



26^o
Workshop
RNP

Desafios e soluções para priorização de vulnerabilidades

Ítalo Cunha

Universidade Federal de Minas Gerais

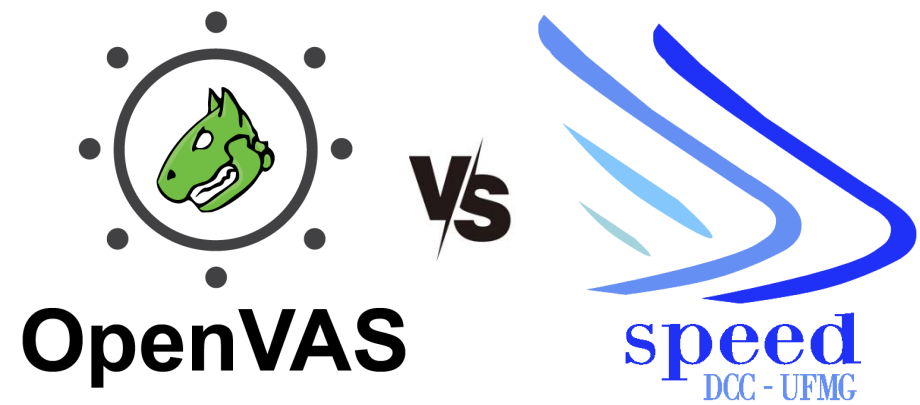
GT-CRIYO

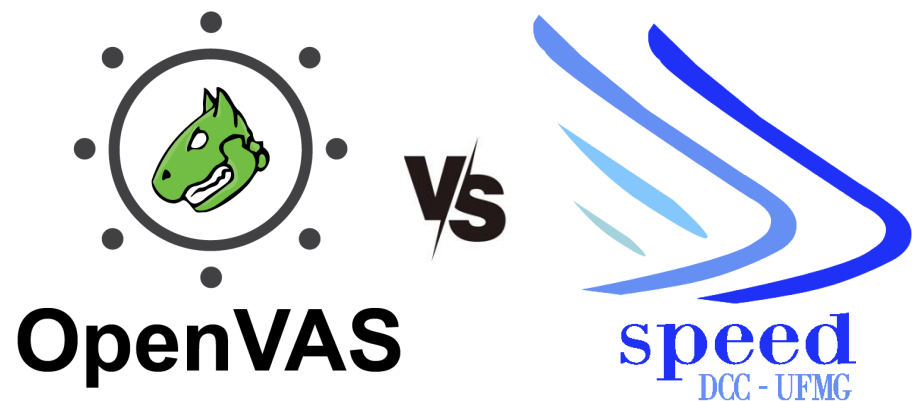


26^o
Workshop
RNP

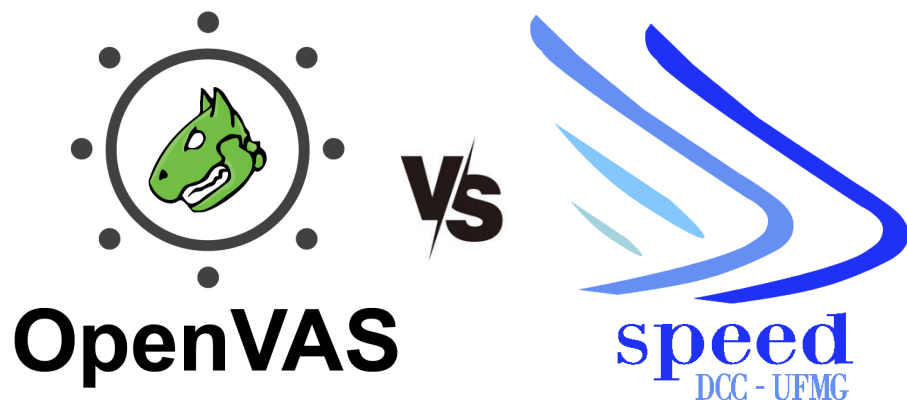
Desafios e soluções para priorização
de vulnerabilidades

Ítalo Cunha
Universidade Federal de Minas Gerais





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

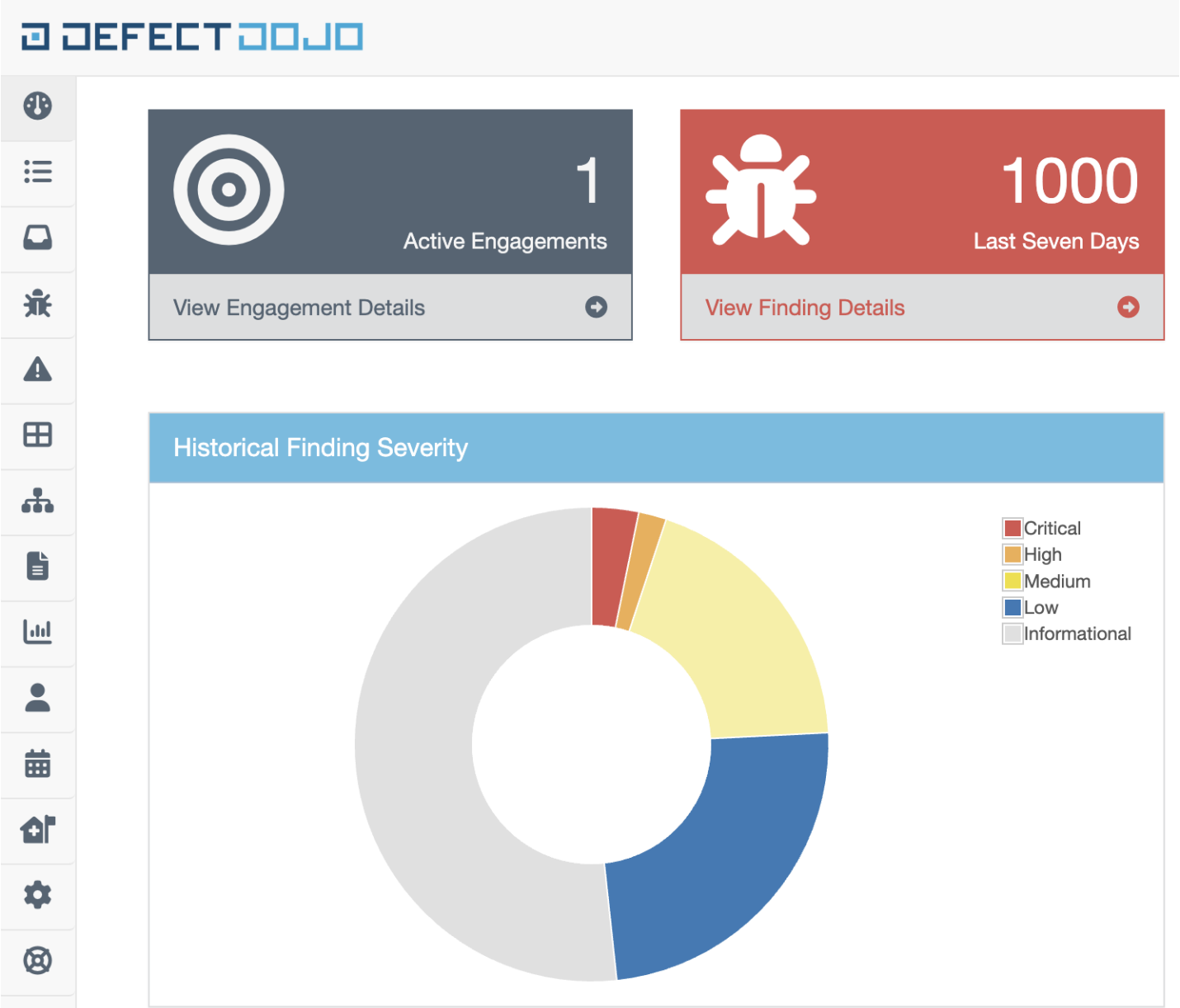


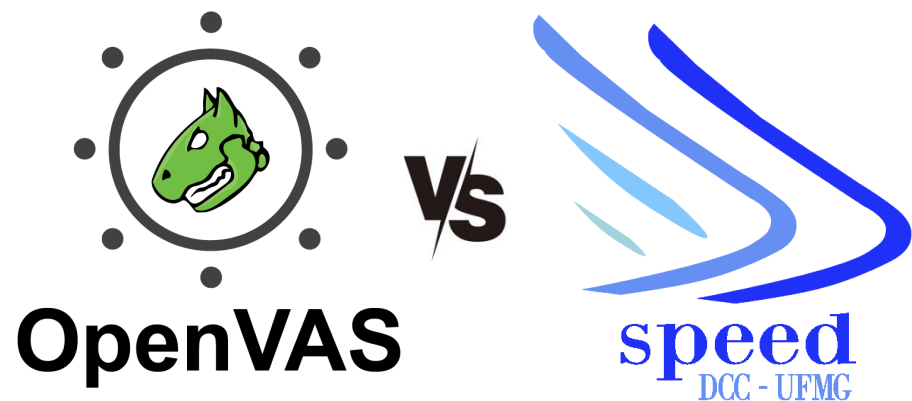
Mais de 1000 vulnerabilidades encontradas pelo OpenVAS nas dezenas de máquinas do laboratório Speed

