SLIPS

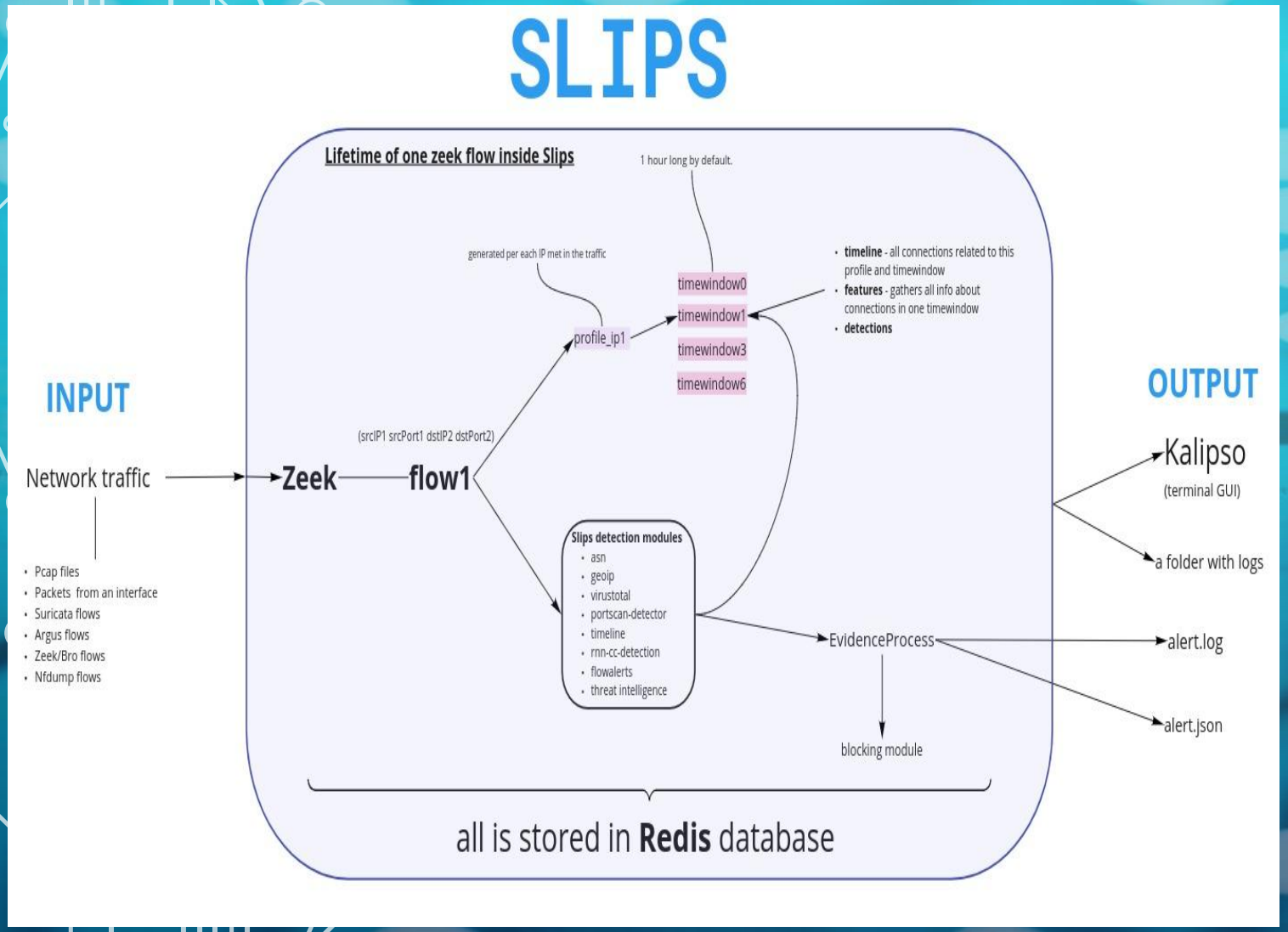
UN SYSTÈME DE DÉTECTION D'INTRUSION RÉSEAU, LIBRE ET BASÉ SUR LE MACHINE LEARNING

