26 Workshop RNP

Desafios e soluções para priorização de vulnerabilidades

Ítalo Cunha
Universidade Federal de Minas Gerais

26 Workshop RNP

GT-CRIPTO

Desafios e soluções para priorização de vulnerabilidades

Ítalo Cunha
Universidade Federal de Minas Gerais

OpenVAS

VS

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

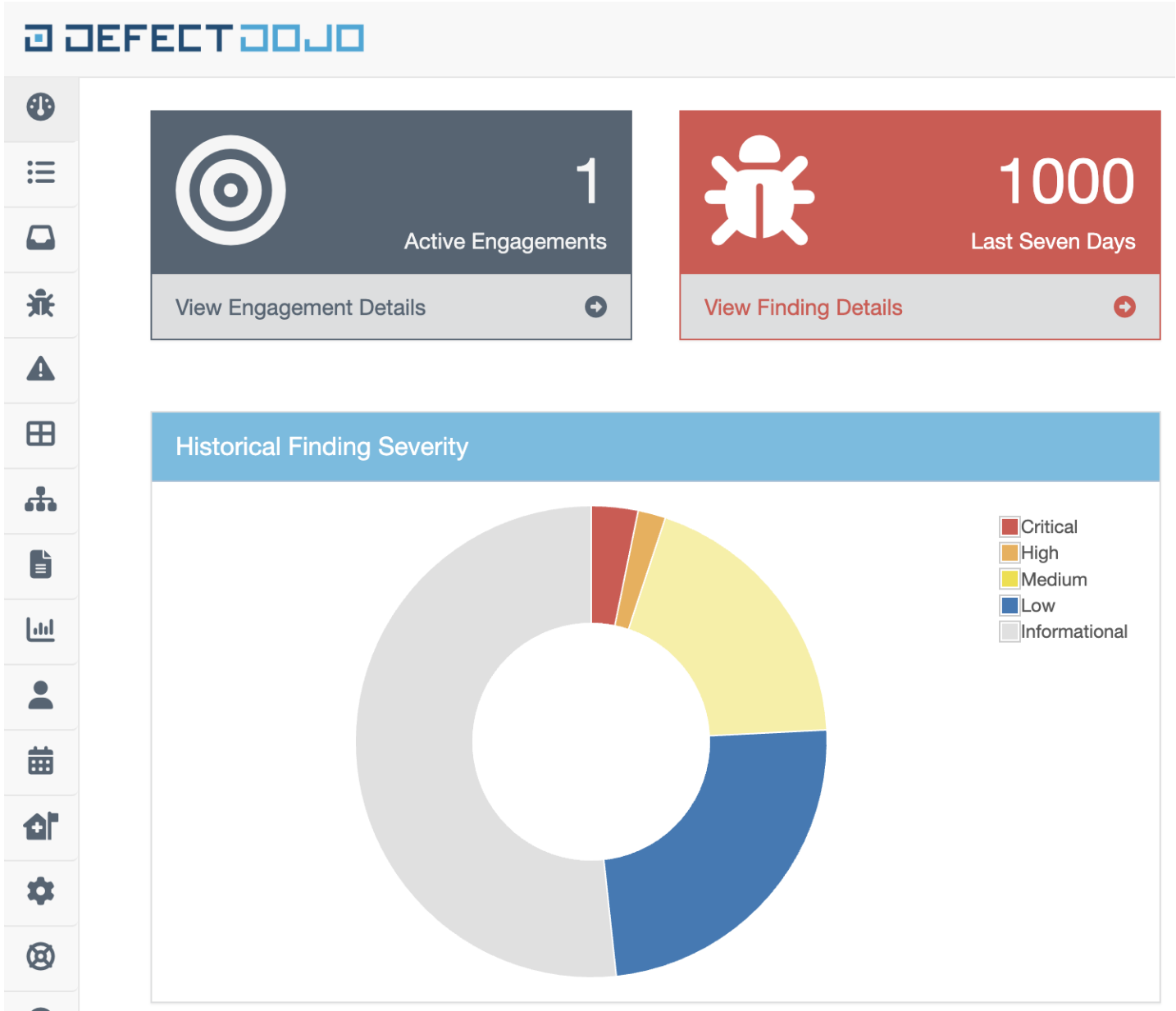
OpenVAS vs speed DCC - UFMG

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

32 críticas

19 graves

191 médias



OpenVAS

VS

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

OpenVAS