32 críticas

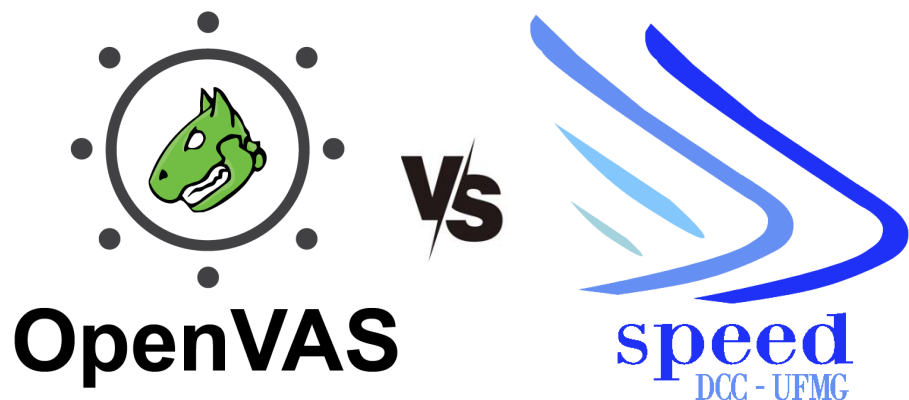
19 graves

191 médias

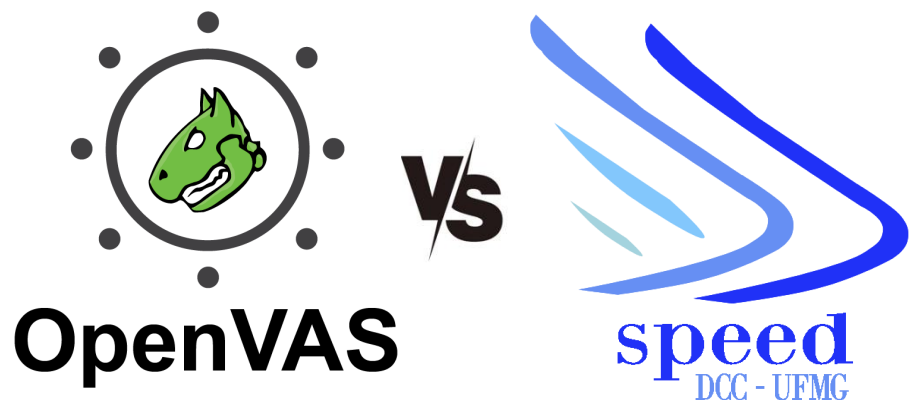




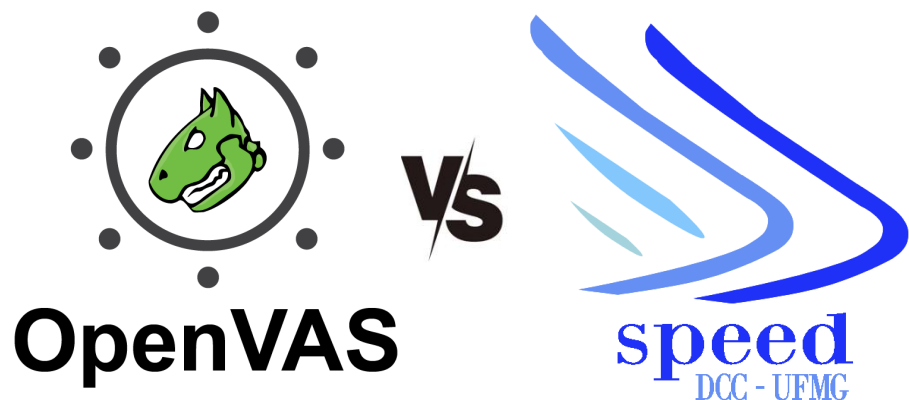
CVSS	Título
10.0	IPMI 'No Auth' Access Mode Enabled
10.0	Operating System Support End of Life
10.0	Apache Hadoop 'Secure Mode' Disabled



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

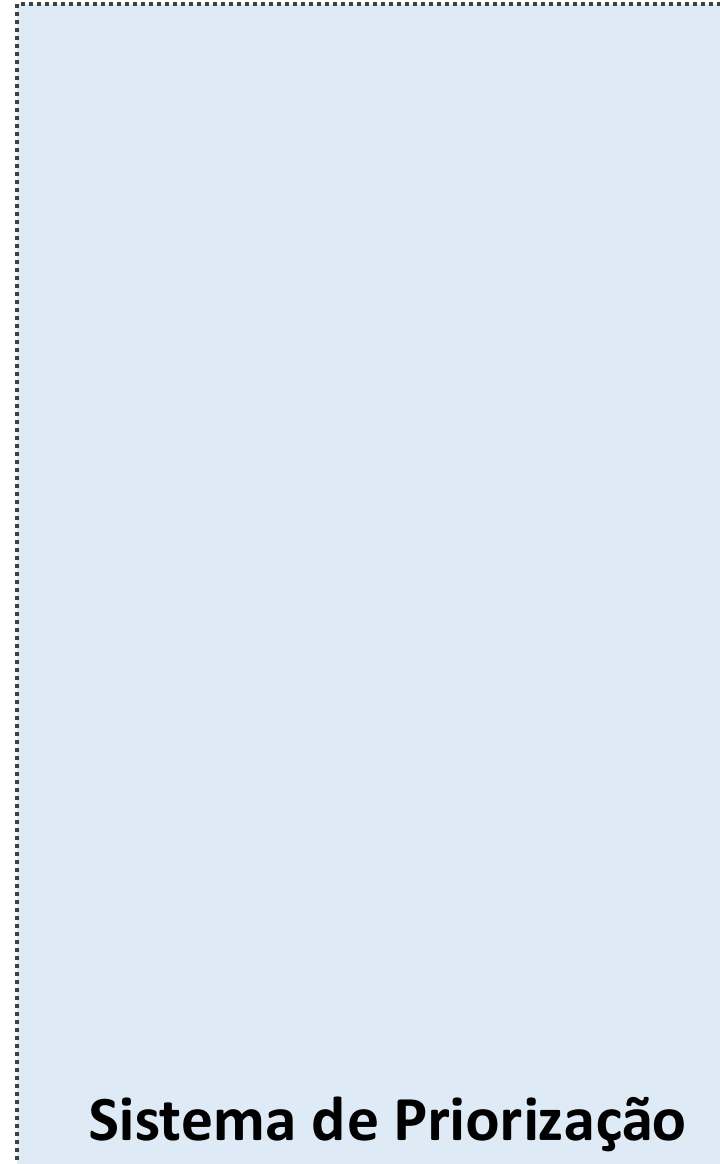


CVSS	Título	Importante?
10.0	IPMI 'No Auth' Access Mode Enabled	Firewall bloqueia
10.0	Operating System Support End of Life	É servidor ou desktop?
10.0	Apache Hadoop 'Secure Mode' Disabled	



