
29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO
JUNE 11-16, 2017
FIGHTING PIRATES AND PRIVATEERS
WWW.FIRST.ORG

Implementing a country-wide sensor infrastructure for proactive detection of malicious activity

Rildo Souza

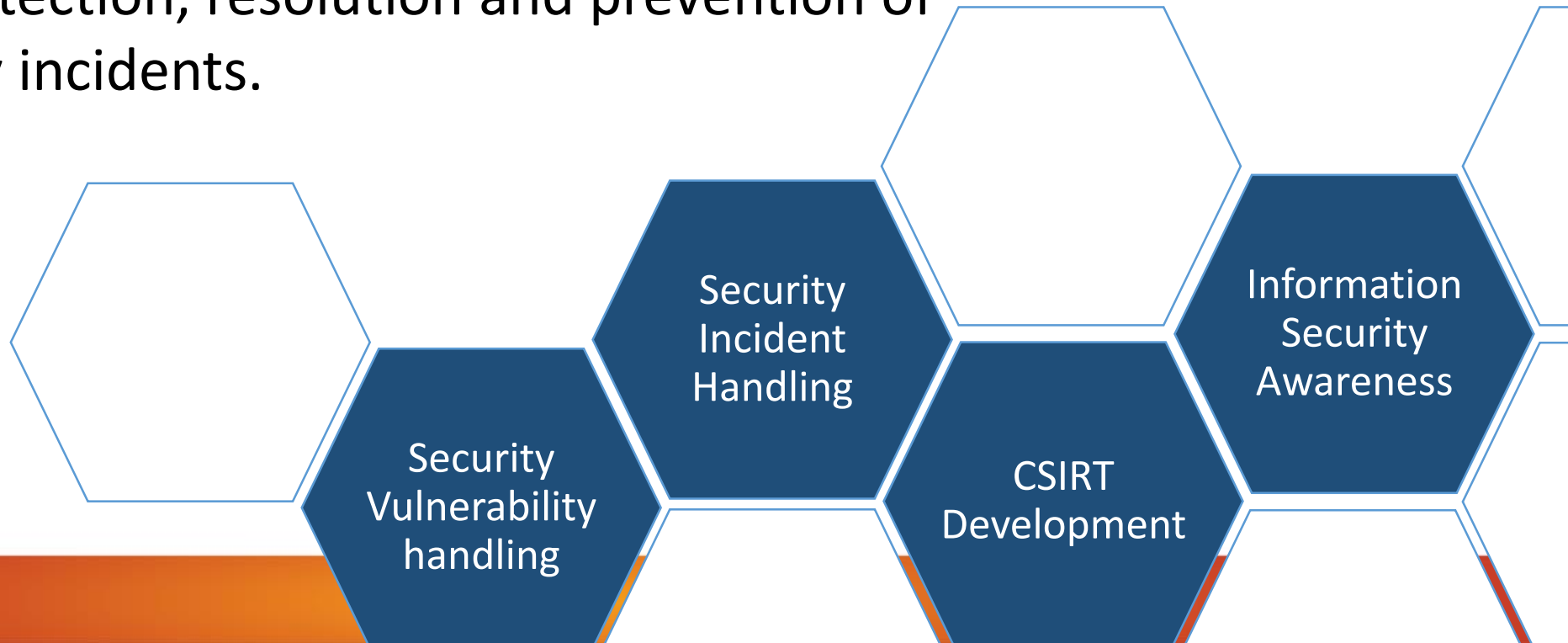
29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO

Regarding the RNP

- Brazilian National Research and Education Network (RNP).
- Created in 1989.
- Implemented the first Latin American fiber network in 2005.

Regarding CAIS

- Coordination CSIRT of Brazilian research and education network since 1997.
- CAIS works in detection, resolution and prevention of network security incidents.