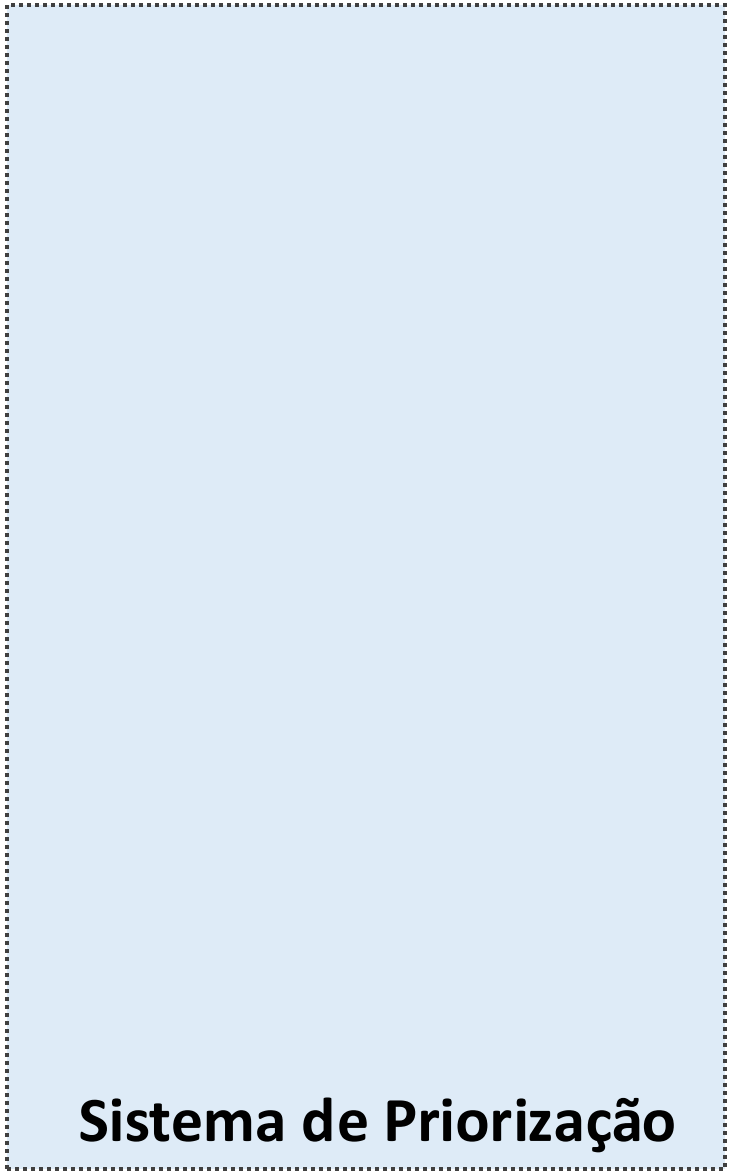
VS

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

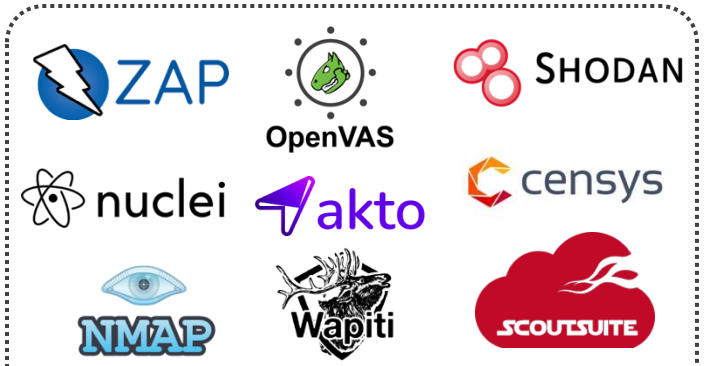


Sistema de priorização de vulnerabilidades

Entradas

Sistema de Priorização

Sistema de priorização de vulnerabilidades



Relatórios de Vulnerabilidades

