STAMUS NETWORKS

Clear NDR Community

Valentin Vivier et Eric Leblond

Qui sommes-nous ?

Éric Leblond

- Co-fondateur et CTO de Stamus Networks
- Membre du conseil d'administration de l'OISF
- Contributeur Suricata depuis 2010

Valentin Vivier

- Directeur de l'ingénierie à Stamus Networks
- Devops all the things

Stamus Networks

Éditeur européen d'une solution de détection réseaux des menaces nommée **Clear NDR**.

Fondée en 2014.

Network Traffic
Cloud & On-premise

IDS Alerts

Protocol
Transactions

Network
Flows

PCAP
Recordings

Extracted
Files

Source: Stamus Networks

Clear NDR Community

Fonctions

Détection des menaces sur le réseaux

Visibilité réseau orienté sécurité

Analyse live et replay

Sonde tout en un :

- Analyse réseau
- Base de données
- Interfaces Utilisateurs
- Ingestion des threat intels

Composants

- **Suricata** : analyse réseau
- **Interfaces dédiées** :
  - Threat hunting
  - Management des signatures
- **Opensearch** & Dashboard
- **FPC** via Arkime
- Agent IA (optionnel)

Installation

- Système existant
- Image ISO dédiée

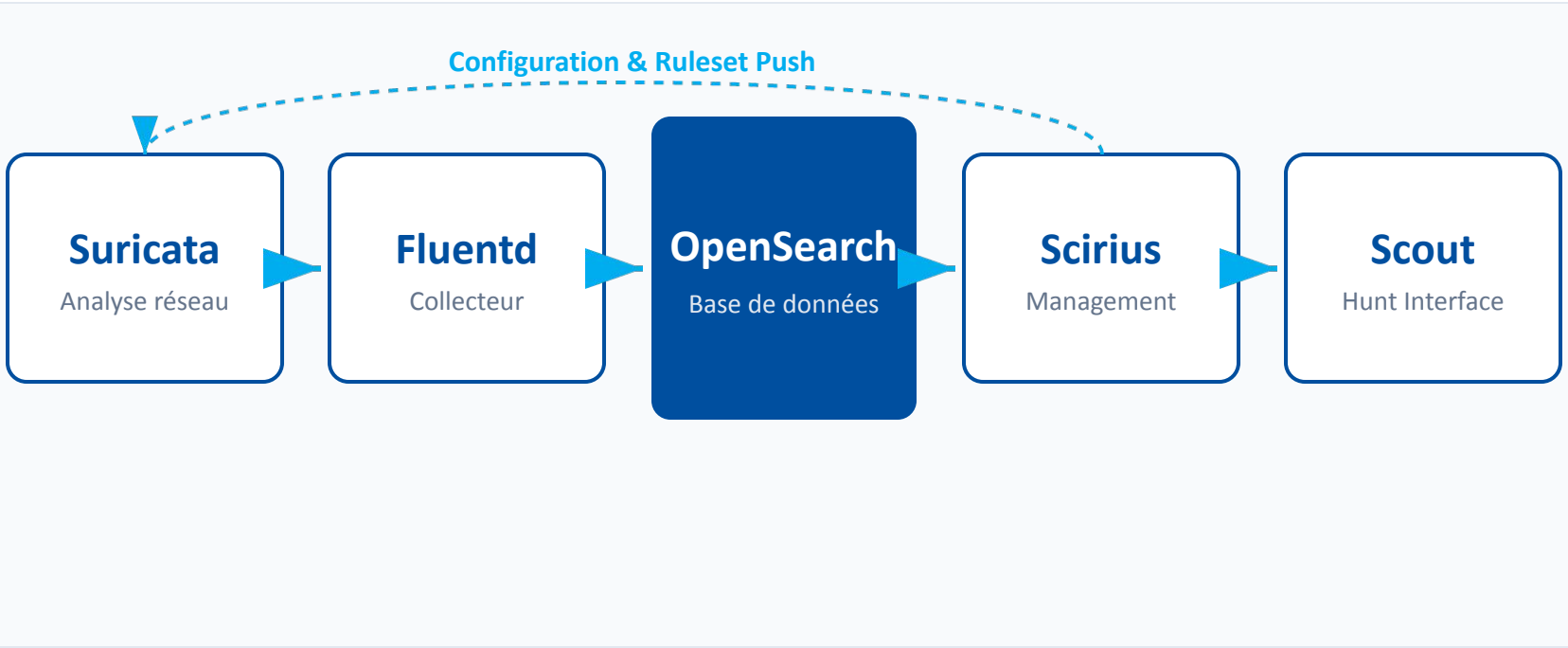
Disponibilité

- Licence **GPLv3**
- Dépôts sur **GitHub**

Documentation

https://docs.clearndr.io/fr/

Clear NDR Architecture



Commandes stamusctl

Initialisation

```
stamusctl compose init
```

Instancie la stack logicielle et prépare l'environnement.

