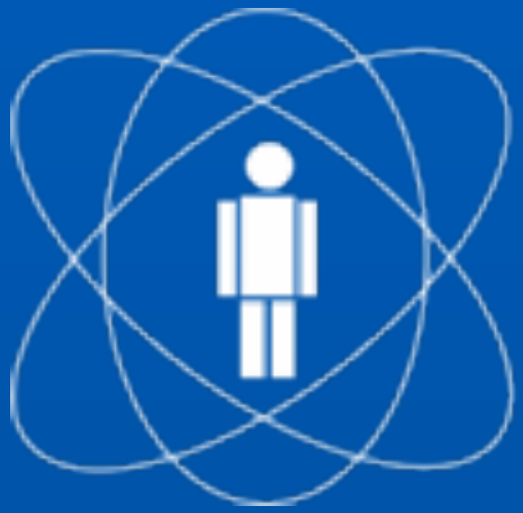


Criando um sistema de reputação

Manoel Domingues Junior (UFRJ)
Marita Maestrelli (CBPF)

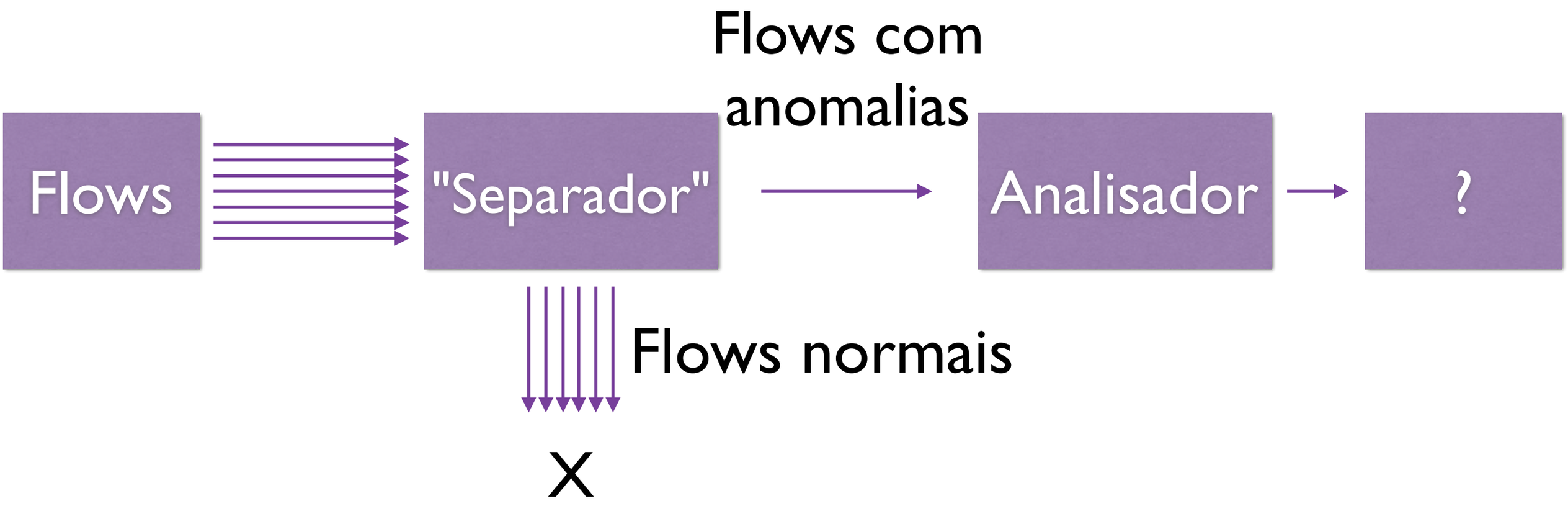
Agenda

- Motivação
- Soluções semelhantes
- Arquitetura de micro-serviços
- Arquitetura da aplicação
- Problemas encontrados
- Interface de administração

Motivação

- Fev/2014
- Detecção de Anomalias através de Netflow
  - Muitos dados
  - Correlação entre eles
  - Escalabilidade