Entradas

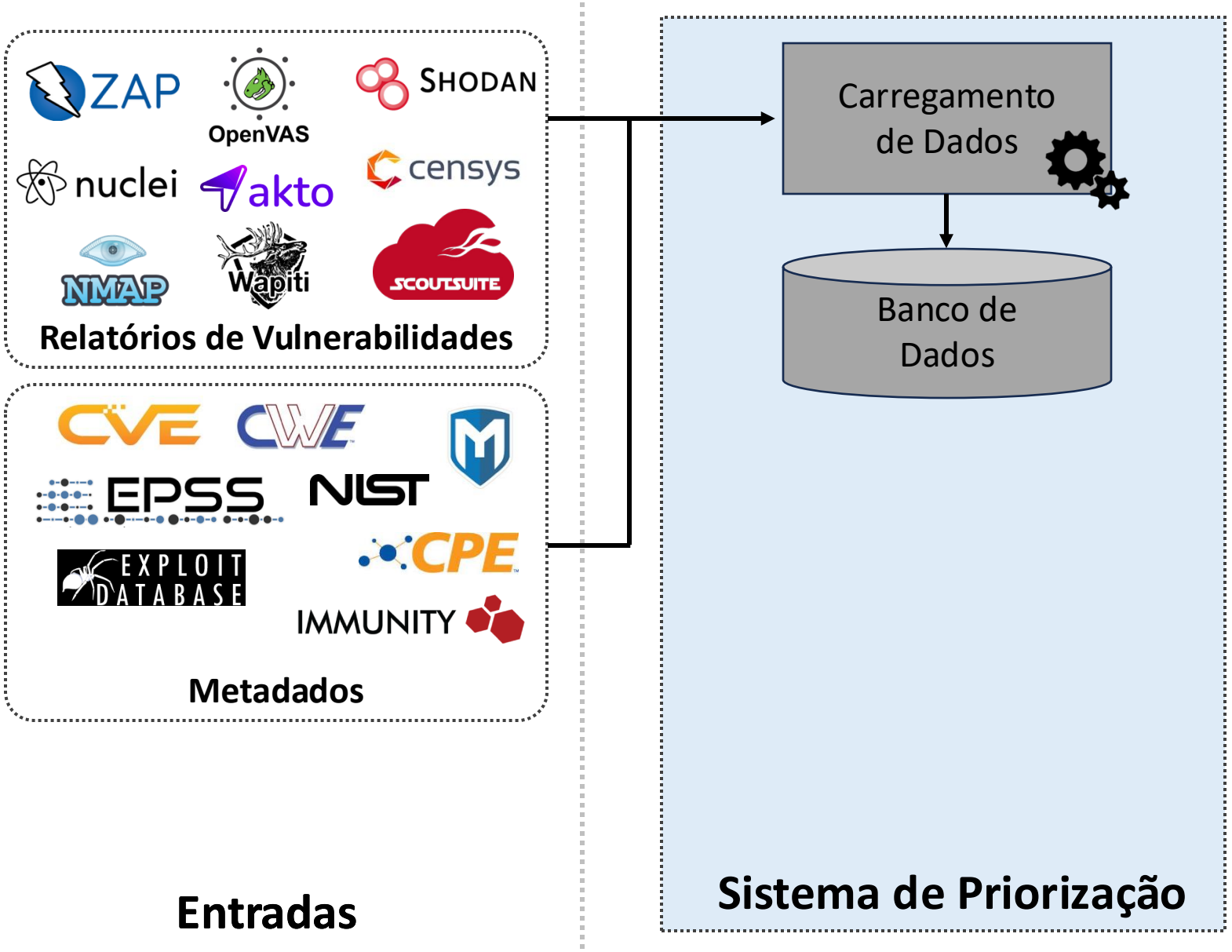
Sistema de Priorização

Sistema de priorização de vulnerabilidades

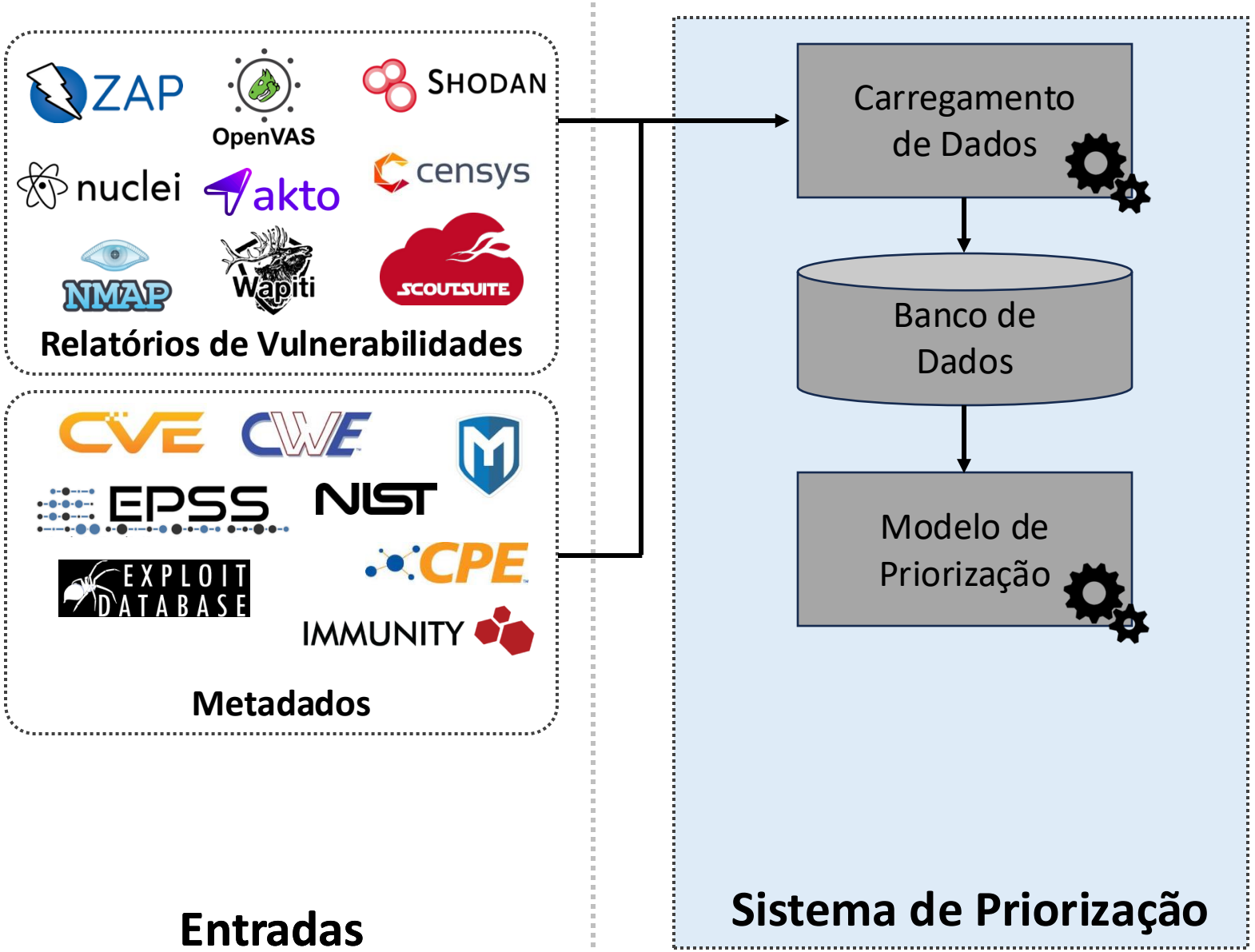
Entradas

Sistema de Priorização

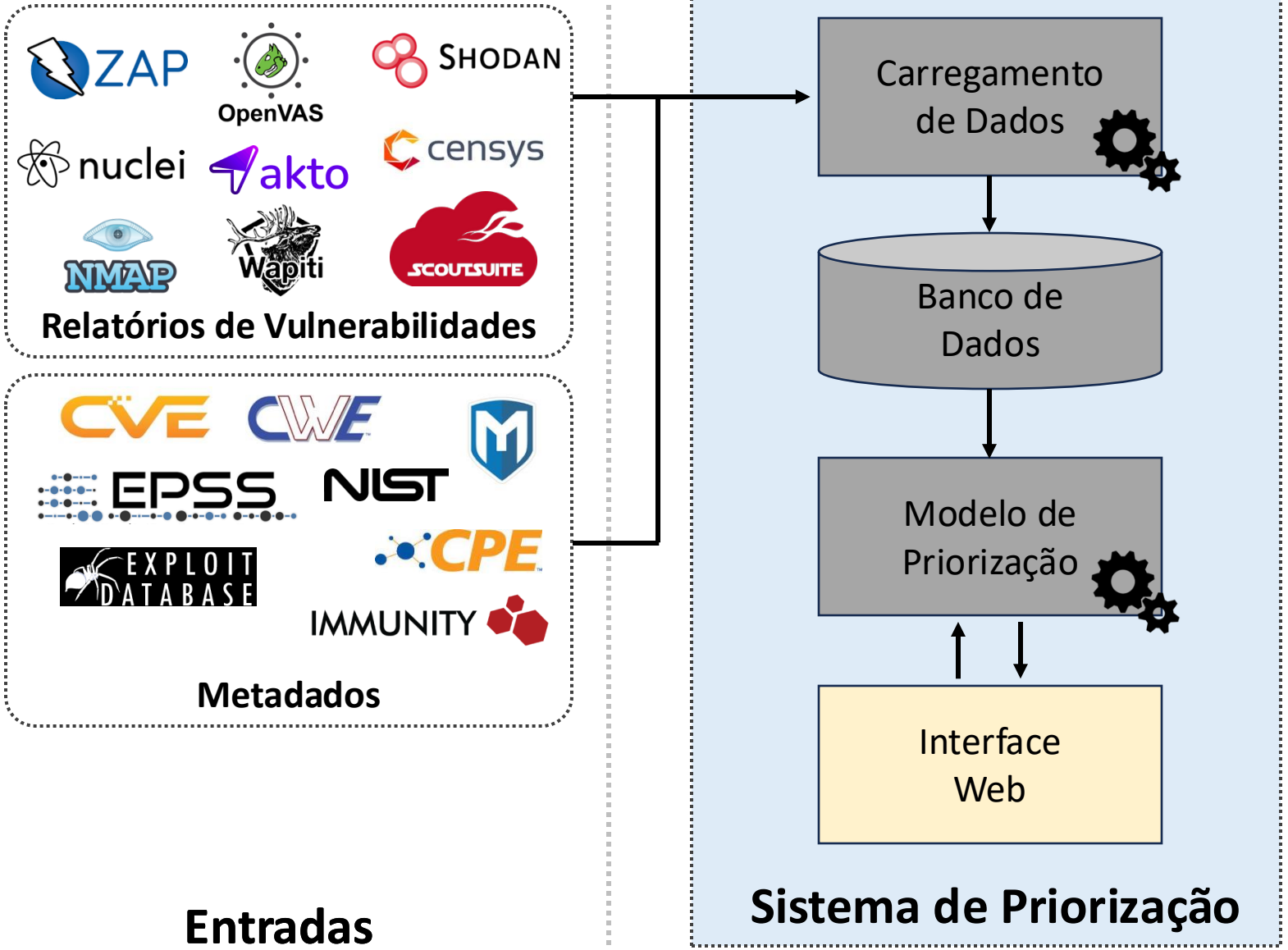
Sistema de priorização de vulnerabilidades



