GT-CRIVO
Priorização Contextualizada de Vulnerabilidades Orientada a Negócio

Ítalo Cunha

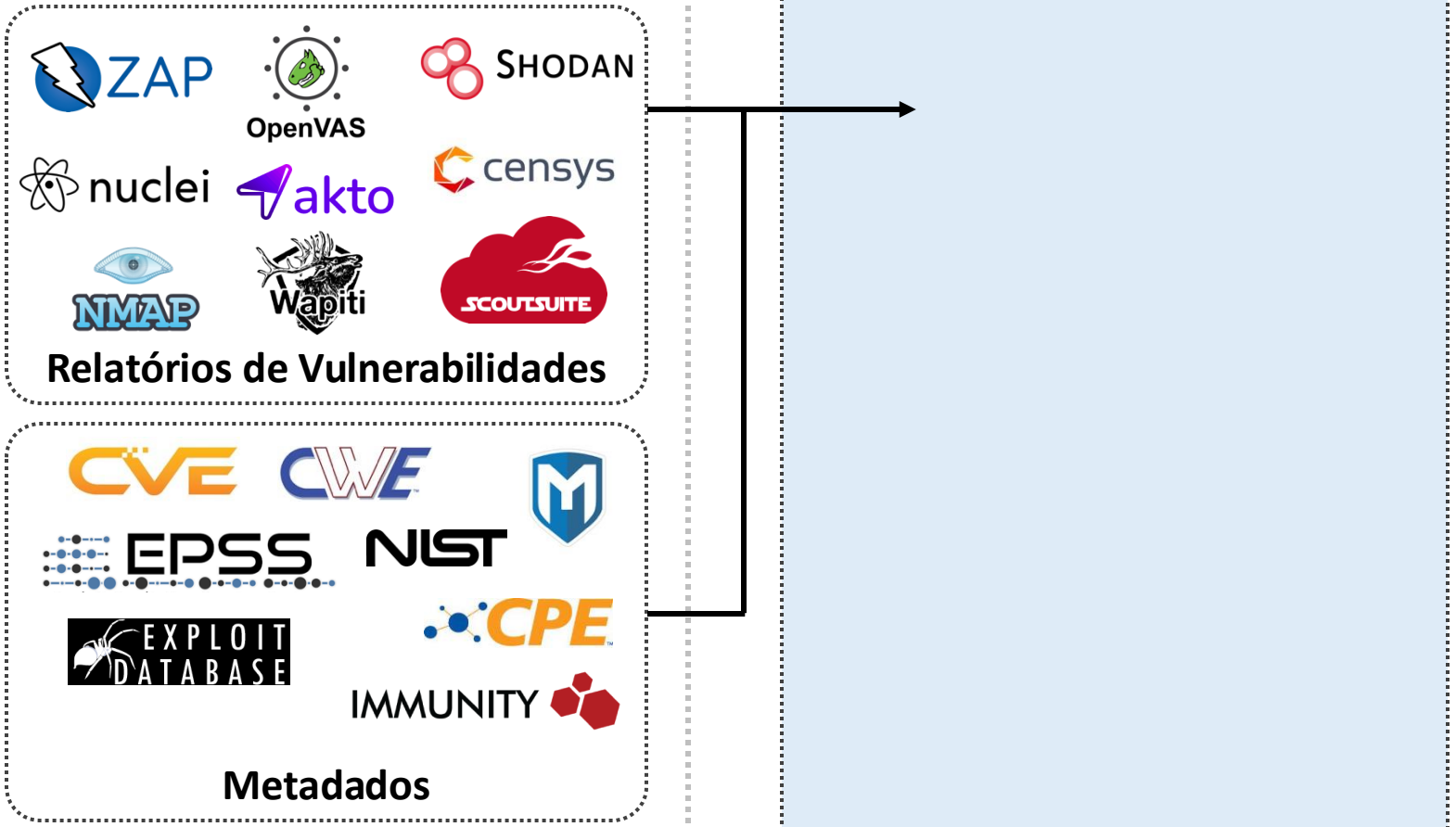
Francisco Aragão, Gabriel Pains, Leonardo Maia,
Lucas Sacramento, Pedro Almeida, Thiago Souza

Universidade Federal de Minas Gerais

Detecção de vulnerabilidades

Catalogação de vulnerabilidades

Sistema de priorização de vulnerabilidades



Tsunami de vulnerabilidades

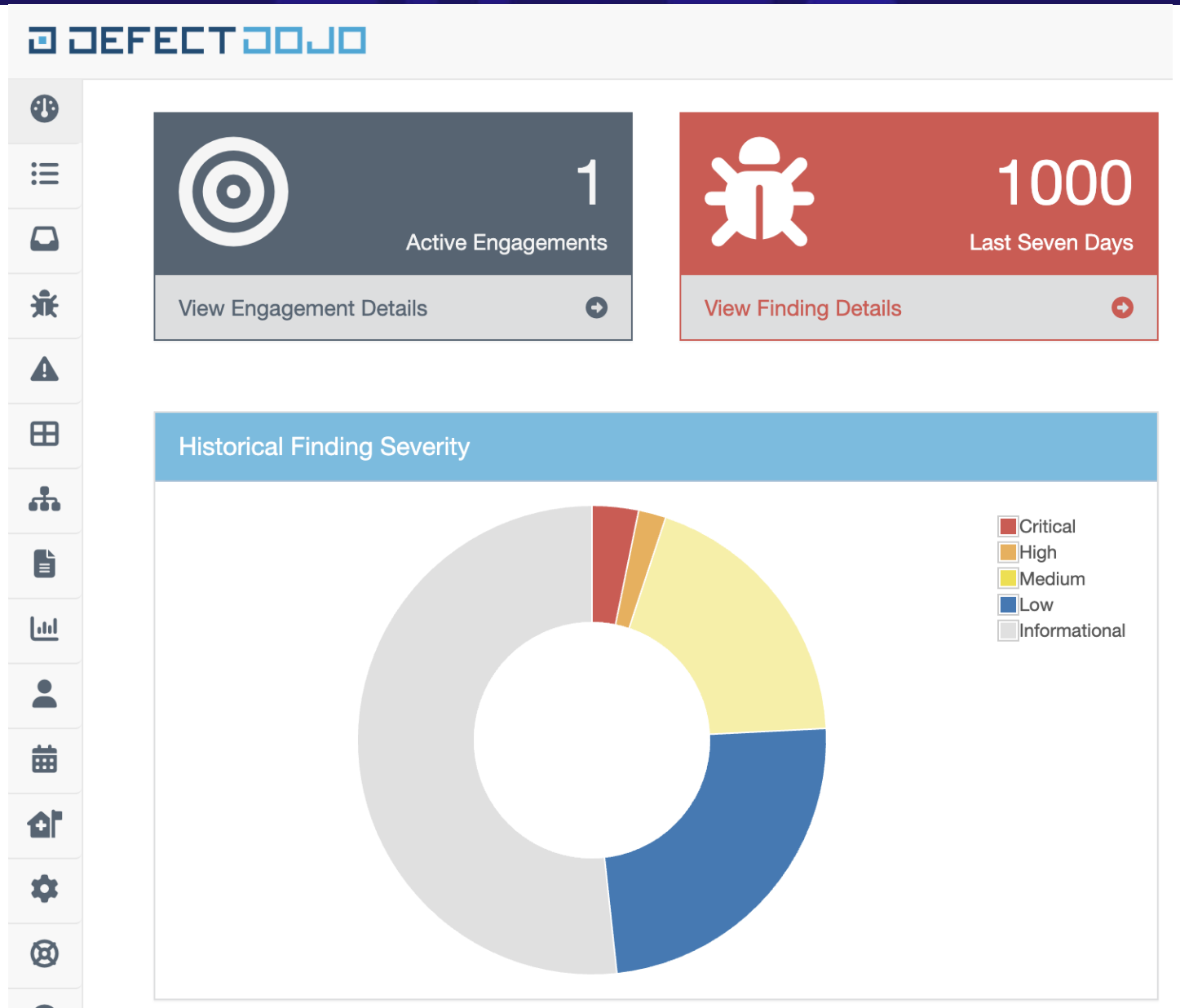
OpenVAS vs speed DCC - UFMG

Mais de 1000 vulnerabilidades encontradas pelo OpenVAS nas dezenas de máquinas do laboratório Speed

32 críticas

19 graves

191 médias



Priorização de vulnerabilidades na UFMG

CVSS	Título
10.0	IPMI 'No Auth' Access Mode Enabled
10.0	Operating System Support End of Life
10.0	Apache Hadoop 'Secure Mode' Disabled