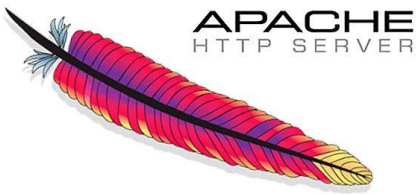


Motivations to create a network CAIS Sensor

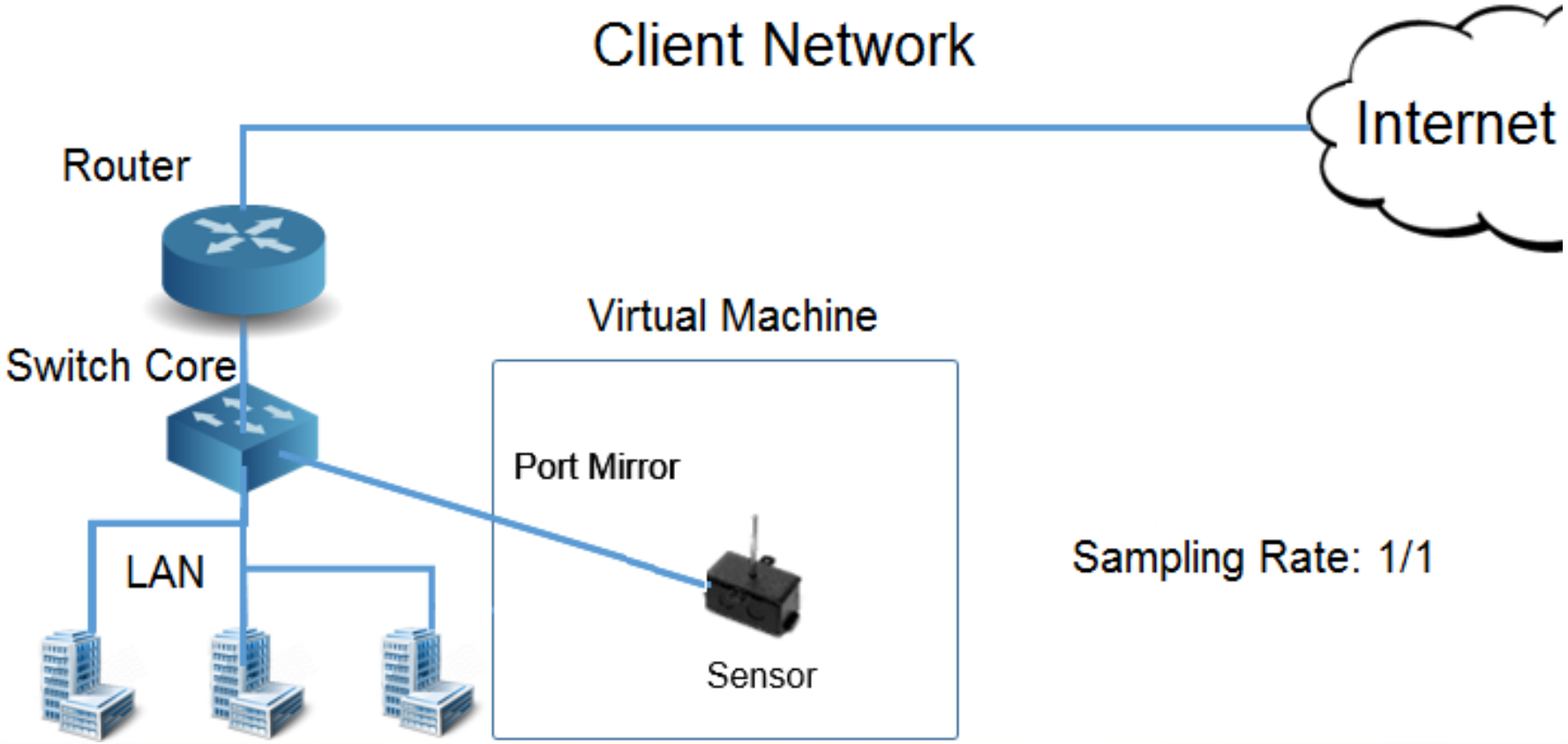
- Highly diversified environment, networks, technologies and maturity of customer’s security teams.
- Increasing our capacity to detect malicious activities.
- Understanding and support better the security actions from our clients .

