CAIS Sensor: Distributed Sensors Network in Brazilian NREN

RNP

Ministério da Cultura

Ministério da Saúde

Ministério da Educação

Ministério da Ciência, Tecnologia e Inovação

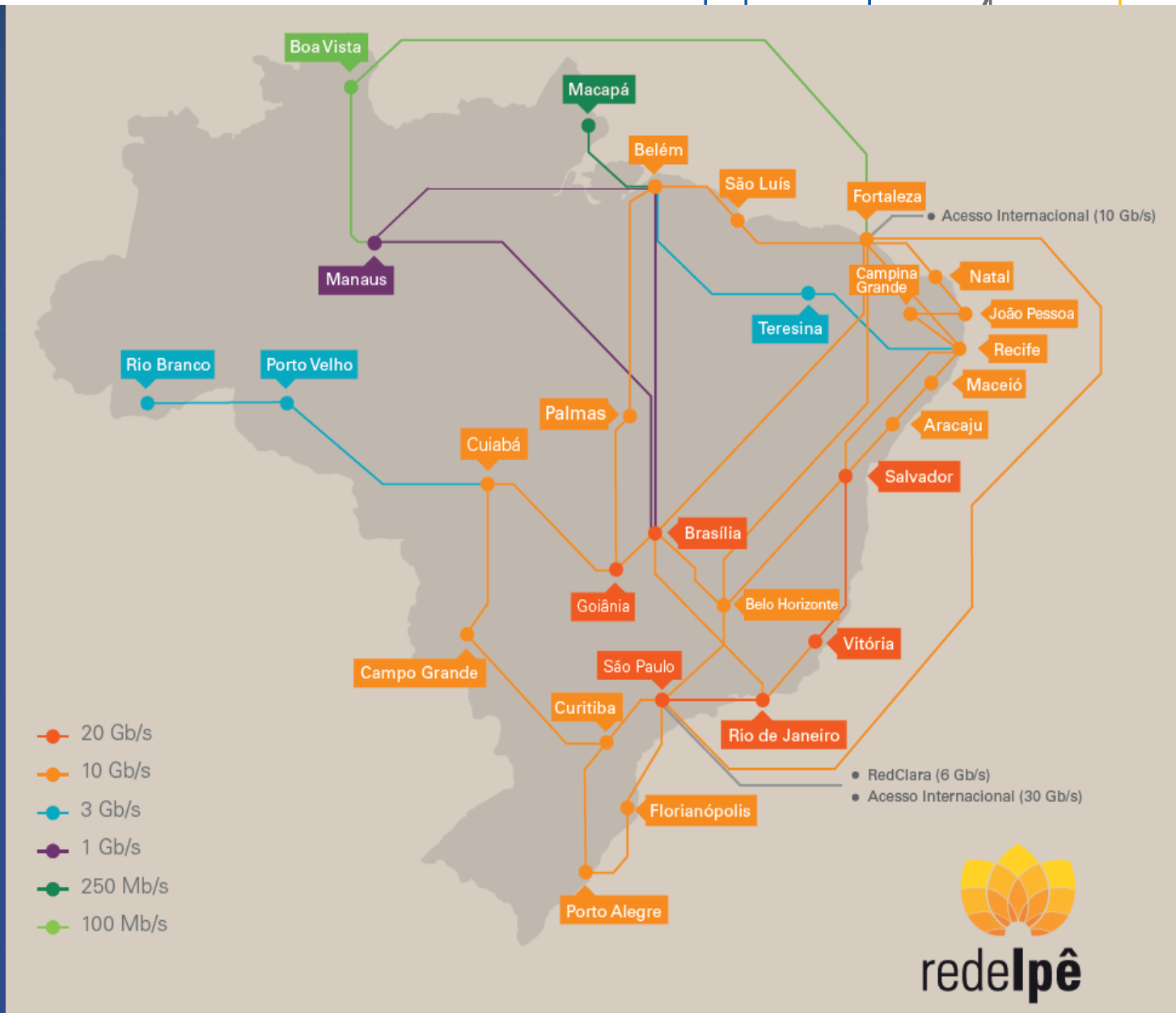
LACSEC

LACNIC27

Regarding RNP

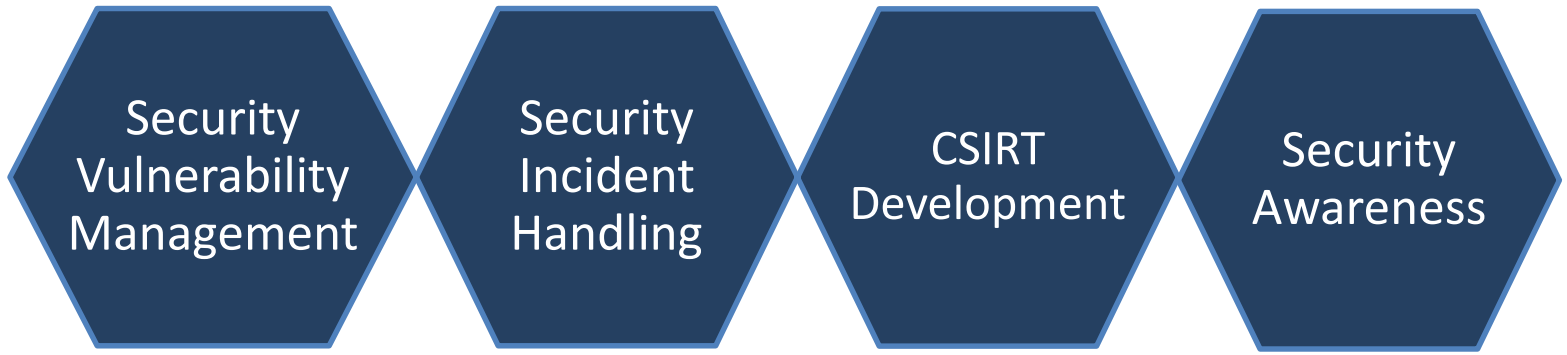
RNP

- Brazilian National Research and Education Network (RNP).
- Created in 1989.
- Implementing 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.