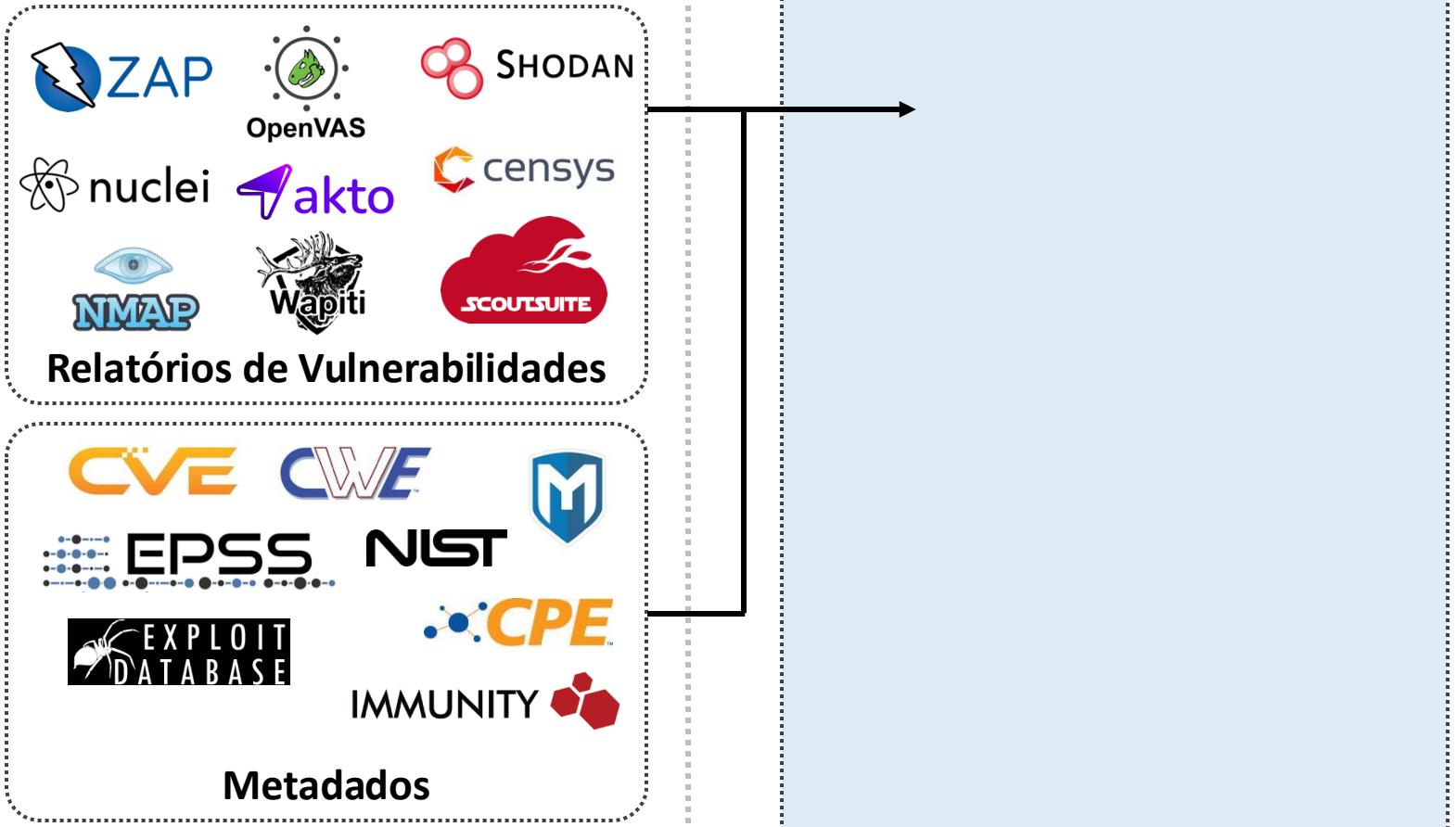
Priorização de vulnerabilidades na UFMG

OpenVAS

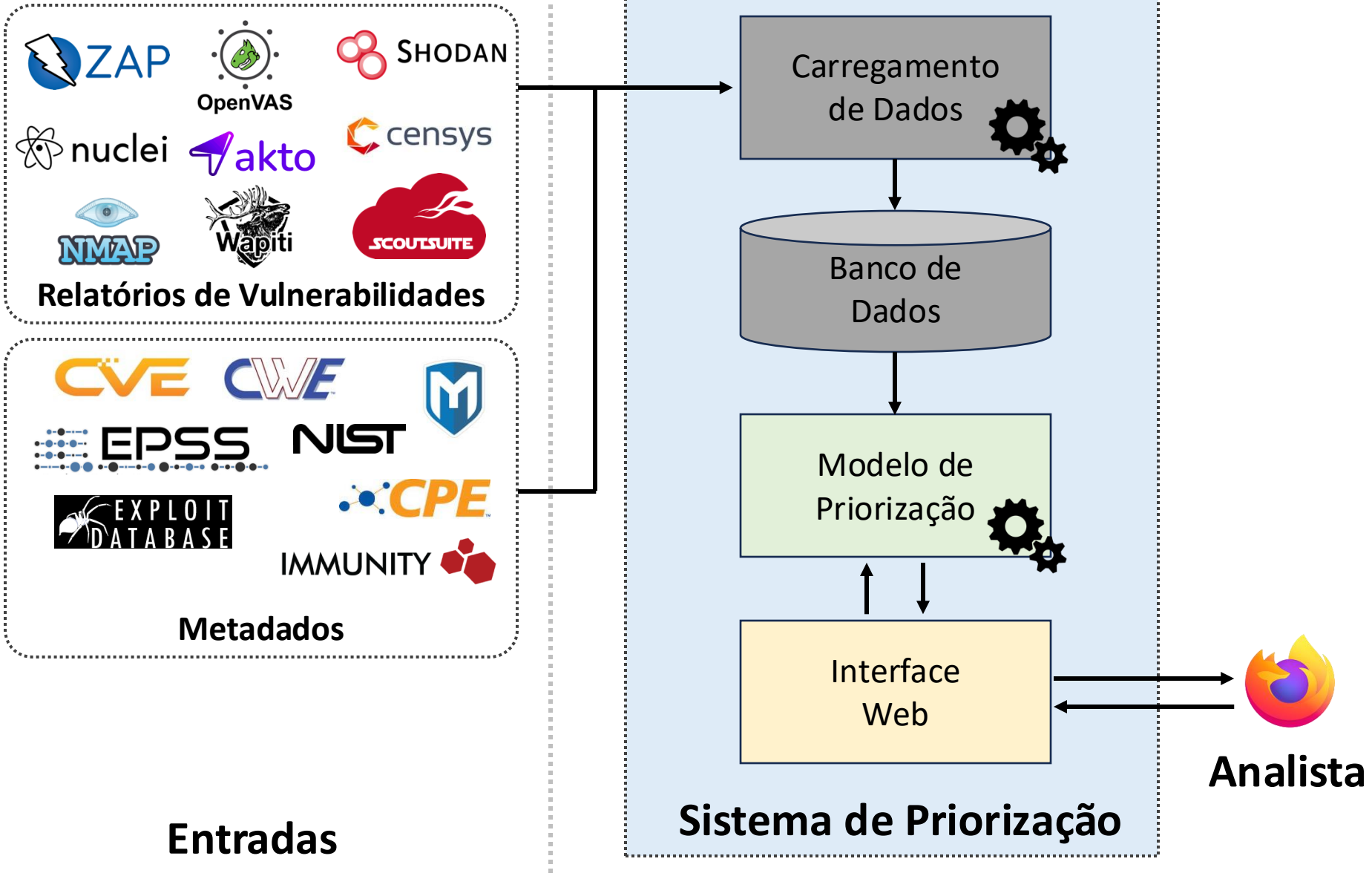
VS

CVSS	Título	Importante?
10.0	IPMI 'No Auth' Access Mode Enabled	Firewall bloqueia
10.0	Operating System Support End of Life	É servidor ou desktop?
10.0	Apache Hadoop 'Secure Mode' Disabled	Bitcoin farm!