CAIS Sensor Requirements

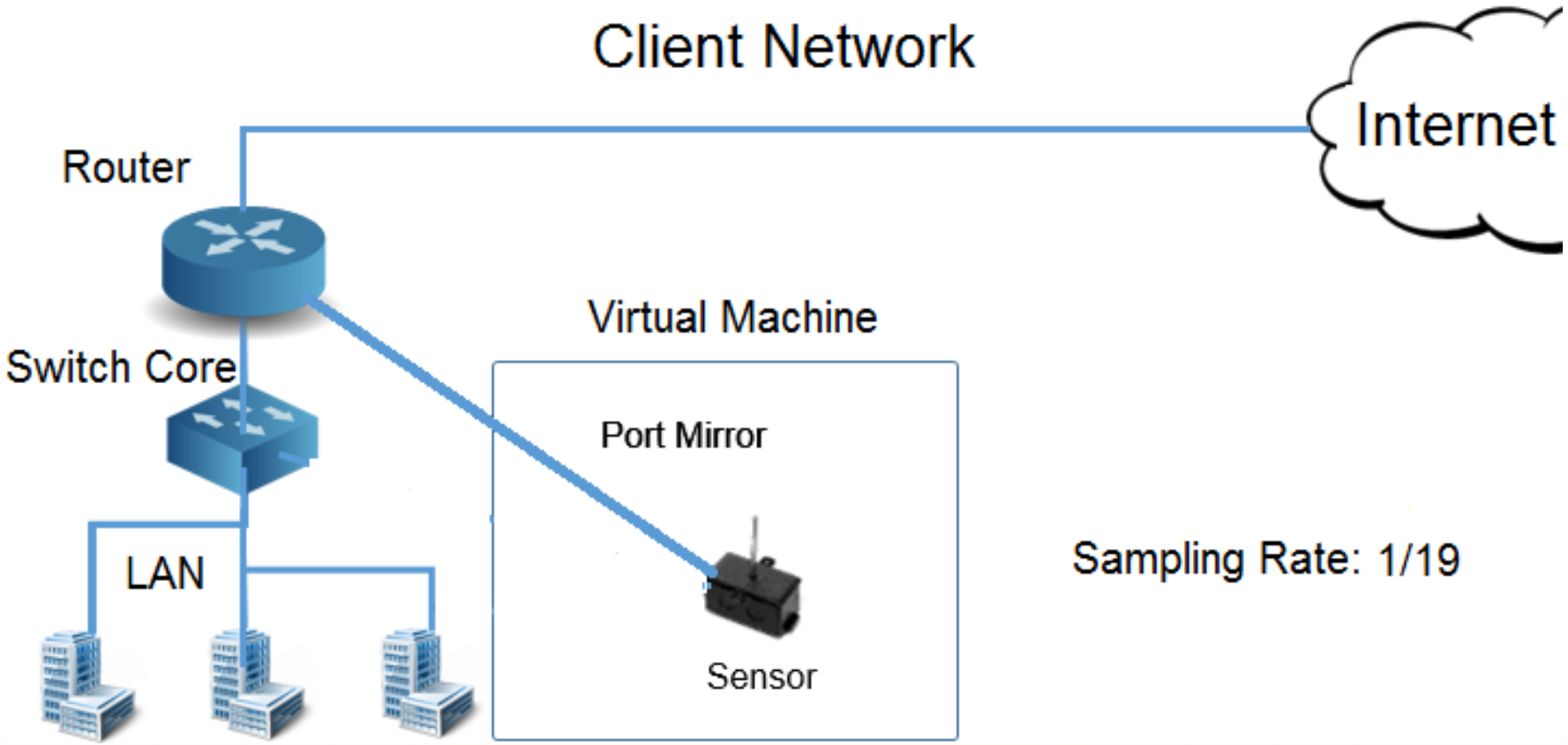
What is CAIS Sensor ?



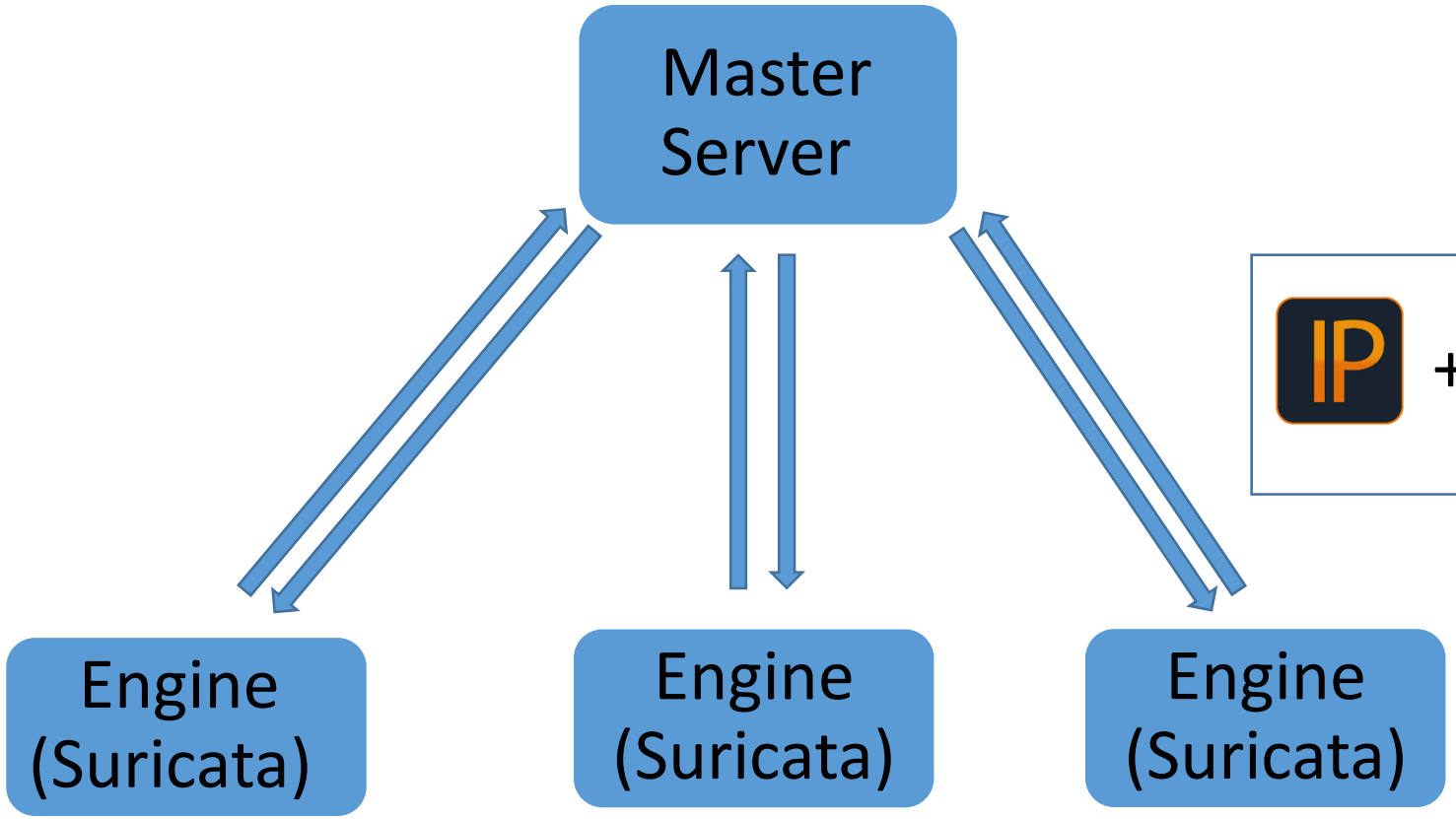
How does the CAIS Sensor analyze traffic ?