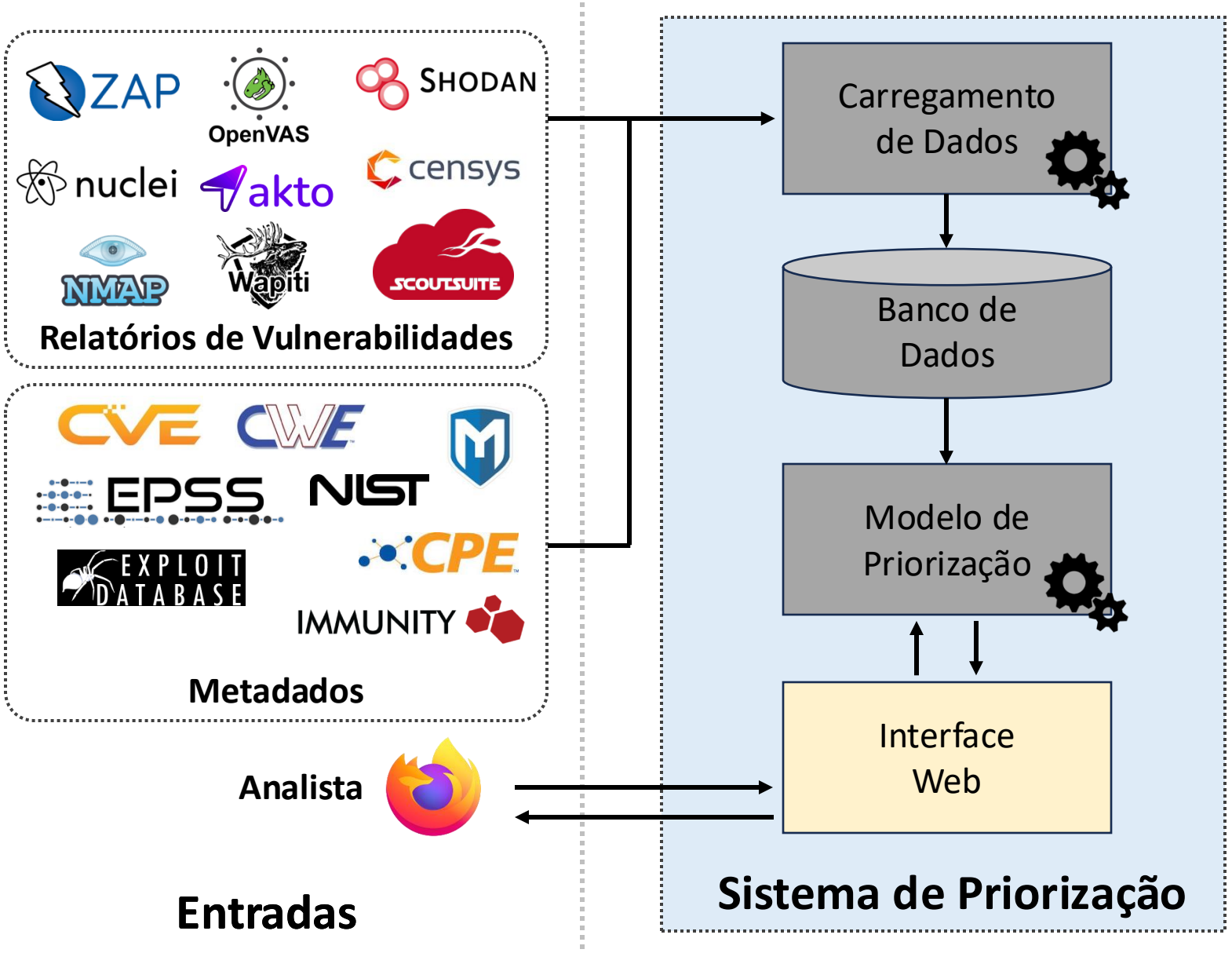
Sistema de priorização de vulnerabilidades