Motivação


Flows com anomalias
Flows
"Separador"
Analisador
?
Flows normais
X

Motivação

Proteção de Perímetro

Proxy Servers

VPNs

NIDS

Firewalls

Anti-SPAM

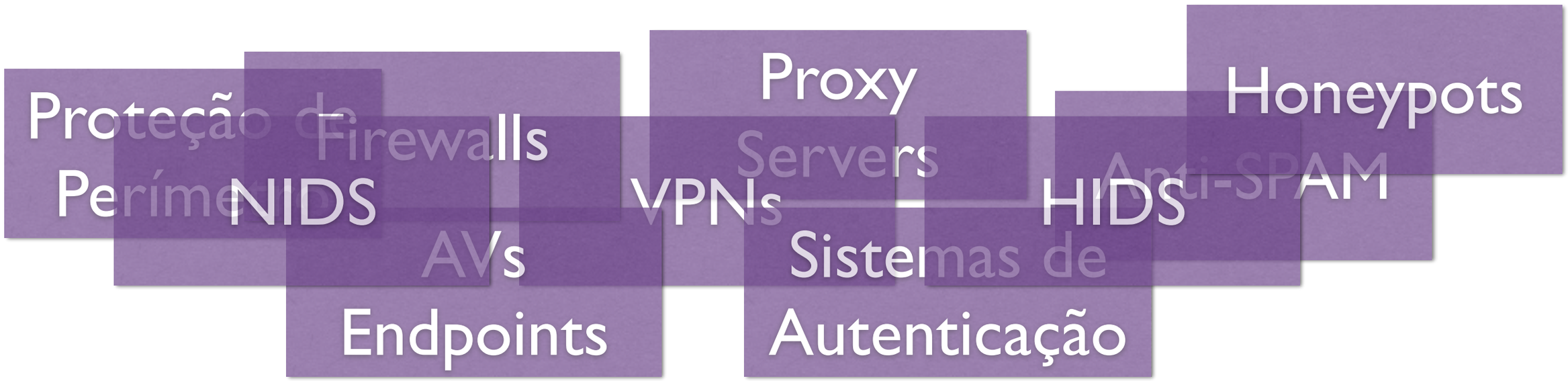
AVs Endpoints

HIDS

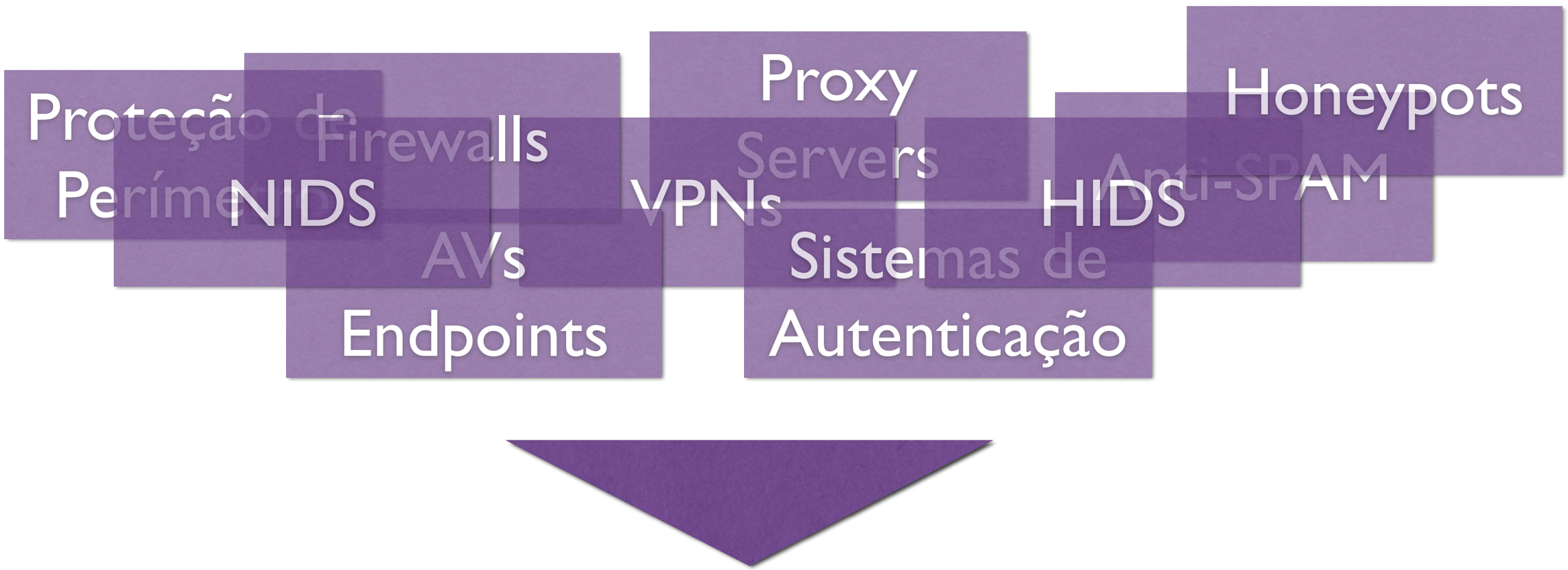
Honeypots

Sistemas de Autenticação

Motivação


Proteção de Perímetro
Firewalls
NIDS
Proxy Servers
VPNs
Honeypots
Anti-SPAM
HIDS
AVs
Endpoints
Sistemas de Autenticação

Motivação


Proteção de Perímetro
Firewalls
NIDS
Proxy Servers
VPNs
Honeypots
Anti-SPAM
HIDS
AVs
Endpoints
Sistemas de Autenticação
Log Server

Motivação

- Fev/2014
- Detecção de Anomalias através de Netflow
  - Muitos dados
  - Correlação entre eles
  - Escalabilidade
- **Padrão: Não auxilia a tomada de decisão**