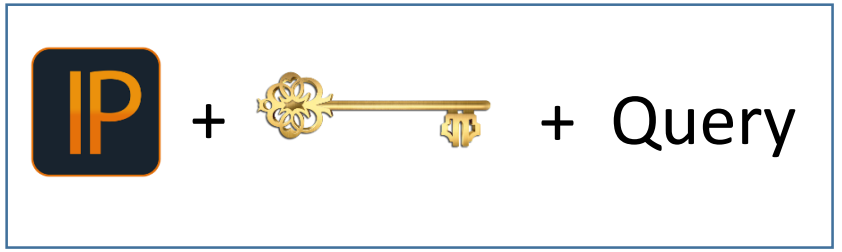


How does the CAIS Sensor analyze traffic ?



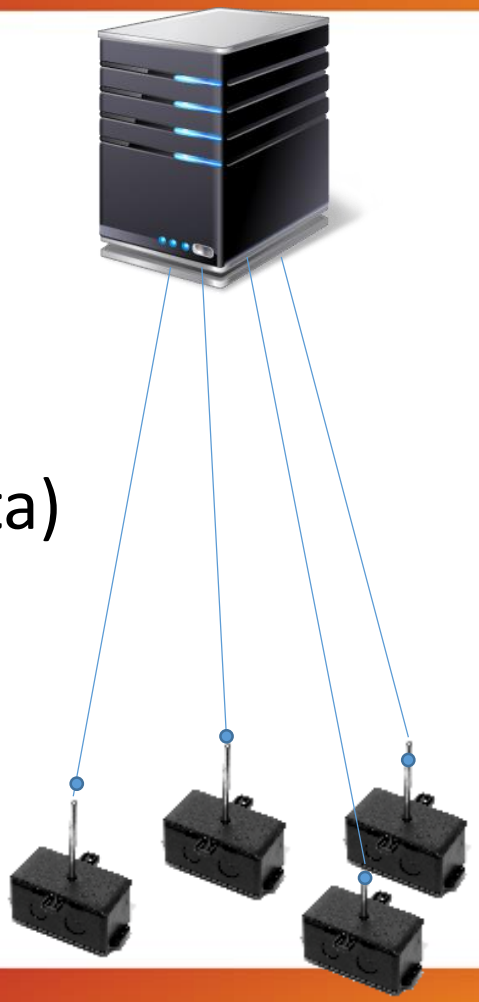
How does the CAIS Sensor Works ?





What does the Master Server do ?

Master

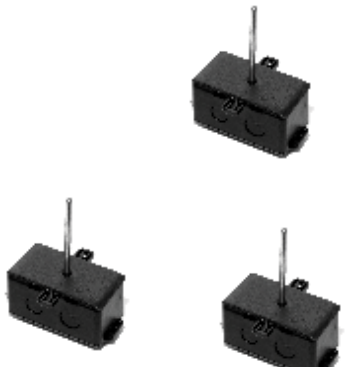


Engines(Suricata)

- Sensor management
- Sensor’s system updates management
- Statistics on malicious activities detected
- Information about sensor’s “health”
- System general administration

Regarding Engines(Suricata)

Engines(Suricata)



SURICATA

- Friendly user interface
- Plug and play
- Less technical knowledge required
- Low maintenance and support
  - Send detections by email
  - Send statistics and status data
  - Update requests

