

Criando um sistema de reputação

Manoel Domingues Junior (UFRJ)
Marita Maestrelli (CBPF)

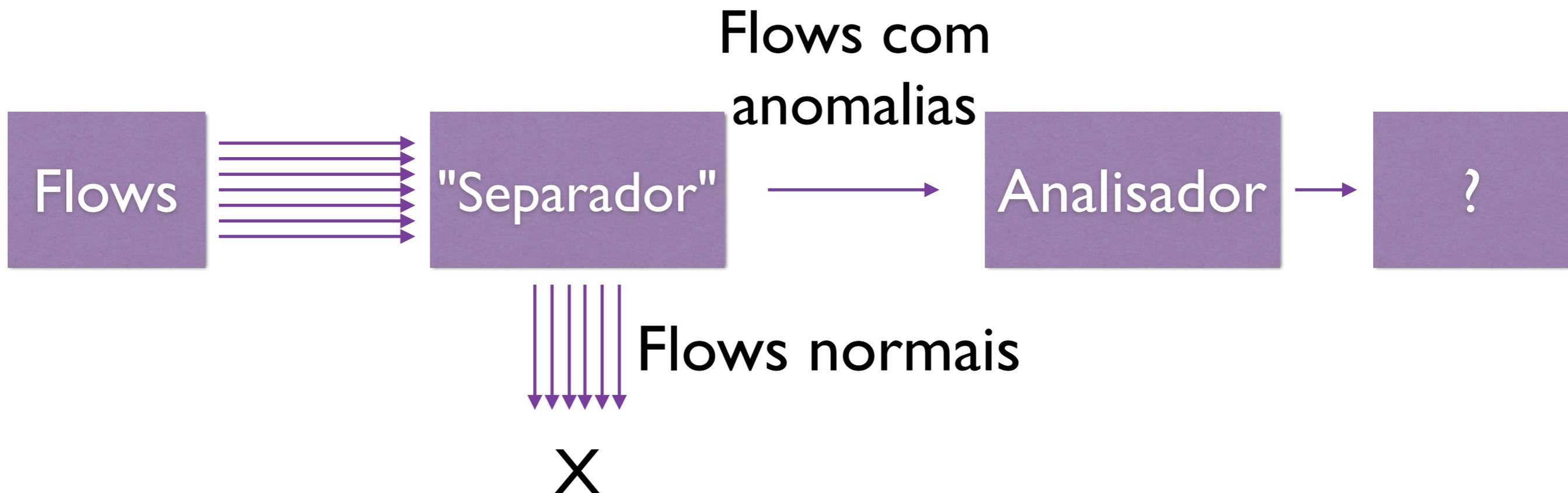
Agenda

- ▶ 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



Motivação

Proteção de
Perímetro

Proxy
Servers

VPNs

NIDS

Firewalls

Anti-SPAM

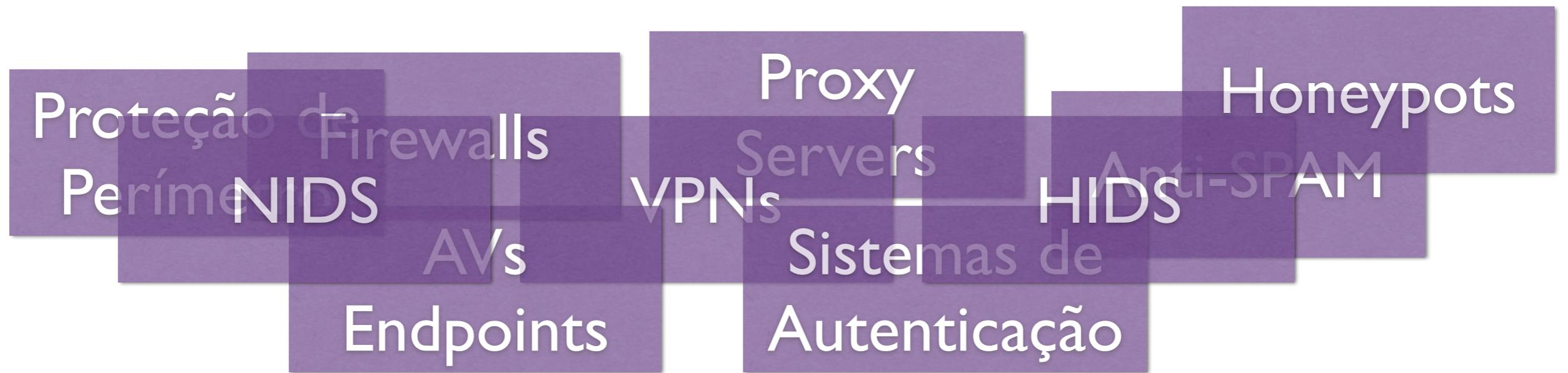
