Grupo de Resposta a Incidentes de Segurança Bahia/Brasil

Rogerio Bastos

https://certbahia.pop-ba.rnp.br

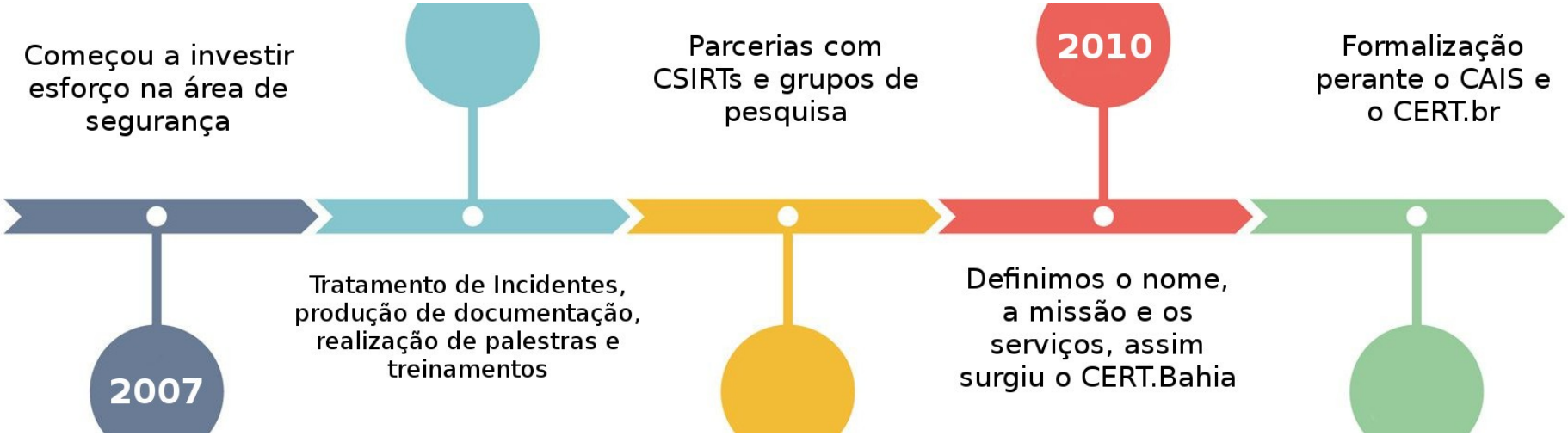
Quem somos

É responsável pela conexão das instituições baianas à rede acadêmica Brasileira (Rede Ipê) e operação da Rede Metropolitana de Salvador (Remessa).

Coordenação de Segurança da Informação e Comunicações da STI/UFBA, responsável pelas questões de segurança digital na Universidade Federal da Bahia.

É um CSIRT de coordenação para as instituições clientes do PoP-BA/RNP e parceiras da Remessa.

Surgimento


Começou a investir esforço na área de segurança
2007
Tratamento de Incidentes, produção de documentação, realização de palestras e treinamentos
Parcerias com CSIRTs e grupos de pesquisa
2010
Definimos o nome, a missão e os serviços, assim surgiu o CERT.Bahia
Formalização perante o CAIS e o CERT.br

CSIRT de Coordenação

- Atua na coordenação das instituições no processo de tratamento e resposta a incidentes de segurança.

- O CSIRT de coordenação também atua de forma a facilitar o compartilhamento das informações e a cooperação entre equipes de segurança das instituições.

- Atuação similar à do CAIS/RNP, mas com uma abrangência reduzida.

Escopo de Atuação

- O escopo de atuação do CERT.Bahia são as instituições conectadas ao Ponto de Presença da RNP na Bahia (PoP-BA/RNP) e instituições parceiras da Rede Metropolitana de Salvador (ReMeSSA).

- Contudo, a atuação do CERT.Bahia não está restrita a o escopo definido.

