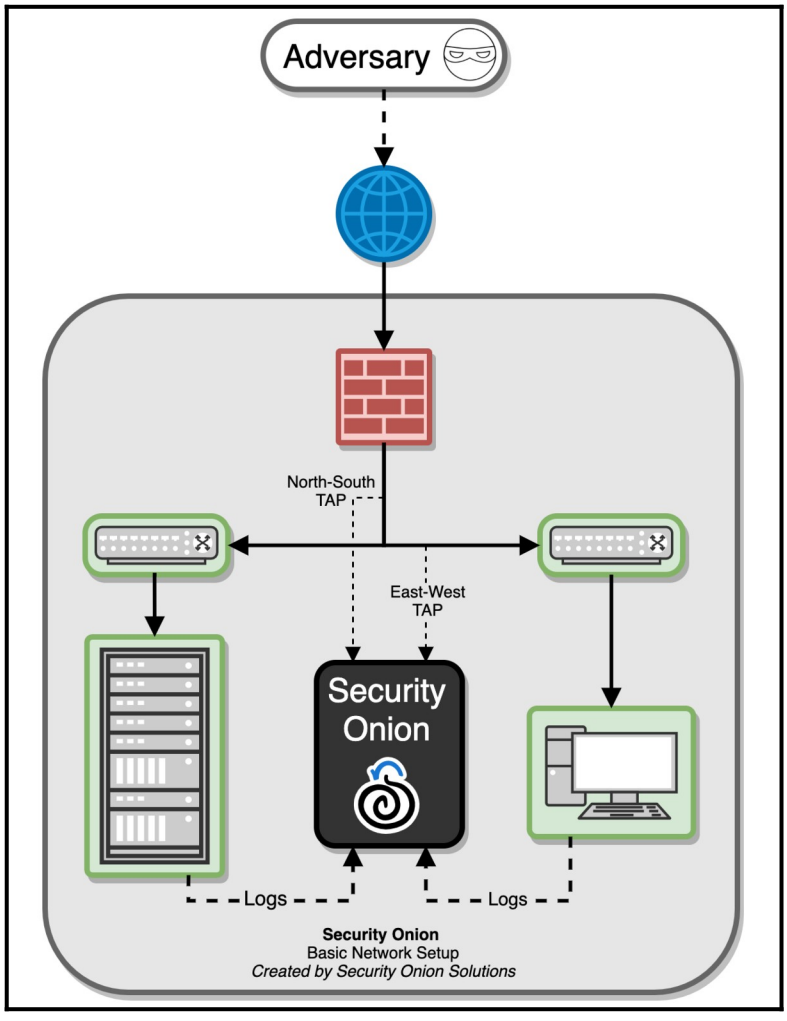
La distribution GNU/Linux

SELKS 3.0 (Suricata Elasticsearch Logstash Kibana Scirius) basée sur debian permet de tester Suricata. Il existe également une image Docker.



# 4#Security Onion

Security Onion est une plate-forme gratuite et ouverte pour la surveillance de la sécurité du réseau (NSM) et la surveillance de la sécurité de l'entreprise (ESM). NSM consiste, en termes simples, à surveiller votre réseau pour les événements liés à la sécurité. Il peut être proactif, lorsqu'il est utilisé pour identifier les vulnérabilités ou l'expiration des certificats SSL, ou il peut être réactif, comme dans la réponse aux incidents et l'investigation du réseau. Que vous suiviez un adversaire ou que vous essayiez de tenir à distance les logiciels malveillants, NSM fournit un contexte, des renseignements et une connaissance de la situation de votre réseau. ESM fait passer NSM au niveau supérieur et inclut la visibilité des terminaux et d'autres télémétries de votre entreprise.



# 2./ Comparatif des outils

| | Snort | Zeek | Suricata | Security Onion |
|---|---|---|---|---|
| Prix | Gratuit(abonnement payant) | Gratuit open source | Gratuit open source | |
| Avantages | - Gestion des risques<br>- Taux d'adaptation large<br>- Solutions rapide face aux nouvelles menaces | - Gestion commerciale<br>- Logs / Surveillance des scripts | - Script Lua<br>- Règles identifiant des conditions<br>- Adaptation aux menaces complexes | - Tableau de bord Kibana<br>- Exécution via du code source de logiciel IPS/IDS tiers |
| Inconvénients | - Conçu pour des infrastructures plus anciennes<br>- Limite face aux nouvelles menaces | - Absence d'interface web utilisateur pour gérer l'outil | - Installation complexe<br>- Ressources et supports manquant limitant l'élargissement des règles | - Complexe à utliser<br>- Manque de documentation<br>- Fonctionnalités des programmes essentiellement assemblées et pas intégrées<br>- Ignorance possible de certains outils |
| Fonctionnalités | - politiques de veille des menaces<br>- Analyse de paquets<br>- Consignation des paquets | - Collecte journaux<br>- Paquet de données<br>- Politique de scripts modifiable | - Combinaison de la détection d'intrusion en temps réel<br>- Importation paquets de règles avec Snort<br>- Stocker et examiner des certificats TLS | - Interrogation du trafic réseau<br>- Recherche autonome d'activités malveillantes<br>- Détection de modifications non autorisés. |

# 3./ Tests de vulnérabilités Snort

**Nmap** = OK

**ICMP** = OK

**Port TCP** = OK

**SSH** = OK

**FTP** = OK

**Trafic Torrent** =OK

**Adresse IP douteuse** = OK

**DoS** = OK

**(Outils utilisés dans la procédure de test : )**
**- Kali Linux**
**- MetaSploit**