Motivação

Proteção de Perímetro

Proxy Servers

VPNs

NIDS

Firewalls

Anti-SPAM

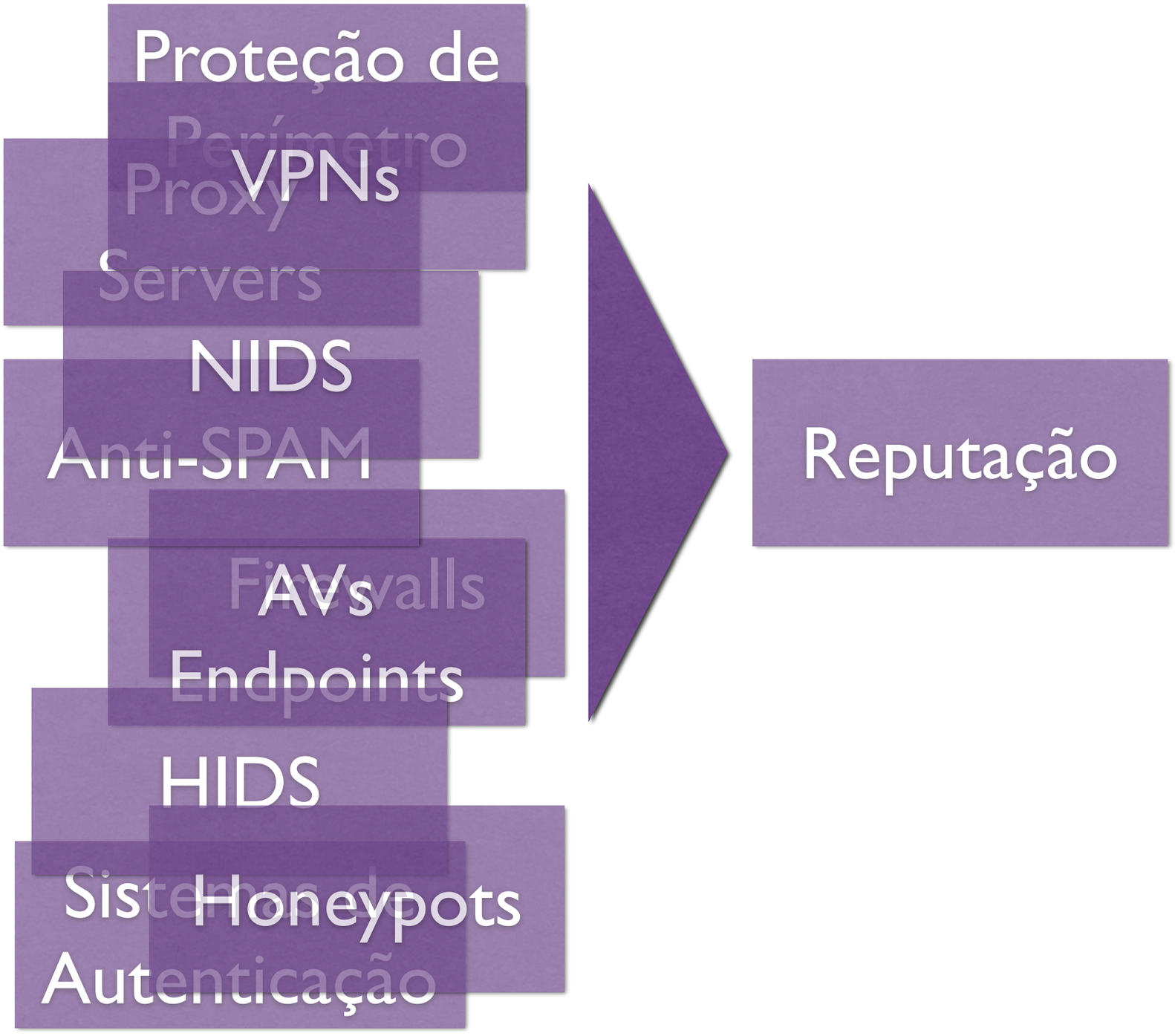
AVs Endpoints

HIDS

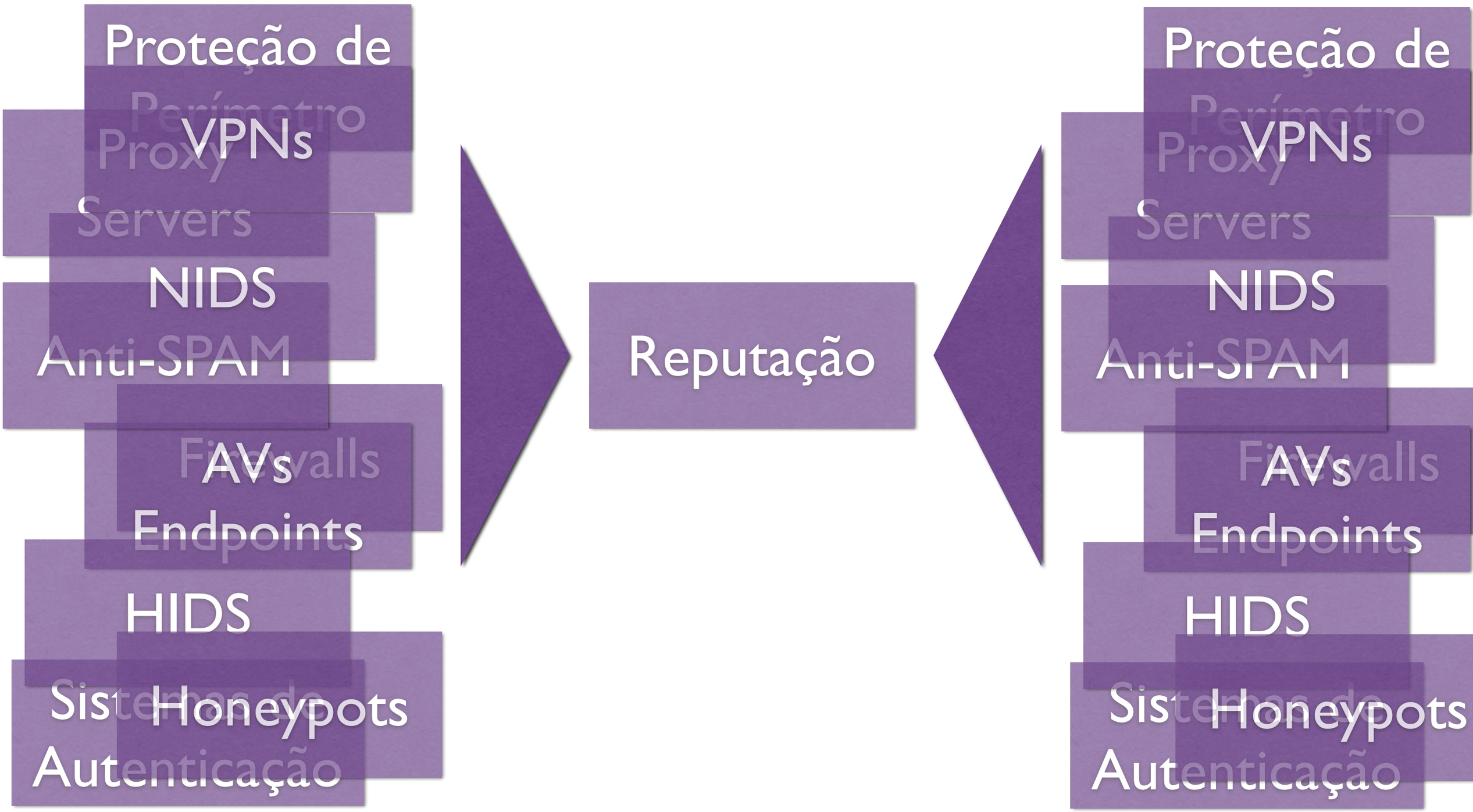
Honeypots

Sistemas de Autenticação

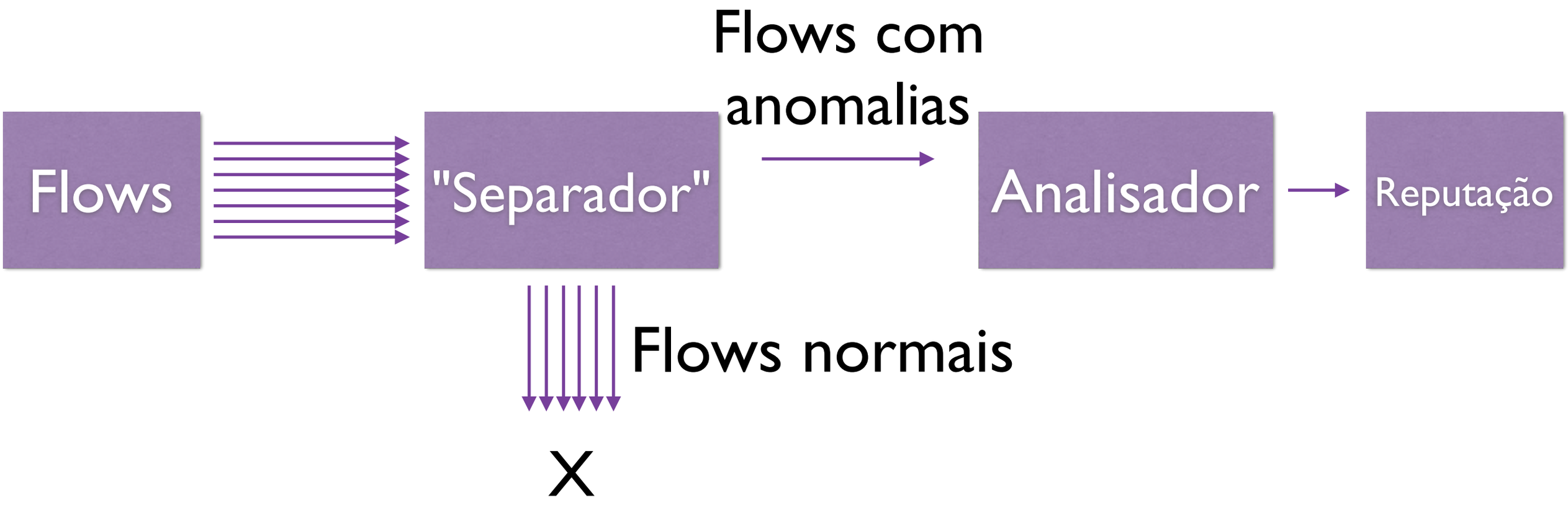
Motivação


Proteção de Perímetro
VPNs
Proxy Servers
NIDS
Anti-SPAM
Firewalls
AVs
Endpoints
HIDS
Sistemas de Autenticação
Honeypots
Reputação