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

Entradas

Sistema de Priorização

Sistema de priorização de vulnerabilidades



Entradas

Sistema de Priorização

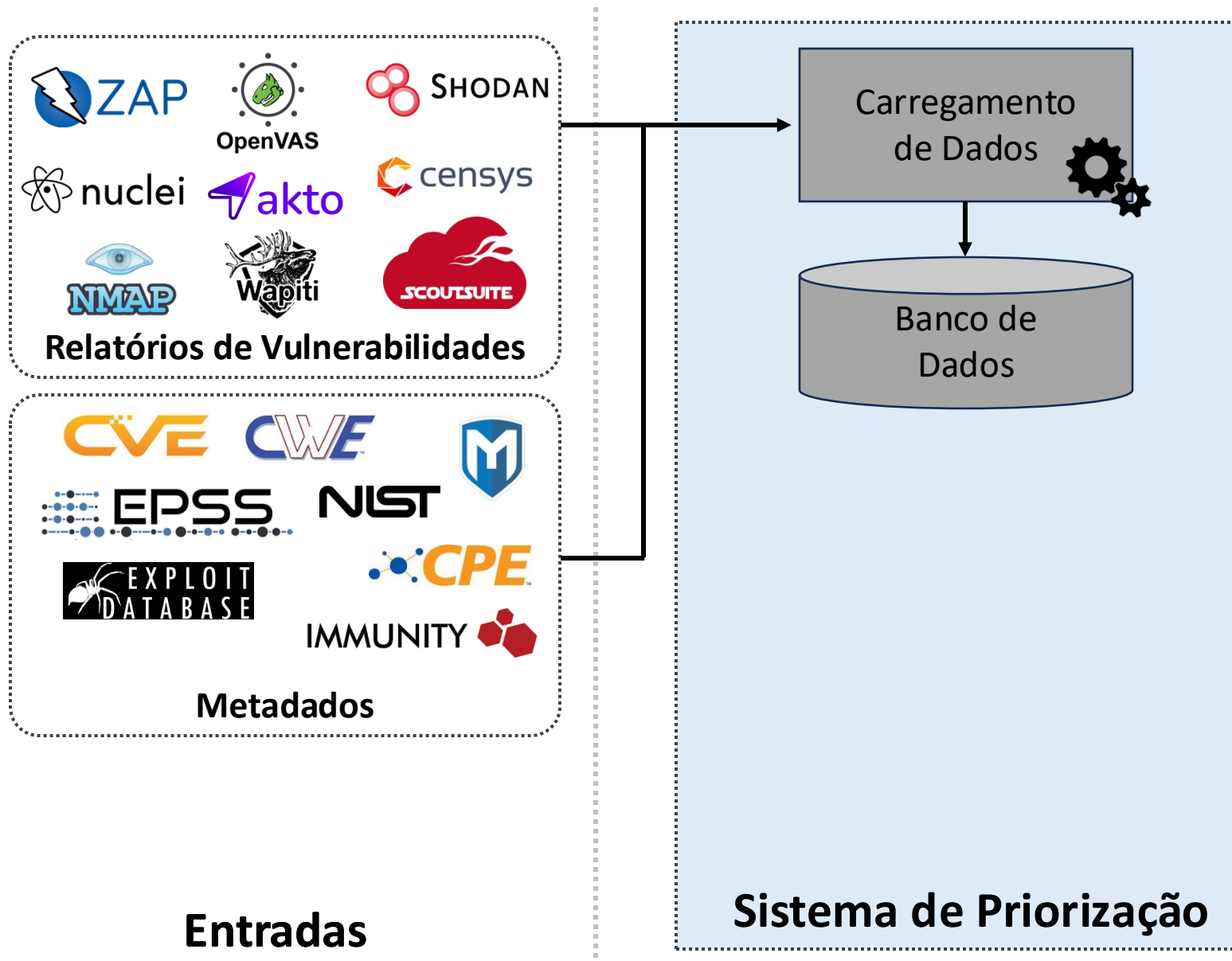
Sistema de priorização de vulnerabilidades