Lancement

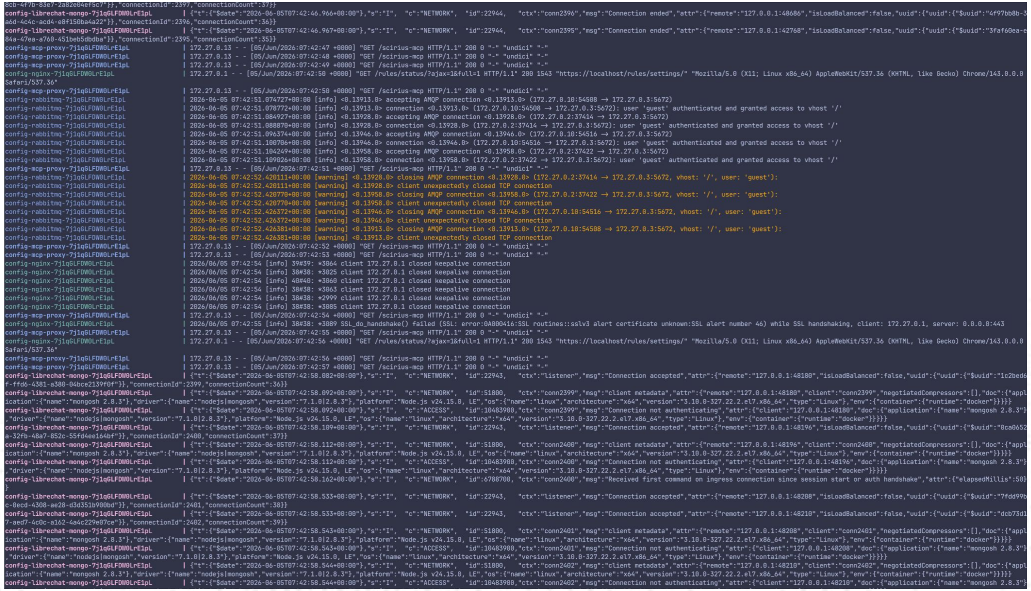
```
stamusctl compose up -d
```

Lance la stack Clear NDR dans des conteneurs Docker (mode détaché).

Demonstration 1 : instanciation

stamusctl compose init

stamusctl compose up -d



Stamusctl tips & tricks with benefits

stamusctl config set –apply nginx.ssl.folder=/path/to/ssl

stamusctl config set –apply opensearch.memory=2G

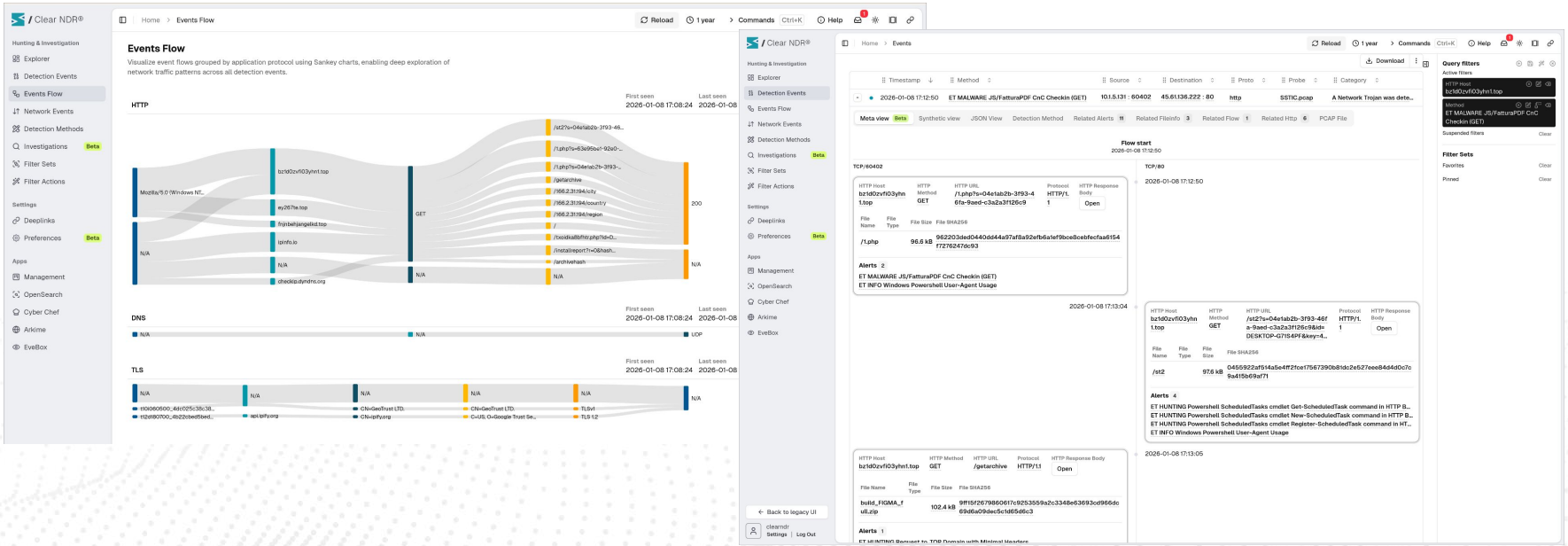
stamusctl compose update && stamusctl compose up -d