Serviços

Tratamento de Incidentes

- O CERT.Bahia atua na coordenação das instituições no processo de tratamento e resposta a incidentes de segurança, facilitando o compartilhamento das informações e a cooperação entre as partes envolvidas.

- O CERT.Bahia também oferece orientação às instituições, de modo que elas possam tratar os incidentes de forma adequada.

Tratamento de Incidentes

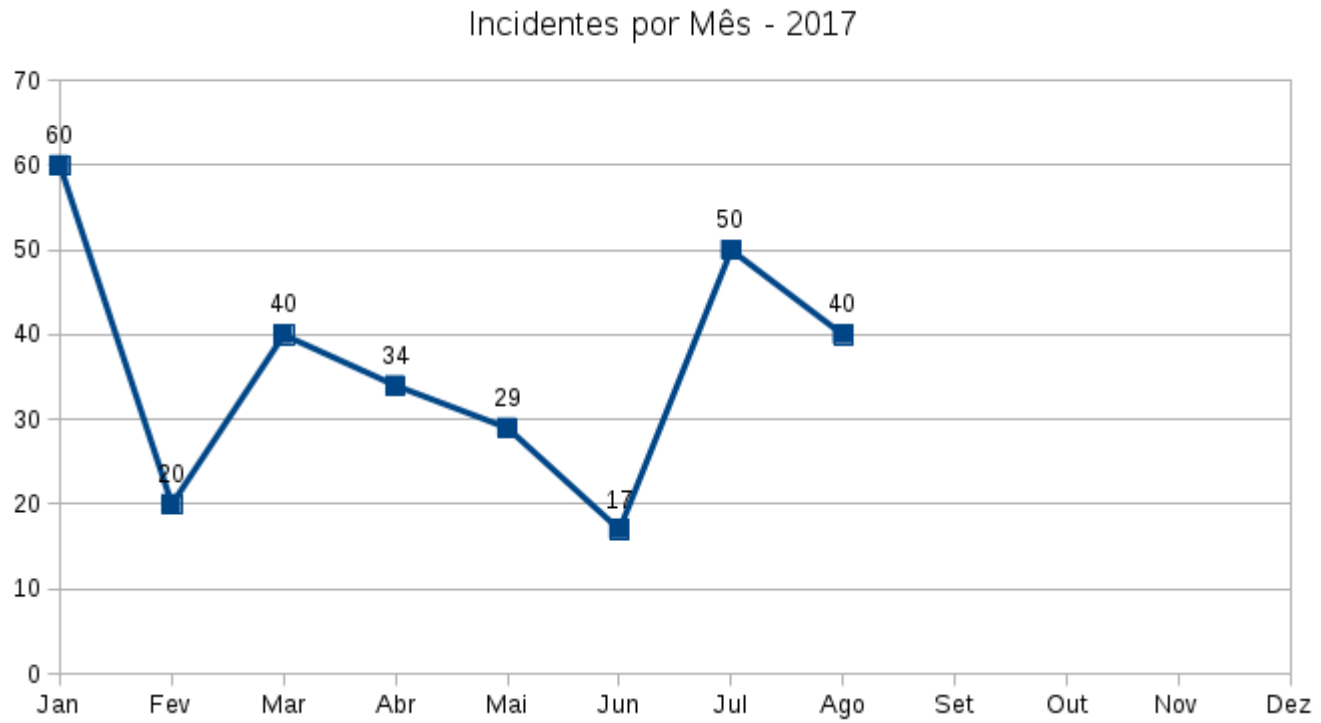
- Além do sistema SGIS do CAIS/RNP [1], utilizamos a ferramenta Request Tracker (RT) [2] para gerenciar as notificações de incidentes de segurança. Assim, é possível ter uma maior flexibilidade para classificar e gerar estatísticas dos incidentes.

- No RT temos campos personalizados para registrar a Instituição que gerou a notificação (e.g. CAIS/RNP e CERT.br), a categoria do incidente (e.g. Defacement, Malware, Phishing), a Instituição que originou o incidente, dentre outros.