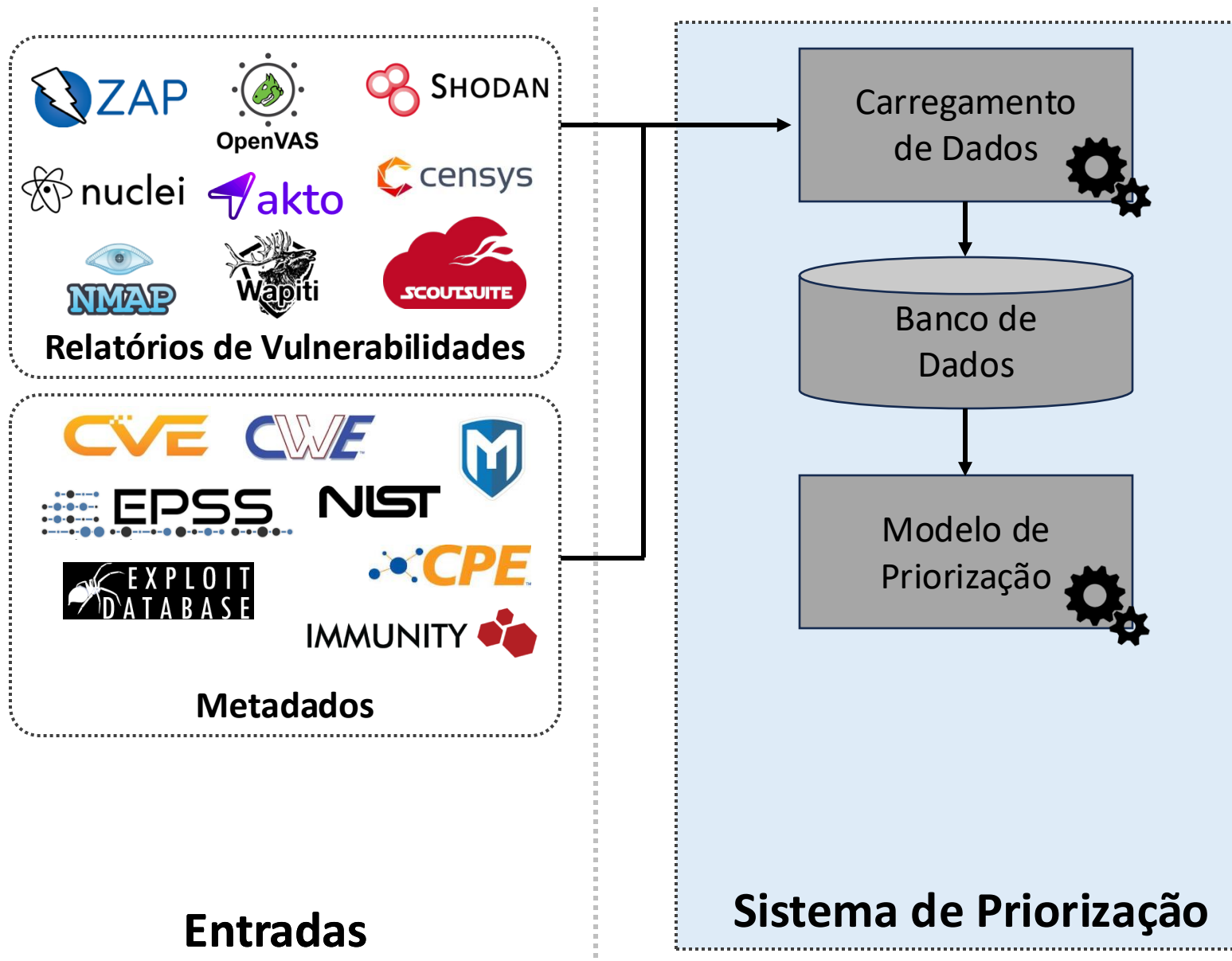
Entradas

Sistema de Priorização

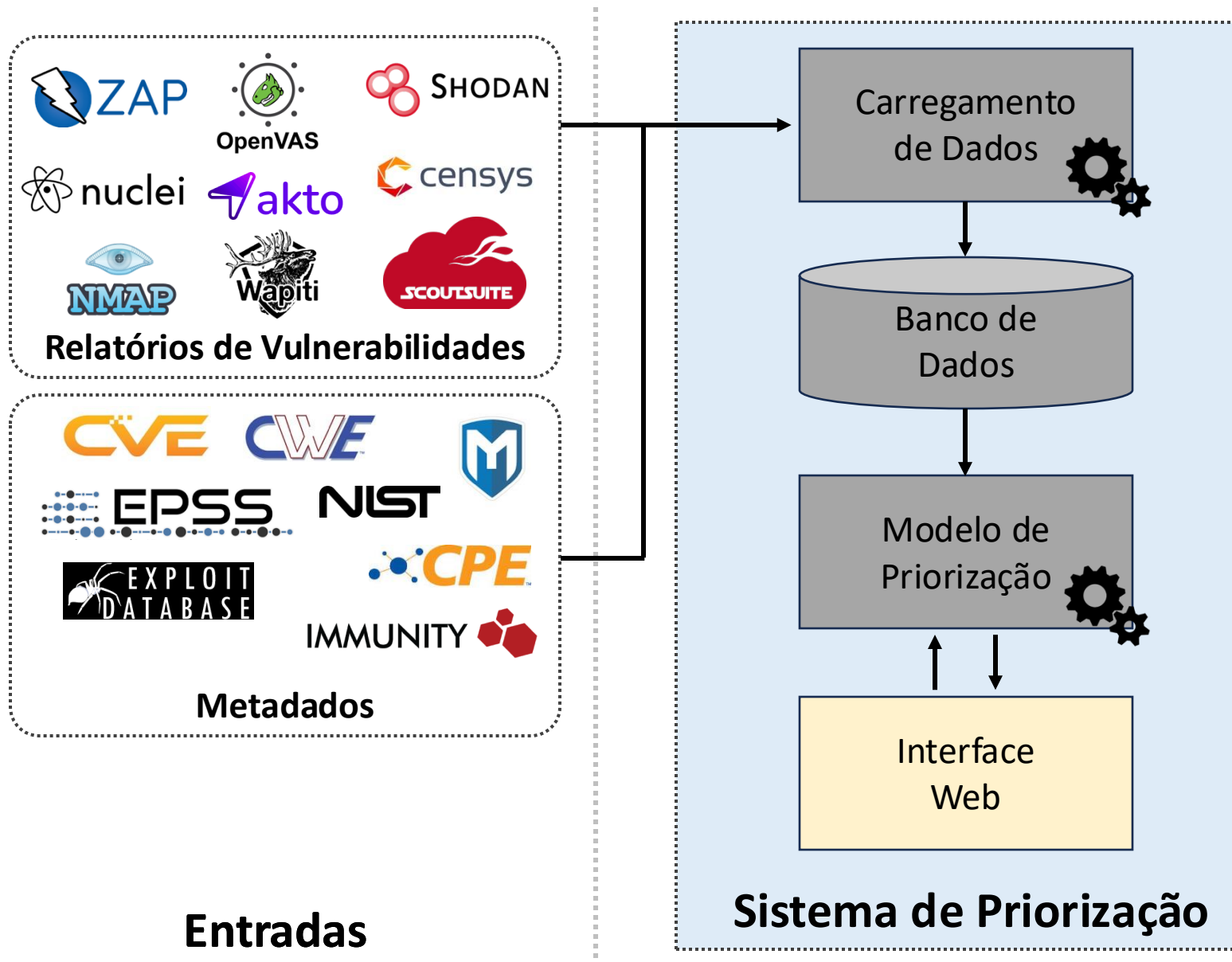
Sistema de priorização de vulnerabilidades



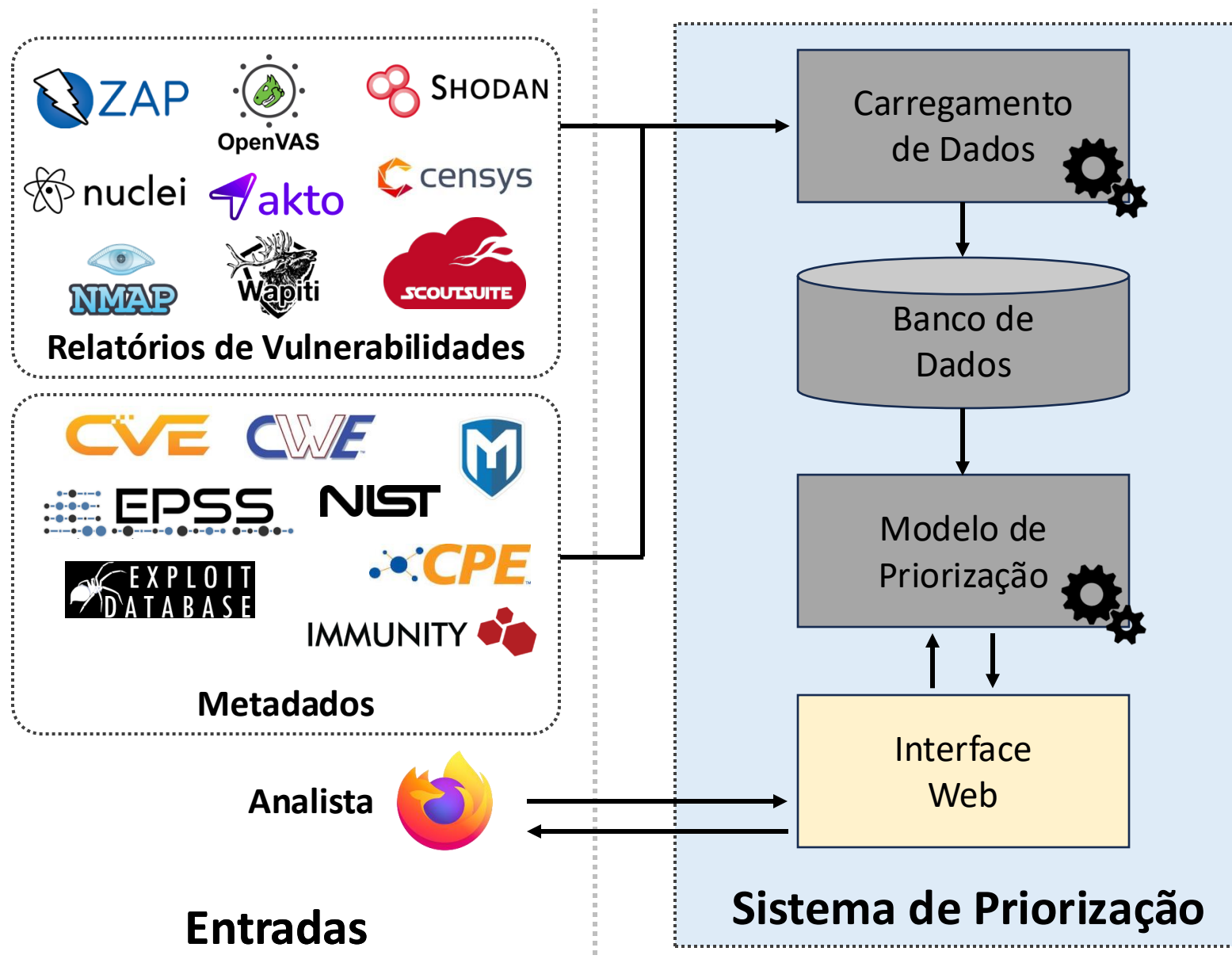
Sistema de priorização de vulnerabilidades



Sistema de priorização de vulnerabilidades



Sistema de priorização de vulnerabilidades





26[•]
Workshop
RNP

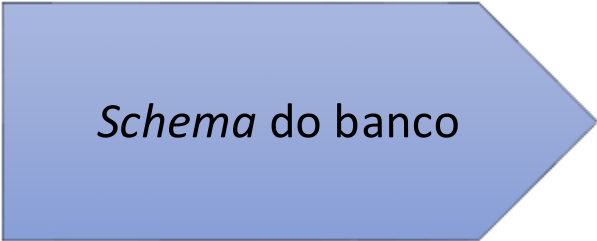
**Desafio para priorização:
Análises de vulnerabilidades
para treino**

Inferência de risco com dados históricos

- Inferência de risco usando bases de dados de sistemas de gerência
- Indicadores de risco
 - Tempo de resposta ao incidente
 - Quantidade de analistas envolvidos
 - Número de interações (mensagens)

Obtendo bases de dados de sistemas de gerência

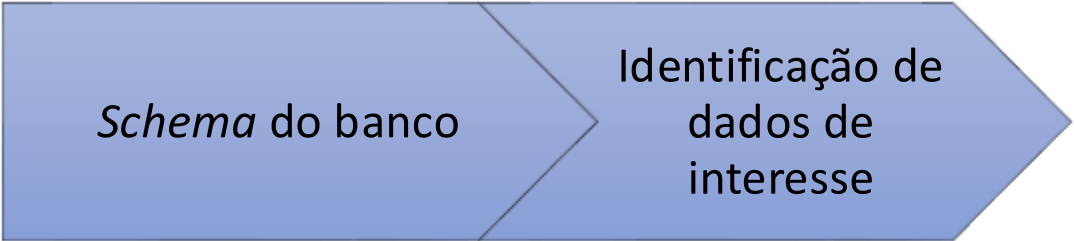
- Controle do risco vs. perda de informações úteis
- Anonimização dos dados específica para o contexto



Schema do banco

Obtendo bases de dados de sistemas de gerência

- Controle do risco vs. perda de informações úteis
- Anonimização dos dados específica para o contexto