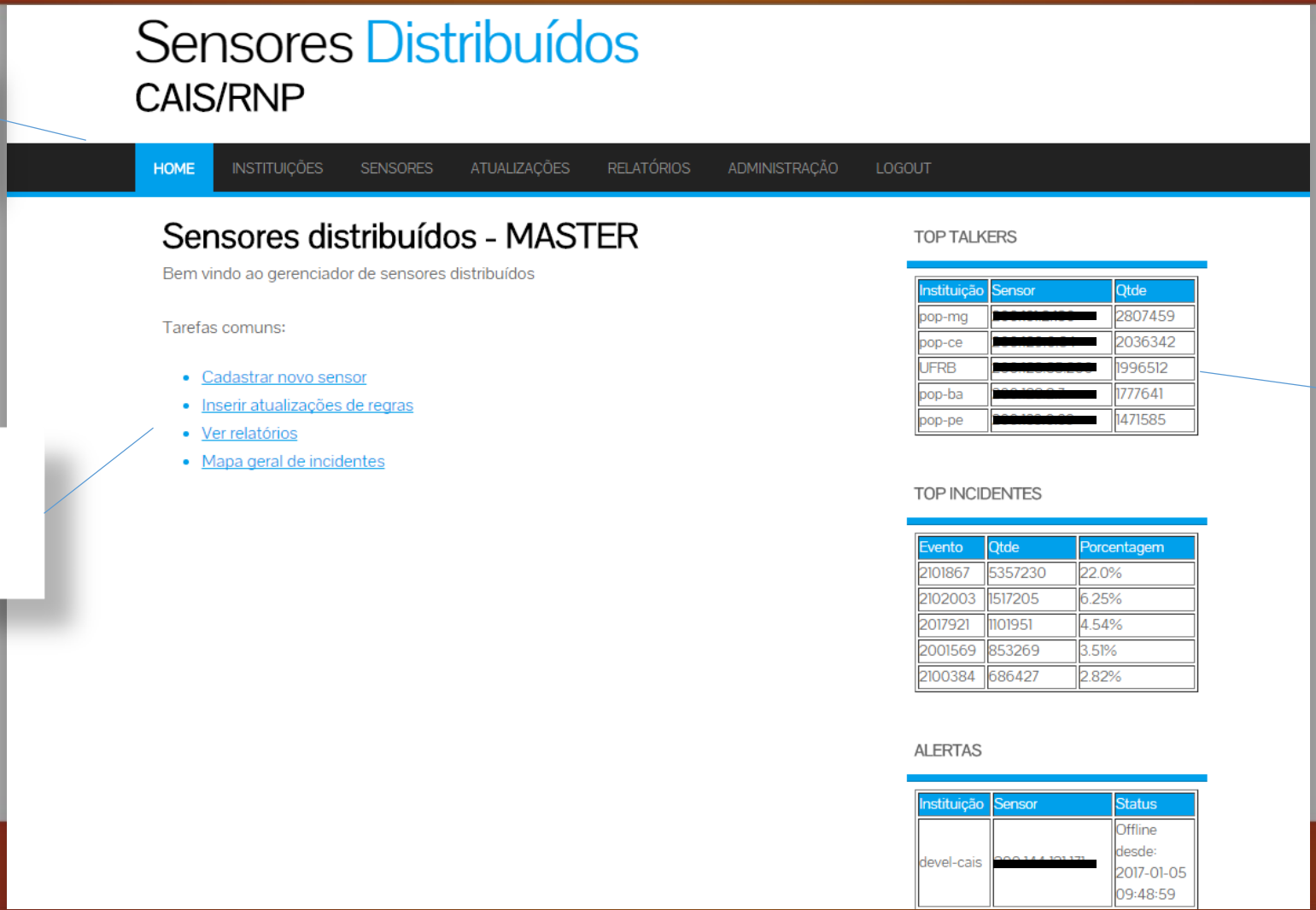
SAN JUAN
PUERTO RICO

The CAIS Sensor (Screenshots)