Demonstration 2: rejeu de fichier pcap

- stamusctl compose readpcap PATH_TO_PCAP
  - Utilise un container Suricata pour relire le pcap
- Pcap utilisé de Malware Traffic Analysis:
  - https://www.malware-traffic-analysis.net/2026/01/08/index.html

Demo : analyse dans l’interface

- Analyse en 2 minutes dans l’interface utilisateur



Model Context Protocol

Présentation du Protocole

Connexion IA-Systèmes
Un standard pour relier l'IA aux outils externes.

- Découverte automatique
- REST API + Documentation

Requiert un LLM avec **Tool Calling**

Plus d'info: https://modelcontextprotocol.io/

Architecture

Agent (Client MCP)
Interface principale orchestrant les appels.

LLM
Décide quel outil utiliser.

Serveurs MCP
Sources de données et outils externes.

MCP et confidentialité des données

Chemin des données

- Agent envoie le prompt au LLM
- LLM envoie à l'agent une demande de requête sur tool MCP
- Agent effectue requête et construit le contexte incluant les données
- Le LLM reçoit le contexte et génère la réponse

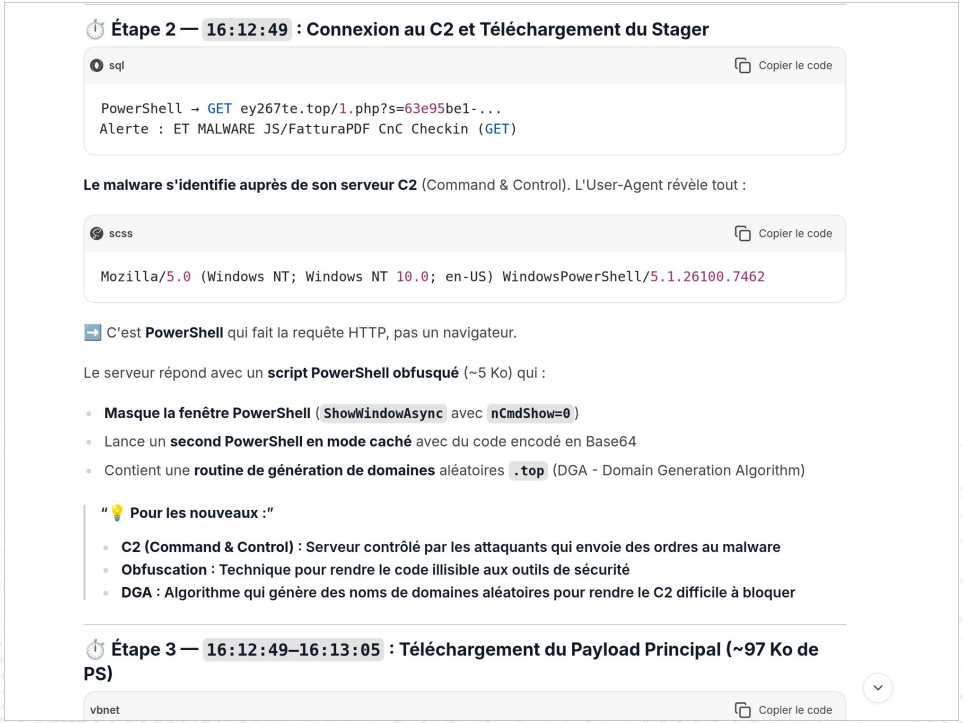
Conséquences

⚠ Les données du serveur MCP sont connues du LLM

🔓 Le LLM déclenche la requête MCP

Démonstration 3: MCP

- Instance Clear NDR avec agent
  - Utilisation de Sonnet 4.6
  - Connectivité LLM local possible
- Interrogation des données du PCAP



⏱️ **Étape 2 — `16:12:49` : Connexion au C2 et Téléchargement du Stager**

sql — Copier le code

```
PowerShell → GET ey267te.top/1.php?s=63e95be1-...
Alerte : ET MALWARE JS/FatturaPDF CnC Checkin (GET)
```

Le malware s'identifie auprès de son serveur C2 (Command & Control). L'User-Agent révèle tout :

scss — Copier le code

```
Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.26100.7462
```

➡️ C'est **PowerShell** qui fait la requête HTTP, pas un navigateur.