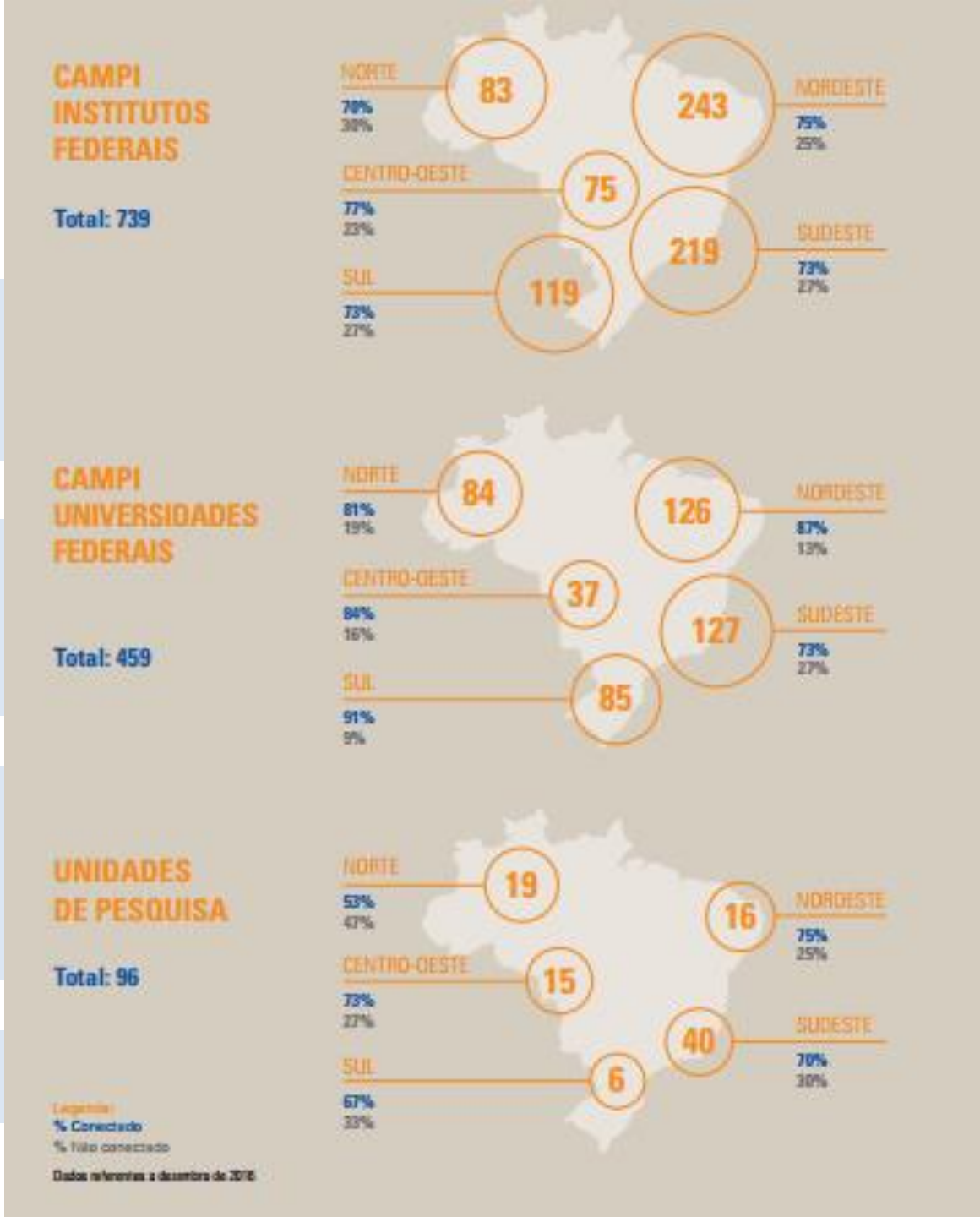
Motivations to create a CAIS Sensor network

Rede Ipê, Brazilian academic network backbone. Built-in capacity of 347 Gbps

Interconnects 1.911 units of RNP's Customers (Universities, Federal Institutes, Research Organizations).

Highly diversified environment, regarding networks, technologies and maturity of customers' security teams.