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



- **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

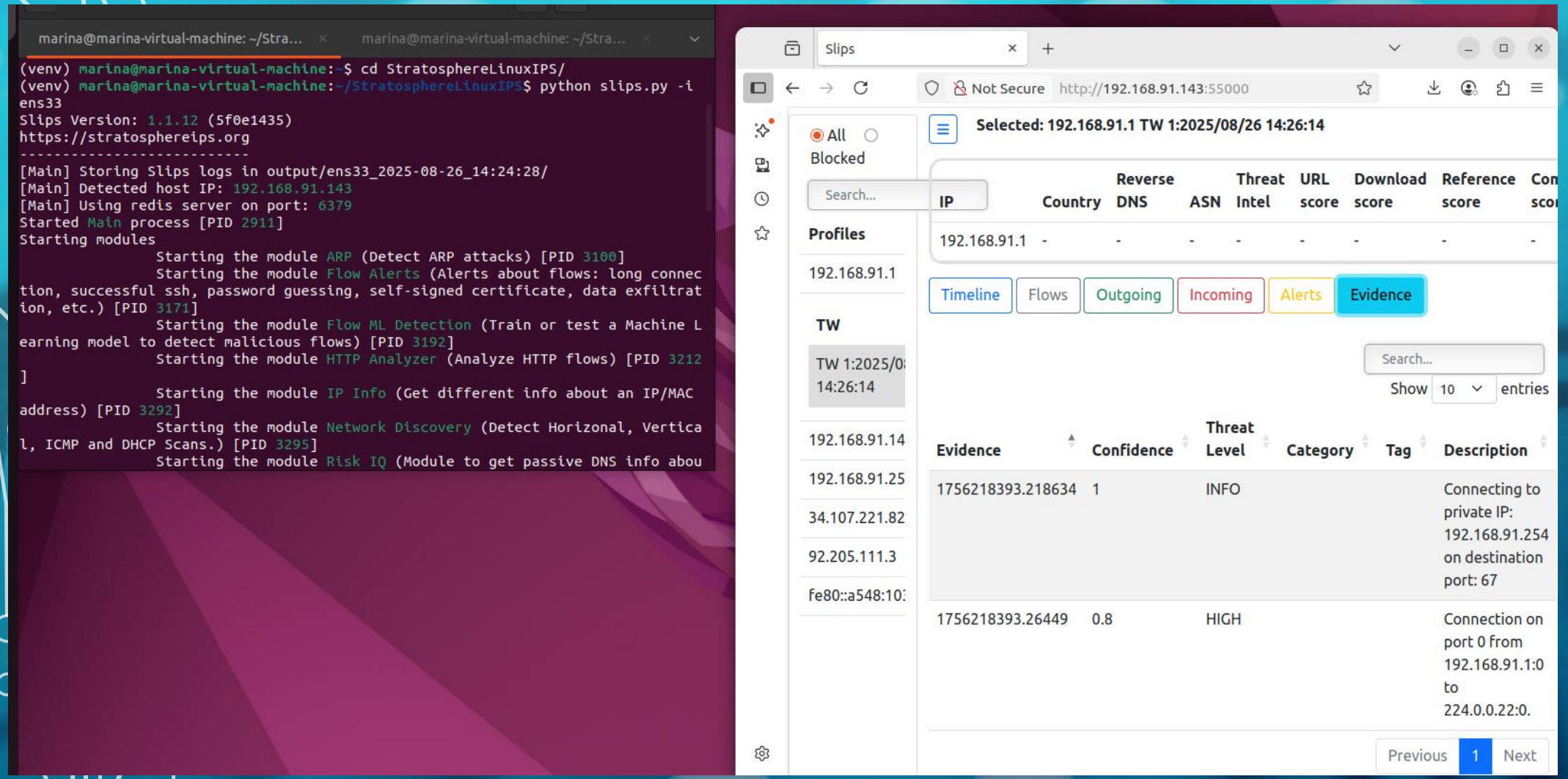
- Entraînement : entrainement du modèle sur un trafic légitime ou illégitime
- Test : analyse en temps réel / PCAP et détection d'anomalies

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



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 Sèmèdéton GBEMENOU
marinagbemenou86@gmail.com
229 0166434738

https://github.com/stratosphereips/StratosphereLinuxIPS
https://stratospherelinuxips.readthedocs.io/en/develop/index.html