Main menu

Quick access tasks

Quick Information dashboard

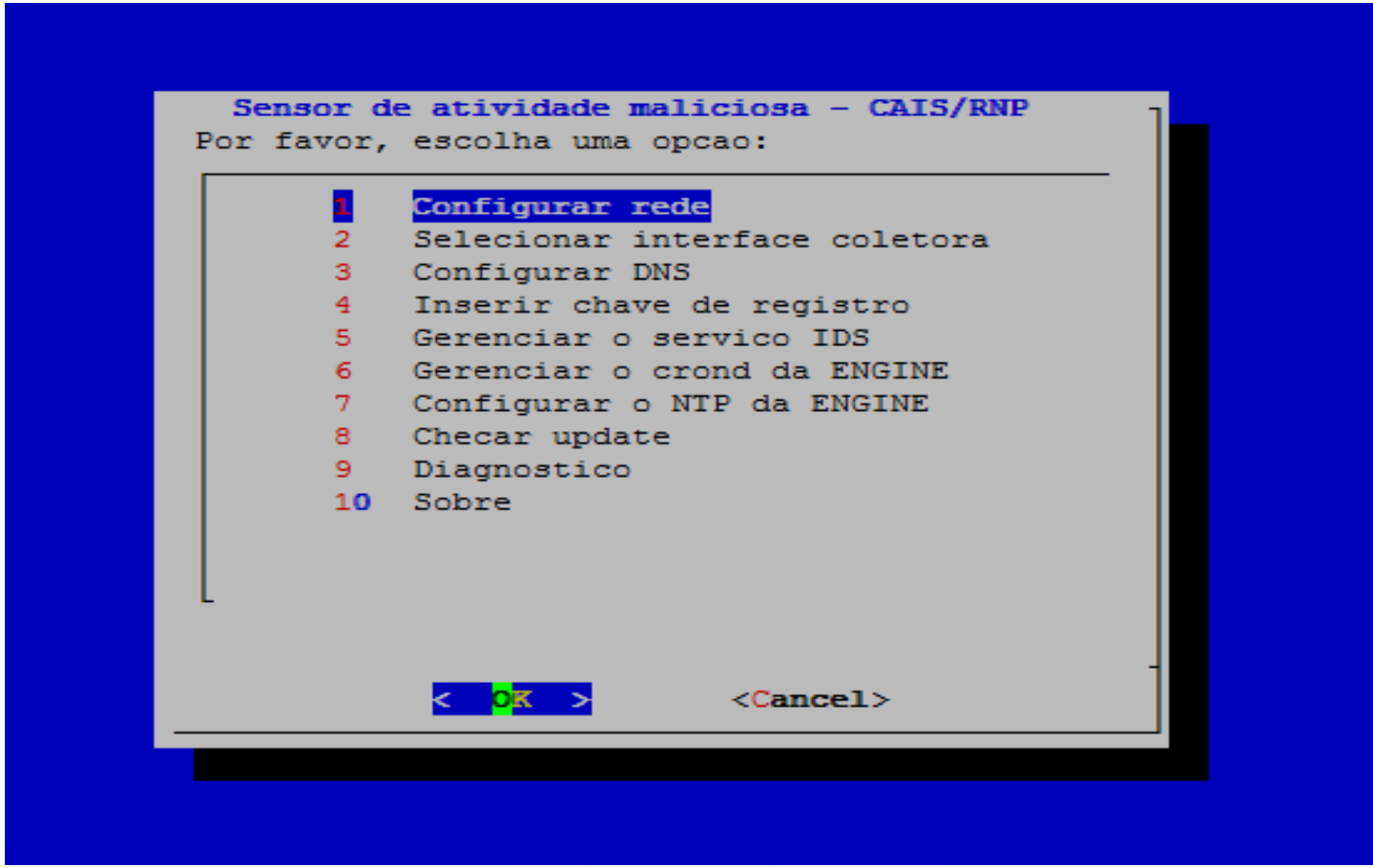


The CAIS Sensor(Screenshots)