Sistema de priorização de vulnerabilidades



Sistema de priorização de vulnerabilidades

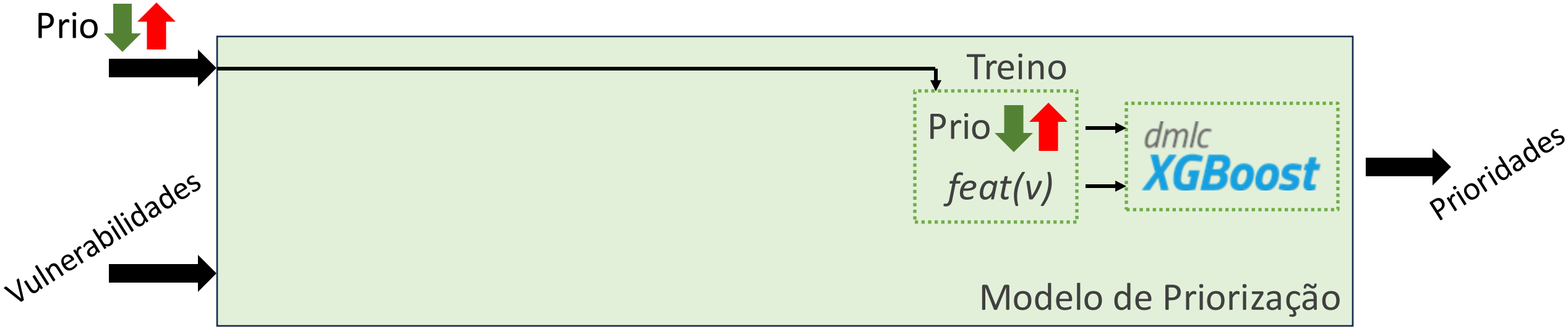


Priorização de vulnerabilidades

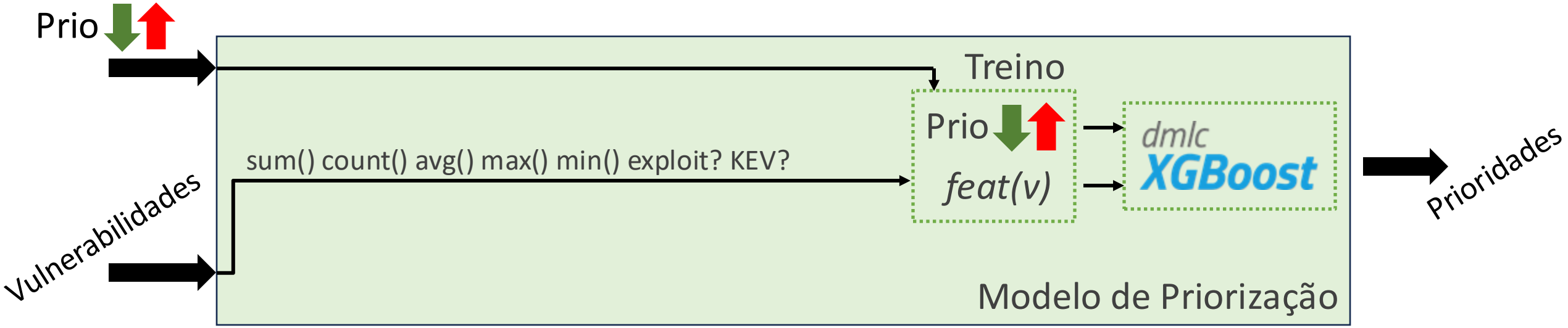
Priorização de vulnerabilidades

Priorização de vulnerabilidades

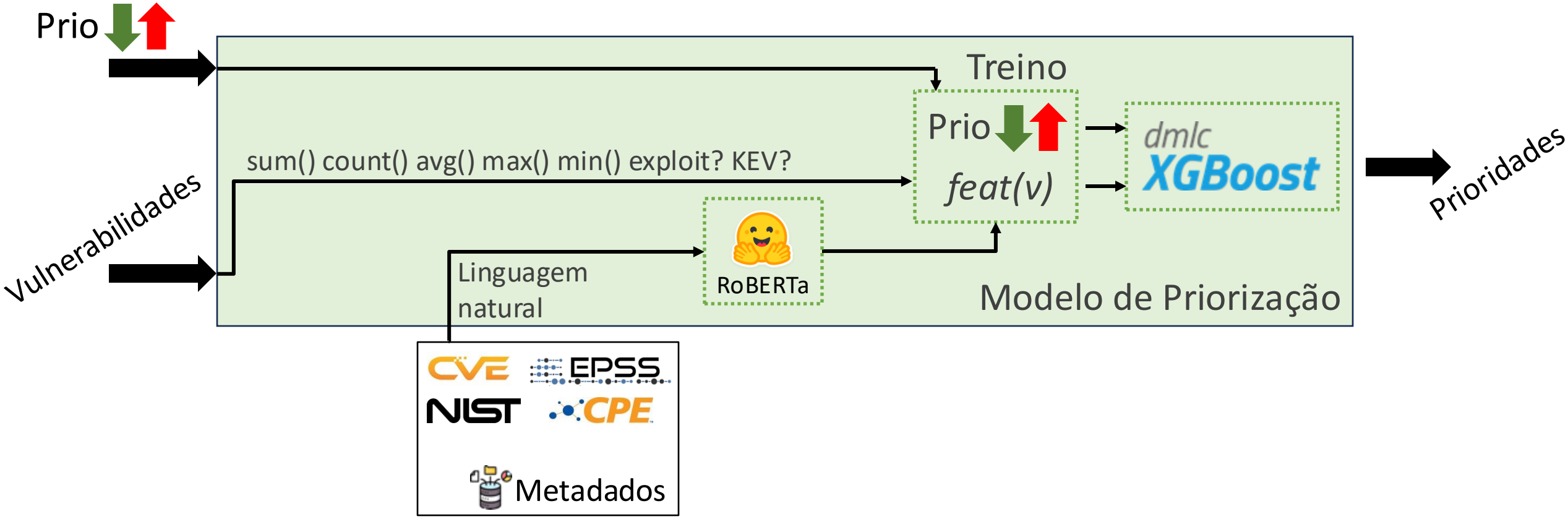
Priorização de vulnerabilidades



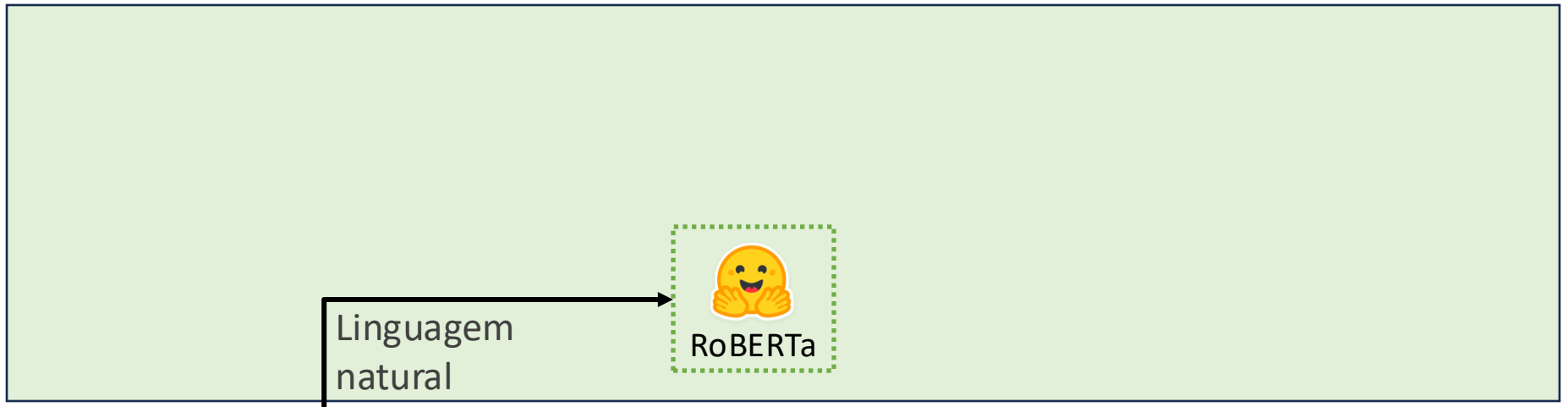
Priorização de vulnerabilidades



Priorização de vulnerabilidades



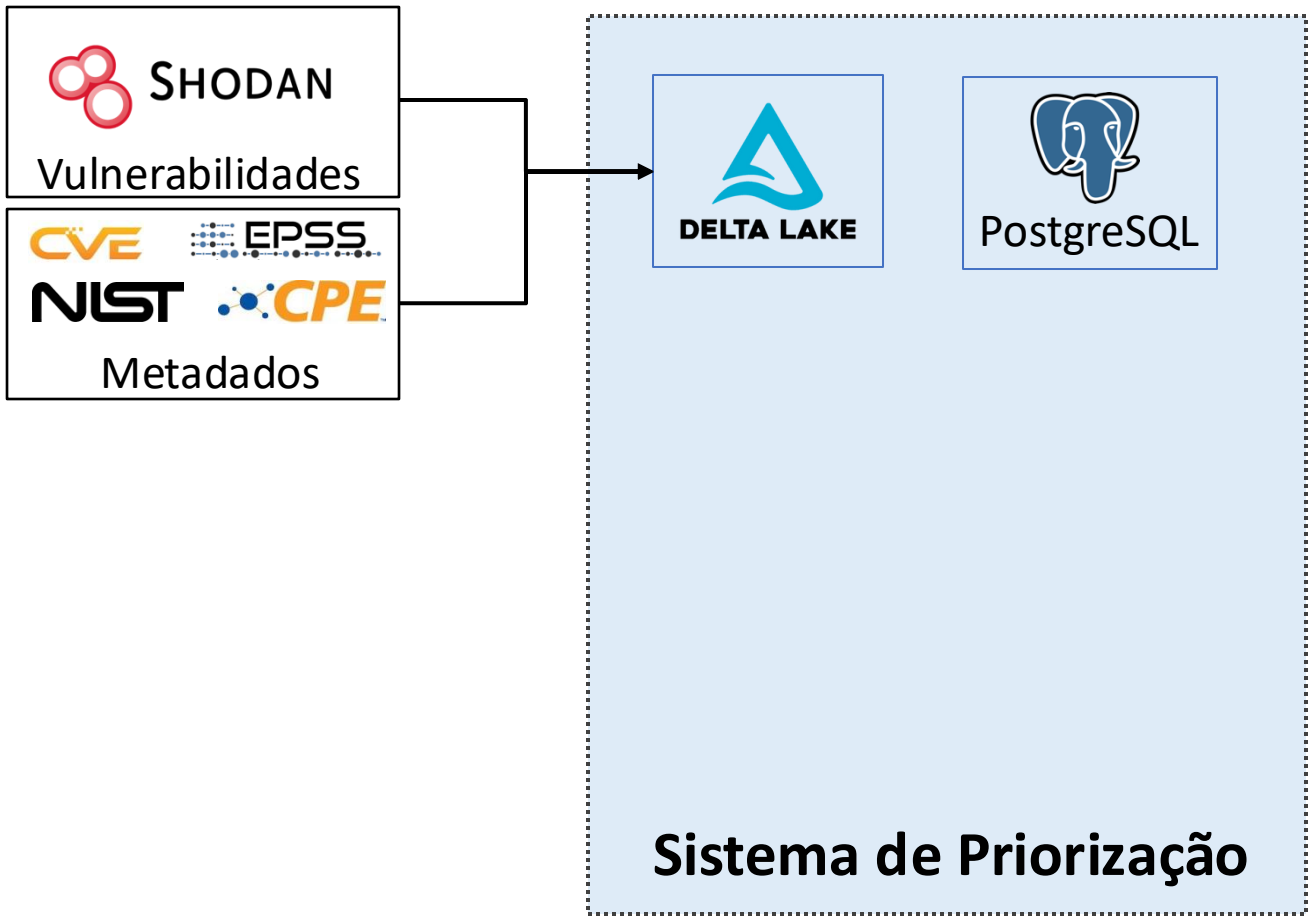
Exemplo de extração de *features*



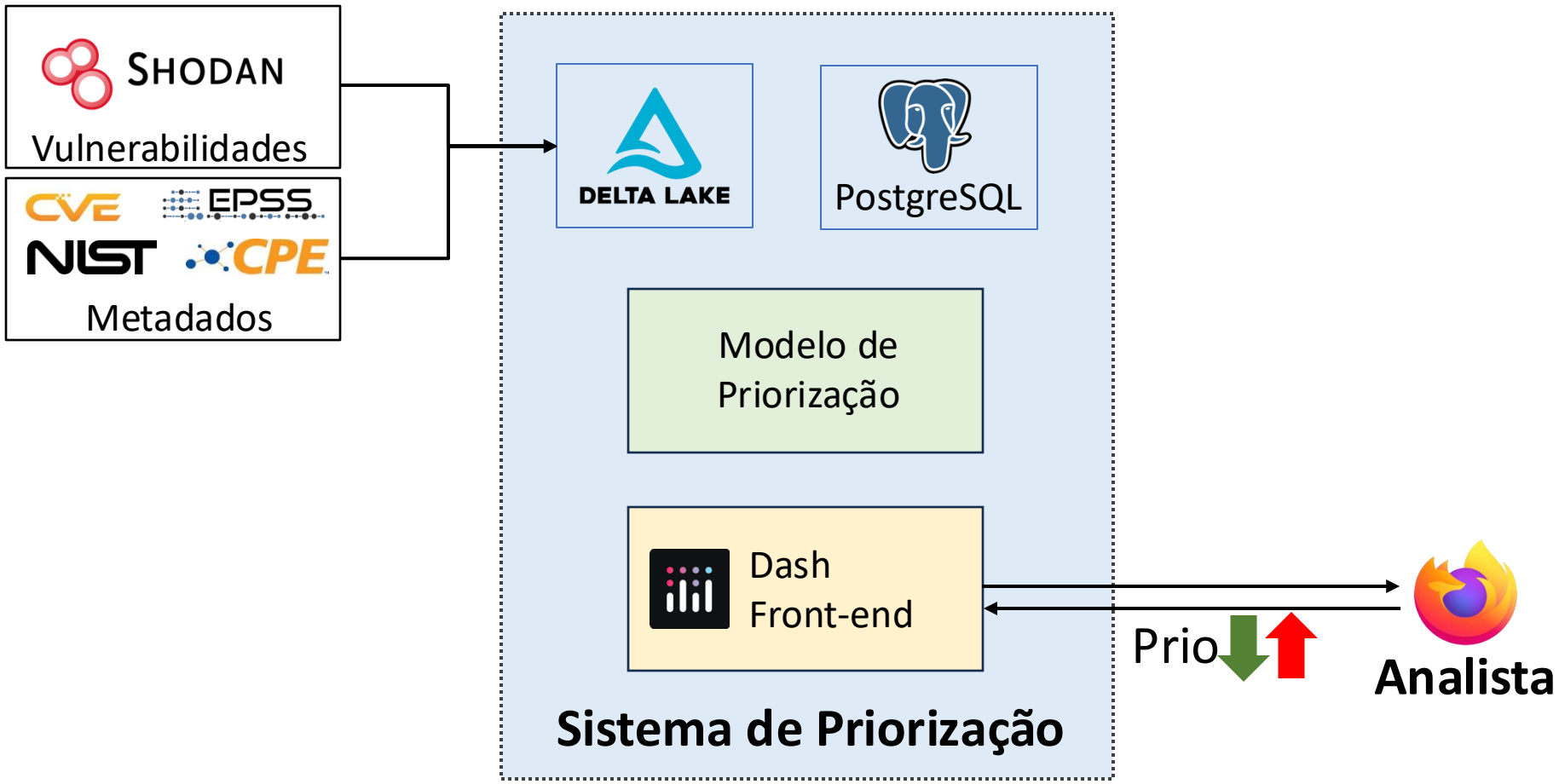
CVE → RoBERTa →

Tag	Peso
Denial of service	0.72
Code execution	0.07
Information disclosure	0.02
Buffer overflow	0.10
Privilege escalation	0.02
XSS	0.06
SQL injection	0.01