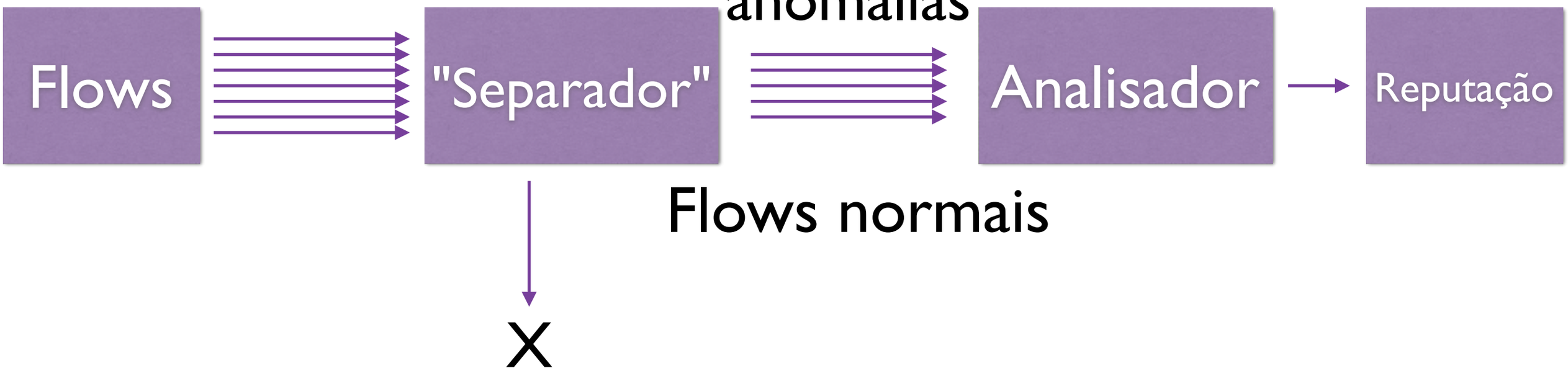
Motivação


Proteção de Perímetro
VPNs
Proxy Servers
NIDS
Anti-SPAM
Firewalls
AVs Endpoints
HIDS
Honeypots
Sistemas de Autenticação
Reputação
Proteção de Perímetro
VPNs
Proxy Servers
NIDS
Anti-SPAM
Firewalls
AVs Endpoints
HIDS
Honeypots
Sistemas de Autenticação

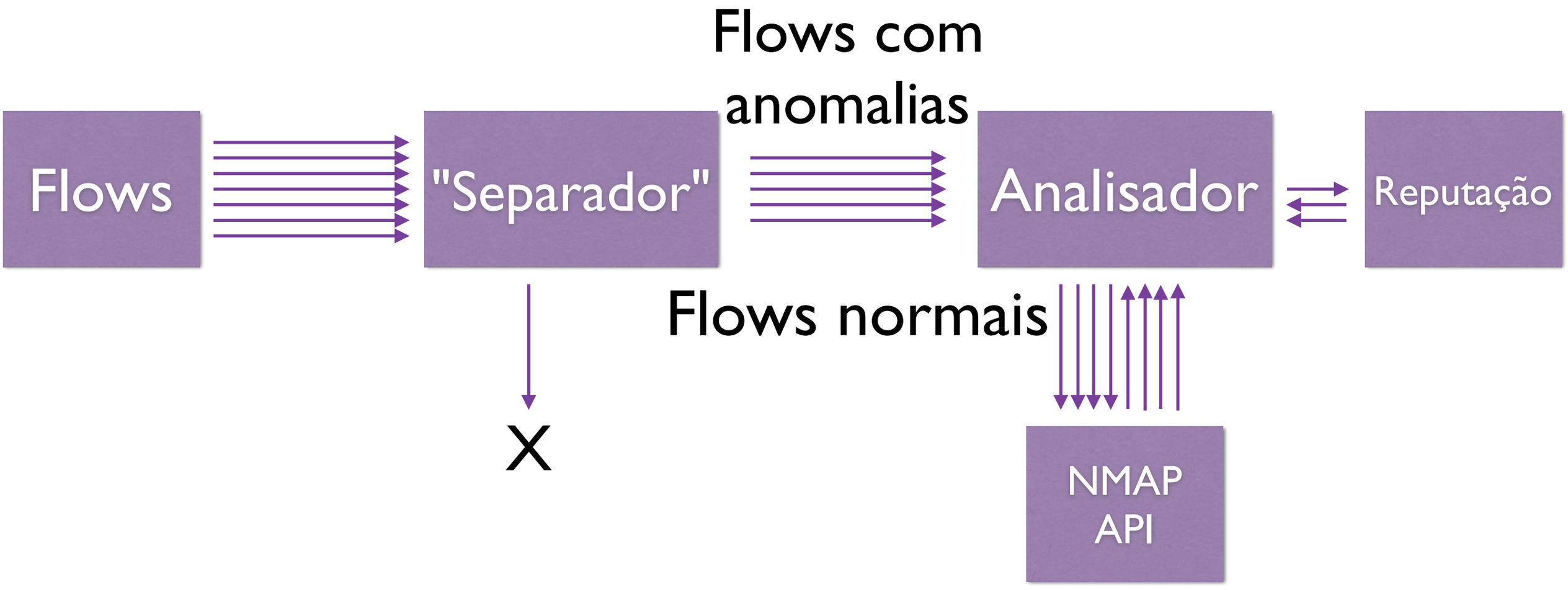
Motivação


Flows com anomalias
Flows
"Separador"
Analisador
Reputação
Flows normais
X

Motivação


Flows com anomalias
Flows
"Separador"
Analisador
Reputação
Flows normais
X

Motivação


Flows com anomalias
Flows
"Separador"
Analisador
Reputação
Flows normais
X
NMAP API

Soluções Semelhantes

- Critical Stack (Feeds)
- ThreatExchange (Graph)
- CIF (Feeds)

Arquitetura em Micro-serviços

- Monolítico vs. Micro-serviço

Arquitetura em Micro-serviços

- Monolítico vs. Micro-serviço
- Monolítico: um sistema que faz tudo
  - Se um componente falha, o funcionamento do sistema é comprometido
  - Maior complexidade para manutenção