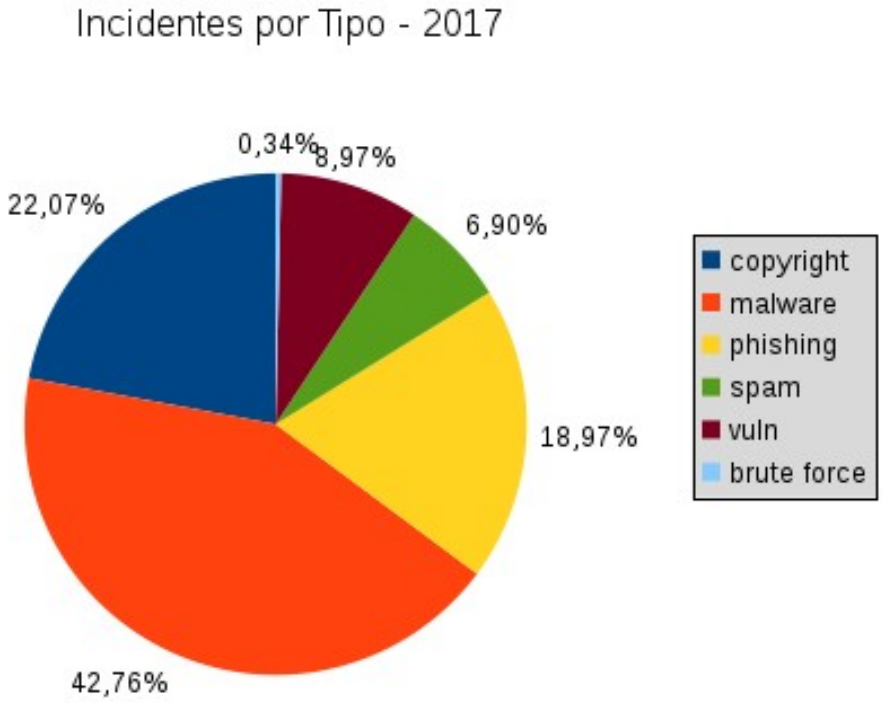
[1] https://sgis.rnp.br/

[2] https://bestpractical.com/request-tracker/

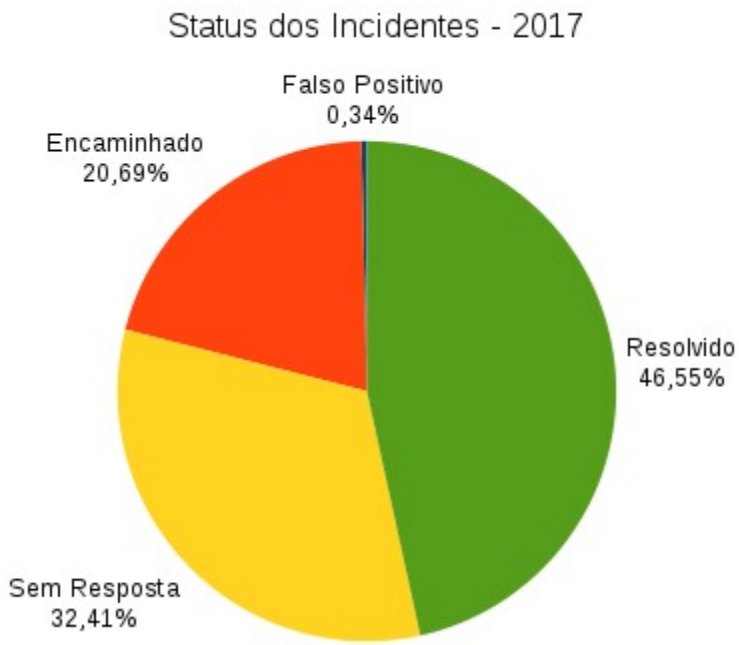
Tratamento de Incidentes



Tratamento de Incidentes



Tratamento de Incidentes



Alertas de Segurança

- Divulgação de informações sobre ataques, vulnerabilidades e ameaças de segurança juntamente com recomendações de como tratar e prevenir os problemas resultantes para que as instituições possam proteger seus sistemas de determinadas ameaças antes destas serem exploradas.
- Os alertas são publicados no site do CERT.Bahia [1] e numa lista de e-mail específica [2].