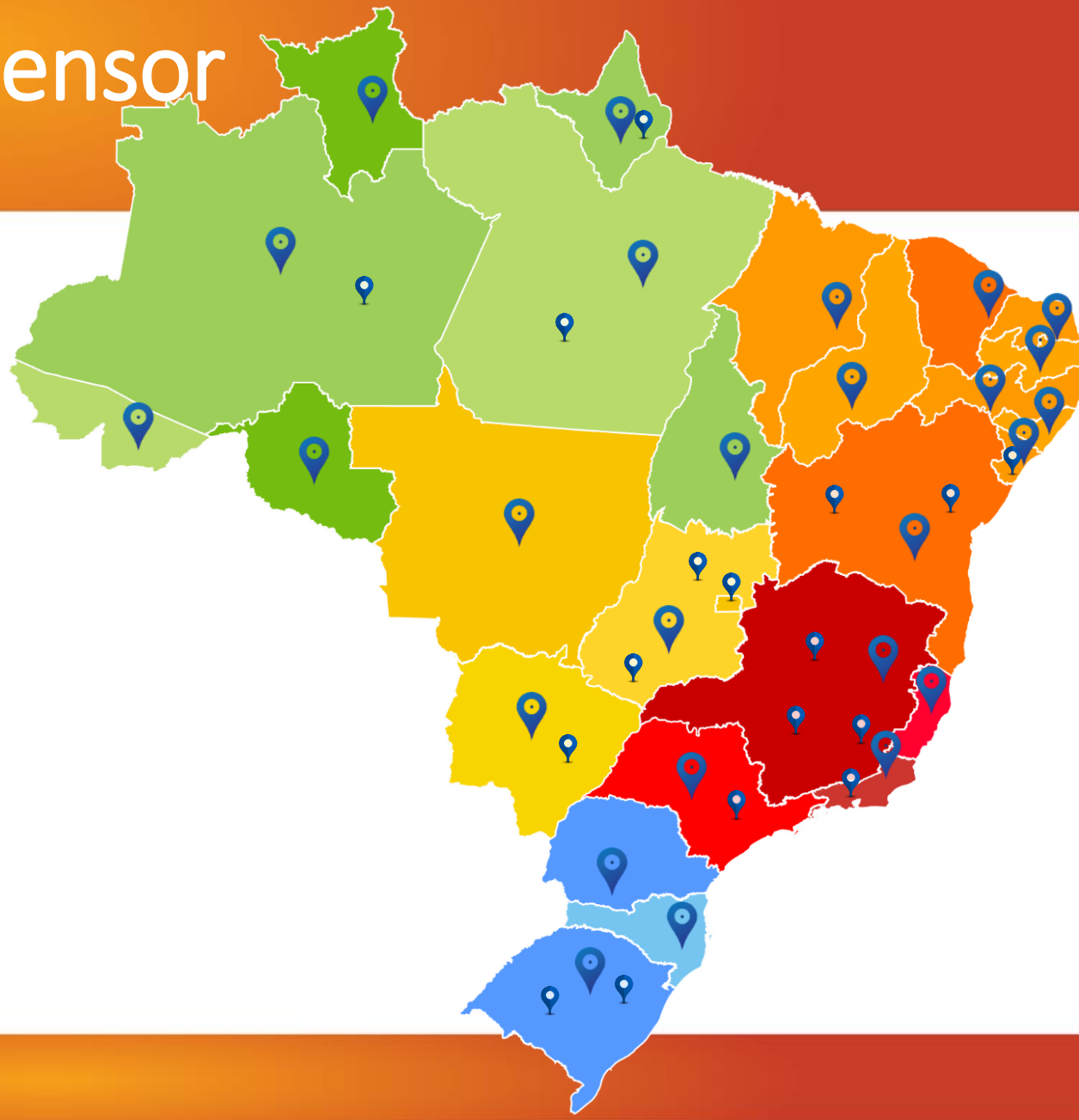
Type	Source	Function
General rules	Emerging Threats	Provide general rules
Customized rules	CAIS	Provide specific rules, on demand.
Rule Exceptions	CAIS	Disable rules without need generate new release.
URL Blacklist	CAIS / APWG / Fraud Catalog Service, etc.	Identify malicious URLs access
IP Blacklist	CAIS / Shadow Server, etc.	Identify malicious IP access, like C&C
Networks	CAIS	Each client has its own network, so the each one variable HOME_NET must be unique, for greater assertiveness.
System updates	CAIS	New sensor system's versions and features, and corrections.

Engine(Screenshots) – Installation Menu

- Network interface configuration.
- Select network pickup interface.
- Put the token.
- Restart Services.