Shogun


SHODAN
Vulnerabilidades
CVE
EPSS
NIST
CPE
Metadados
DELTA LAKE
PostgreSQL
Sistema de Priorização

Shogun


SHODAN
Vulnerabilidades
CVE
EPSS
NIST
CPE
Metadados
DELTA LAKE
PostgreSQL
Modelo de Priorização
Dash Front-end
Prio
Analista
Sistema de Priorização

Shogun – Ordenação por EPSS

SAM/CRIVO Cybersecurity Dashboards

2024-06-26

cunha

Advanced Analysis (IP Data) | View 1 - EPSS summary | View 2 - by organizations/IP | View 3 - More details by CVE | View 4 - Maps | -

Shodan's banners about IPs with vulnerabilities in Brazil. Using this interface, users can filter banners by each column, ranking its vulnerabilities and clicking on IP column to check details.

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	E.. ↓	PRIO	VOTE
HTTP/1.1 Server: Apache Date: Wed, 26 Jun 2024 11:40:01 GMT	138.118.57.54	443	Itaquaquecetuba		Globaltech Telecomunicacoes E Informatica			0.9757	7.2275	9
HTTP/1.1 Date: Wed, 26 Jun 2024 23:04:21 GMT	201.83.152.102	9443	São Paulo		Claro Nxt Telecomunicacoes	c9539866.virtua.com.br	virtua.com.br	0.9755	7.3774	Skip
HTTP/1.1 Server: Microsoft-IIS/7.5 Date: Wed, 26 Jun 2024 01:42:35 GMT	187.85.15.242	23424	Bauru	Windows	Ultrawave Telecom	187-85-15-242.dynamic.ultrawave.com.br	ultrawave.com.br	0.9754	4.6598	Skip
HTTP/1.1 Server: Microsoft-IIS/8.5	189.1.84.92	82	Suzano	Windows	Centroeste Carnes E Derivados	i29-189-1-84-92.i29.com.br	i29.com.br	0.9754	4.3351	Skip

Shogun – Ordenação por prioridade

HACKERS DO BEM

SAM/CRIVO Cybersecurity Dashboards

2024-06-26

cunha

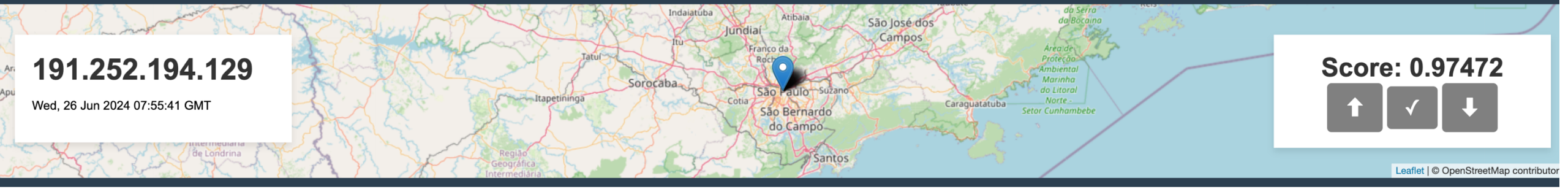
Advanced Analysis (IP Data) | View 1 - EPSS summary | View 2 - by organizations/IP | View 3 - More details by CVE | View 4 - Maps | -

Shodan's banners about IPs with vulnerabilities in Brazil. Using this interface, users can filter banners by each column, ranking its vulnerabilities and clicking on IP column to check details.

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	EPSS	P.. ↓	VOTE
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenS Date: Wed, 26 Jun 2024 23:20:32 GM	201.49.165.149	443	Cuiabá		Centro De Proc De Dados Do Estado De Mato Grosso	www.sac.mti.mt.gov.br, sac.mti.mt.gov.br	mti.mt.gov.br	0.9747	8.4260	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenS Date: Wed, 26 Jun 2024 10:54:49 GM	187.191.100....	443	São Paulo		Claranet Technology	unisuam.edu.br	unisuam.edu.br	0.9747	8.2722	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenS Date: Wed, 26 Jun 2024 07:50:51 GMT	191.252.194....	443	São Paulo		Locaweb Servicos De Internet	vps16051.publiccloud .com.br,fertipraxis.co m.br,www.fertipraxis.c	publiccloud.com.br,fe rtipraxis.com.br	0.9747	8.1484	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenS	200.130.18.51	443	Brasília		Rede Nacional De Ensino E Pesquisa	capes.gov.br,sdiold.c apes.gov.br	capes.gov.br	0.9735	7.5451	Skip

Shogun – Detalhes sobre vulnerabilidade

IP Details



IP Info

City: São Paulo

Organization: Locaweb Servicos De Internet

Operating System: N/A

CPE23:

cpe:2.3:a:apache:http_server:2.4.6 cpe:2.3:a:jquery:jquery cpe:2.3:a:mysql:mysql cpe:2.3:a:openssl:openssl:1.0.2k cpe:2.3:a:php:php cpe:2.3:a:php:php:7.2.22 cpe:2.3:a:wordpress:wordpress:5.2.4

Hostnames:

vps16051.publiccloud.com.br fertipraxis.com.br www.fertipraxis.com.br

Data

HTTP/1.1 200 OK

Date: Wed, 26 Jun 2024 07:50:51 GMT

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.22

X-Powered-By: PHP/7.2.22

Link: <https://fertipraxis.com.br/wp-json/>; rel="https://api.w.org/"

Link: <https://fertipraxis.com.br/>; rel=shortlink

Transfer-Encoding: chunked

Content-Type: text/html; charset=UTF-8

Shogun – Vulnerabilidades repetidas

Date: Wed, 26 Jun 2024 10:54:49 GMT									
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenS Date: Wed, 26 Jun 2024 07:50:51 GMT	191.252.194....	443	São Paulo	Locaweb Servicos De Internet	vps16051.publiccloud.com.br,fertipraxis.com.br,www.fertipraxis.c	publiccloud.com.br,fertipraxis.com.br	0.9747	8.1484	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenS Date: Wed, 26 Jun 2024 19:48:46 GMT	200.130.18.51	443	Brasília	Rede Nacional De Ensino E Pesquisa	capes.gov.br,sdiold.capes.gov.br	capes.gov.br	0.9735	7.5451	Skip
HTTP/1.1 Server: nginx Date: Wed, 26 Jun 2024 17:46:30 GMT	150.162.2.10	443	Florianópolis	Universidade Federal De Santa Catarina	paginas.ufsc.br	ufsc.br	0.9556	7.5357	Skip
HTTP/1.1 Server: nginx Date: Wed, 26 Jun 2024 18:10:16 GMT	150.162.2.10	443	Florianópolis	Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br	ufsc.br	0.9556	7.5354	Skip
HTTP/1.1 Server: nginx Date: Wed, 26 Jun 2024 20:26:15 GMT	150.162.2.10	443	Florianópolis	Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br	ufsc.br	0.9556	7.5354	Skip
HTTP/1.1 Server: nginx Date: Wed, 26 Jun 2024 16:31:30 GMT	150.162.2.10	443	Florianópolis	Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br	ufsc.br	0.9556	7.5354	Skip

Agrupamento de vulnerabilidades

- Ferramentas podem encontrar vulnerabilidades de diferentes formas
- Ferramentas podem reportar vulnerabilidades “diferentes” para teste idêntico

Classificação dos scripts de detecção

- Utilizamos modelos de linguagem para sumarizar o funcionamento do script

- **O quê** é detectado?
  - Vulnerabilidade
    - Aplicação
    - Versão
  - *Software* sem manutenção ou end-of-life
    - *Software*
    - Versão
  - Propriedade/configuração problemática
    - Descrição
    - Valor

Classificação dos scripts de detecção

- Utilizamos modelos de linguagem para sumarizar o funcionamento do script

- **O quê** é detectado?
- **Como** a detecção é feita?
  - Ataque simulado ou *exploit*
    - Execução de código remoto
    - Login não autorizado
    - Acesso a informação protegida
    - Negação de serviço
  - Varredura com acesso ao dispositivo
    - Análise de pacotes instalados
    - Verificação de configuração
    - Análise de log
  - Execução de requisição pela rede
    - Verificação de *banner*
    - Verificação do estado de uma resposta
    - Verificação da existência de uma URL ou endpoint
    - Outras sondagens de rede para descobrimento de informação