[1] https://certbahia.pop-ba.rnp.br/

[2] certbahia-alertas [em] listas.pop-ba.rnp.br

Alertas de Segurança

- É importante se atentar à confiabilidade das informações divulgadas para que os alertas enviados pelo CSIRT não percam a credibilidade.

- Algumas fontes de informações sobre ataques, vulnerabilidades e ameaças de segurança:
  - http://listas.rnp.br/mailman/listinfo/rnp-alerta
  - https://www.us-cert.gov/
  - https://nmap.org/mailman/listinfo/fulldisclosure
  - http://www.openwall.com/lists/oss-security/

Alertas de Segurança

- No episódio do HeartBleed, enviamos alerta para todos os clientes e foi feito contato com os clientes vulneráveis identificados através de scanner.
- Realizamos Webinar para conscientizar os clientes.
- O HeartBleed foi uma vulnerabilidade crítica no OpenSSL que foi divulgada em 2014.

Educação e Treinamento

- Divulgação e realização de atividades de educação e treinamento sobre segurança da informação, incluindo palestras, eventos e a produção de materiais de apoio.

- Campanha de incentivo a adoção de DNSSEC com cursos, tutoriais e webinars.

Educação e Treinamento

- O Encontro de Segurança em Informática (EnSI) é o principal evento realizado pelo CERT.Bahia.
- Começou como o DISI do PoP-BA e se transformou num evento independente. Nos últimos anos tem sido realizado na mesma semana do WTR.
- Em 2017 teve um público de mais de 200 pessoas, além de transmissão online.
- Site do evento: https://ensi.pop-ba.rnp.br/

