Slips

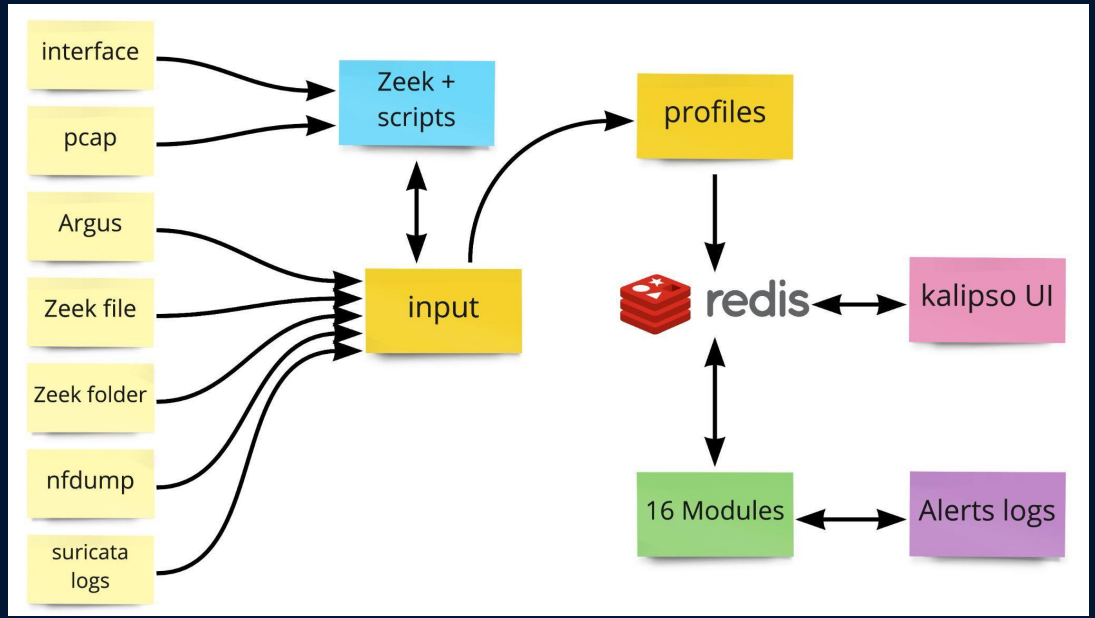
A Machine-Learning Based, Free-Software, Network Intrusion Prevention System

Alya Gomaa, Sebastian Garcia

What is Slips

- Intrusion Prevention System
  - Uses iptables in Linux to block attackers automatically
- Designed for endpoint devices
- Behavioral detection
  - Detects attacks based on their behavior
- Machine Learning
  - Together with an ensembling algorithm
  - Models are open source

Slips Architecture



Profiles

- Create profiles for devices
- Time windows analysis
- All traffic in and out is analyzed

Top Features

- Behavioral time-based rules for detection of infections
- Machine Learning detections
- Ensembling evidences in Alerts
- P2P
- Modularity for new functionality
- Whitelists for organisations