AVs
Endpoints

HIDS

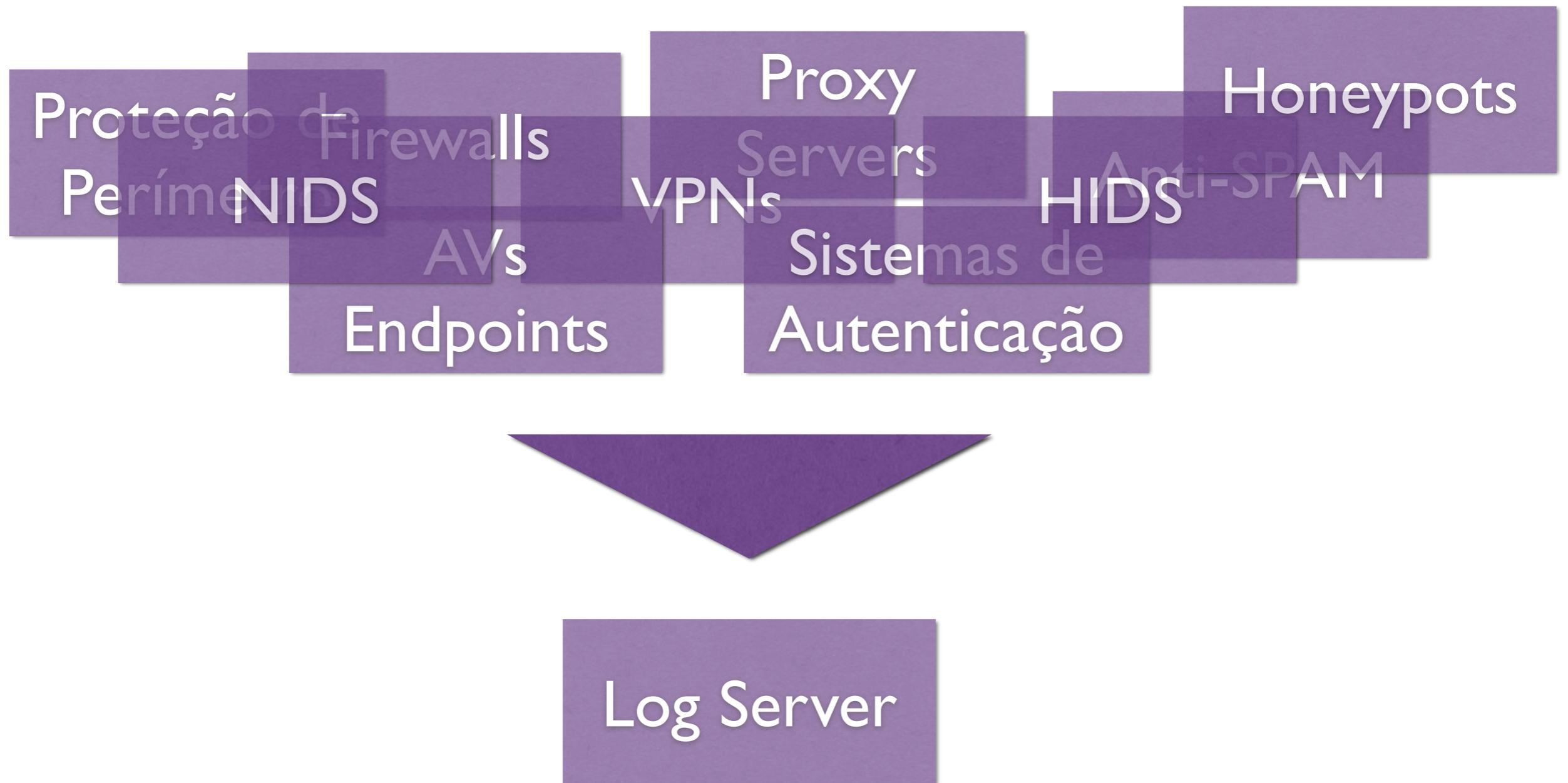
Honeypots

Sistemas de
Autenticação

Motivação



Motivação



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

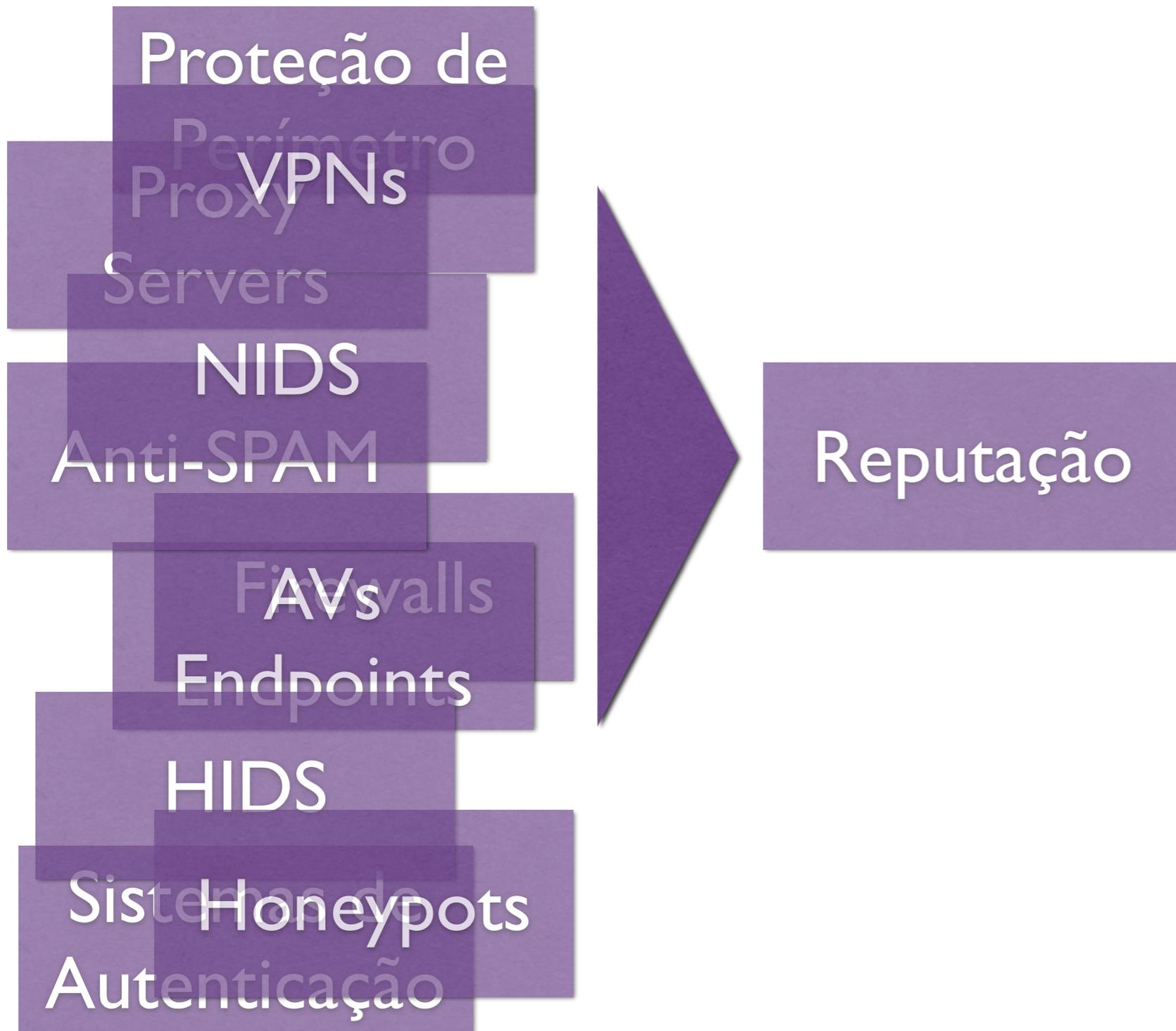
AVs
Endpoints

HIDS

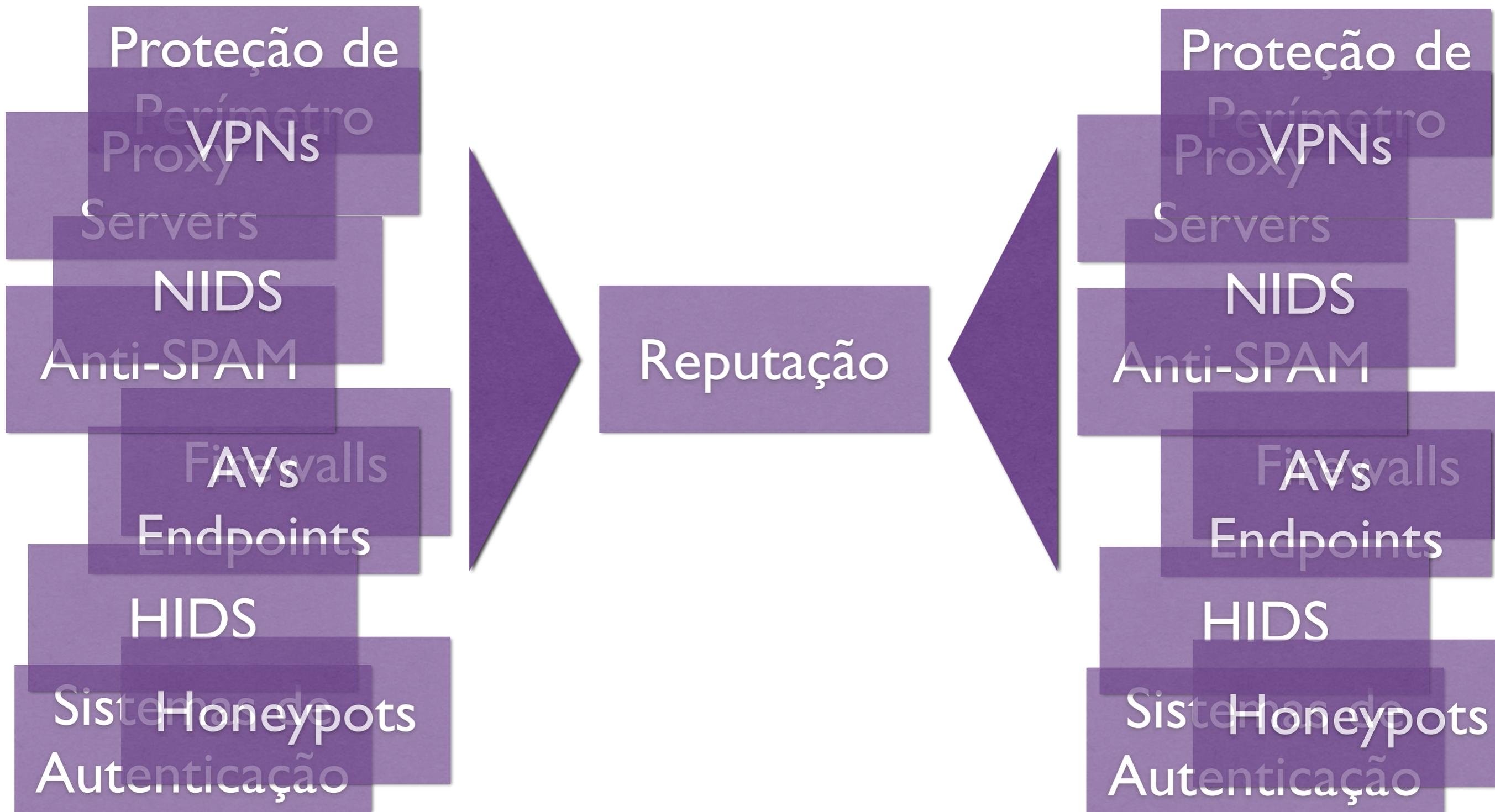
Honeypots

Sistemas de