Arquitetura em Micro-serviços

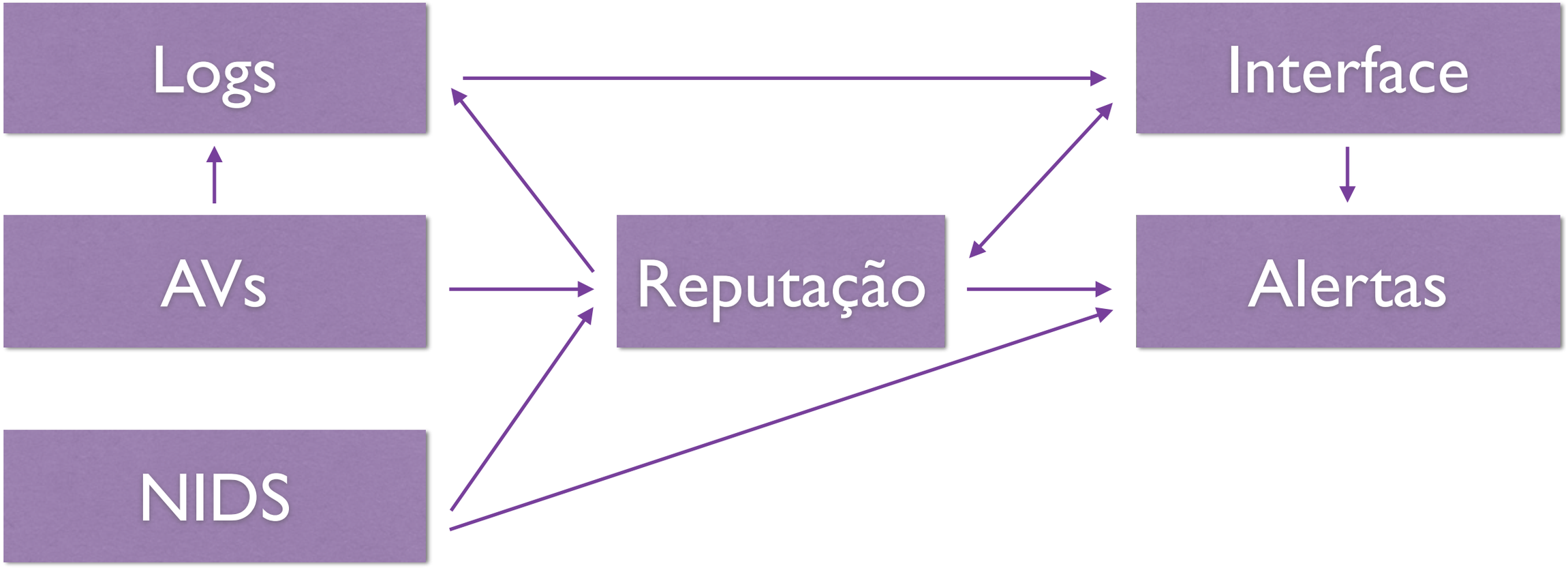
- Monolítico vs. Micro-serviço
- Monolítico: um sistema que faz tudo

Arquitetura em Micro-serviços

- Monolítico vs. Micro-serviço
- Micro-serviço: um sistema especialista
  - Os sistema completo é composto de vários componentes
  - Cada componente é independente, mas usa padrões para se comunicar com os outros componentes
  - Se um componente falha, só uma parte do sistema fica indisponível

Arquitetura em Micro-serviços

- Monolítico vs. Micro-serviço
- Micro-serviço: um sistema especialista



Arquitetura da aplicação

- Pontos importantes:
  - Vários outros sistemas consultando informações
  - Diferentes tipos de dados sendo inseridos
  - Necessidade de recuperar os eventos já tratados e evitar duplicações

Arquitetura da aplicação

- Pontos importantes:
  - Vários outros sistemas consultando informações
    - Guardar informações na memória
  - Diferentes tipos de dados sendo inseridos
  - Necessidade de recuperar os eventos já tratados e evitar duplicações

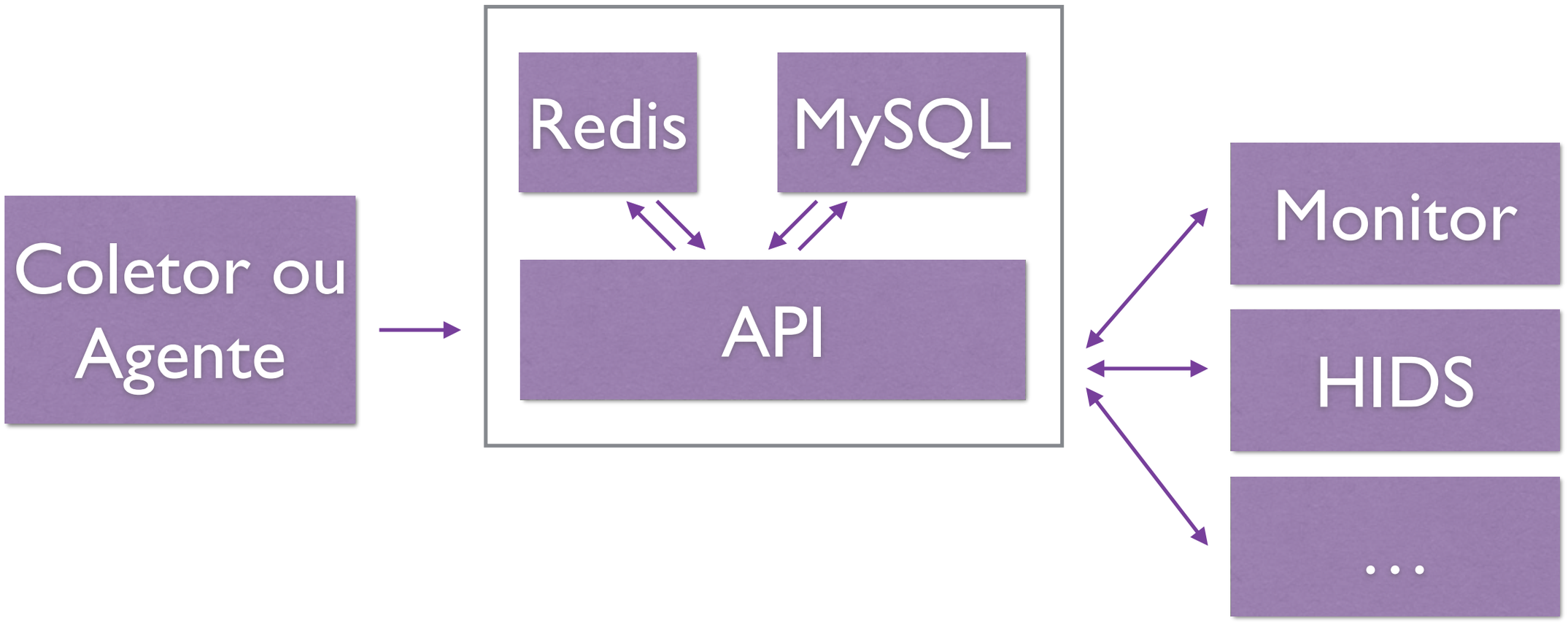
Arquitetura da aplicação

- Pontos importantes:
  - Vários outros sistemas consultando informações
    - Guardar dados na memória
  - Diferentes tipos de dados sendo inseridos
    - Categorização
  - Necessidade de recuperar os eventos já tratados e evitar duplicações