Slips local P2P network

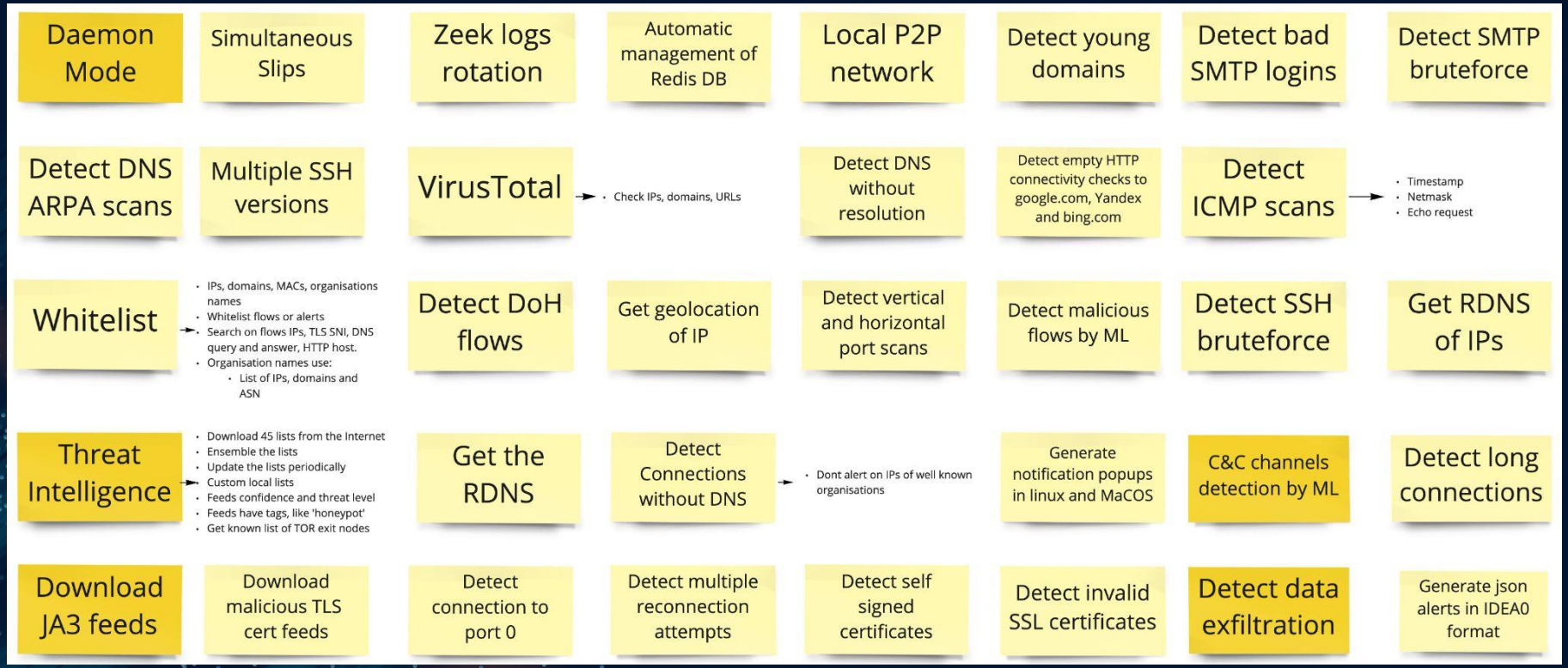
- A module that creates and maintains a local P2P network.
- Slips Peers find each other automatically using multicast.
- Slips peers can:
  - Ask other peer what they think about an IoC
  - Receive requests for opinion about an IoC
  - Send alerts for IoC that should were detected to the network
- Trust Model to be resilient against adversarial peers

DEMO

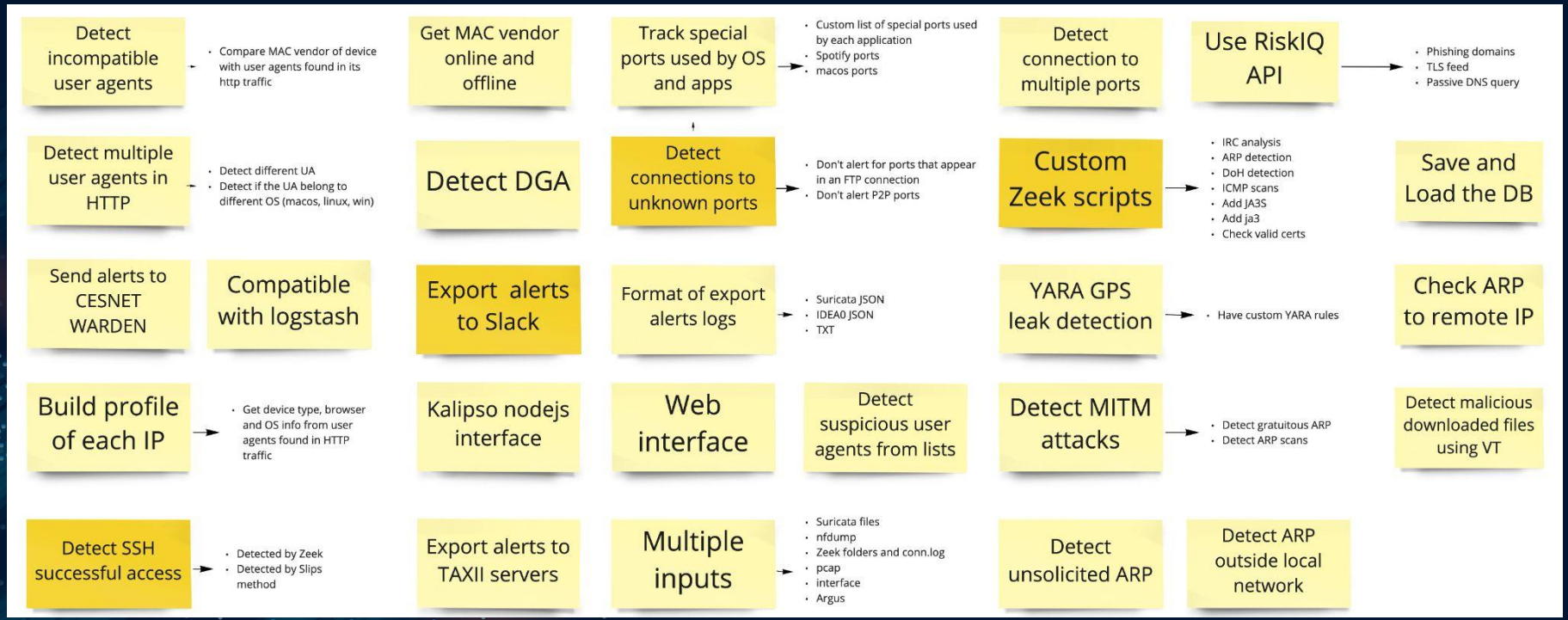
See Slips in Action!