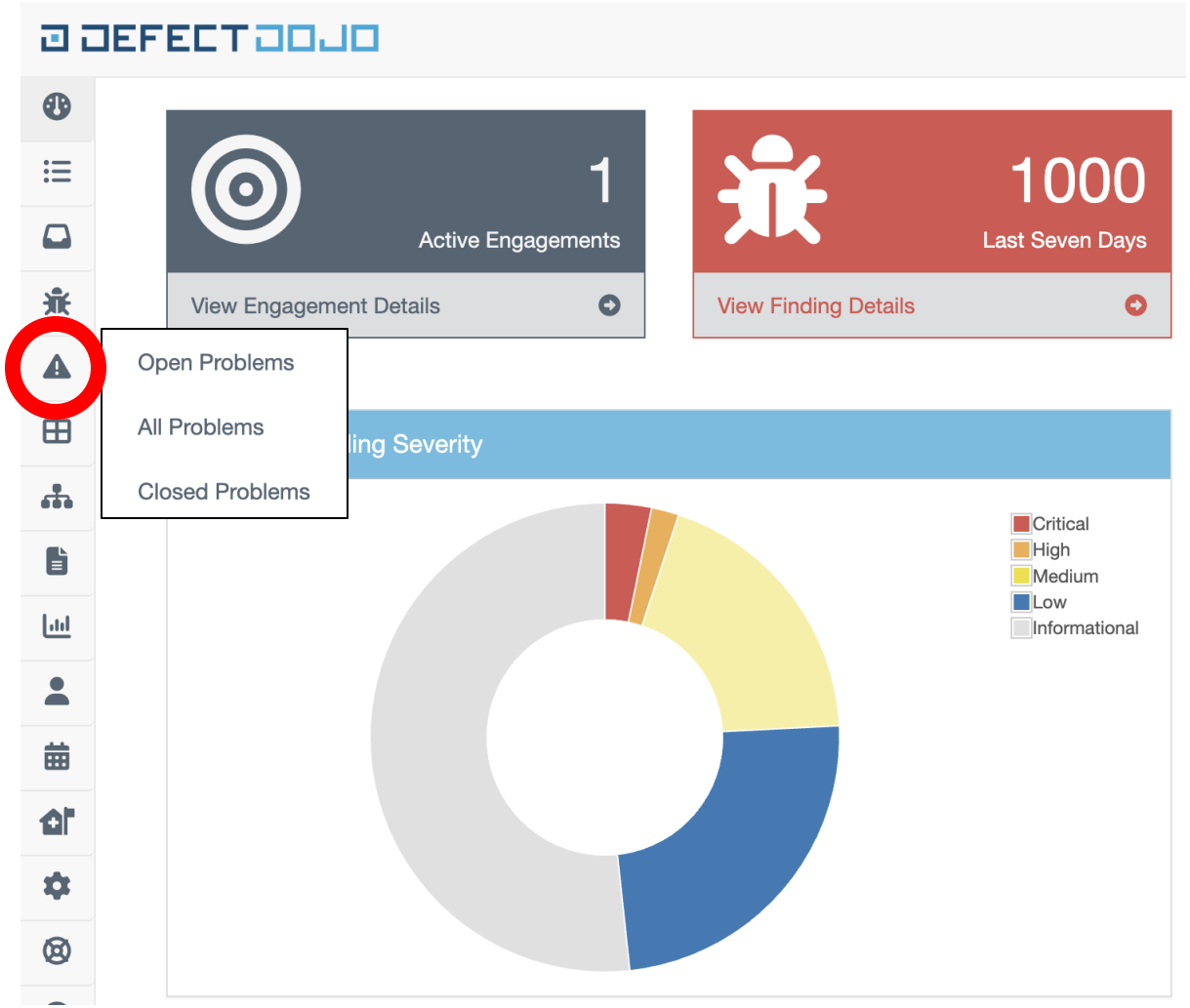
Classificação dos scripts de detecção

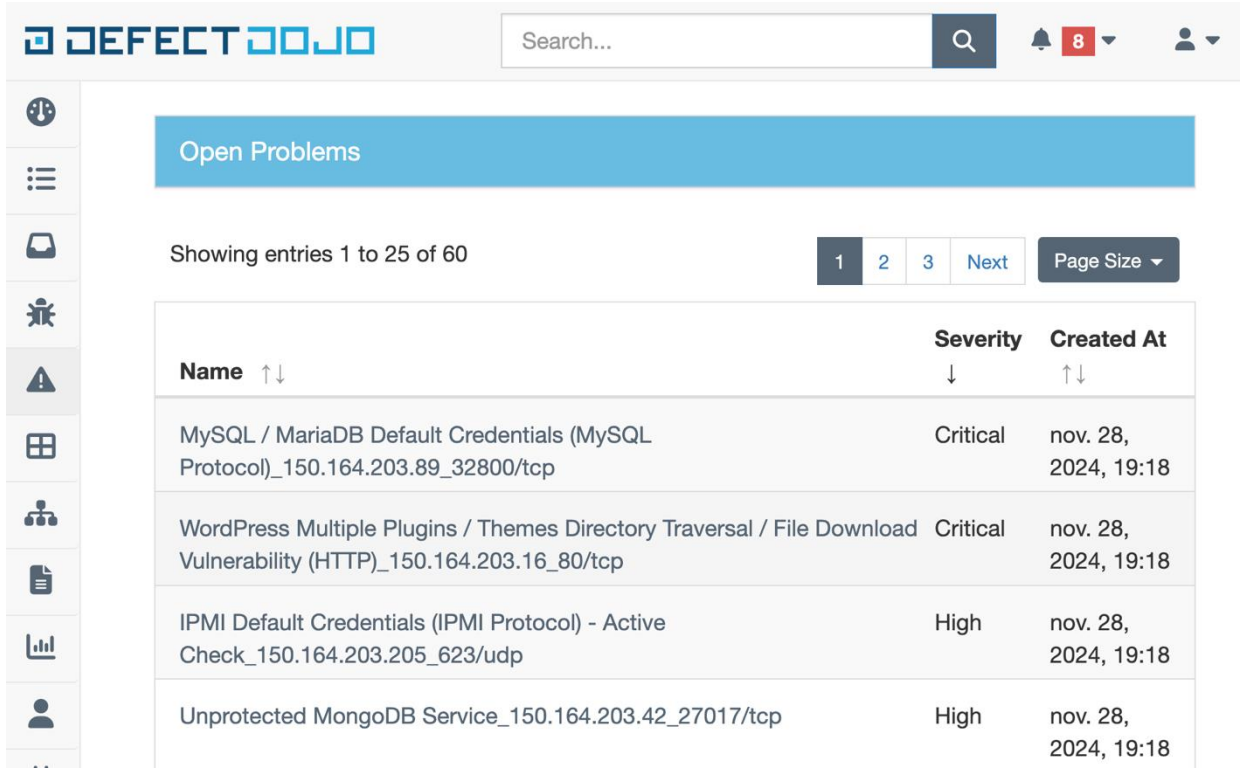
		O que está sendo detectado					
		Vulnerabilidade		Versão antiga ou end-of-life		Propriedades ou configurações	
Como está sendo detectado							
Ataque ou *exploit*	Execução de código						
	Login não autorizado						
	...						
Varredura	Pacotes instalados						
	Configuração						
	Análise de log						
...	...						

Classificação dos scripts de detecção

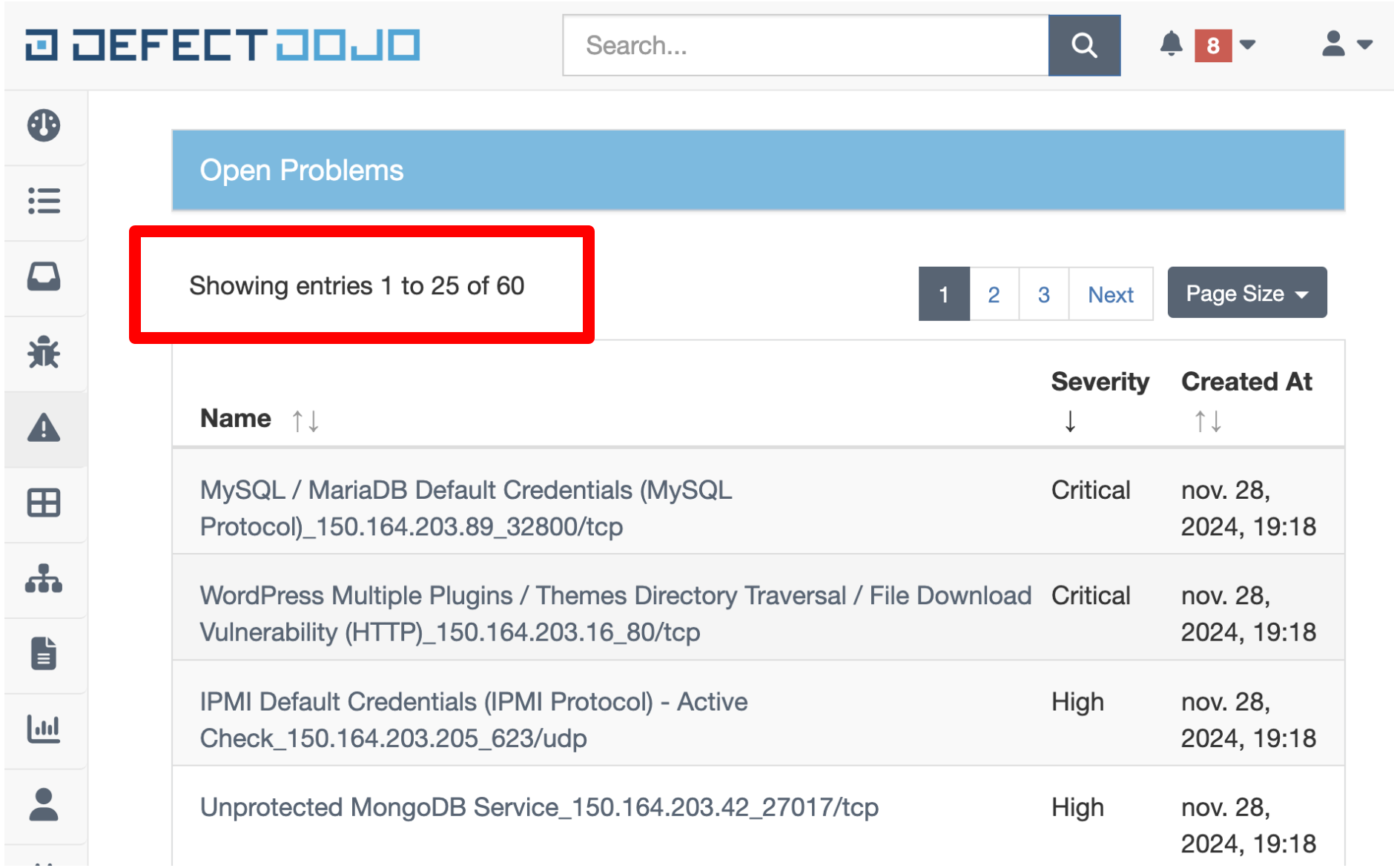
		O que está sendo detectado					
Como está sendo detectado		Vulnerabilidade		Versão antiga ou end-of-life		Propriedades ou configurações	
Ataque ou *exploit*	Execução de código						
	Login não autorizado						
	...						
Varredura	Pacotes instalados						
	Configuração						
	Análise de log						
...	...						