Arquitetura da aplicação

- Pontos importantes:
  - Vários outros sistemas consultando informações
    - Guardar dados na memória
  - Diferentes tipos de dados sendo inseridos
    - Categorização
  - Necessidade de recuperar os eventos já tratados e evitar duplicações
    - Envio dos eventos, mas categorizarão externa

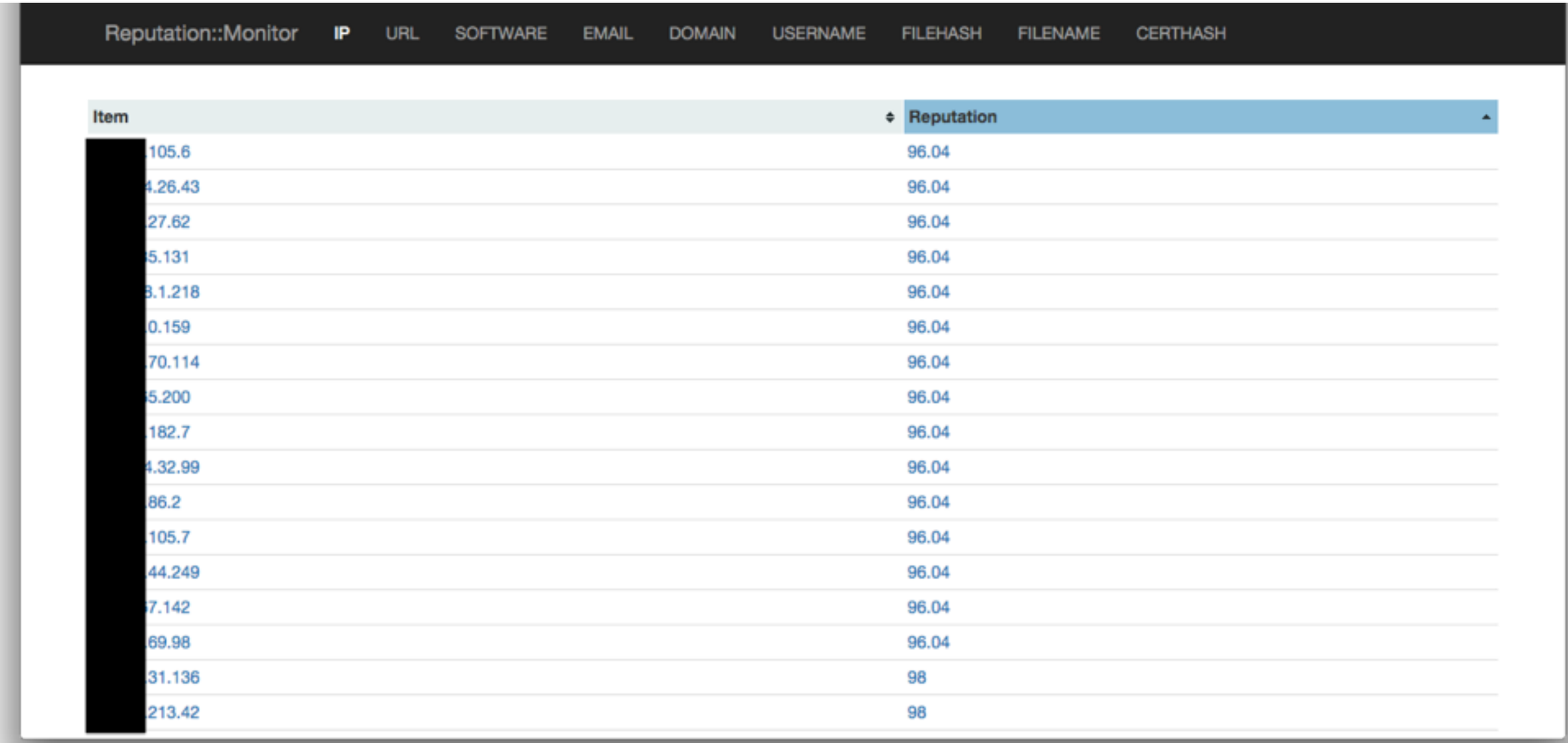
Arquitetura da aplicação



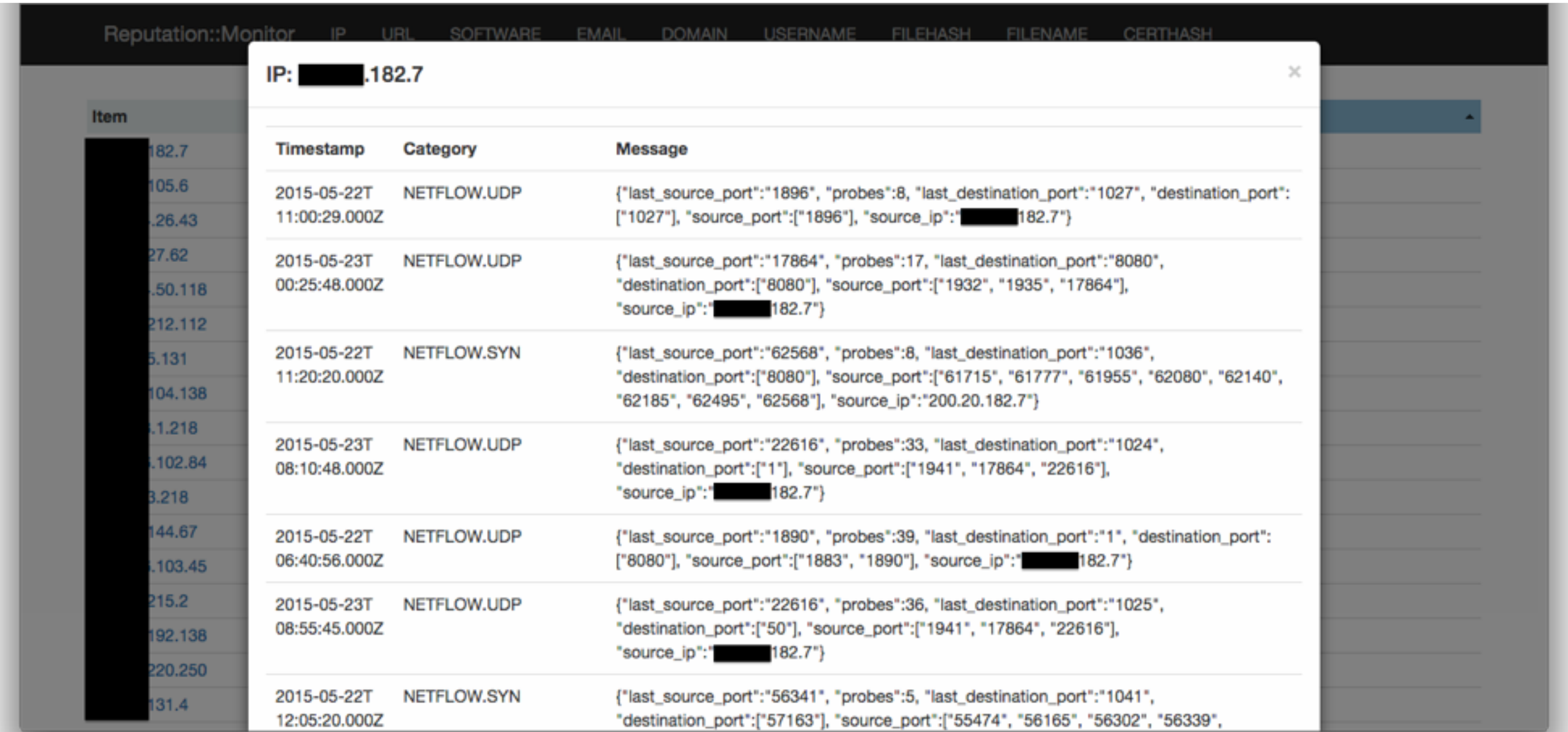
Problemas encontrados

- Reputação incremental
- Eventos maliciosos, suspeitos e confiáveis
- Reputação eterna
- Identificação única dos eventos
- Alterações de reputação

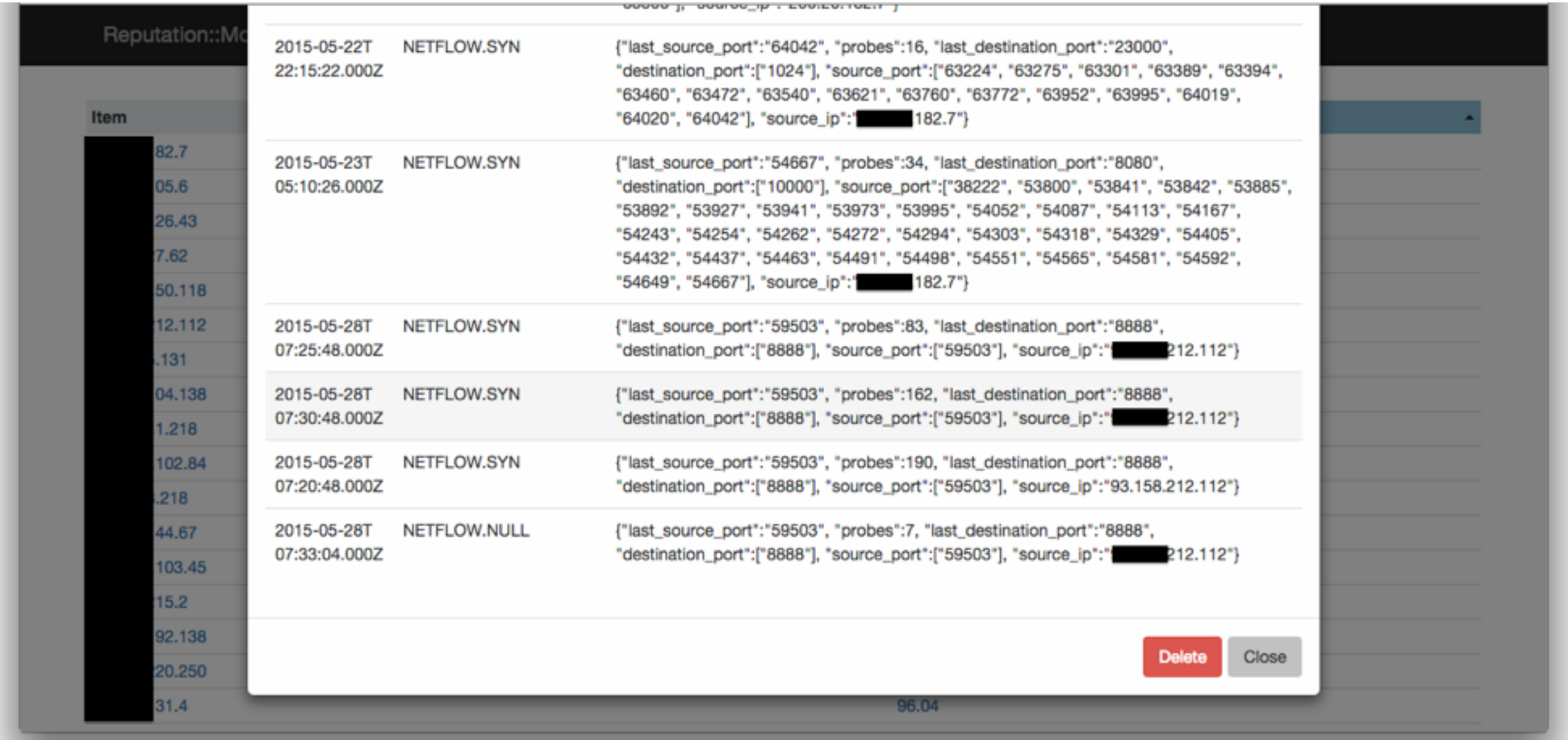
Interface de administração



Interface de administração



Interface de administração



NMAP API - Dados


```
    status: "up",
    mac_addr: null,
  - data: [
      - {
            proto: "tcp",
            rpc: null,
            version: null,
            fingerprint: null,
            service: "vnc",
            port: "5900",
          - additional_info: {
              - banner: {
                    output: "RFB 003.007"
                }
            },
            product: "VNC"
        },
      - {
            proto: "tcp",
            rpc: null,
            version: "5.5p1 Debian 6+squeeze3",
            fingerprint: null,
            service: "ssh",
            port: "6000",
          - additional_info: {
              - banner: {
                    output: "SSH-2.0-OpenSSH_5.5p1 Debian-6+squeeze3"
                },
              - ssh-hostkey: {
                    output: "1024 3f:90:08:c4:83:a7:5f:c0:ba:4d:6d:a2:d0:53:85:d2 (DSA) 2048
                    3f:a6:01:1e:48:13:ec:a9:d2:b0:cf:ec:ae:41:19:7d (RSA)"
                }
            },
            product: "OpenSSH"
```