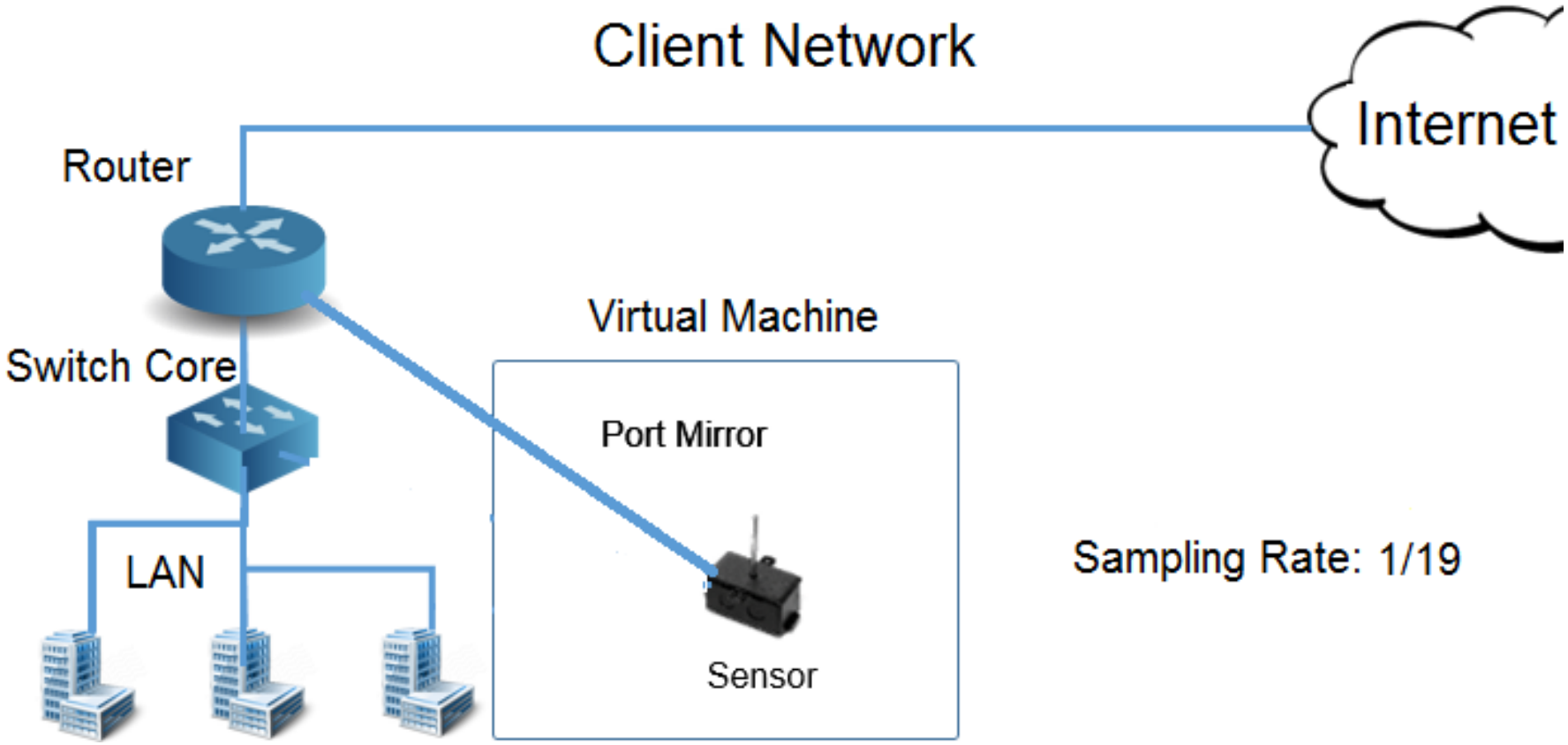
Difficulties for efficient detection.



CAIS Sensor Requirements

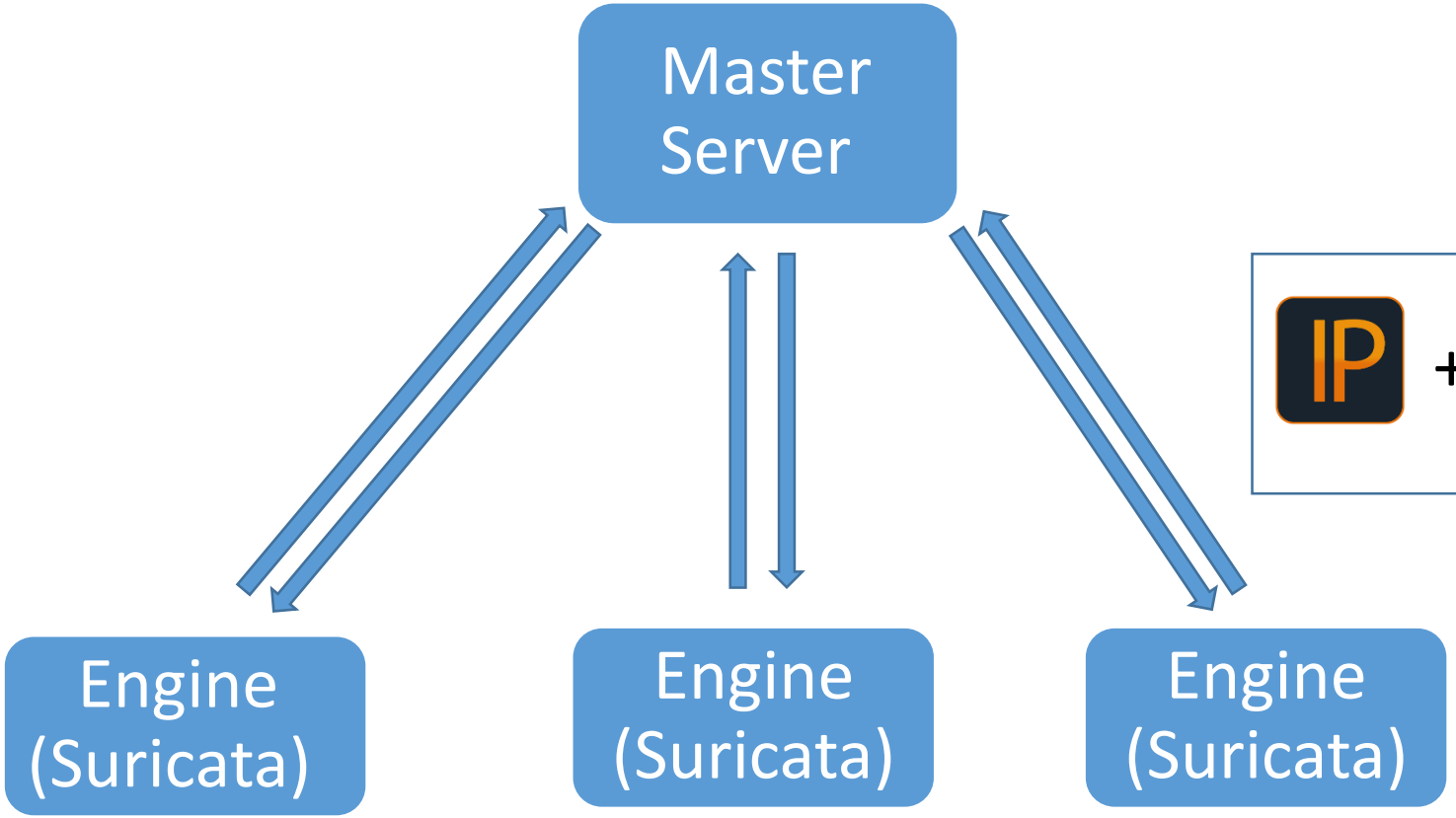
What is the CAIS Sensor?