Sistema de priorização de vulnerabilidades



Sistema de priorização de vulnerabilidades



26 Workshop RNP

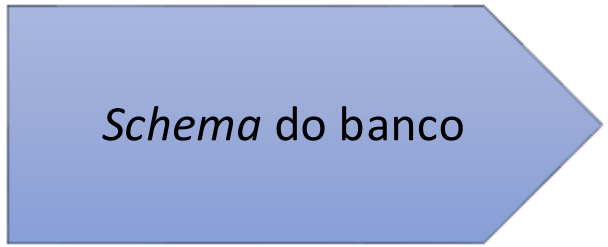
Desafio para priorização: Análises de vulnerabilidades para treino

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)

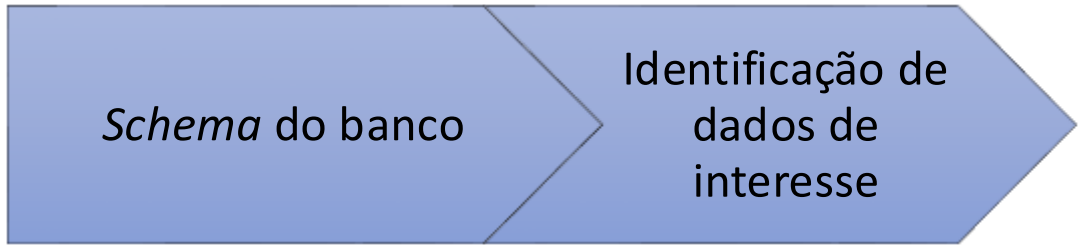
Obtendo bases de dados de sistemas de gerência

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



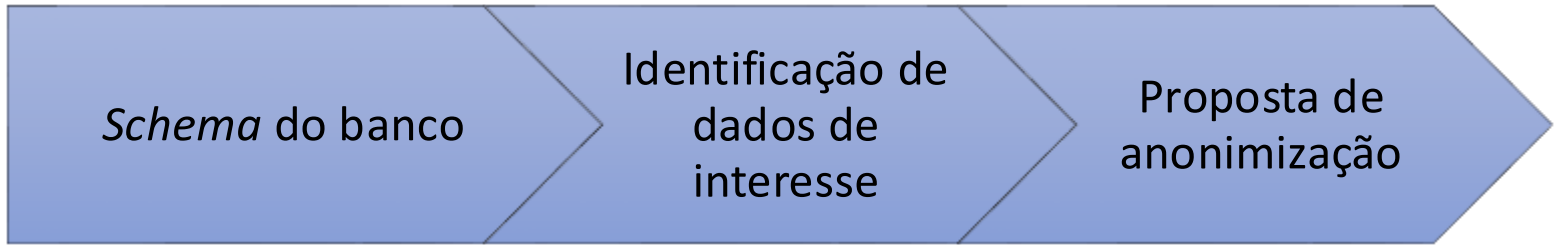
Obtendo bases de dados de sistemas de gerência

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



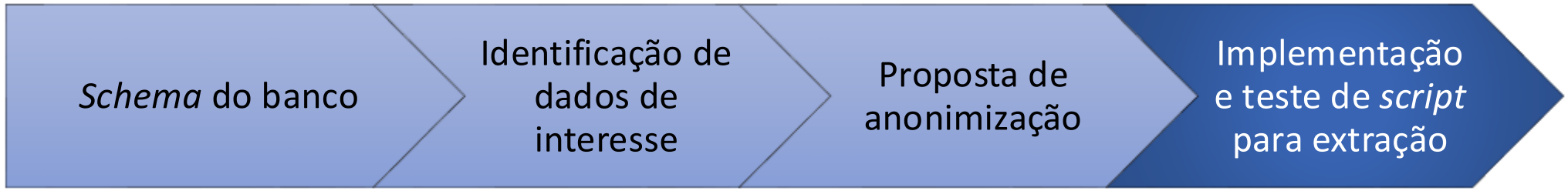
Obtendo bases de dados de sistemas de gerência