Autenticação

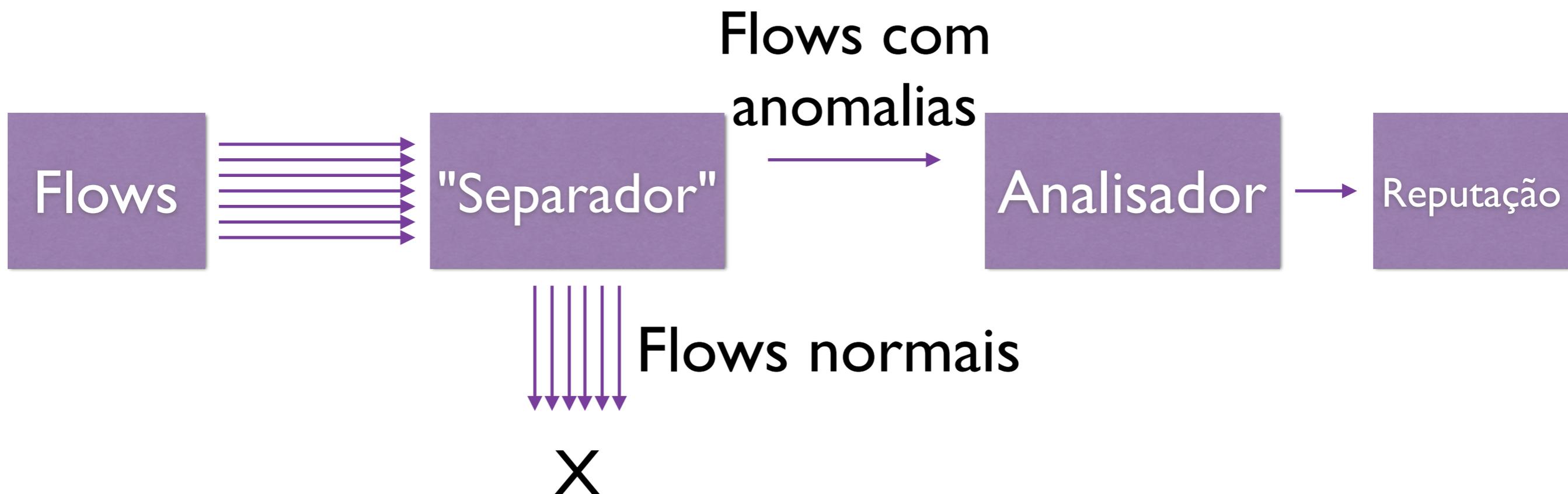
Motivação



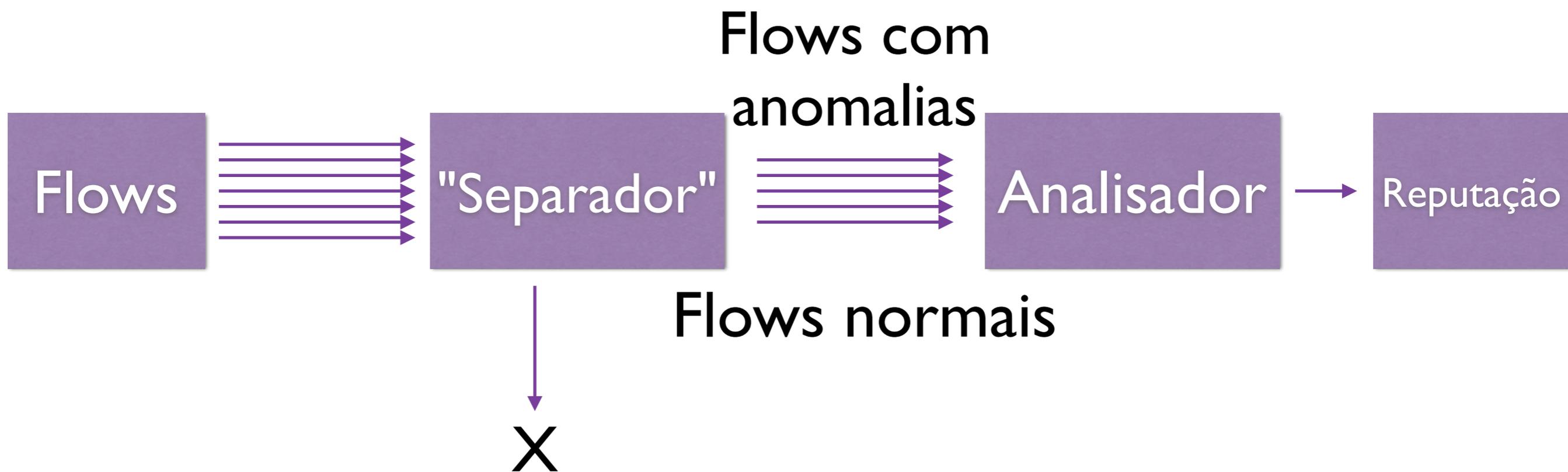
Motivação



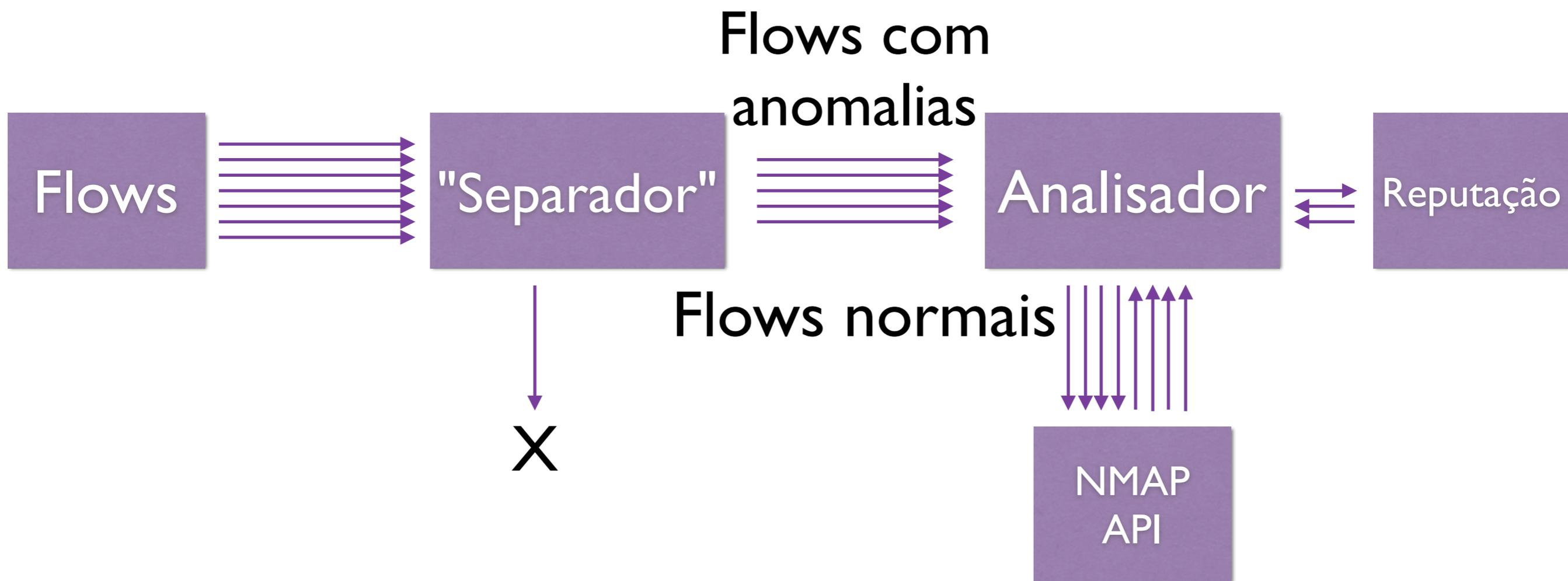
Motivação



Motivação



Motivação



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

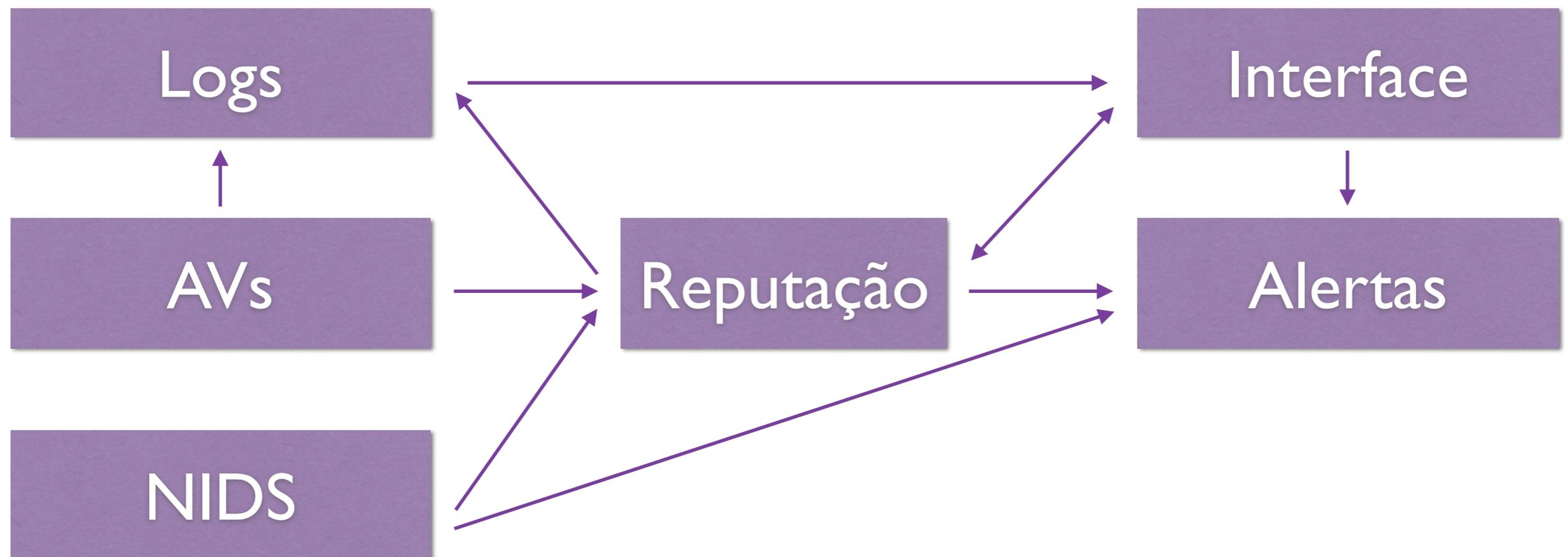


Arquitetura em Micro-serviços