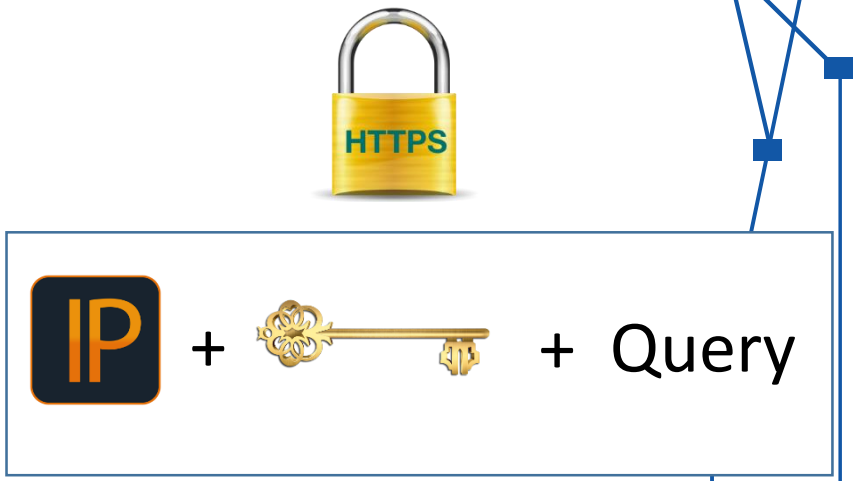
How does CAIS Sensor analyze traffic?



Sampling Rate: 1/19

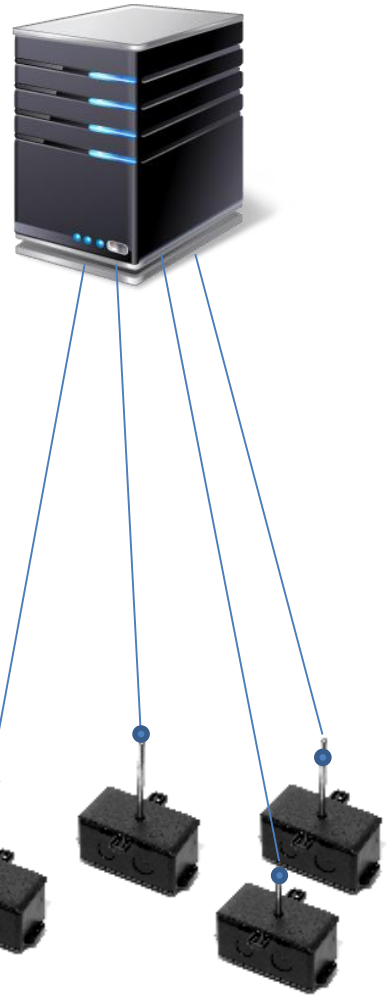
How does CAIS Sensor work?





What does Master Server do?

Master

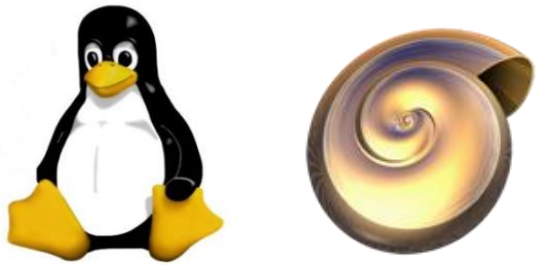


Engines(Suricata)

- Sensor management
- Sensor’s system updates management
- Statistics of 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

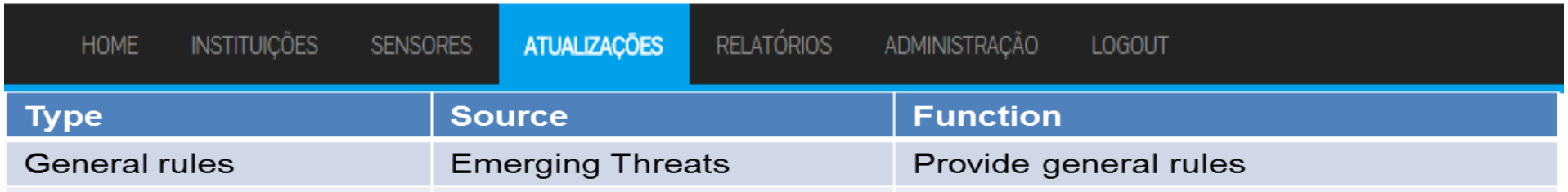
The CAIS Sensor(Screenshots)