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



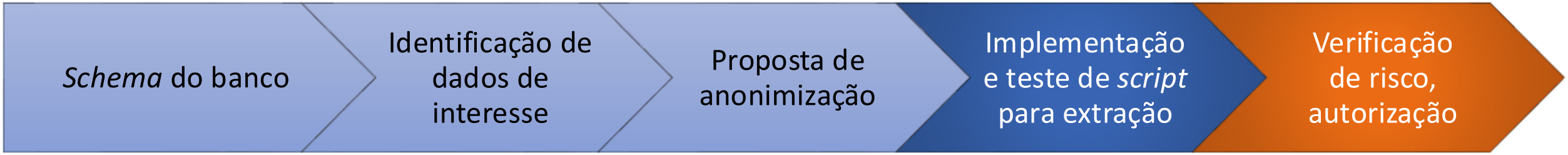
Obtendo bases de dados de sistemas de gerência

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



Obtendo bases de dados de sistemas de gerência

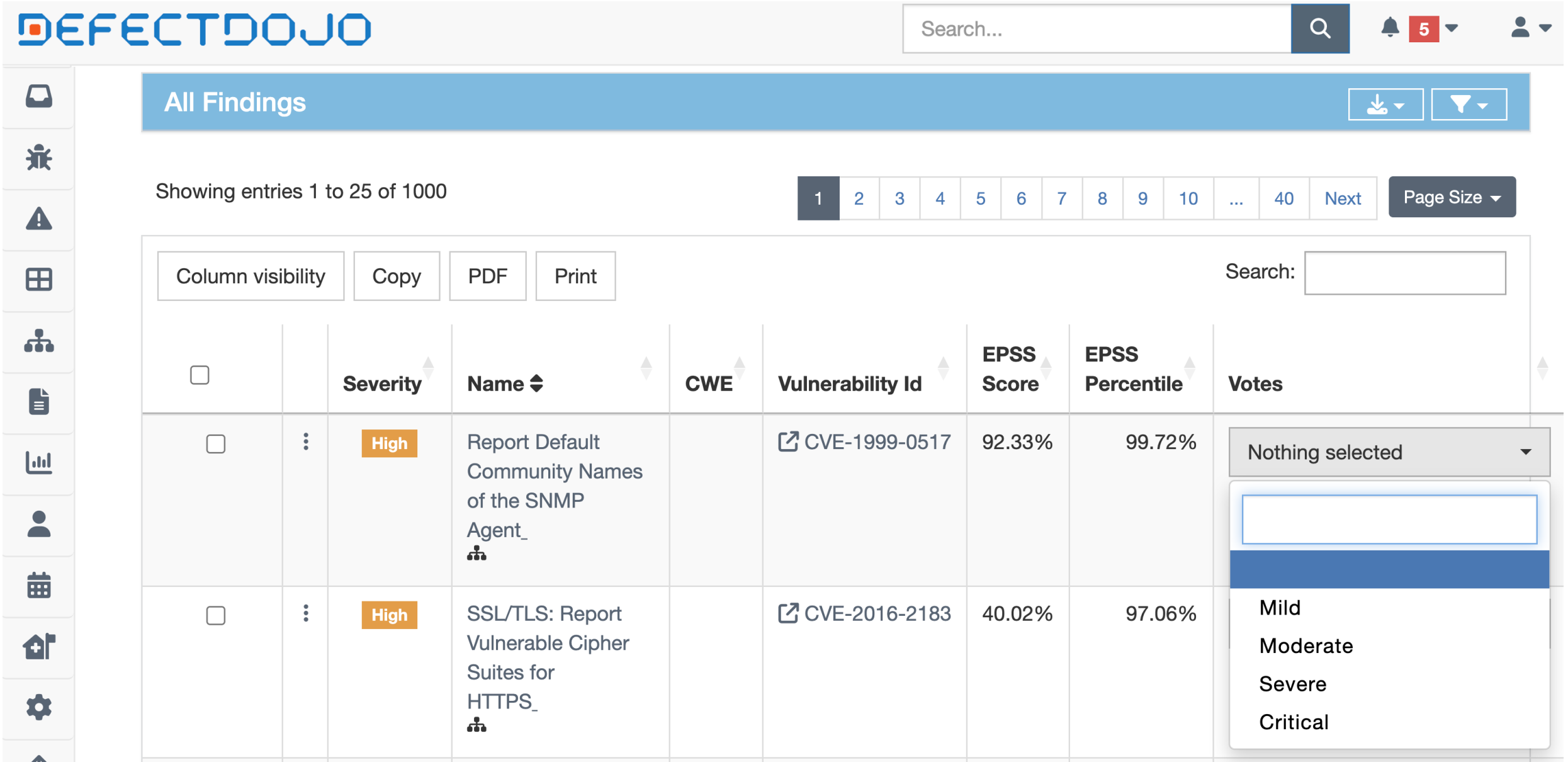
- Controle do risco vs. perda de informações úteis
- Anonimização dos dados específica para o contexto