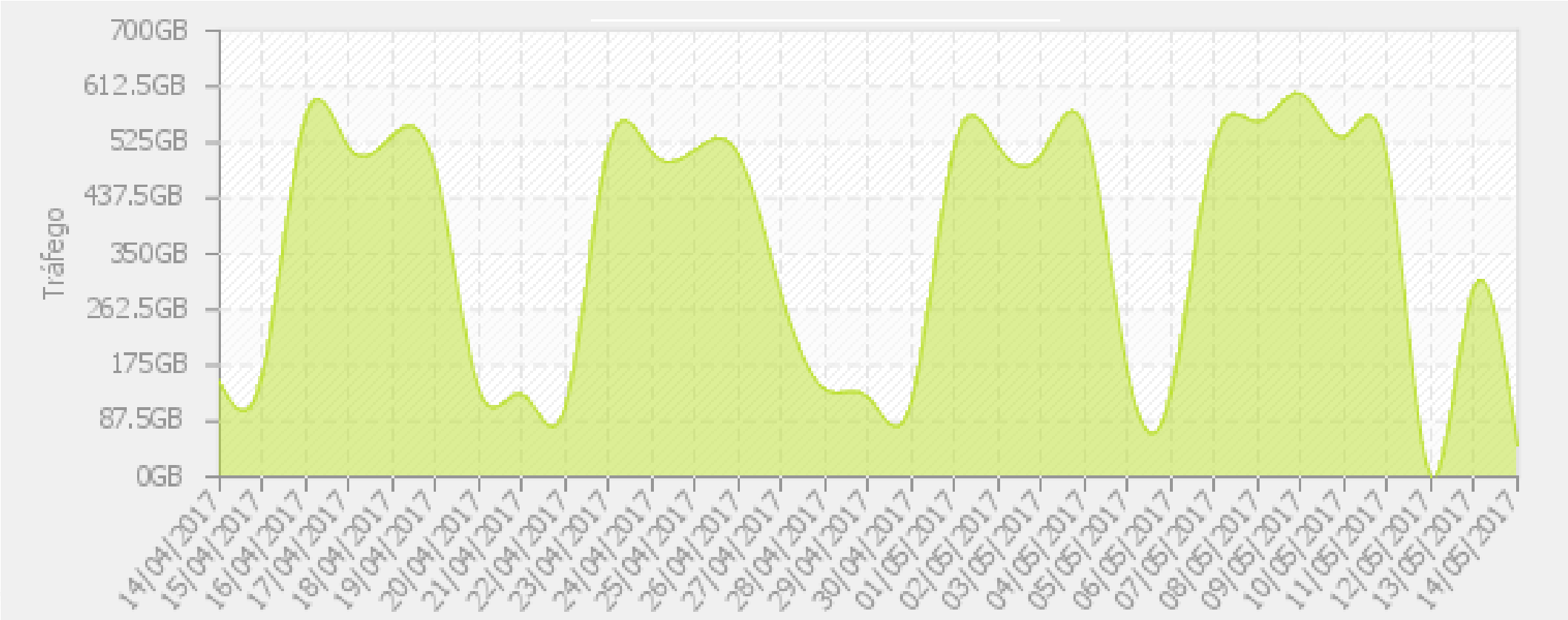
Implementation of CAIS Sensor



- ✓ 27 RNP Points of Presence
- ✓ 17 Customers

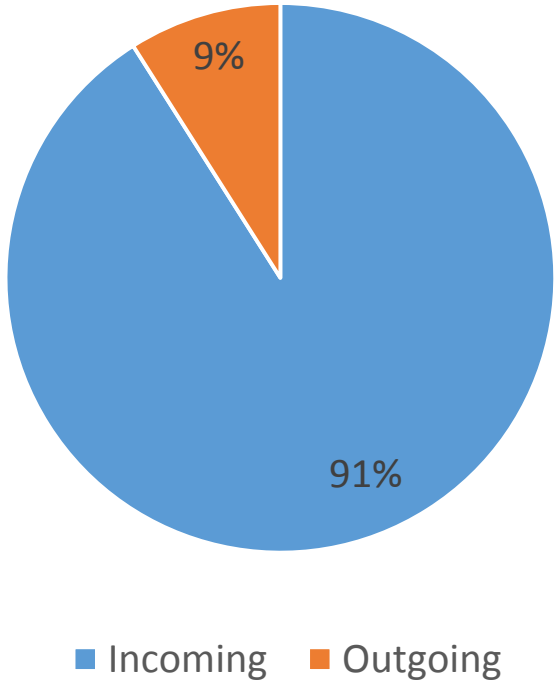
44 Sensors Installed

Statistics – Average Analyzed Traffic

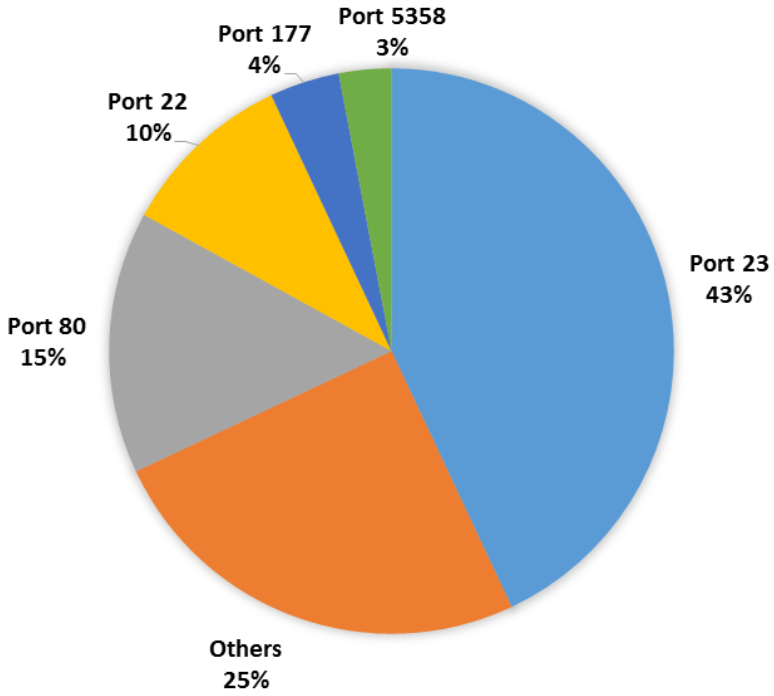


Statistics

Malicious activity flow



Most attacked ports



Statistics - Main types of malicious activity detected

DDoS Attempts(protocol xdmcp)	702,345
DDoS Attack (protocol NTP)	535,204
Malwares	236,985
DDoS Attack (protocol SNMP)	102,478

Statistics – Types of detected events

Statistics - Botnets

nicaze.net

Zeus

XcodeGhost

PCRat/Gh0st

Kelihos

Bladabindi/njrat

Beacon

Feodo

Palevo

DealPly

Next Steps

- Optimize reports
- Integrate with other sources (URLs blacklist, IPs blacklist, others)
- Increase number of sensors in educational institutions and RNP customers
- Finalize and expand the partnership model

Questions ?

Thank You !

The Brazilian Academic and Research Network

Rildo Souza
Security Analyst
rildo.souza@rnp.br