Main menu

Quick access tasks

Quick Information dashboard

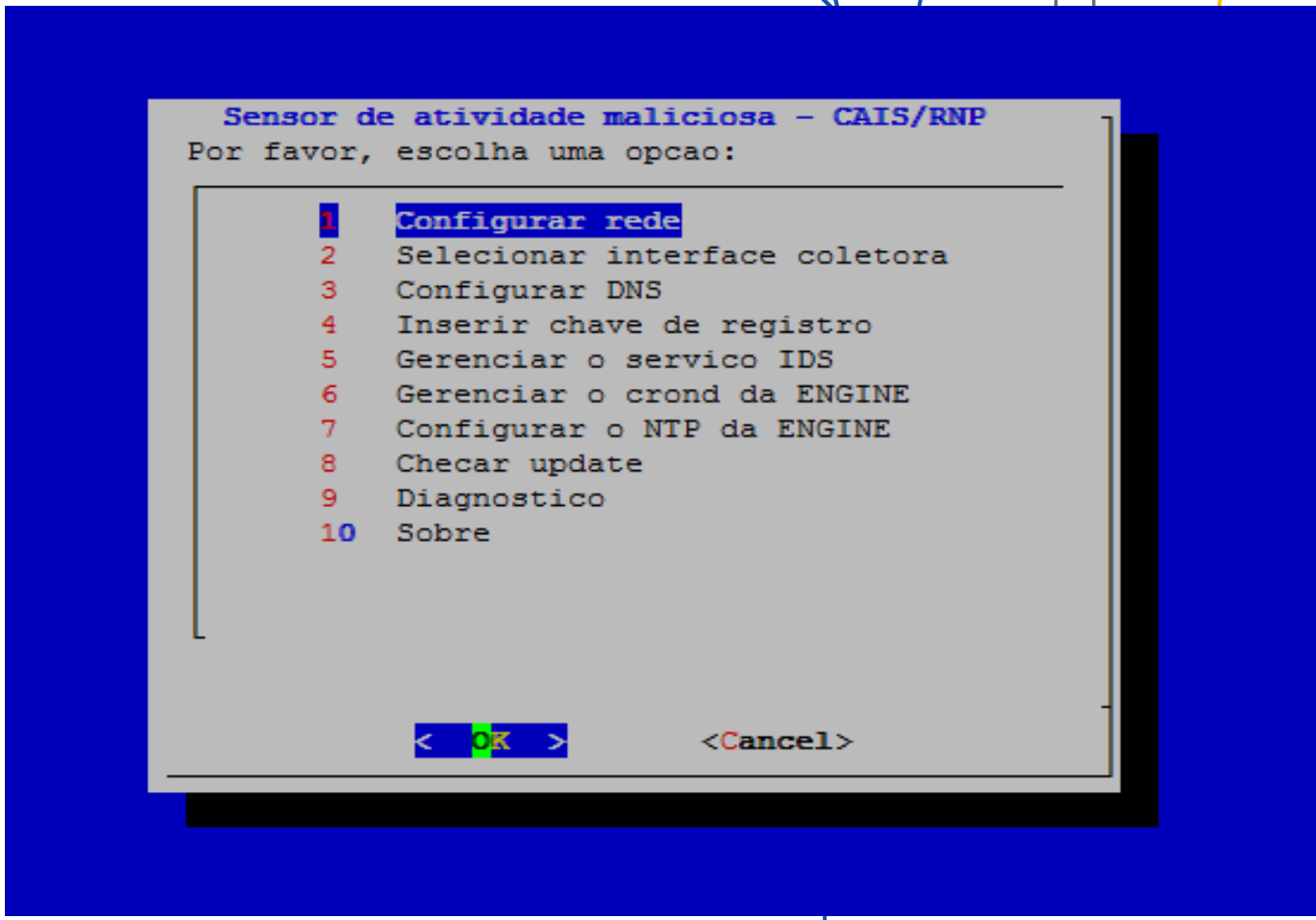
The CAIS Sensor(Screenshots)



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

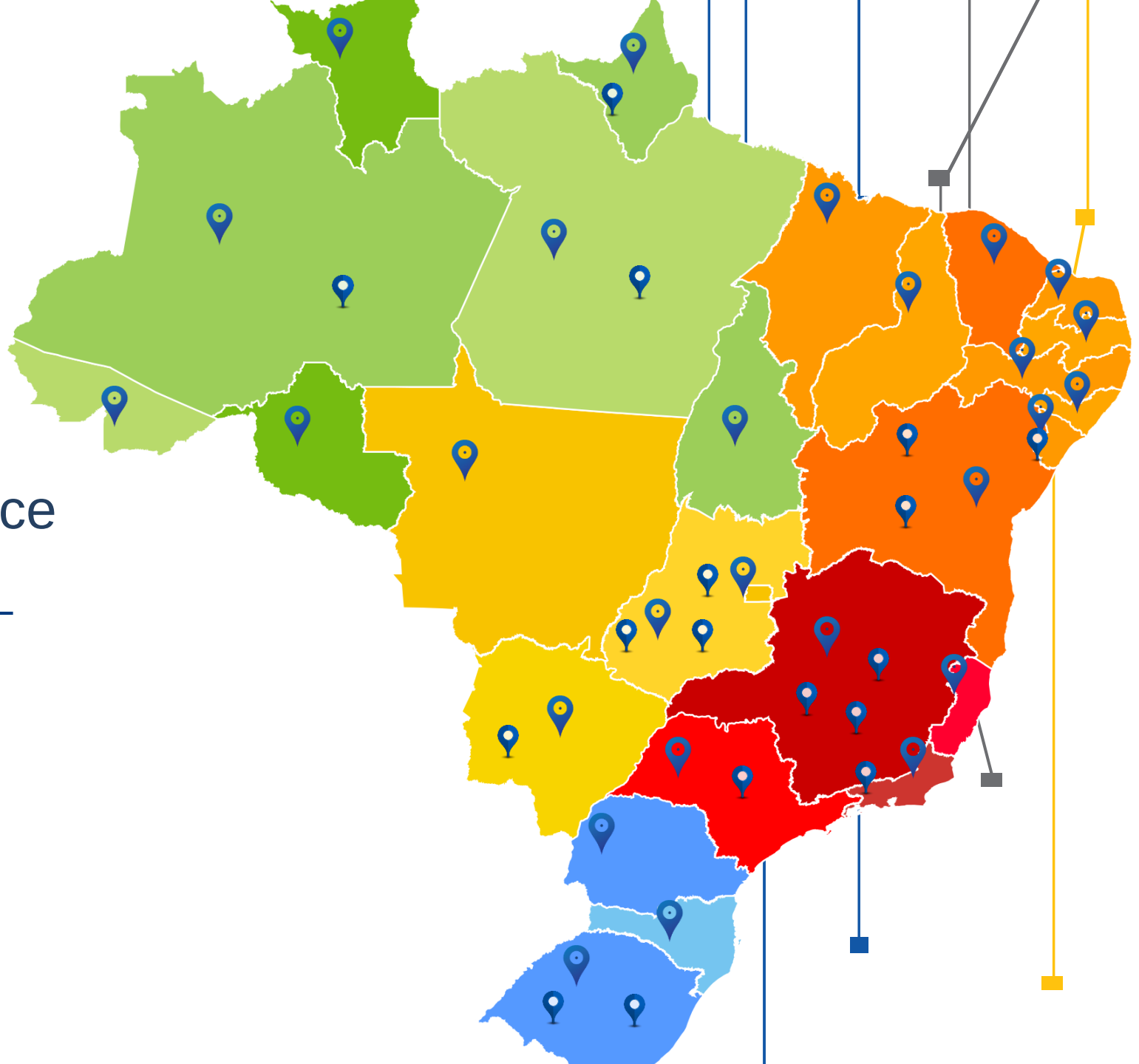
- Network interface configuration.
- Select network pickup interface.
- Restart Services.
- Use license configuration.