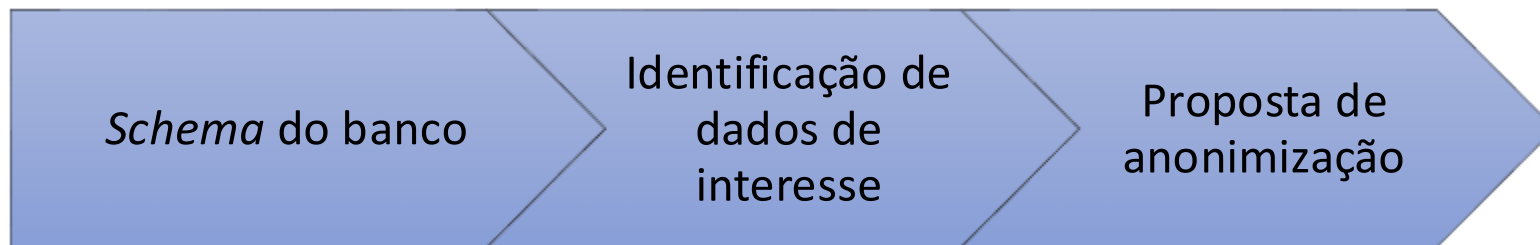


Schema do banco

Identificação de
dados de
interesse

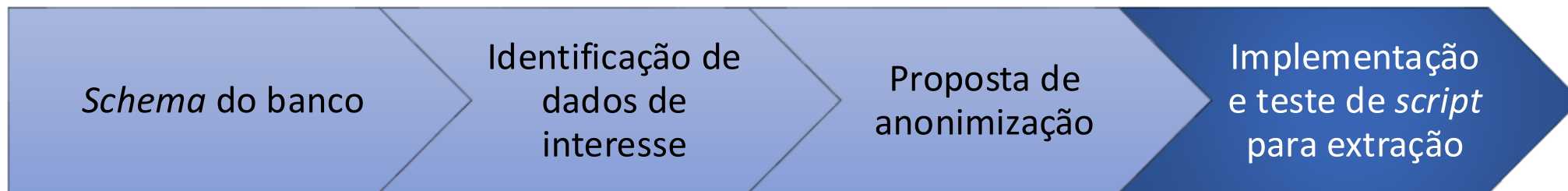
Obtendo bases de dados de sistemas de gerência

- Controle do risco vs. perda de informações úteis
- Anonimização dos dados específica para o contexto



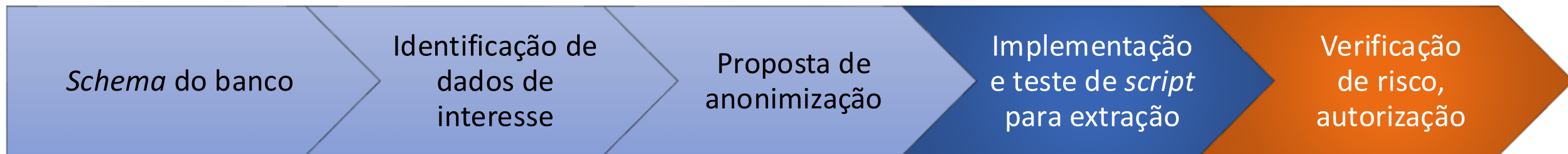
Obtendo bases de dados de sistemas de gerência

- Controle do risco vs. perda de informações úteis
- Anonimização dos dados específica para o contexto



Obtendo bases de dados de sistemas de gerência

- Controle do risco vs. perda de informações úteis
- Anonimização dos dados específica para o contexto



Criação de bases para treino

- Obtenção de dados de varreduras de rede
- Análises de vulnerabilidades por analistas de segurança

Extensões ao DefectDojo

All Findings



Showing entries 1 to 25 of 1000

1

2

3

4

5

6

7

8

9

10

...

40

Next

Page Size ▾

Column visibility

Copy

PDF

Print

Search:



Severity ▴

Name ⇅

CWE ▴

Vulnerability Id ▴

EPSS
Score ▴

EPSS
Percentile ▴

Votes



High

Report Default
Community Names
of the SNMP
Agent_
👤

🔗 CVE-1999-0517

92.33%

99.72%

Nothing selected ▾



High

SSL/TLS: Report
Vulnerable Cipher
Suites for
HTTPS_
👤

🔗 CVE-2016-2183

40.02%

97.06%

Mild
Moderate
Severe
Critical

Metadatos sobre vulnerabilidades

DEFECTDOJO

Search...



5



SSL/TLS: Report Vulnerable Cipher Suites for HTTPS_150.164.23.203_443/tcp Last Reviewed today by Admin User (admin), Last Status Update today, Created today , Last Mentioned in (Re)Import: today as created



Metadata



* Cards with a black border have a KEV (Known Exploited Vulnerability) associated with them!

CVE-2020-29583

EPSS 0.94
CVSSv3 9.8

Privilege Escalation
CWE-522

CVE-1999-0502

EPSS 0.53
CVSS Missing 0.0

CVE-2009-3710

EPSS 0.03
CVSS Missing 0.0

Privilege Escalation
Remote Code Execution

CVE-2012-4577

EPSS 0.03
CVSSv2 10.0

Privilege Escalation
Remote Code Execution

Korenix Jetport



KEV

CPE

Criação de bases para treino

- Obtenção de dados de varreduras de rede
- Análises de vulnerabilidades por
 - Integrantes do projeto
 - Residentes do programa Hackers do Bem

Criação de bases para treino

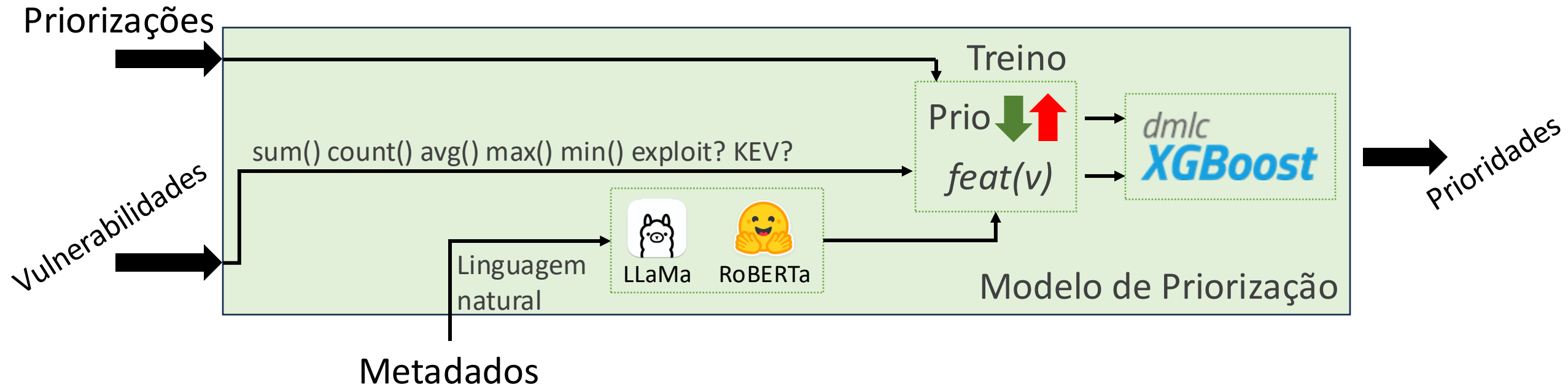
- Obtenção de dados de varreduras de rede
- Análises de vulnerabilidades por
 - Integrantes do projeto
 - Residentes do programa Hackers do Bem
- Pouco realismo
 - Bolsistas e residentes não são responsáveis pela segurança
 - Bolsistas e residentes não atuam em conjunto