Integração no DefectDojo

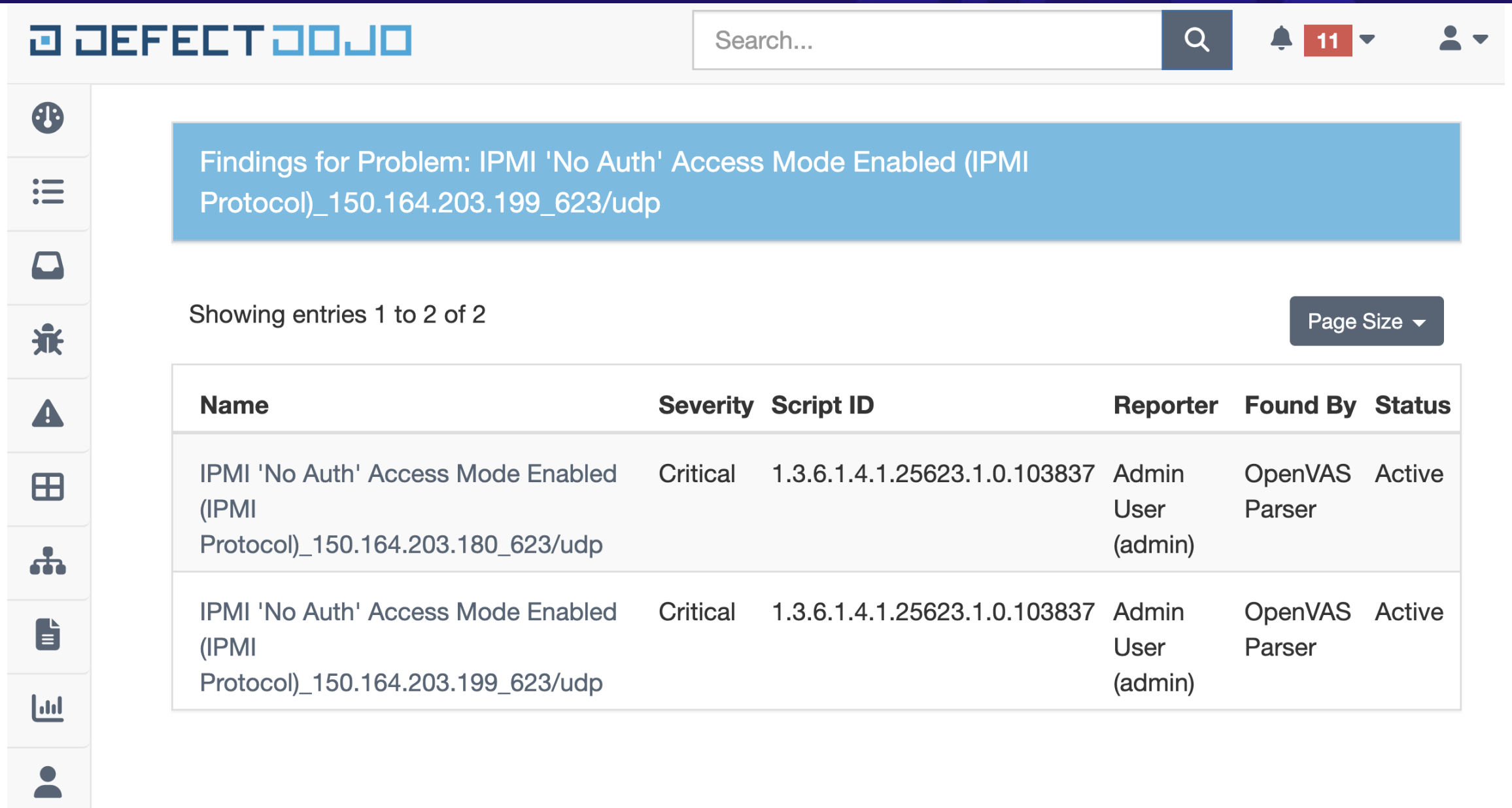




Integração no DefectDojo

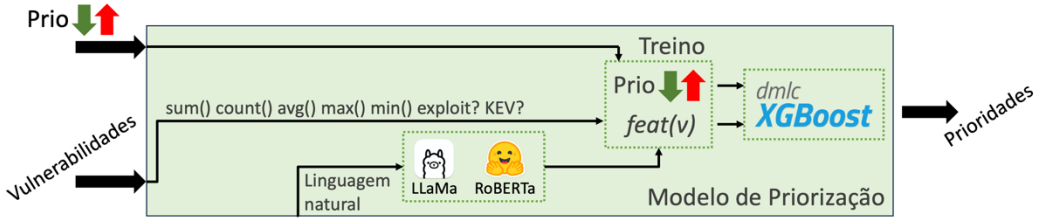


Integração no DefectDojo



Contribuições

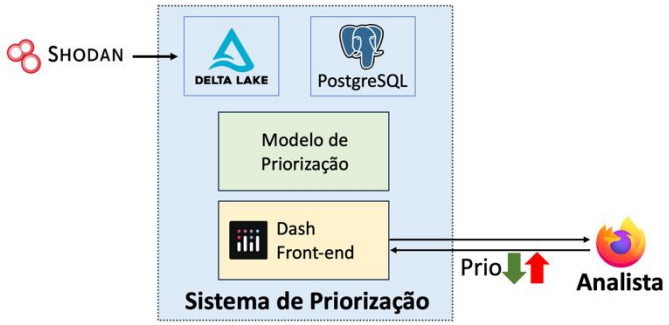
- *Pipeline* para treino dos modelos de priorização
  - Processamento dos metadados



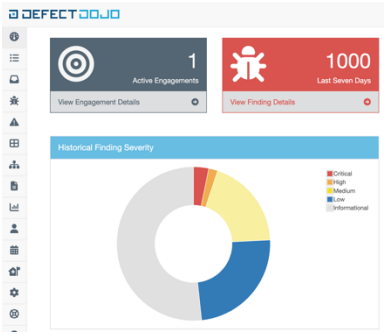
- Agrupamento de scripts de detecção de vulnerabilidades

Como está sendo detectado		O que está sendo detectado					
		Vulnerabilidade		Versão antiga ou end-of-life		Propriedades ou configurações	
Ataque ou *exploit*	Execução de código						
	Login não autorizado						
	...						
Varredura	Pacotes instalados						
	Configuração						
	Análise de log						
...	...						