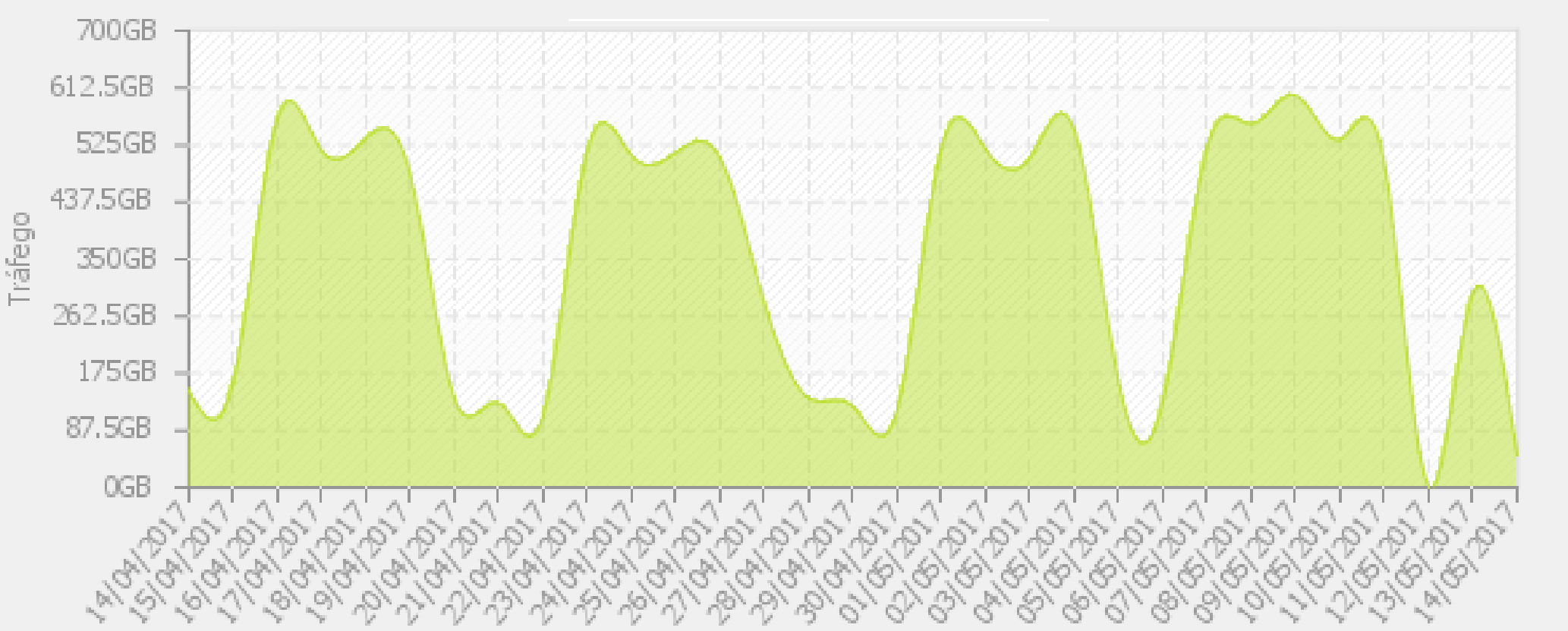
CAIS Sensor Implementation

- ✓ 27 RNP Points of Presence
- ✓ 17 Customers

44 Sensors Installed

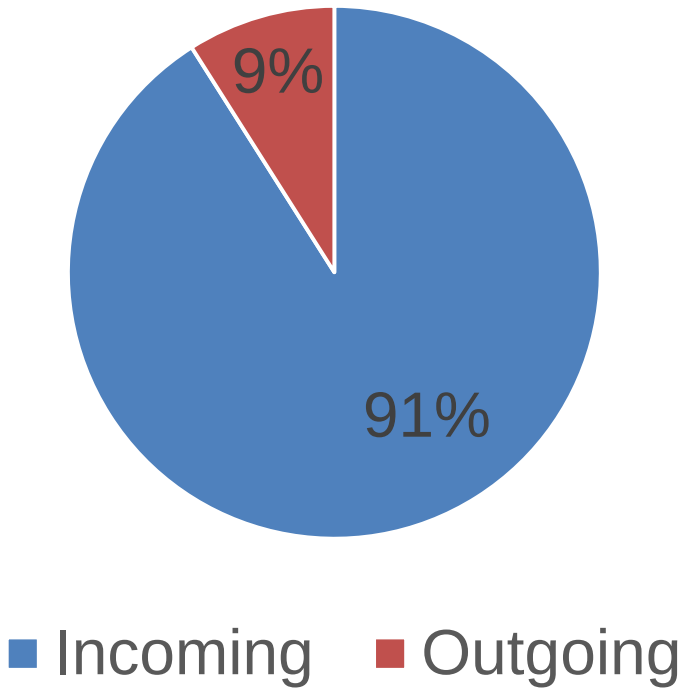


Statistics – Average Analyzed Traffic

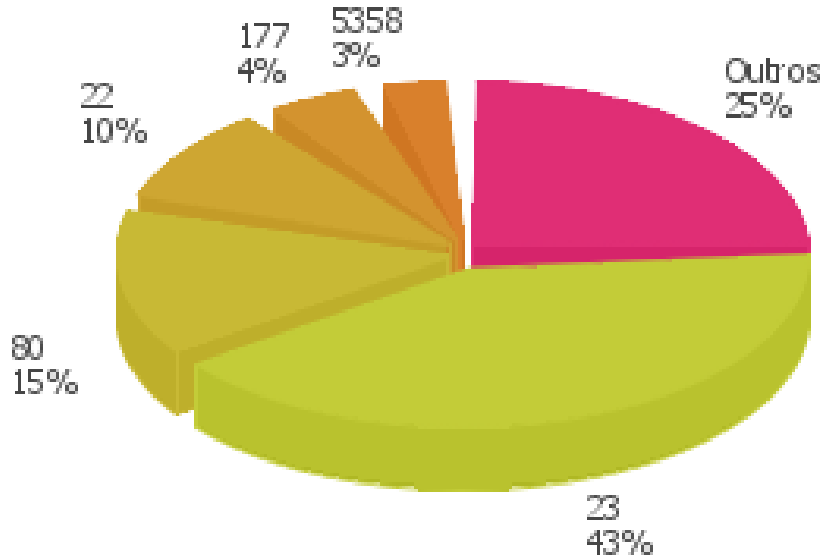


Statistics

Malicious activity flow

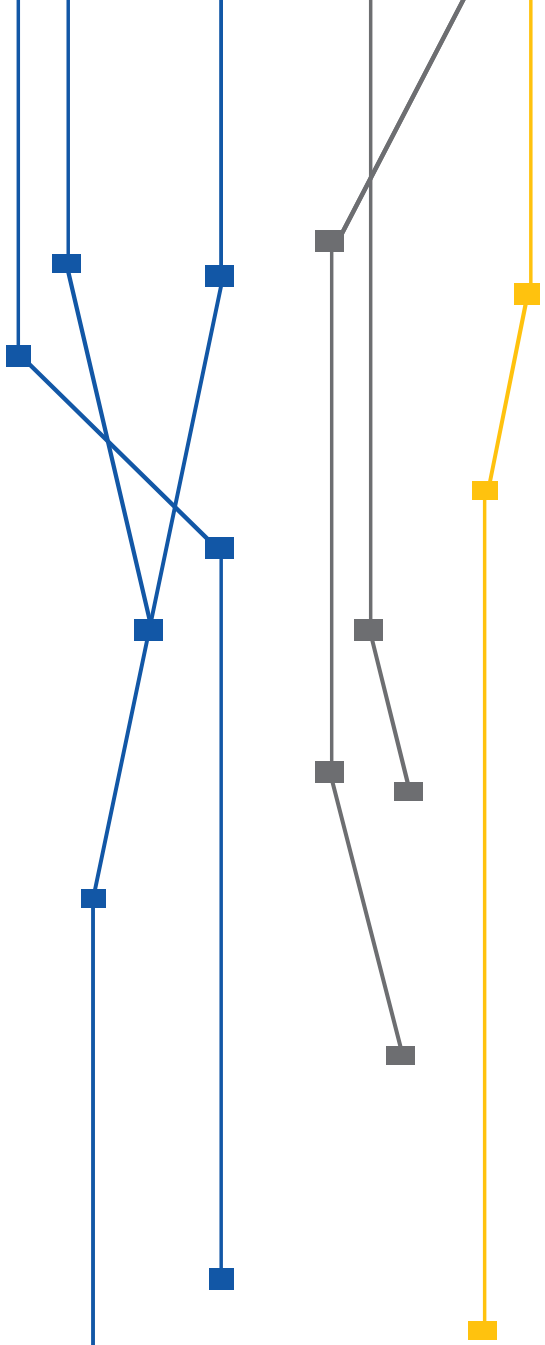


Most attacked ports