- ▶ 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

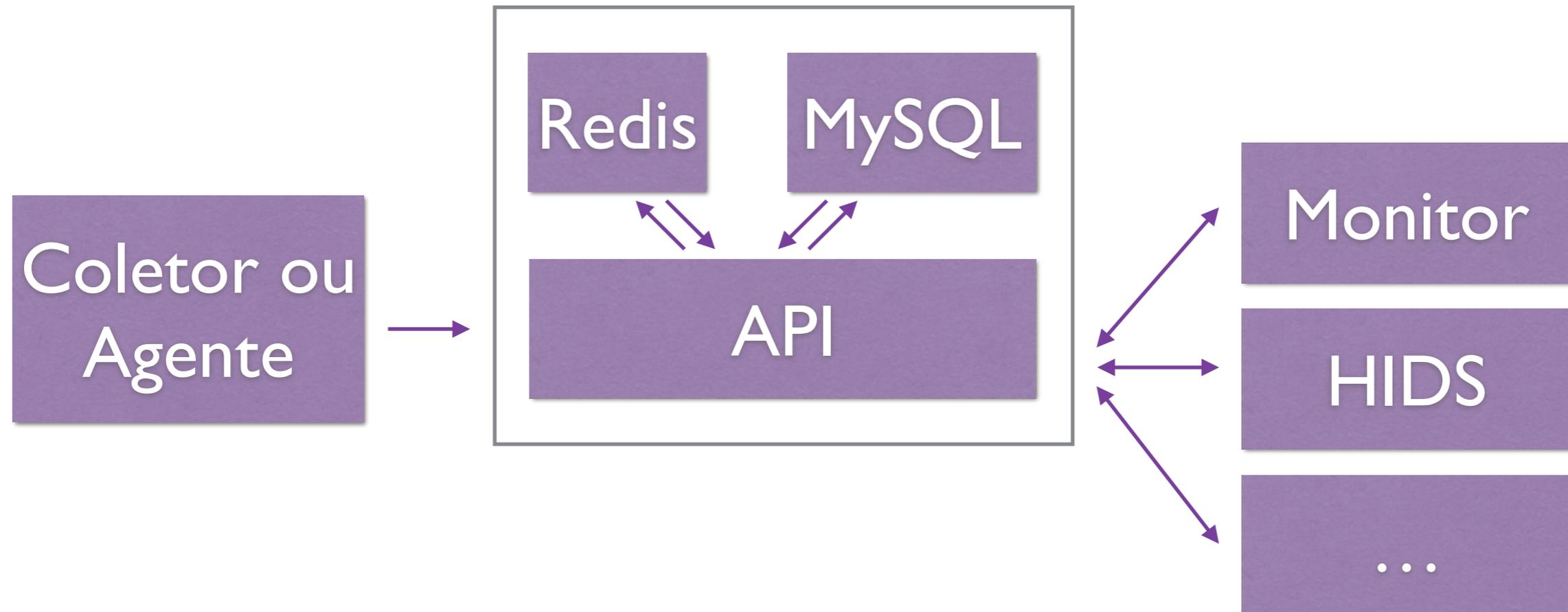
Arquitetura da aplicação

- ▶ 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

Reputation::Monitor	IP	URL	SOFTWARE	EMAIL	DOMAIN	USERNAME	FILEHASH	FILENAME	CERTHASH
Item	Reputation								
[REDACTED] 105.6	96.04								
[REDACTED] 4.26.43	96.04								
[REDACTED] 27.62	96.04								
[REDACTED] 5.131	96.04								
[REDACTED] 3.1.218	96.04								
[REDACTED] 0.159	96.04								
[REDACTED] 70.114	96.04								
[REDACTED] 5.200	96.04								
[REDACTED] 182.7	96.04								
[REDACTED] 4.32.99	96.04								
[REDACTED] 86.2	96.04								
[REDACTED] 105.7	96.04								
[REDACTED] 44.249	96.04								
[REDACTED] 7.142	96.04								
[REDACTED] 69.98	96.04								
[REDACTED] 31.136	98								
[REDACTED] 213.42	98								

Interface de administração

Reputation::Monitor IP URL SOFTWARE EMAIL DOMAIN USERNAME FILEHASH FILENAME CERTHASH