How Slips detects problems in the network

All Slips features 1/2



All Slips features 2/2



THANKS!

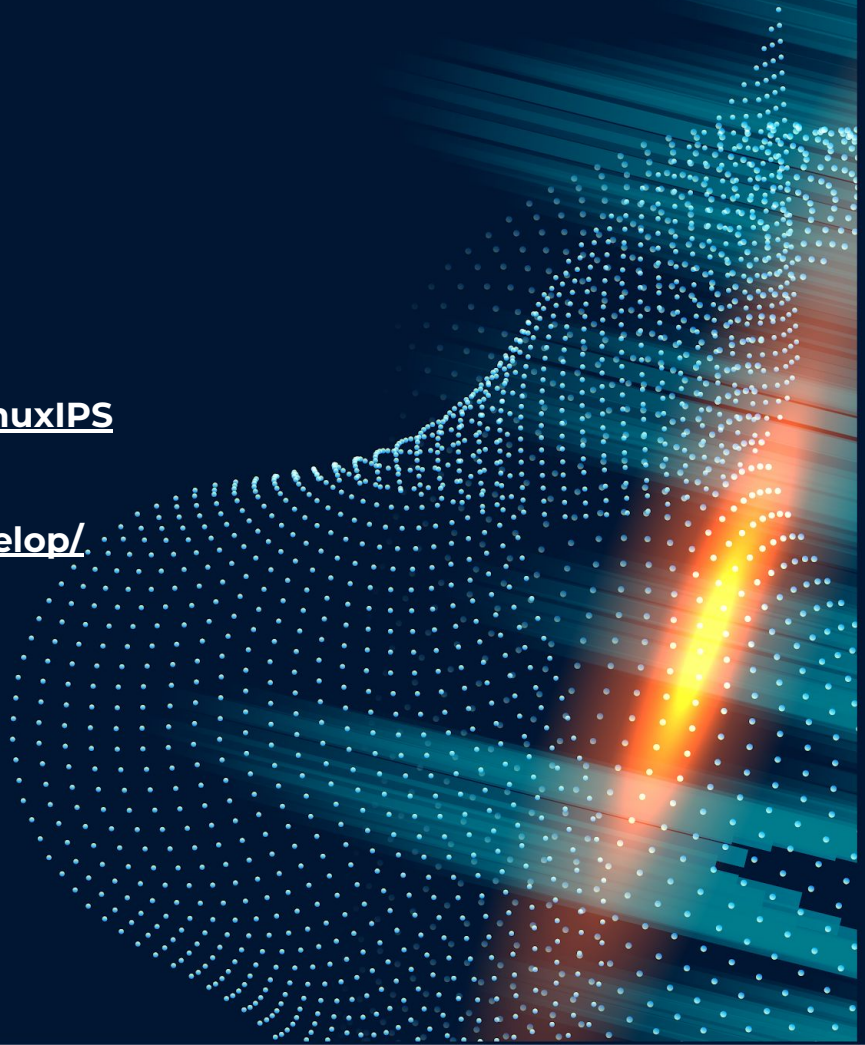
Alya Gomaa
alyaggomaa@gmail.com
@coreflood_

Sebastian Garcia
eldraco@gmail.com
@eldracote

https://github.com/stratosphereips/StratosphereLinuxIPS

Documentation:
https://stratosphereLinuxips.readthedocs.io/en/develop/

Slides: https://bit.ly/BHUSSlips2022



Example of GPS leak detection

1970-01-01T00:56:31.946939+00:00: Src IP 10.0.2.15 (TINY71) . Detected NETWORK gps location leaked to destination address: 172.217.18.174 AS: GOOGLE, US AS15169 SNI: www.google-analytics.com, rDNS: fra15s29-in-f14.1e100.net port: 80/tcp http. Leaked location: ll=48.850113,2.306764

```
1970-01-01 01:56:31.946939  IP 10.0.2.15.51217 > 172.217.18.174.80: Flags [P.
E...%.@.....
..........Pn$.A%v..P...B...GET /?ie=UTF8&ll=48.850113,2.306764&spn=0.002513,0
Host: maps.google.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.unesco.org/new/en/unesco/about-us/where-we-are/visit-us/
Cookie: NID=102=CgWrVrywC3uFGNLitTaINFmAgYWMxK5DwDggl0X93bQYXBRG3XvUYfK5iaeif
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```