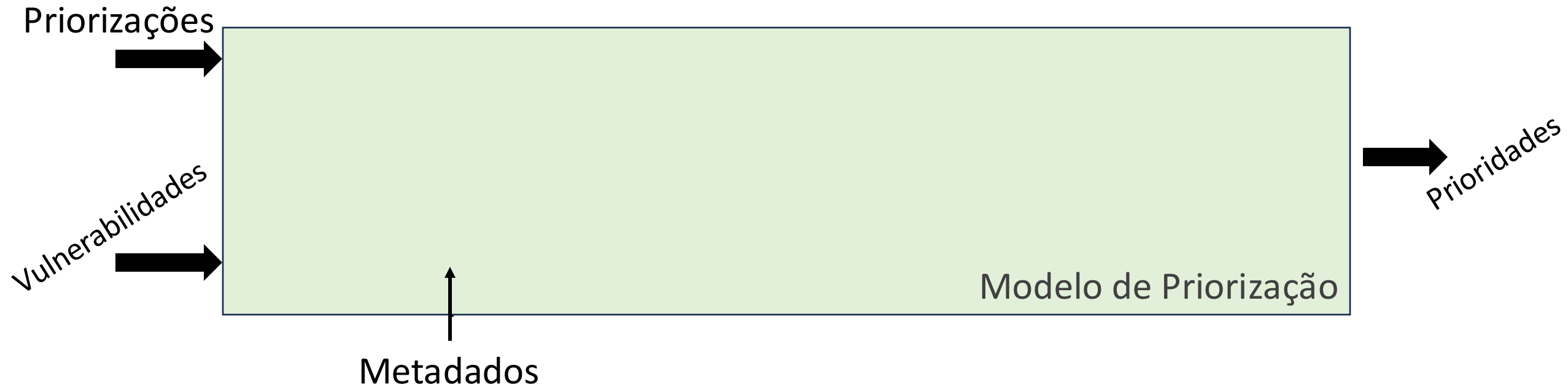
26[•]
Workshop
RNP

Priorização de vulnerabilidades

Modelo de priorização de vulnerabilidades

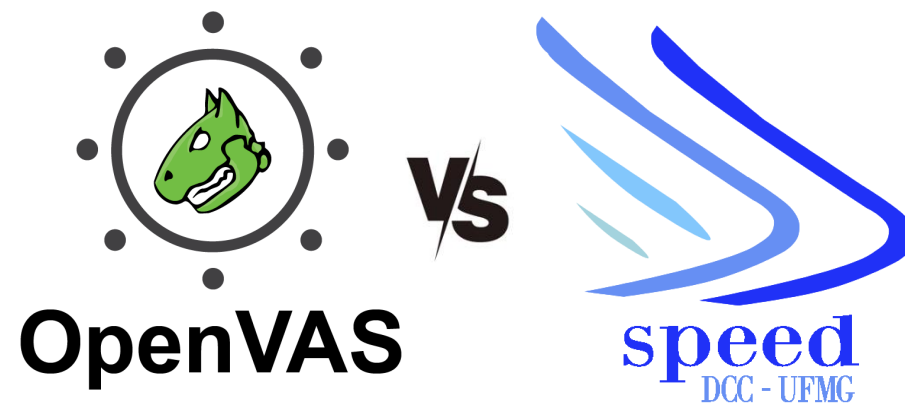


Modelo de priorização de vulnerabilidades



Fatores que impactam a precisão do modelo

- Diversidade das vulnerabilidades
 - Bases de teste balanceadas



32 críticas

19 graves

191 médias

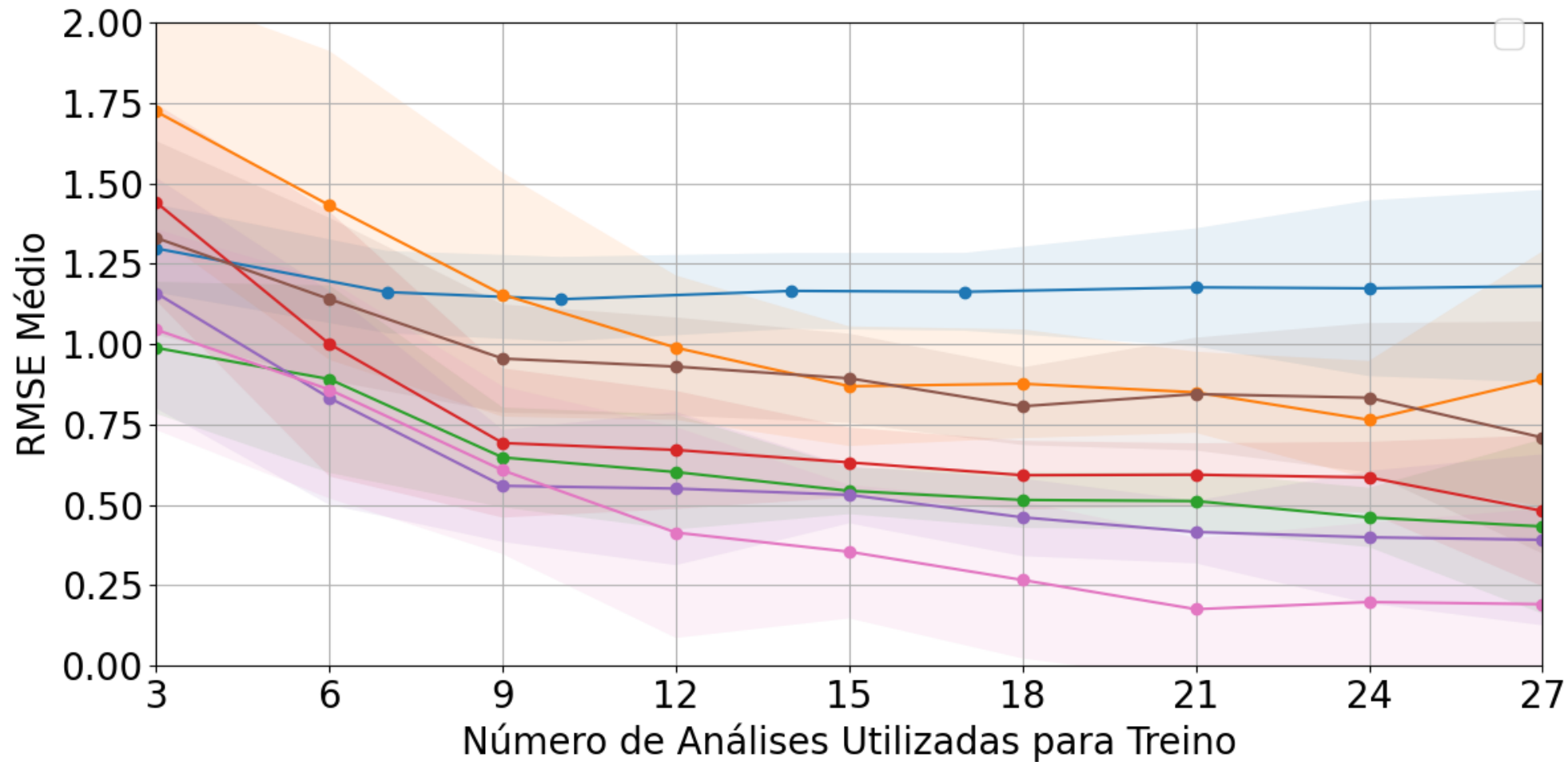
Fatores que impactam a precisão do modelo

- Diversidade das vulnerabilidades
 - Bases de teste balanceadas
- Perfil do analista
 - Grave para um, moderado para outro
 - Maior ou menor alinhamento com a média

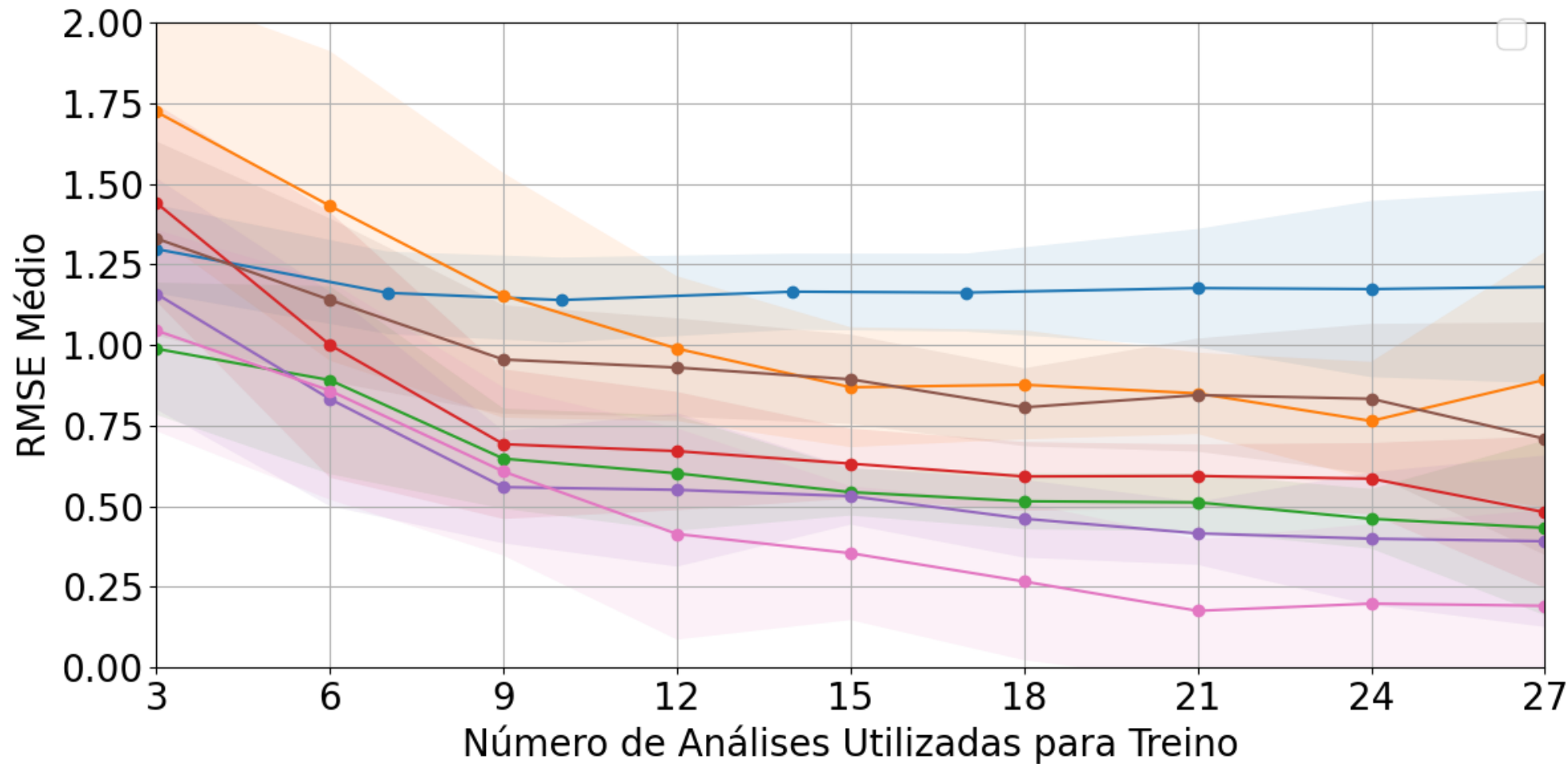
Fatores que impactam a precisão do modelo

