

SLIPS

UN SYSTÈME DE DÉTECTION D'INTRUSION RÉSEAU, LIBRE ET
BASÉ SUR LE MACHINE LEARNING

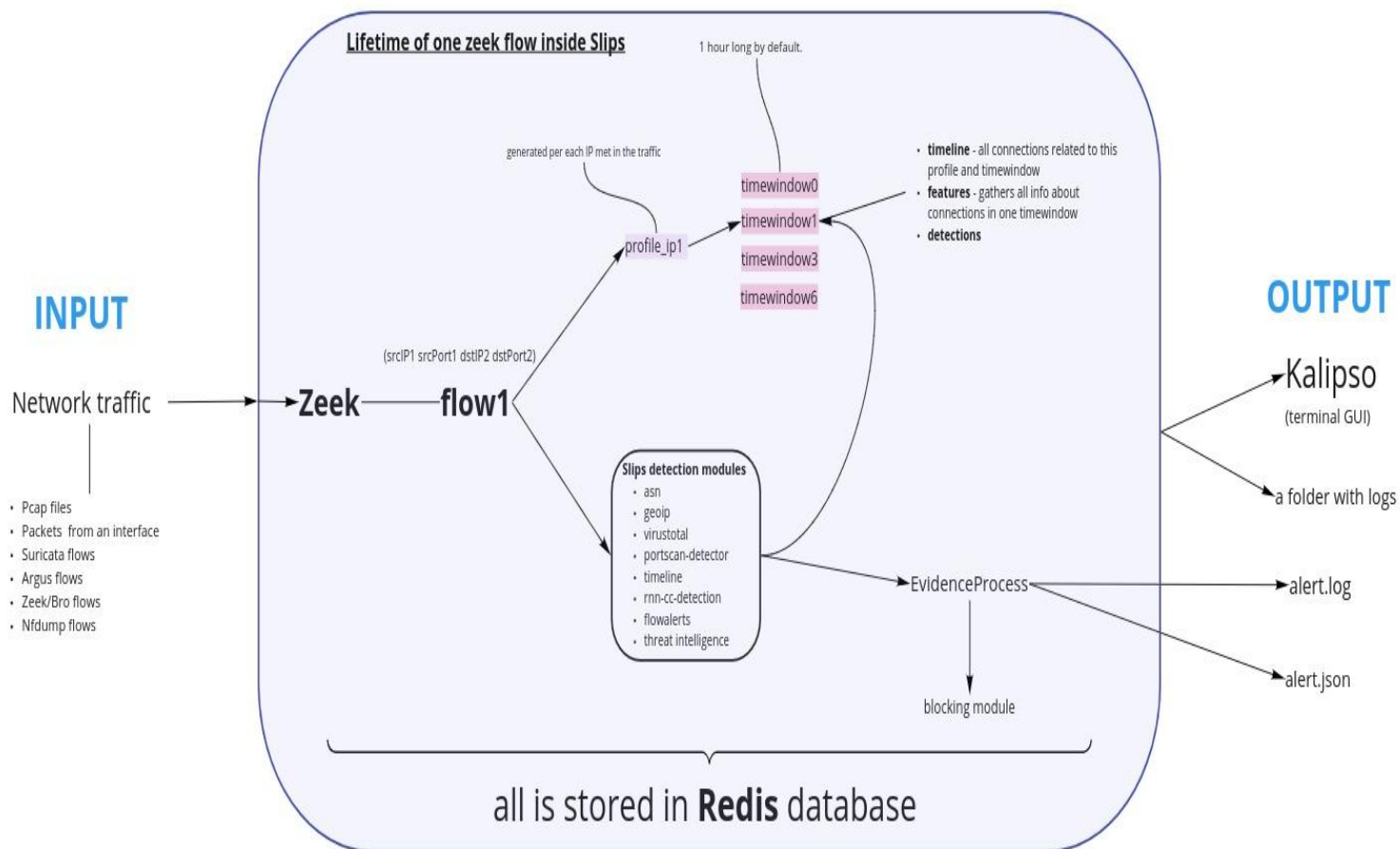
Marina Sèmèdéton GBEMENOU

QU'EST-CE QUE SLIPS(STRATOSPHERE LINUX IPS)?