- Sistema para análise de vulnerabilidades do Shodan



- Integração com o DefectDojo



Equipe

FRANCISCO
Graduando/Desenvolvedor

GABRIEL
Graduando/Desenvolvedor

ITALO
Coordenador

THIAGO
Mestrando/Desenvolvedor

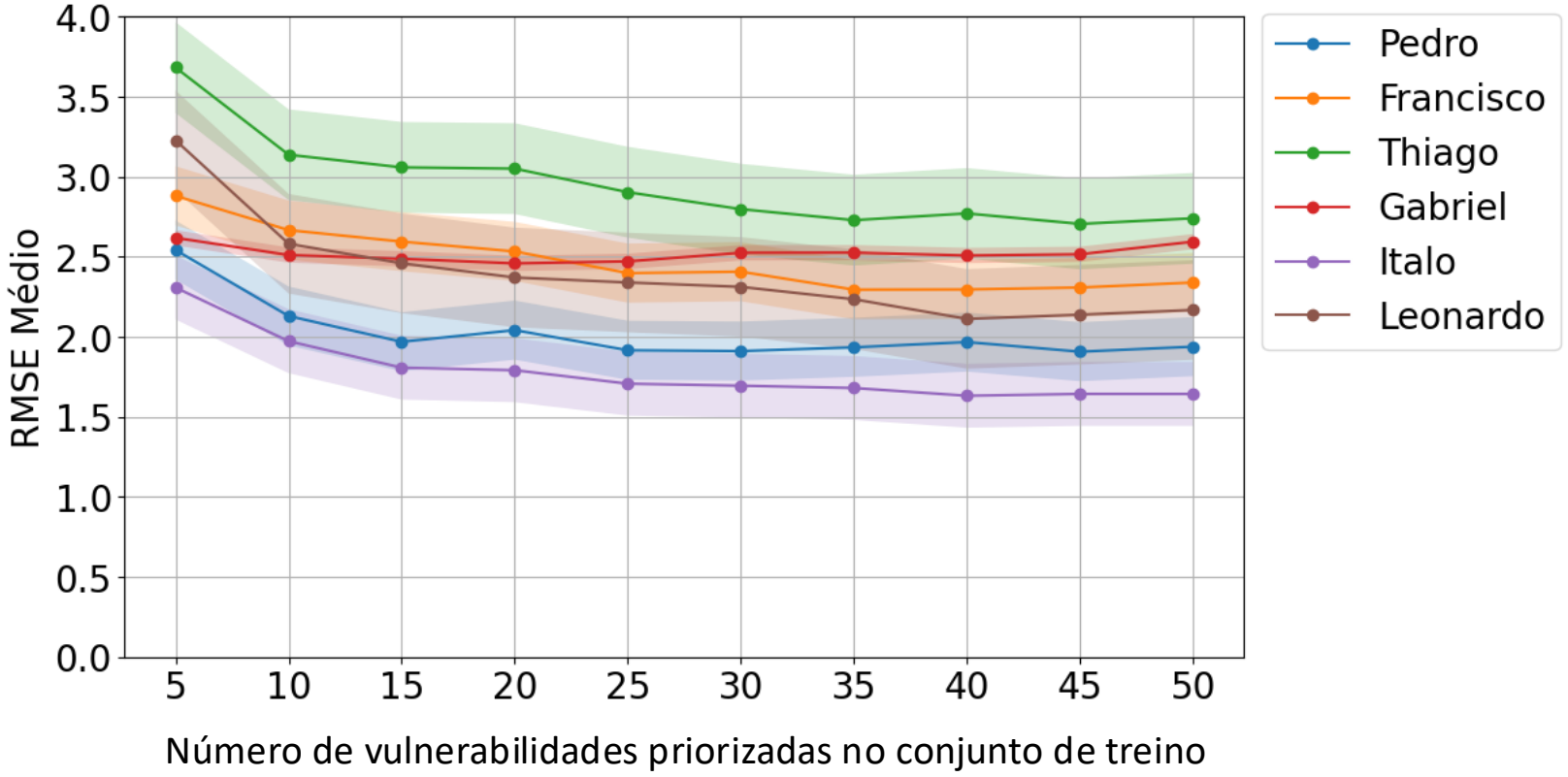
LEONARDO
Graduando/Desenvolvedor

LUCAS
Graduando/Desenvolvedor

PEDRO
Graduando/Desenvolvedor

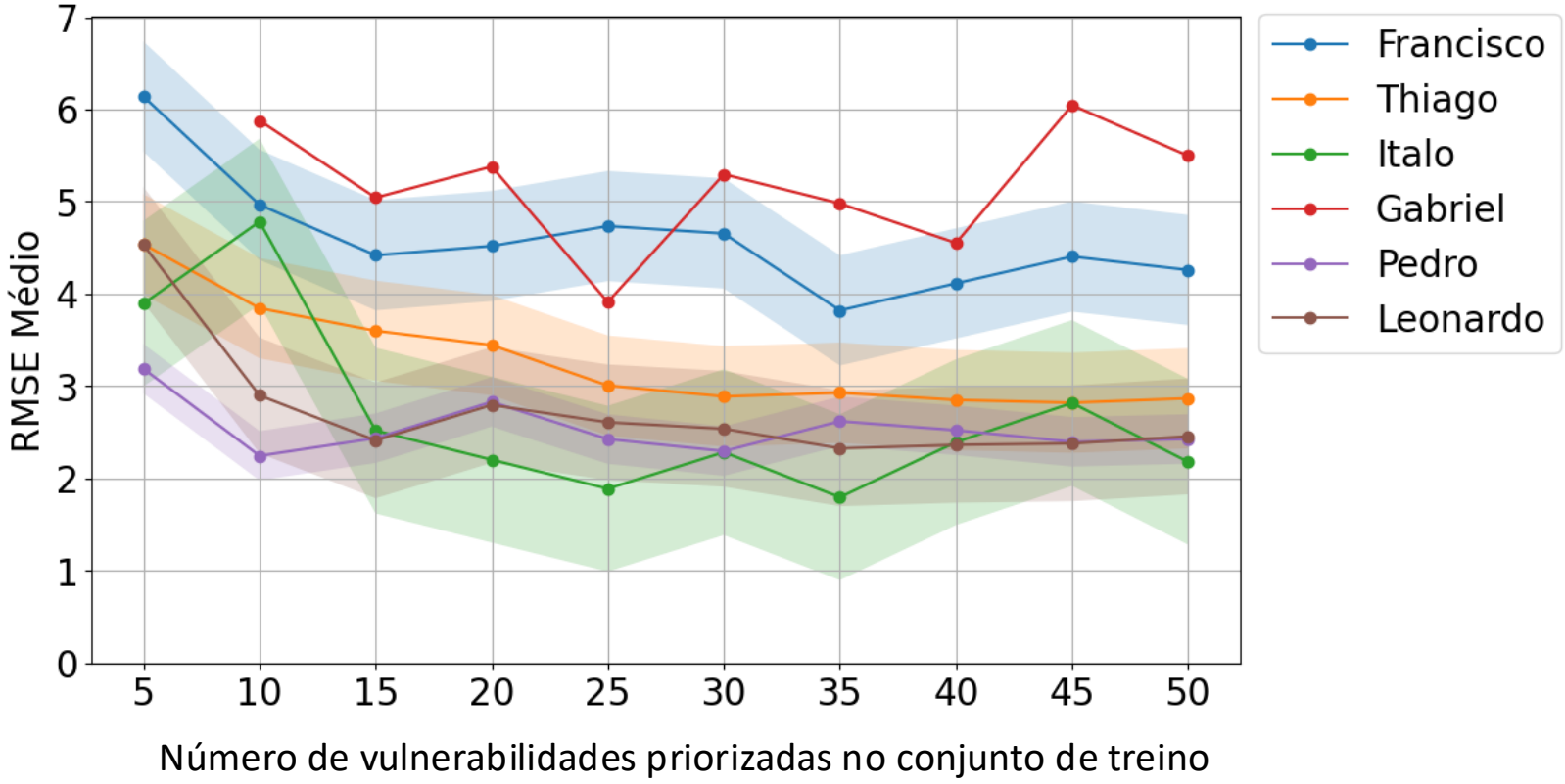
Backup Slides

Quantos votos são necessários para priorizar vulnerabilidades precisamente



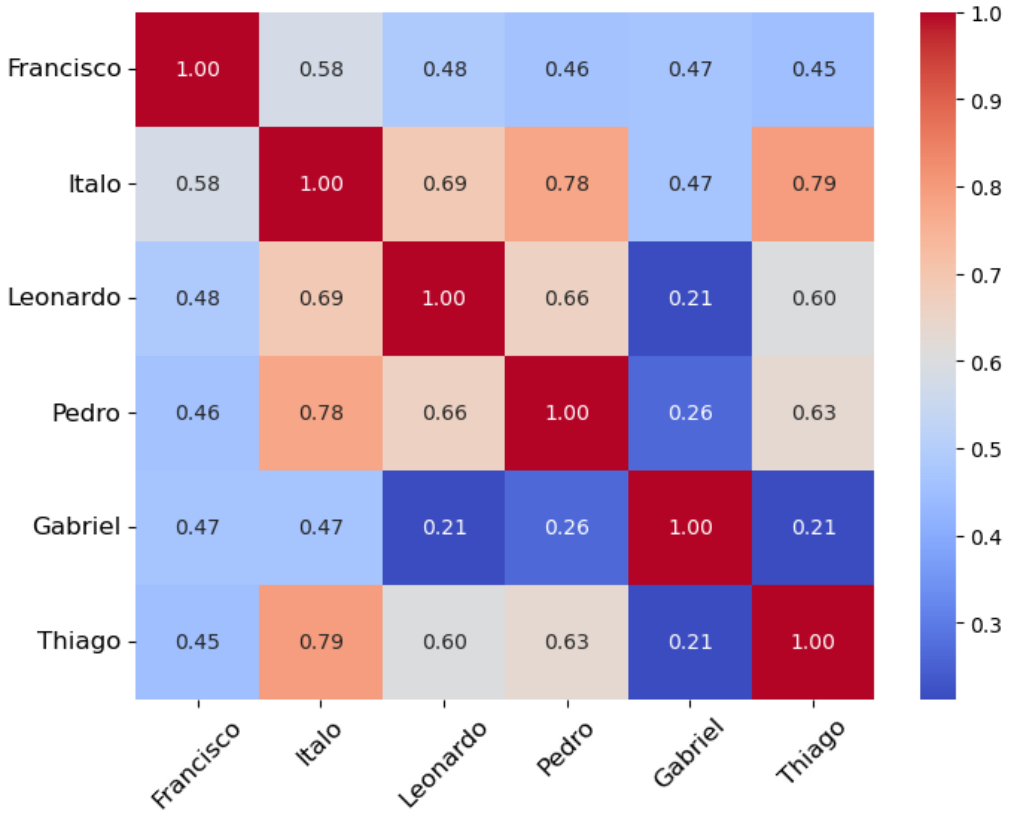
Maior redução do erro de predição concentrado antes de 40 priorizações

Quantos votos são necessários para priorizar vulnerabilidades precisamente



Predição dos votos para vulnerabilidades graves têm maior taxa de erro

Correlação de priorizações entre integrantes do projeto

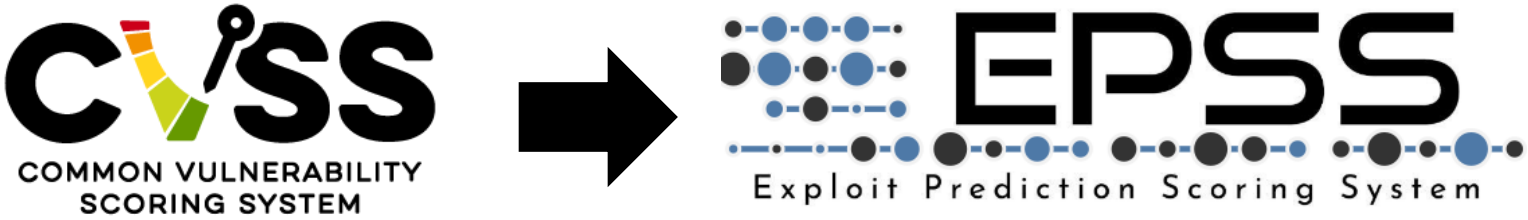


Baixa correlação entre votos indica que analistas associam prioridades muito diferentes a uma vulnerabilidade.

Soluções de priorização existentes

- Propriedades da vulnerabilidade

Soluções de priorização existentes

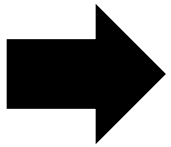


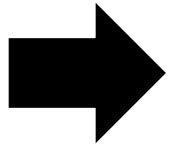
- Propriedades da vulnerabilidade

- Propriedades da vulnerabilidade

- Disponibilidade de exploits
- Explorações reportadas
- Monitoramento de “redes sociais”
- Análise temporal