- Diversidade das vulnerabilidades
 - Bases de teste balanceadas
- Perfil do analista
 - Grave para um, moderado para outro
 - Maior ou menor alinhamento com a média
- Incerteza no risco
 - Graves, moderadas, leves
 - “Hum... depende”

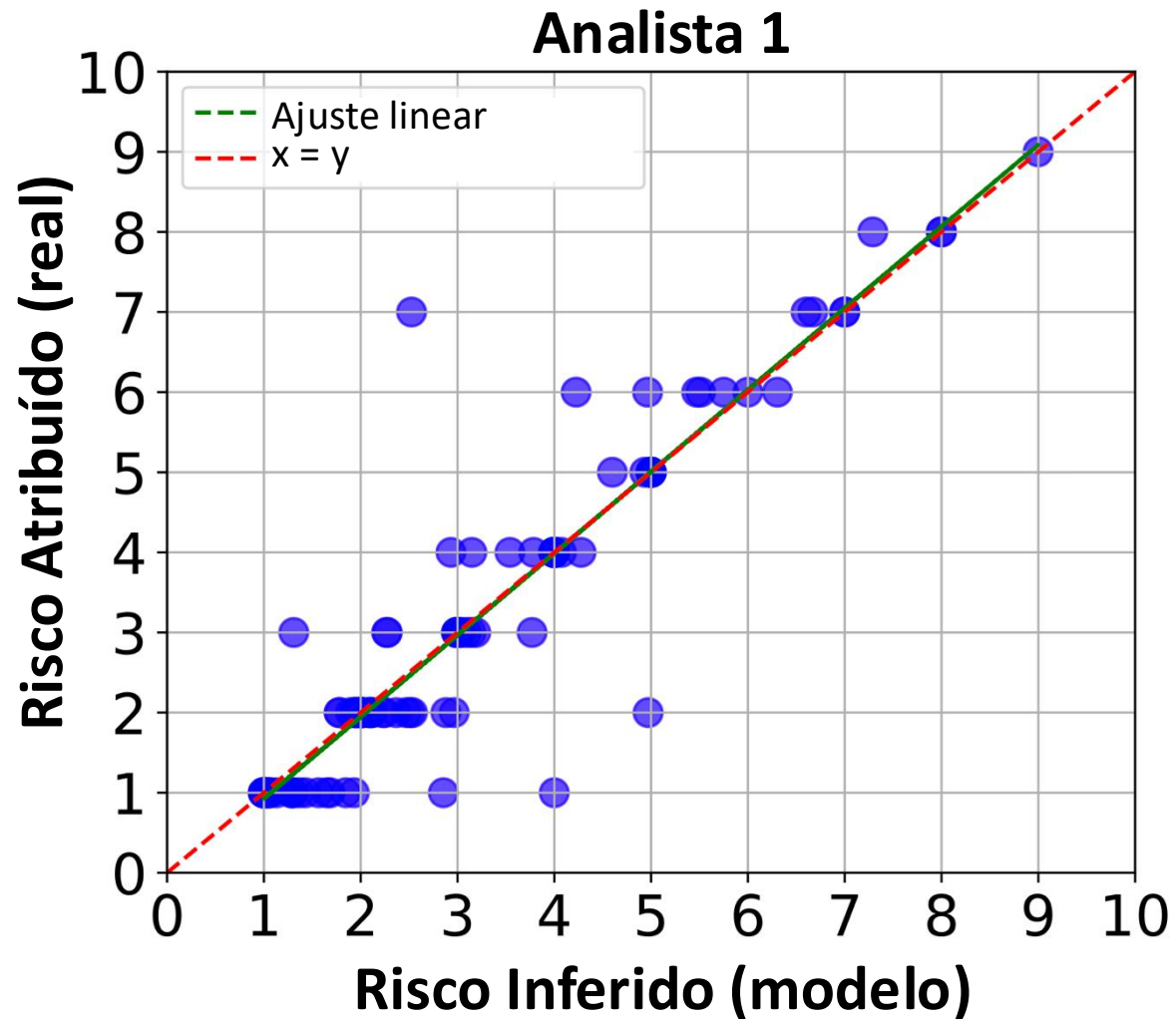
Quantas análises são necessárias para treino?