API de Reputação - 1.0


```
{
  - itens: [
      - {
            created: 1391732329,
            detection: "darknet",
            ip: "[redacted]93.67",
            status: "malicious",
            report_time: 1393637234,
          - _id: {
                $oid: "52f42669fae403557d000054"
            },
            counter: 2869524
        },
      - {
            created: 1391892327,
            detection: "darknet",
            ip: "[redacted]93.51",
            status: "malicious",
            report_time: 1393834176,
          - _id: {
                $oid: "52f69767fae403460e0000cb"
            },
            counter: 2224569
        },
      - {
            created: 1397661633,
            detection: "darknet",
            ip: "[redacted]173.11",
            status: "malicious",
            report_time: 1399314902,
          - _id: {
                $oid: "534e9fc10d16084b2e000000"
```

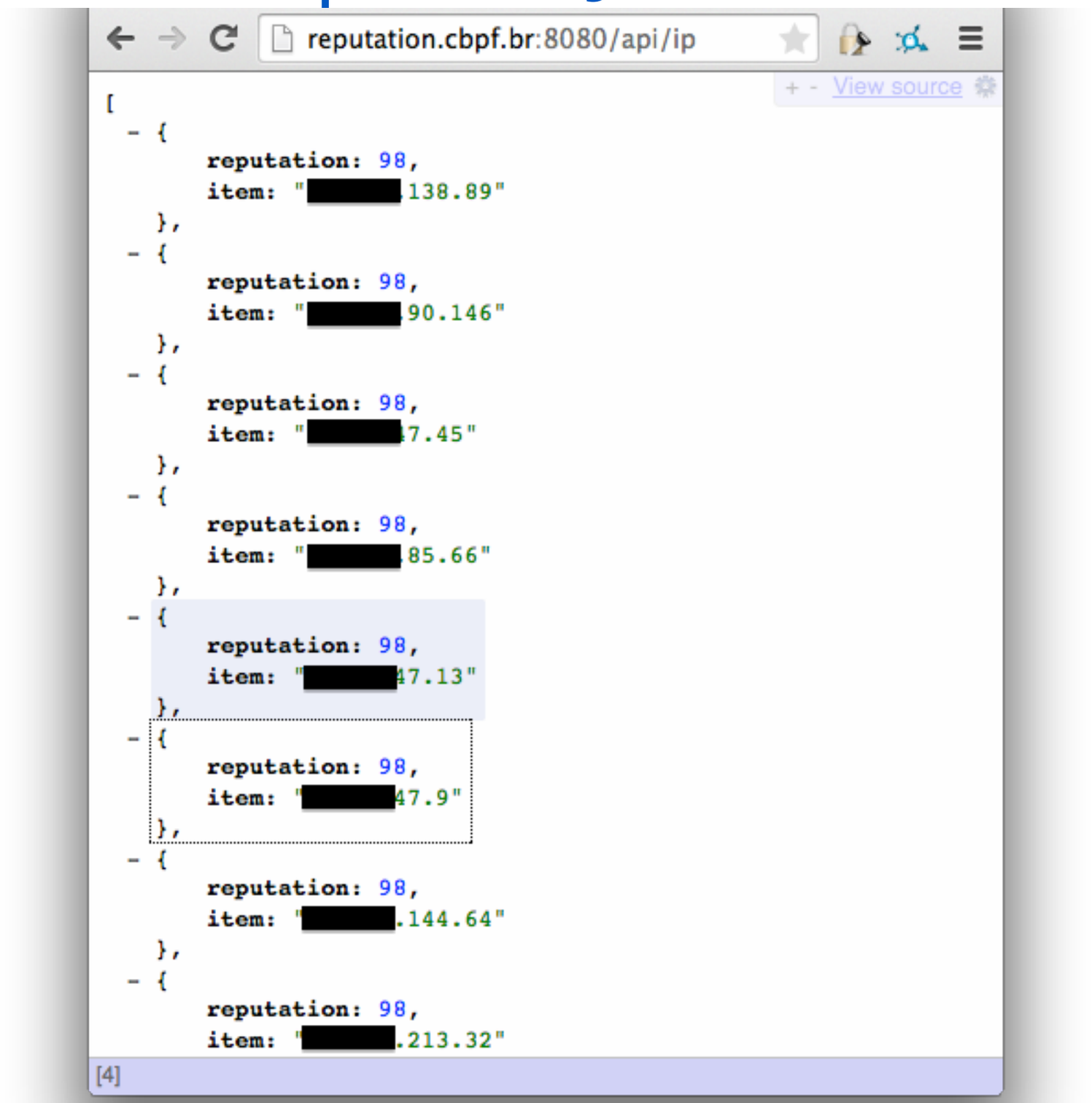
API de Reputação - 2.0

API de Reputação - 2.0

reputation.cbpf.br:8080/api/events/ip/[redacted]104.138


```
[
  - {
      msg: "{"last_source_port":"36877","probes":7,"last_destination_port":"23","destination_port":["110"],"source_port":
      ["6861","26977","36877"],"source_ip":"[redacted]104.138"}",
      timestamp: "1432207216",
      item: "[redacted]104.138",
      category: "NETFLOW.SYN",
      collection: "ip",
      id: "3339",
      log_id: "ip58bf28fe93b59609e48c00d05f50d3b4"
    },
  - {
      msg: "{"last_source_port":"40540","probes":5,"last_destination_port":"3306","destination_port":["110"],"source_port":
      ["6861","26977","40540"],"source_ip":"[redacted]104.138"}",
      timestamp: "1432194016",
      item: "[redacted]104.138",
      category: "NETFLOW.SYN",
      collection: "ip",
      id: "1410",
      log_id: "ipa36e973ef677a67bf73b673dd71db23e"
    },
  - {
      msg: "{"last_source_port":"40540","probes":7,"last_destination_port":"3306","destination_port":["110"],"source_port":
      ["6861","26977","37079","40540"],"source_ip":"[redacted]104.138"}",
      timestamp: "1432194316",
      item: "[redacted]104.138",
      category: "NETFLOW.SYN",
      collection: "ip",
      id: "1481",
      log_id: "ip4b8d9ea5effd9323408a66cf9f9db5d0"
    },
  - {
      msg: "{"last_source_port":"40540","probes":15,"last_destination_port":"3306","destination_port":["143"],"source_port":
      ["26977","36877","37079","40540"],"source_ip":"[redacted]104.138"}",
      timestamp: "1432308022",
[3]
```

API de Reputação - 2.0



Onde encontrar?

- https://github.com/mdjunior/reputation-api
- https://github.com/mdjunior/reputation-monitor

- https://github.com/mdjunior/fail2ban
- https://github.com/mdjunior/anomalia-reputation-api

- https://github.com/mdjunior/nmap-api
- https://github.com/mdjunior/flow-collector

Perguntas?

manoel@cbpf.br

Obrigado