Educação e Treinamento

Educação e Treinamento

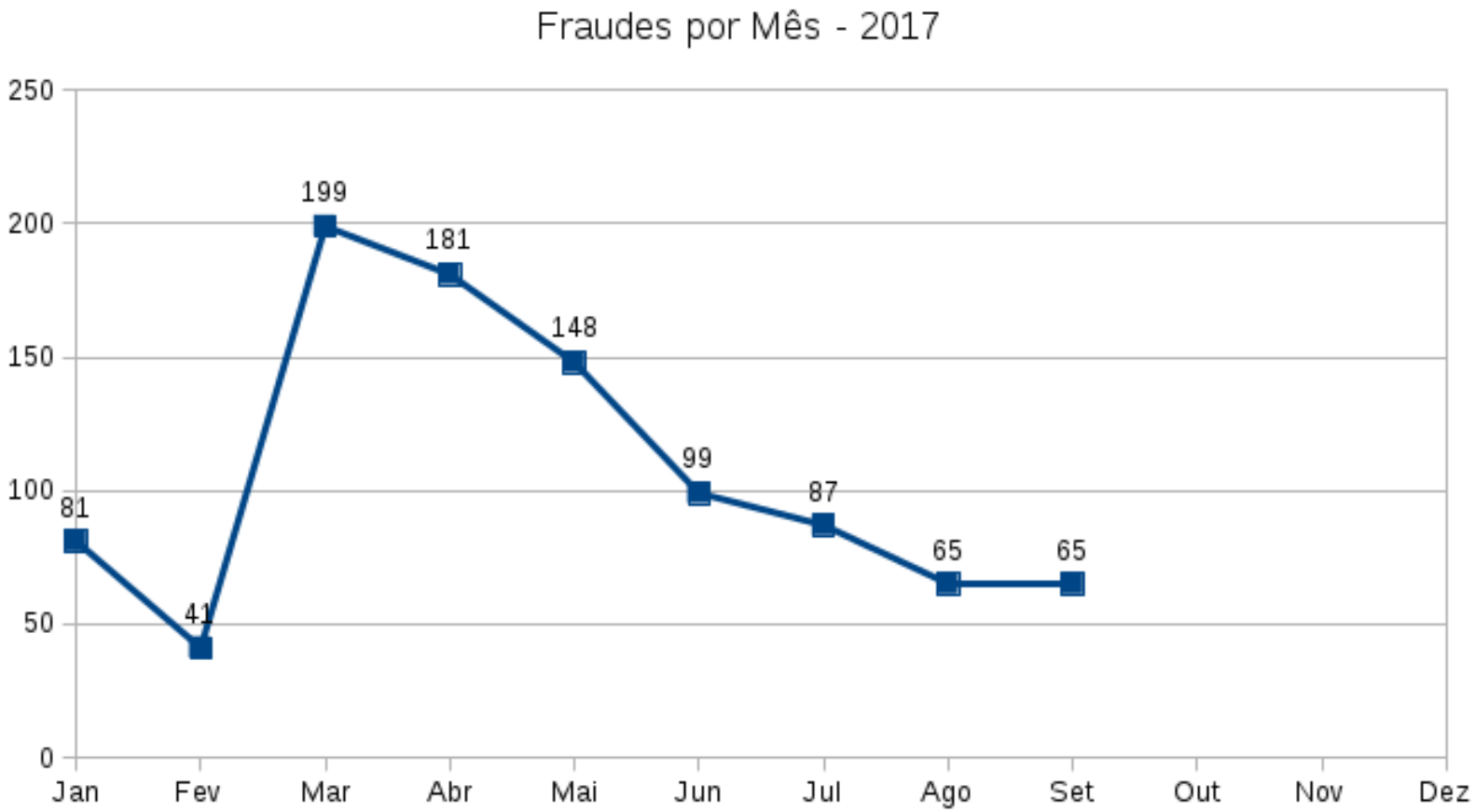
Parcerias

Parceria com o CAIS/RNP

- O CERT.Bahia através de parceria com o CAIS/RNP faz a manutenção do conteúdo do serviço de Catálogo de Fraudes da RNP [1].

[1] https://www.rnp.br/servicos/seguranca/catalogo-fraudes

Parceria com o CAIS/RNP

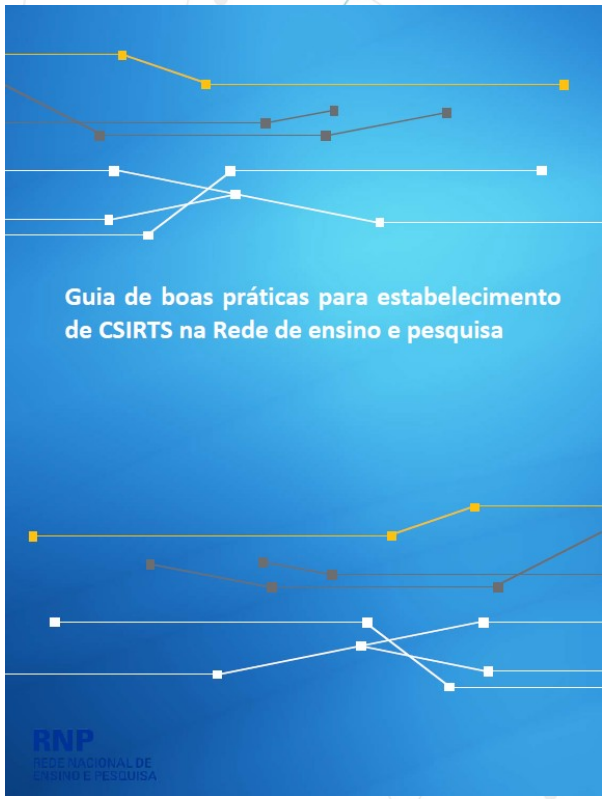


Parceria com o CAIS/RNP

- Publicações sobre o Catálogo de Fraudes:
  - Catálogo de Fraudes da RNP: 7 anos de experiência no tratamento de fraudes eletrônicas brasileiras. ICCyber2015.
  - Catálogo de Fraudes e Catálogo de URLs Maliciosas: Identificação e Combate a Fraudes Eletrônicas na Rede Acadêmica Brasileira. TICAL2016.

