Lundi de la cybersécurité du 17/03/2025

Détection de menaces sur le réseau avec SURICATA

Et les règles

PAWPATRULES.FR

Supervision réseau : pourquoi ?

- **Il n'est pas possible d'installer un agent sur toutes les machines** (systèmes non supportés, OT, contraintes réglementaires, contraintes techniques, contraintes éditeur…)

- L'antivirus / EDR peut être **contourné** ou **désactivé** par les attaquants (Black Out / EDR Sandblast / Reflective Loading)

- L'antivirus / EDR peut être **mal configuré** ou **manquer de visibilité** sur certaines actions… (actions non tracées, outils légitimes utilisés...)

La supervision réseau à la rescousse

La supervision réseau (IDS, NSM, NDR) permet d'élargir le périmètre de détection

Elle permet de détecter de nombreux incidents de sécurité, mauvaises pratiques, shadow it, vulnérabilités, actions malveillantes, connexions à des C2 connus…

Sans agent

Difficile à contourner

Vue complémentaire

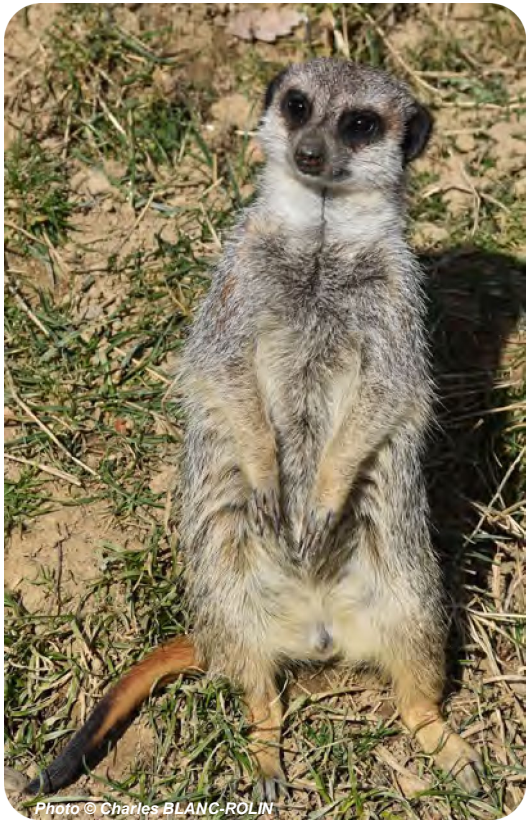
SURICATA

- Né en **2009** (première version beta)

- Un logiciel (dépourvu d'interface graphique) libre et communautaire porté par l'**OISF** (Open Information Security Foundation), un consortium d'acteurs de la cybersécurité, dont l'ANSSI fait partie

- Une solution de **supervision réseau orientée sécurité** (NSM)

- L'outil sur lequel s'appuie les **sondes** de détection **souveraines qualifiées** par l'**ANSSI**



SURICATA

- Il **historise le trafic**, **analyse les flux** et **émet des alertes** à partir de règles définies

- Il reconnaît automatiquement de nombreux protocoles réseaux

- Il calcule des empreintes clients et serveurs TLS (JA3), mais aussi SSH (hassh)

- Il écrit ses **traces** dans le format standard **JSON**

- Permet d'exporter au format PCAP les paquets enregistrés (ensemble des flux ou alertes uniquement)

- *Calcule la volumétrie de données envoyées / reçues (Suricata V8 en dév)*

PAWPATRULES.FR

- Une collection gratuite de plus 21 400 règles de détection

- Projet initié en 2020 et rendu publique en 2022

- Intégration au projet Suricata en 2024

- Implémentable dans toute solution NDR basée sur Suricata

- Utilisation par des universités en Europe et en Asie, des CH + CHU et des Ministères français, une société ferroviaire nationale en Europe de l'EST, un CERT privé, un service de renseignement, des professionnels de la cybersécurité…

Pour plus d’infos :

pawpatrules.fr