Soluções de priorização existentes





- Propriedades da vulnerabilidade

- Propriedades da vulnerabilidade

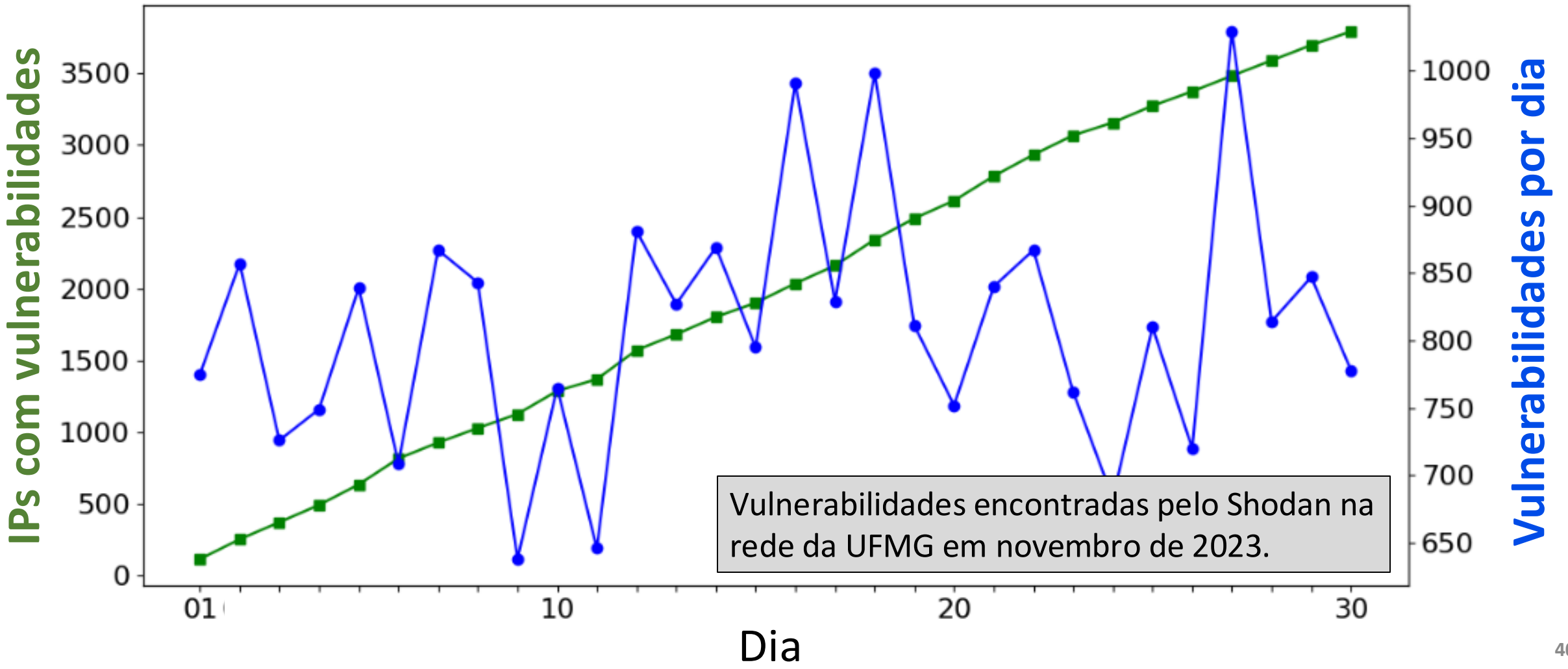
- Disponibilidade de exploits
- Explorações reportadas
- Monitoramento de “redes sociais”
- Análise temporal

- Propriedades da vulnerabilidade

- Disponibilidade de exploits
- Explorações reportadas
- Monitoramento de “redes sociais”
- Análise temporal

- Propriedades da empresa
- Propriedades do analista

SHODAN Vs UFMG



Vulnerabilidades encontradas pelo Shodan na rede da UFMG em novembro de 2023.

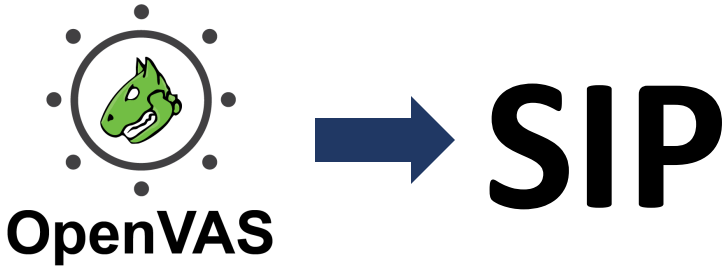
Priorização de vulnerabilidades

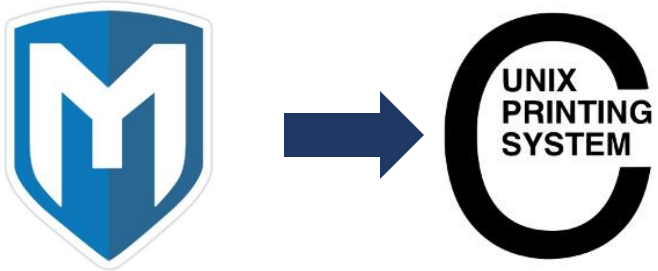
- Vazamento de dados
- Violação de privacidade

- Desempenho da aplicação
- Funcionamento da infraestrutura

Desambiguamento de vulnerabilidades

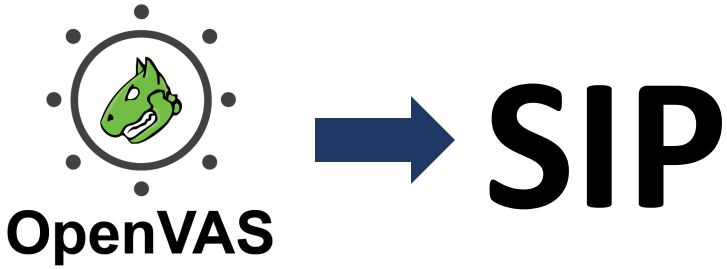
Varredura por ShellShock
CVE-2014-6271





Desambiguamento de vulnerabilidades

Varredura por ShellShock CVE-2014-6271



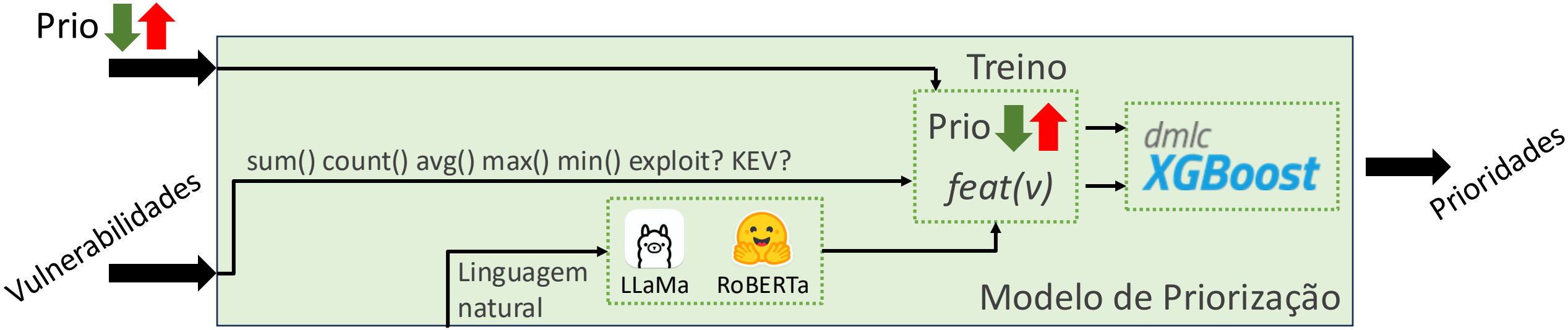
Algoritmos de autenticação fracos (sem CVE)

Processo de classificação dos scripts

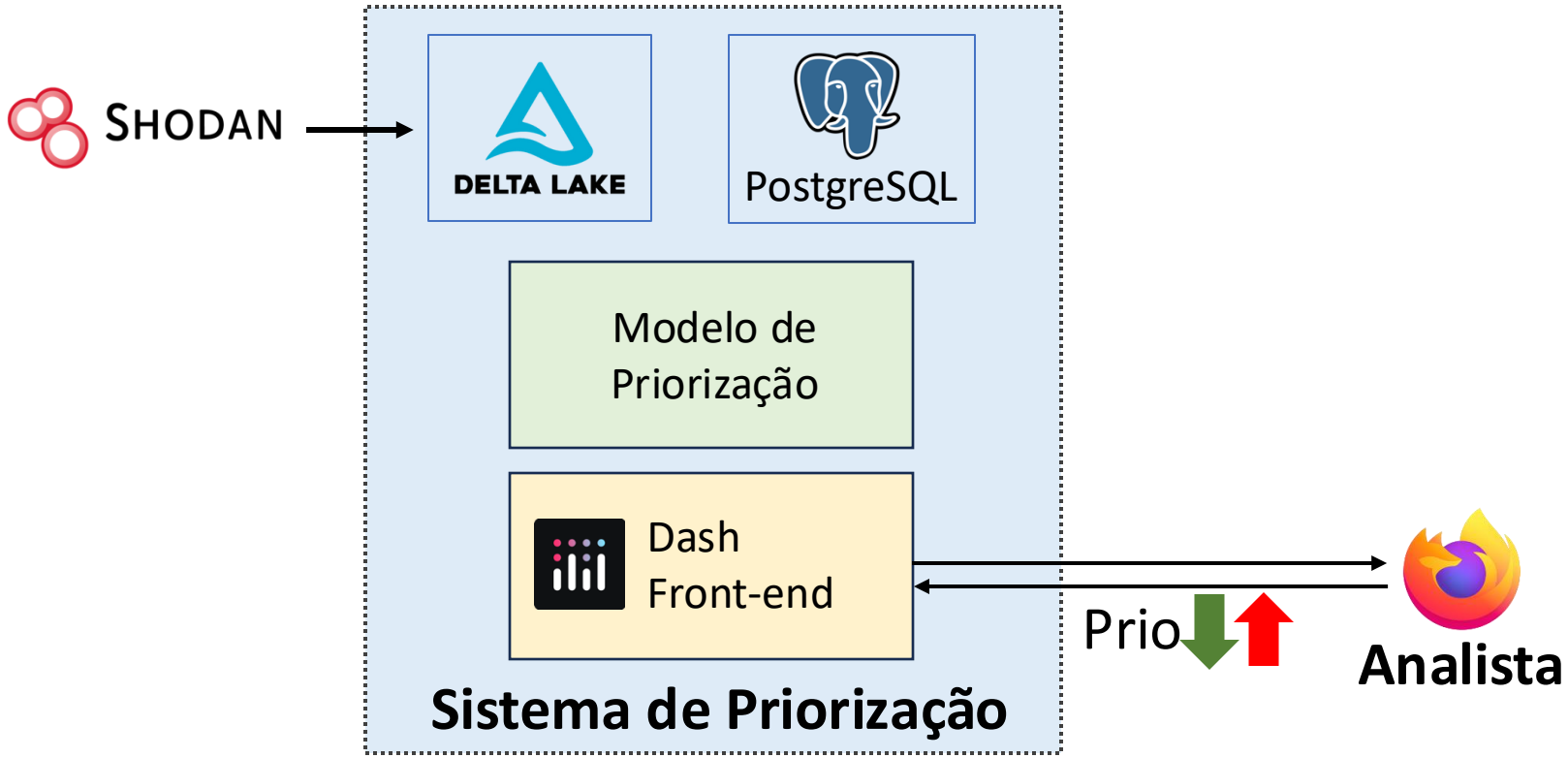
- Classificação requer significativos recursos computacionais
  - Dezenas de milhares de scripts de detecção
  - Necessário executar uma vez para cada script de detecção

- Humano precisa conhecer a ferramenta para construção do *prompt*
  - Múltiplos prompts por aplicação → simplificação e melhoria de precisão

Priorização de vulnerabilidades



Shogun


SHODAN
DELTA LAKE
PostgreSQL
Modelo de Priorização
Dash Front-end
Sistema de Priorização
Prio
Analista