Parceria com o CAIS/RNP

- Programa de apoio à organização e criação de equipes de segurança nas instituições clientes da RNP.



Parceria com o CERT.br

- Hospedamos sensores do Projeto de Honeypots Distribuído.

- Somos notificados sobre máquinas que pertencem ao nosso bloco de endereçamento e conectam aos sensores de honeypot distribuídos pelo Brasil.

[1] https://honeytarg.cert.br/honeypots/

Parceria com SaferNet

- SaferNet é uma organização não governamental, sem fins lucrativos, que tem como missão defender e promover os Direitos Humanos na Internet.

- A SaferNet nos apoia na realização do EnSI e com a divulgação de material educativo.

Parceria com Dragon Research Group

- O Dragon Research Group (DRG) é uma organização dedicada ao desenvolvimento de conhecimento e ferramentas para o combate a crimes digitais na Internet.

- O CERT.Bahia hospedava sensores Honeypot do projeto DRG.

Pesquisa e Desenvolvimento

L2M

- O objetivo do L2M [1] é manter um histórico da tabela ARP dos equipamentos.
- Assim é possível manter um registro de associação entre endereços MAC e IPs na rede.

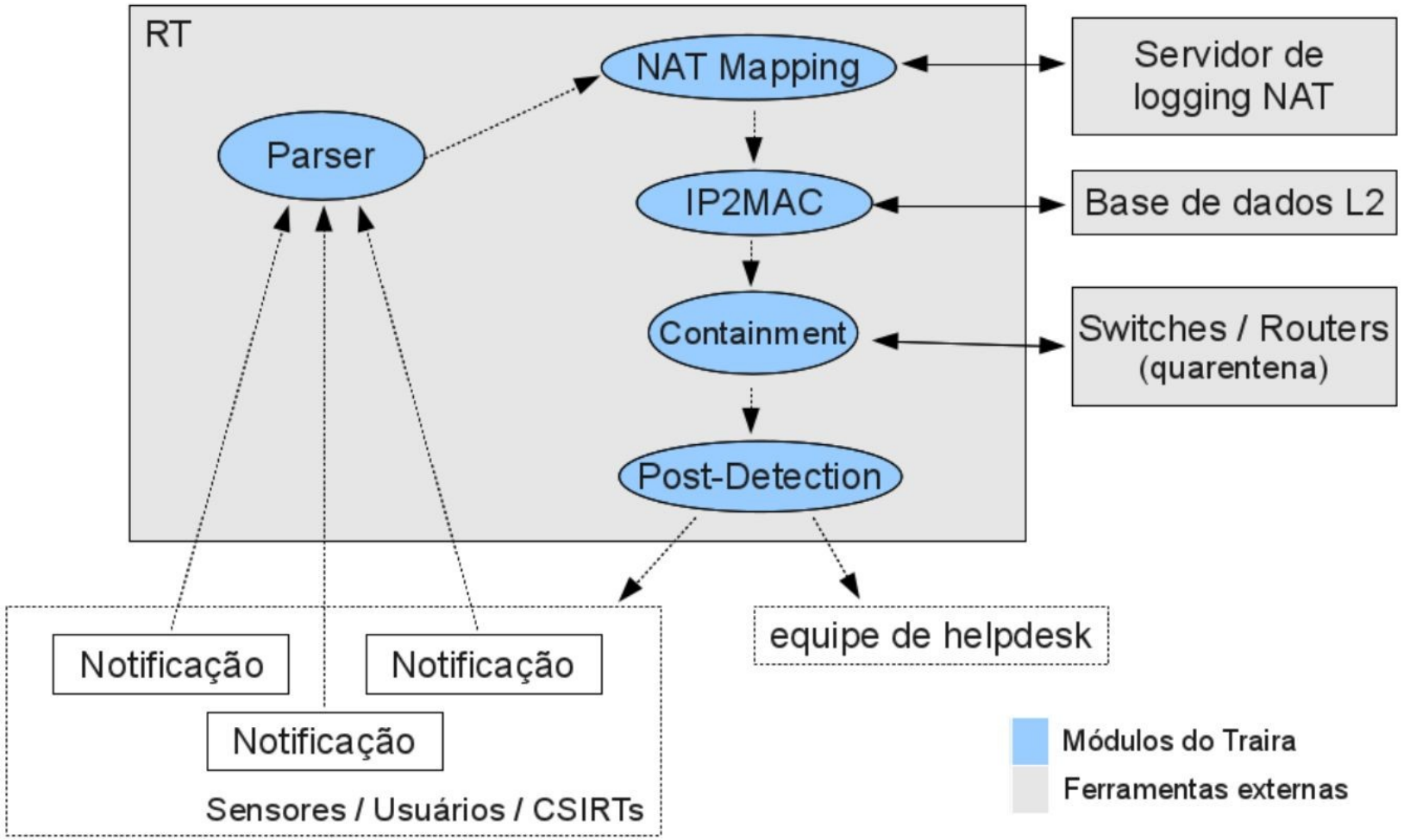
[1] https://certbahia.pop-ba.rnp.br/projects/l2m/