Item

Item	IP
182.7	[REDACTED].182.7
105.6	[REDACTED].105.6
26.43	[REDACTED].26.43
27.62	[REDACTED].27.62
50.118	[REDACTED].50.118
212.112	[REDACTED].212.112
5.131	[REDACTED].5.131
104.138	[REDACTED].104.138
1.218	[REDACTED].1.218
102.84	[REDACTED].102.84
3.218	[REDACTED].3.218
144.67	[REDACTED].144.67
103.45	[REDACTED].103.45
215.2	[REDACTED].215.2
192.138	[REDACTED].192.138
220.250	[REDACTED].220.250
131.4	[REDACTED].131.4

IP: [REDACTED].182.7

Timestamp	Category	Message
2015-05-22T 11:00:29.000Z	NETFLOW.UDP	{"last_source_port": "1896", "probes": 8, "last_destination_port": "1027", "destination_port": ["1027"], "source_port": ["1896"], "source_ip": "[REDACTED].182.7"}
2015-05-23T 00:25:48.000Z	NETFLOW.UDP	{"last_source_port": "17864", "probes": 17, "last_destination_port": "8080", "destination_port": ["8080"], "source_port": ["1932", "1935", "17864"], "source_ip": "[REDACTED].182.7"}
2015-05-22T 11:20:20.000Z	NETFLOW.SYN	{"last_source_port": "62568", "probes": 8, "last_destination_port": "1036", "destination_port": ["8080"], "source_port": ["61715", "61777", "61955", "62080", "62140", "62185", "62495", "62568"], "source_ip": "200.20.182.7"}
2015-05-23T 08:10:48.000Z	NETFLOW.UDP	{"last_source_port": "22616", "probes": 33, "last_destination_port": "1024", "destination_port": ["1"], "source_port": ["1941", "17864", "22616"], "source_ip": "[REDACTED].182.7"}
2015-05-22T 06:40:56.000Z	NETFLOW.UDP	{"last_source_port": "1890", "probes": 39, "last_destination_port": "1", "destination_port": ["8080"], "source_port": ["1883", "1890"], "source_ip": "[REDACTED].182.7"}
2015-05-23T 08:55:45.000Z	NETFLOW.UDP	{"last_source_port": "22616", "probes": 36, "last_destination_port": "1025", "destination_port": ["50"], "source_port": ["1941", "17864", "22616"], "source_ip": "[REDACTED].182.7"}
2015-05-22T 12:05:20.000Z	NETFLOW.SYN	{"last_source_port": "56341", "probes": 5, "last_destination_port": "1041", "destination_port": ["57163"], "source_port": ["55474", "56165", "56302", "56339"], "source_ip": "[REDACTED].182.7"}

Interface de administração

The screenshot displays an administration interface. On the left, a sidebar titled 'Reputation:Mc' contains a list of items with numerical values. The main area shows a detailed view of a specific record.

Item	Value
[Redacted]	82.7
[Redacted]	05.6
[Redacted]	26.43
[Redacted]	7.62
[Redacted]	50.118
[Redacted]	12.112
[Redacted]	.131
[Redacted]	04.138
[Redacted]	1.218
[Redacted]	102.84
[Redacted]	.218
[Redacted]	44.67
[Redacted]	103.45
[Redacted]	15.2
[Redacted]	92.138
[Redacted]	20.250
[Redacted]	31.4

Date	Type	Details
2015-05-22T 22:15:22.000Z	NETFLOW.SYN	{"last_source_port": "64042", "probes": 16, "last_destination_port": "23000", "destination_port": ["1024"], "source_port": ["63224", "63275", "63301", "63389", "63394", "63460", "63472", "63540", "63621", "63760", "63772", "63952", "63995", "64019", "64020", "64042"], "source_ip": "[Redacted] 182.7"}
2015-05-23T 05:10:26.000Z	NETFLOW.SYN	{"last_source_port": "54667", "probes": 34, "last_destination_port": "8080", "destination_port": ["10000"], "source_port": ["38222", "53800", "53841", "53842", "53885", "53892", "53927", "53941", "53973", "53995", "54052", "54087", "54113", "54167", "54243", "54254", "54262", "54272", "54294", "54303", "54318", "54329", "54405", "54432", "54437", "54463", "54491", "54498", "54551", "54565", "54581", "54592", "54649", "54667"], "source_ip": "[Redacted] 182.7"}
2015-05-28T 07:25:48.000Z	NETFLOW.SYN	{"last_source_port": "59503", "probes": 83, "last_destination_port": "8888", "destination_port": ["8888"], "source_port": ["59503"], "source_ip": "[Redacted] 212.112"}
2015-05-28T 07:30:48.000Z	NETFLOW.SYN	{"last_source_port": "59503", "probes": 162, "last_destination_port": "8888", "destination_port": ["8888"], "source_port": ["59503"], "source_ip": "[Redacted] 212.112"}
2015-05-28T 07:20:48.000Z	NETFLOW.SYN	{"last_source_port": "59503", "probes": 190, "last_destination_port": "8888", "destination_port": ["8888"], "source_port": ["59503"], "source_ip": "93.158.212.112"}
2015-05-28T 07:33:04.000Z	NETFLOW.NULL	{"last_source_port": "59503", "probes": 7, "last_destination_port": "8888", "destination_port": ["8888"], "source_port": ["59503"], "source_ip": "[Redacted] 212.112"}