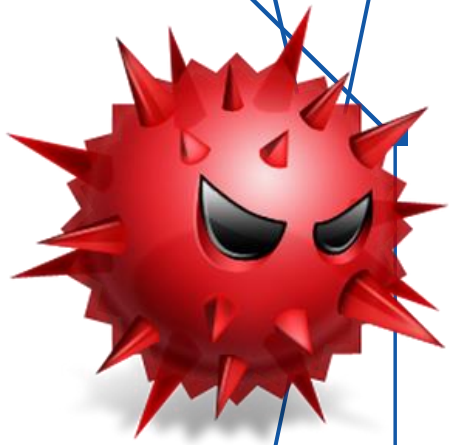


Statistics - Main types of malicious activity detected

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

PCRat/Gh0st

Beacon

Zeus

Kelihos

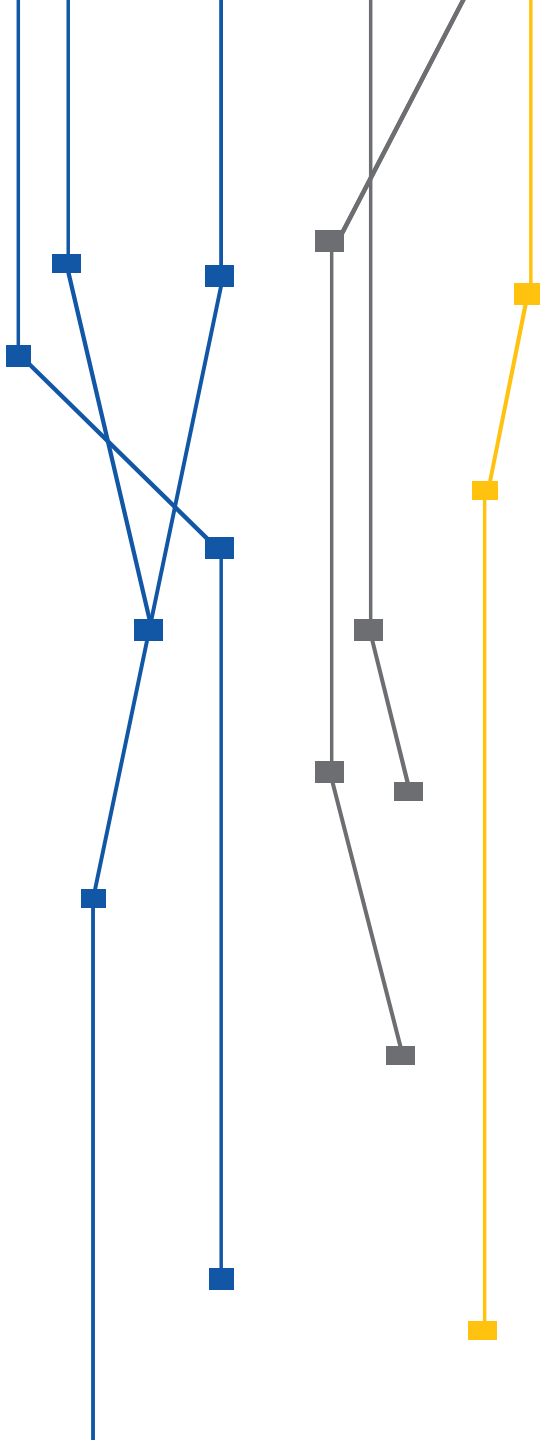
Feodo

DealPly

XcodeGhost

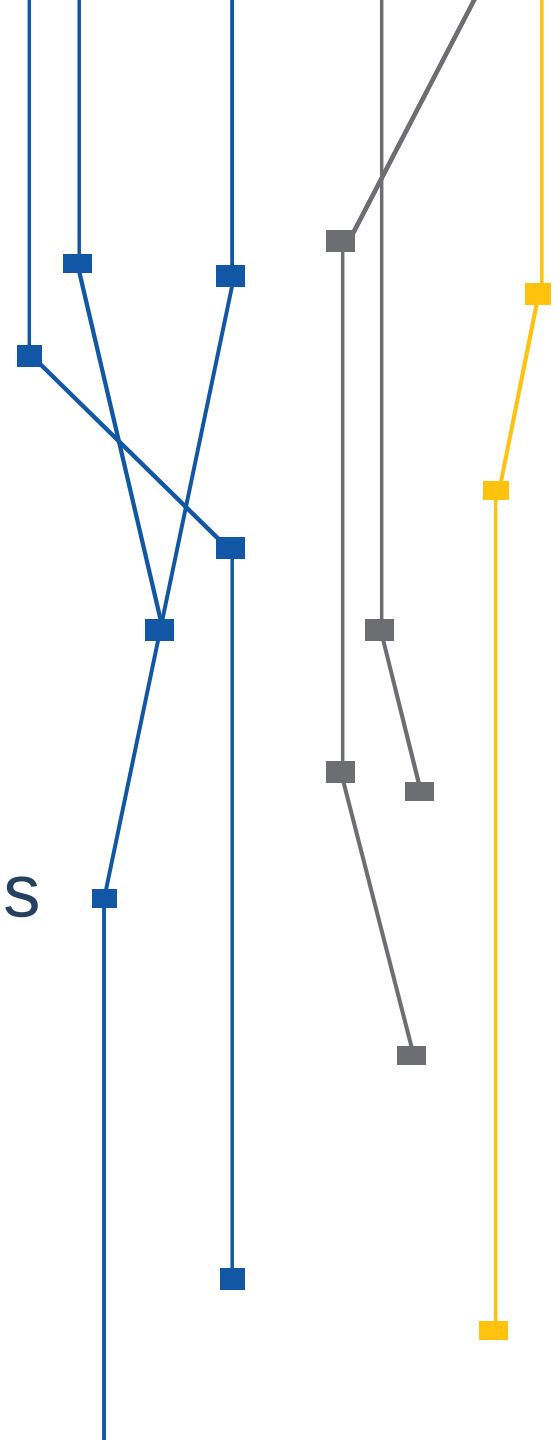
Bladabindi/njrat

Palevo

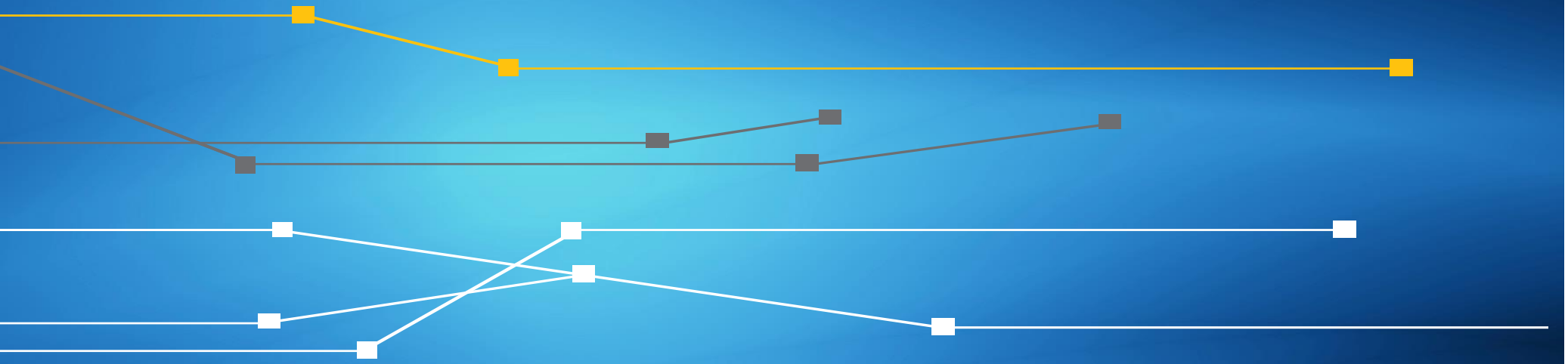


Next Steps

- 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 ?



Thanks!

RNP – Brazilian Educational and Research Network

CAIS – RNP Incident Security Response Team

Rildo Souza
Security Analyst
rildo.souza@rnp.br

Yuri Alexandro
Security Analyst
yuri.ferreira@rnp.br

RNP

Ministério da Cultura

Ministério da Saúde

Ministério da Educação

Ministério da Ciência, Tecnologia e Inovação