Le serveur répond avec un **script PowerShell obfusqué** (~5 Ko) qui :

- **Masque la fenêtre PowerShell** (`ShowWindowAsync` avec `nCmdShow=0`)
- Lance un **second PowerShell en mode caché** avec du code encodé en Base64
- Contient une **routine de génération de domaines** aléatoires `.top` (DGA - Domain Generation Algorithm)

> **" 💡 Pour les nouveaux :"**
>
> - **C2 (Command & Control) :** Serveur contrôlé par les attaquants qui envoie des ordres au malware
> - **Obfuscation :** Technique pour rendre le code illisible aux outils de sécurité
> - **DGA :** Algorithme qui génère des noms de domaines aléatoires pour rendre le C2 difficile à bloquer

⏱️ **Étape 3 — `16:12:49–16:13:05` : Téléchargement du Payload Principal (~97 Ko de PS)**

vbnet — Copier le code

Clear NDR Community

Simple à déployer

Installation rapide et configuration intuitive pour une mise en service immédiate.

Performance suffisante

Optimisé pour les réseaux de petite et moyenne taille.

Exploration des données

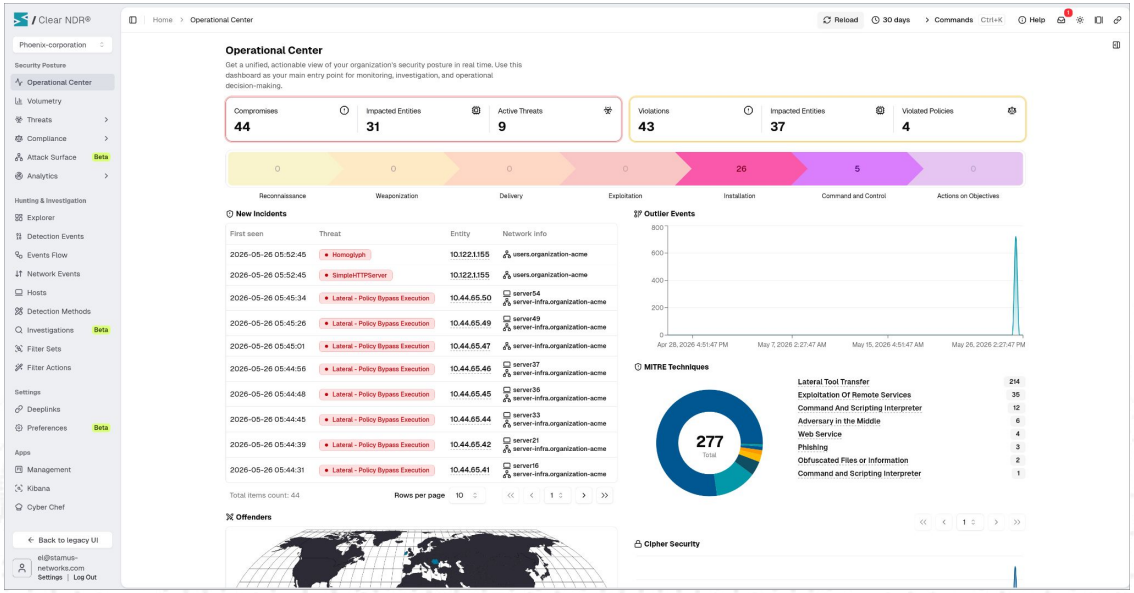
- Détection avancée des menaces
- Visibilité réseau complète

Prêt pour l'IA

Conçu pour s'intégrer avec des agents IA.

Comparaison avec Clear NDR Enterprise

- Architecture multi sondes
- Limitation du bruit grâce au concept d'incident
  - État sur un asset
  - Non événementiel
- Détections avancées
- Connectivité vers les SIEM
- Sondes jusque 100Gbps
- Support des environnements déconnectés



Questions ?

- Stamus Networks : https://www.stamus-networks.com/
- Documentation de Clear NDR Community : https://docs.clearndr.io/
- Malware traffic analysis : https://www.malware-traffic-analysis.net/
- Suricata : https://suricata.io