TRAIRA

- O TRAIRA [1] automatiza os procedimentos de detecção, identificação e isolamento dos dispositivos geradores de incidentes de segurança em redes locais.

[1] https://certbahia.pop-ba.rnp.br/projects/traira/

TRAIRA


RT
NAT Mapping
Parser
IP2MAC
Containment
Post-Detection
Servidor de logging NAT
Base de dados L2
Switches / Routers (quarentena)
Notificação
Notificação
Notificação
Sensores / Usuários / CSIRTs
equipe de helpdesk
Módulos do Traira
Ferramentas externas

CaUMa

- O Catálogo de URLs Maliciosas (CaUMa) é uma base de URLs identificadas como maliciosas.
- Permite consultas através de uma interface web ou API.

[1] https://cauma.pop-ba.rnp.br/

CaUMa

- A grande maioria das fraudes contêm links para sites falsos ou arquivos maliciosas, inclusive fraudes propagadas por outros meios como SMS e redes sociais.
- Serviços como Google Safebrowsing e Phishtank tem baixa eficiência contra as fraudes que circulam no Brasil.
- O CaUMa pode ser utilizado como blacklist em browsers e servidores de e-mail.

Ferramenta de Detecção de Atividades Maliciosas

- Desenvolvimento de ferramentas que permita a detecção de atividades maliciosas em redes de alta velocidade.
- Começou como parte do GT-EWS em 2015, atualmente é tocado como um projeto do CERT.Bahia.
- Estamos desenvolvendo ferramentas que utilizam os logs das consultas DNS para detectar servidores de C&C, sites de phishing, arquivos maliciosos, etc.

Testbed de RPKI

- O *Resource Public Key Infrastructure* (RPKI) é um conjunto de protocolos, padrões e sistemas que melhoram a segurança da infraestrutura de roteamento na Internet.
- Estamos construindo um testbed de RPKI para permitir a experimentação e o desenvolvimento de conhecimento sobre essa tecnologia, uma vez que o Registro.br ainda não implementou.

DNmap

- Ferramenta para execução programada e distribuída de scanner com nmap.
- Tem como objetivo diminuir o tempo de execução e facilitar a comparação dos relatórios gerados pelo nmap.
- Status: em desenvolvimento.

OBRIGADO