- **Système de détection d'intrusion**
- **Open source**
- **Apprentissage automatique(Machine Learning)**
- **Développé par le Stratosphere Research Lab**

SLIPS ARCHITECTURE

SLIPS



- **Collector** : capture du trafic réseau
- **Flow Generator** : transformation des paquets en flux.
- **Modules ML** : détection d'anomalies
- **Interface Visualisation** : Web ou Kalipso

Fonctionnement

Profils

- Divise le flux en profils
- Chaque profils est divisé en fenêtre temporelle

Modes de fonctionnement

- Entraînement : entraînement du modèle sur un trafic légitime ou illégitime
- Test : analyse en temps réel / PCAP et détection d'anomalies

Démo

Voir SLIPS en action

**Comment SLIPS détecte les
comportements suspect qui
nécessitent une analyse
approfondie et mets en évidence
les résultats?**

Analyse en temps réel sur l'interface réseau ens33

```
marina@marina-virtual-machine: ~/Stra... x marina@marina-virtual-machine: ~/Stra... x
(venv) marina@marina-virtual-machine:~$ cd StratosphereLinuxIPS/
(venv) marina@marina-virtual-machine:~/StratosphereLinuxIPS$ python slips.py -i ens33
Slips Version: 1.1.12 (5f0e1435)
https://stratosphereips.org
-----
[Main] Storing Slips logs in output/ens33_2025-08-26_14:24:28/
[Main] Detected host IP: 192.168.91.143
[Main] Using redis server on port: 6379
Started Main process [PID 2911]
Starting modules
  Starting the module ARP (Detect ARP attacks) [PID 3100]
  Starting the module Flow Alerts (Alerts about flows: long connection, successful ssh, password guessing, self-signed certificate, data exfiltration, etc.) [PID 3171]
  Starting the module Flow ML Detection (Train or test a Machine Learning model to detect malicious flows) [PID 3192]
  Starting the module HTTP Analyzer (Analyze HTTP flows) [PID 3212]
]
  Starting the module IP Info (Get different info about an IP/MAC address) [PID 3292]
  Starting the module Network Discovery (Detect Horizontal, Vertical, ICMP and DHCP Scans.) [PID 3295]
  Starting the module Risk IQ (Module to get passive DNS info about
```

Slips

Not Secure http://192.168.91.143:55000

Selected: 192.168.91.1 TW 1:2025/08/26 14:26:14

IP	Country	Reverse DNS	ASN	Threat Intel	URL score	Download score	Reference score	Confidence
192.168.91.1	-	-	-	-	-	-	-	-

Profiles

192.168.91.1

TW

TW 1:2025/08/26 14:26:14

Timeline Flows Outgoing Incoming Alerts Evidence

Search...

Show 10 entries

Evidence	Confidence	Threat Level	Category	Tag	Description
1756218393.218634	1	INFO			Connecting to private IP: 192.168.91.254 on destination port: 67
1756218393.26449	0.8	HIGH			Connection on port 0 from 192.168.91.1:0 to 224.0.0.22:0.

Previous 1 Next

SLIPS en entreprise

- **Détection de scans réseau internes.**
- **Analyse d'exfiltration de données.**
- **Détection d'activités internes malveillantes.**
- **Détection de malwares**

Avantages pour l'entreprise

- **Surveillance en temps réel.**
- **Détection proactive basée ML.**
- **Faible taux de faux positifs.**
- **Adapté aux SOC et analystes sécurité.**
- **Conforme aux bonnes pratiques de cybersécurité.**

Comment l'installer?

Docker: `docker run -it --rm --net=host stratosphereips/slips:latest
./slips.py -f capture.pcap`

Native: `git clone https://github.com/stratosphereips/StratosphereLinuxIPS.git
cd StratosphereLinuxIPS/
./install.sh
python slips.py -f capture.pcap
./kalipso.sh or ./webinterface.sh`

Exigences:

- Python 3.10.12
- 5 Go d'espace disque (pour l'image Docker)
- au moins 4 Go de RAM

Merci !

Marina Sèmédéton GBEMENOU

marinagbemenou86@gmail.com

229 0166434738

<https://github.com/stratosphereips/StratosphereLinuxIPS>

<https://stratospherelinuxips.readthedocs.io/en/develop/index.html>