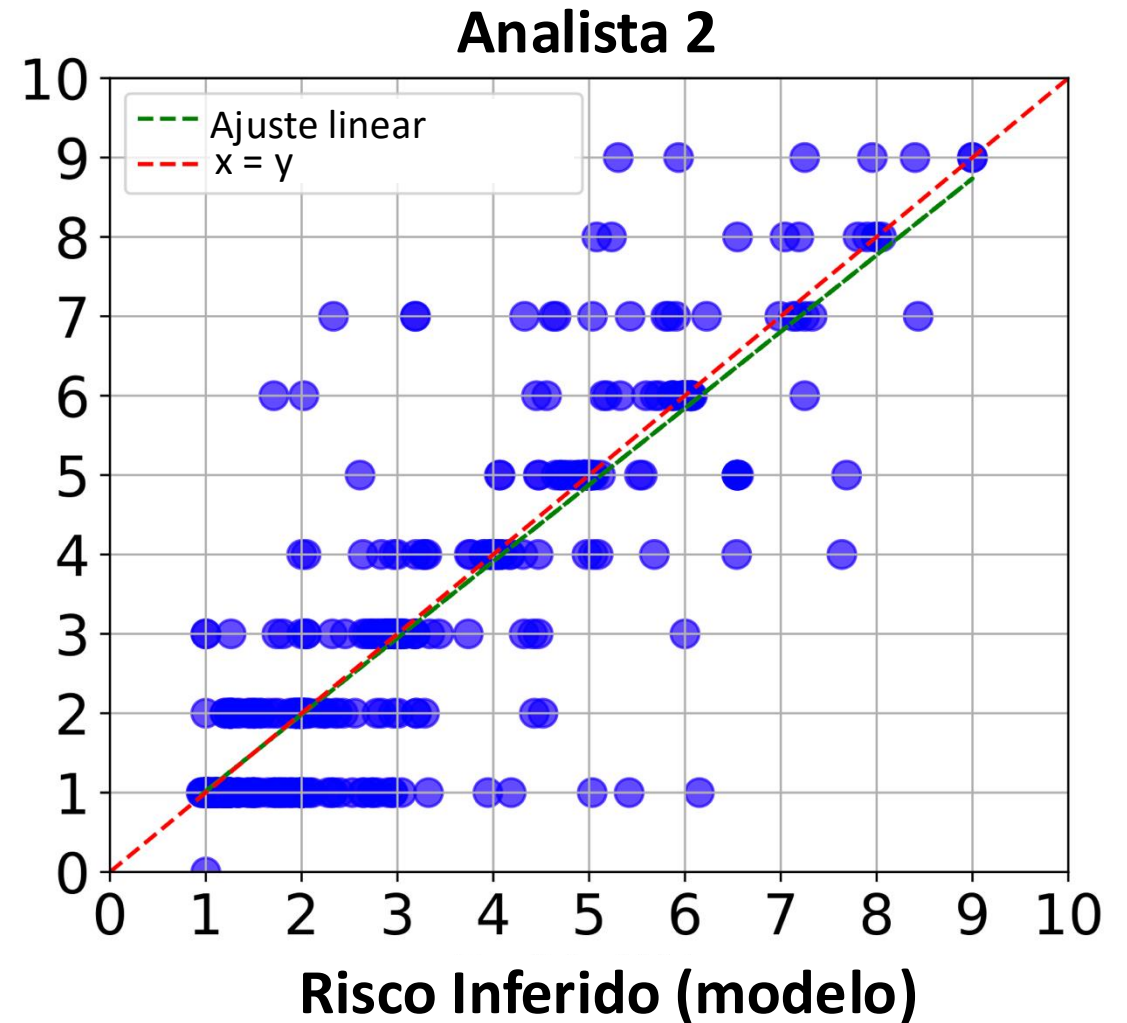
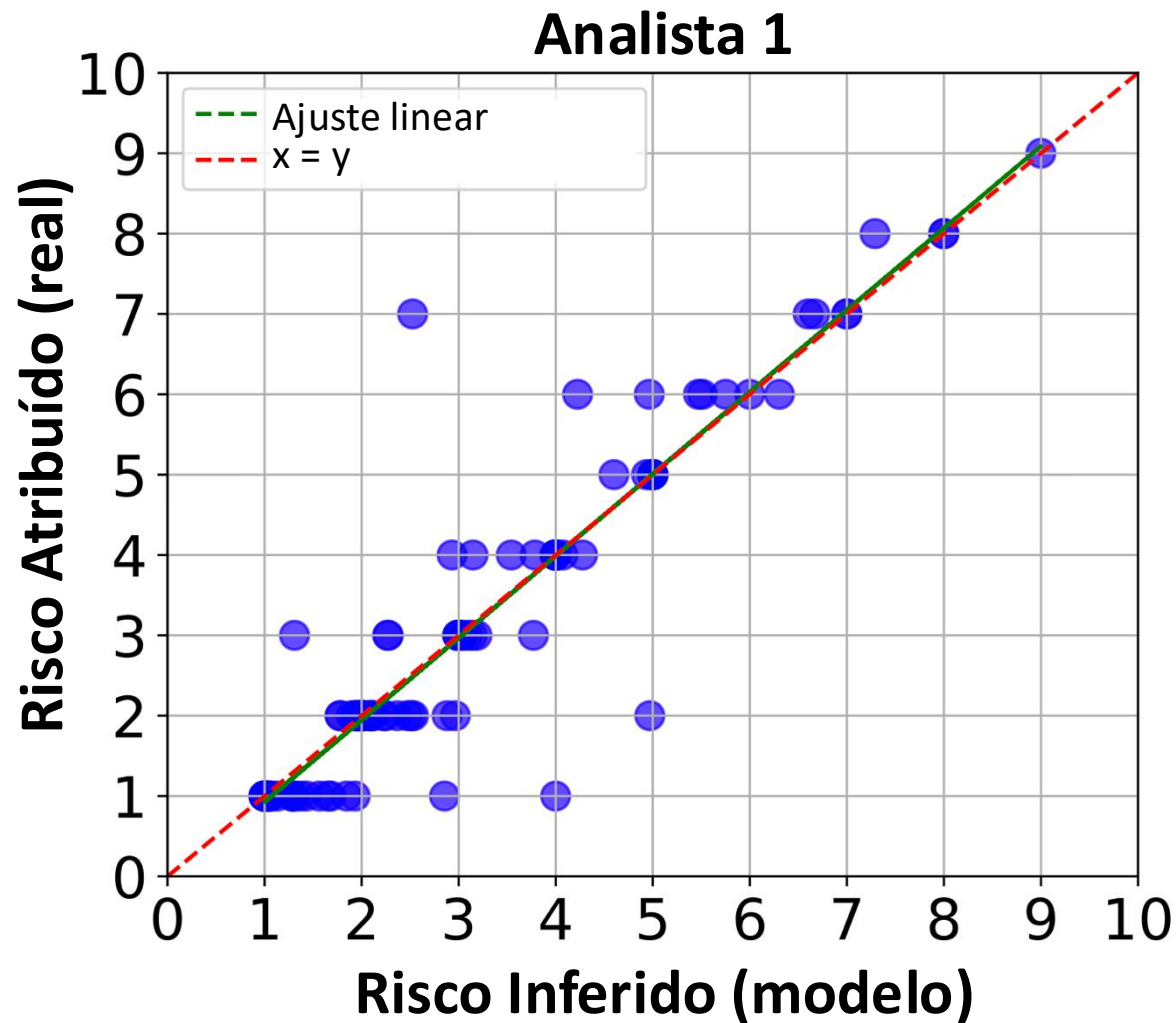
Quantas análises são necessárias para treino?



Previsões correlacionadas com os votos



Previsões correlacionadas com os votos





26[•]
Workshop
RNP

Aplicações de IA para priorização de vulnerabilidades

Extração de dados de linguagem natural

- Muita informação sobre vulnerabilidades em linguagem natural
 - Descrição do CVE, CWE, *exploits*
 - Mensagens de discussão de vulnerabilidades
 - Listas de discussão
 - Fóruns
 - Sistemas de gerência de vulnerabilidades
 - Páginas Web

Extração de dados de linguagem natural

- Muita informação sobre vulnerabilidades em linguagem natural
 - Descrição do CVE, CWE, *exploits*
 - Mensagens de discussão de vulnerabilidades
 - Listas de discussão
 - Fóruns
 - Sistemas de gerência de vulnerabilidades
 - Páginas Web
- Geração de propriedades (*features*) que podem ser usadas como entrada para modelos de IA

Metadatos relacionados a vulnerabilidades

CVE-2020-29583 [↗](#)

Privilege Escalation

CWE-522 [↗](#)

EPSS 0.94
CVSSv3 9.8

CVE-1999-0502 [↗](#)

EPSS 0.53
CVSS Missing 0.0

CVE-2009-3710 [↗](#)

Privilege Escalation
Remote Code Execution

EPSS 0.03
CVSS Missing 0.0

CVE-2012-4577 [↗](#)

Privilege Escalation
Remote Code Execution

EPSS 0.03
CVSSv2 10.0

Korenix Jetport

CPE

KEV

Metadados relacionados a vulnerabilidades

CVE-2020-29583 [↗](#)

Privilege Escalation
CWE-522 [↗](#)

EPSS 0.94
CVSSv3 9.8

KEV

CVE-2009-3710 [↗](#)

Privilege Escalation
Remote Code Execution

EPSS 0.03
CVSS Missing 0.0

Inferências de propriedades a partir de descrições textuais usando LLMs

- Descrição do CVE
- Procedimento de mitigação
- Código do *script* de detecção
- Nomes de organização
- Conteúdo de página Web

Identificação de vulnerabilidades relacionadas

- Modelos generativos para analisar os *scripts* das ferramentas
- Caracterizamos os scripts em múltiplas dimensões

Identificação de vulnerabilidades relacionadas

- Modelos generativos para analisar os *scripts* das ferramentas
- Caracterizamos os scripts em múltiplas dimensões



Anonimização de nomes de domínio (DNS)

- Proteger a identidade do dispositivo
- Capturar informações relacionadas a possível impacto

Anonimização de nomes de domínio (DNS)

- Proteger a identidade do dispositivo
- Capturar informações relacionadas a possível impacto

esxi.dcomp.uni.edu.br → aplicação (hypervisor)

staging.dcomp.uni.edu.br → contexto (ambiente de testes)



26[•]
Workshop
RNP

**Ideias para
o futuro**

Ideias para o futuro

- Modelos de priorização explicáveis
 - Não só priorizar as vulnerabilidades
 - Justificar a priorização em função dos dados disponíveis
- Agentes inteligentes para cibersegurança
 - Construção de planos e auxílio para correção de vulnerabilidades
 - Execução de varreduras mais sofisticadas



26^o
Workshop
RNP

Desafios e soluções para priorização de vulnerabilidades

Ítalo Cunha

Universidade Federal de Minas Gerais