Buttons: Delete, Close

Page number: 96.04

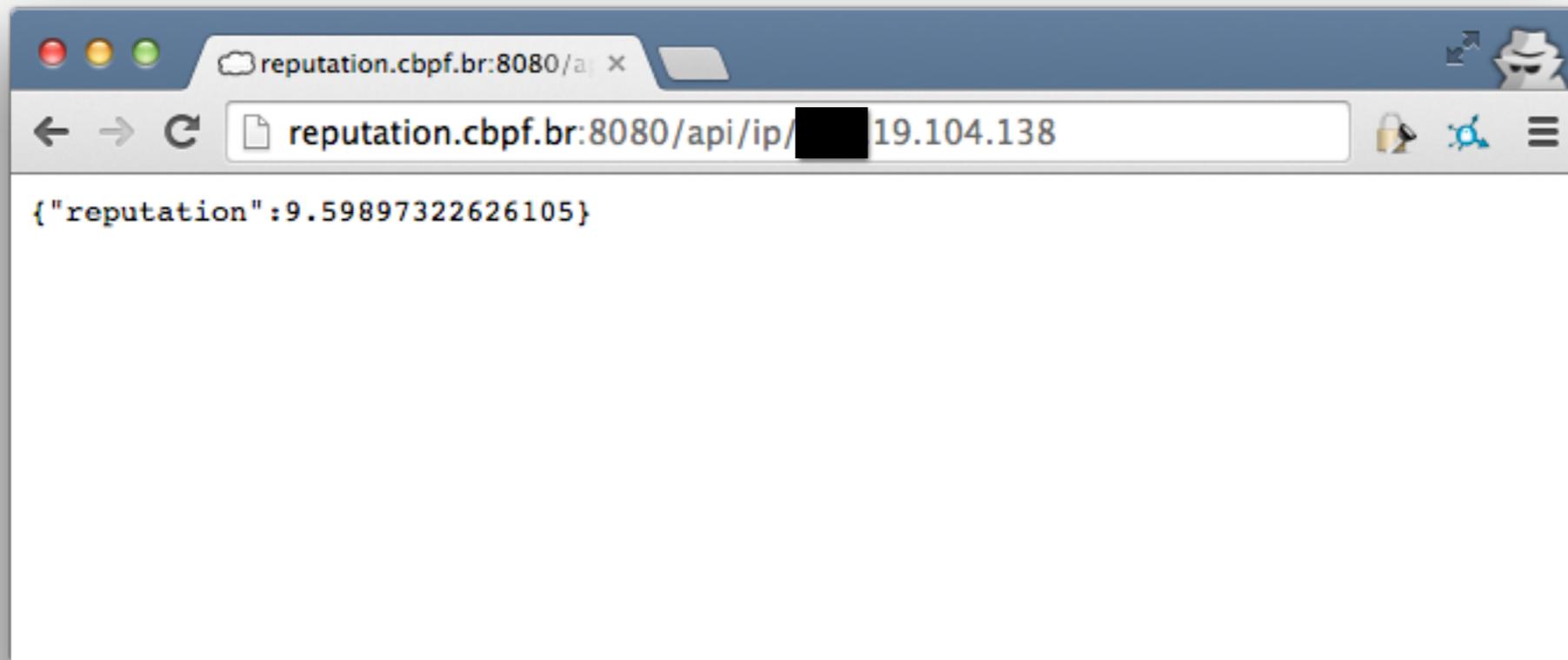
NMAP API - Dados

```
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: "████████ 93.67",
      status: "malicious",
      report_time: 1393637234,
      - _id: {
        $oid: "52f42669fae403557d000054"
      },
      counter: 2869524
    },
    - {
      created: 1391892327,
      detection: "darknet",
      ip: "████████ 93.51",
      status: "malicious",
      report_time: 1393834176,
      - _id: {
        $oid: "52f69767fae403460e0000cb"
      },
      counter: 2224569
    },
    - {
      created: 1397661633,
      detection: "darknet",
      ip: "████████ 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/██████████104.138

[
- {
  msg: {"last_source_port": "36877", "probes": 7, "last_destination_port": "23", "destination_port": ["110"], "source_port":
["6861", "26977", "36877"], "source_ip": "██████████104.138"},
  timestamp: "1432207216",
  item: "██████████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": "██████████104.138"},
  timestamp: "1432194016",
  item: "██████████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": "██████████104.138"},
  timestamp: "1432194316",
  item: "██████████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": "██████████104.138"},
  timestamp: "1432308022",
```

API de Reputação - 2.0



The screenshot shows a web browser window with the address bar displaying `reputation.cbpf.br:8080/api/ip`. The page content is a JSON array of objects, each containing a reputation score and an IP address. The JSON is formatted with syntax highlighting. A light blue highlight is applied to the object with IP `17.13`, and a dotted box highlights the object with IP `47.9`. The status bar at the bottom left shows `[4]`.

```
[
- {
  reputation: 98,
  item: "██████████138.89"
},
- {
  reputation: 98,
  item: "██████████90.146"
},
- {
  reputation: 98,
  item: "██████████47.45"
},
- {
  reputation: 98,
  item: "██████████85.66"
},
- {
  reputation: 98,
  item: "██████████17.13"
},
- {
  reputation: 98,
  item: "██████████47.9"
},
- {
  reputation: 98,
  item: "██████████.144.64"
},
- {
  reputation: 98,
  item: "██████████.213.32"
}
```

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