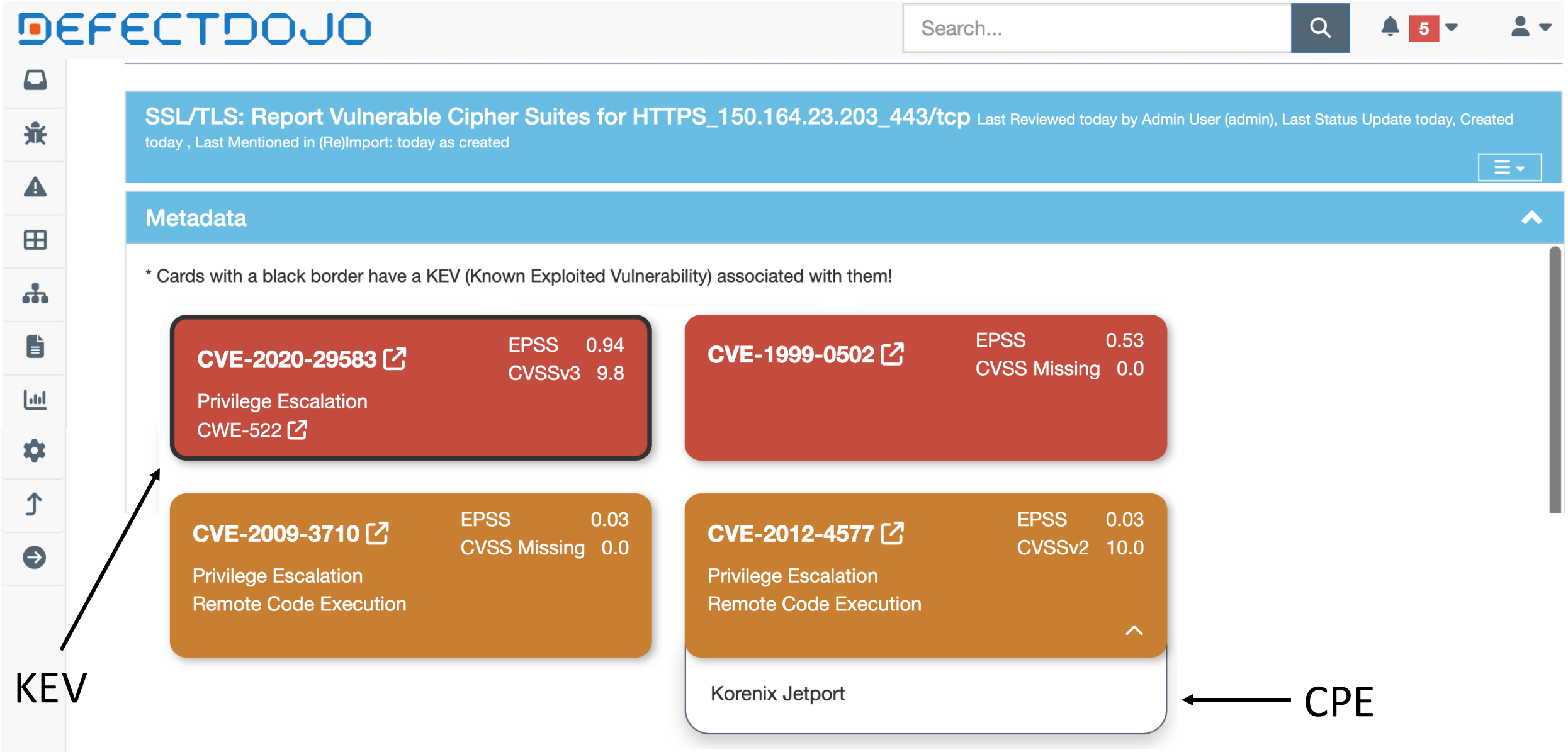
Criação de bases para treino

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

Extensões ao DefectDojo



Metadados sobre vulnerabilidades



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

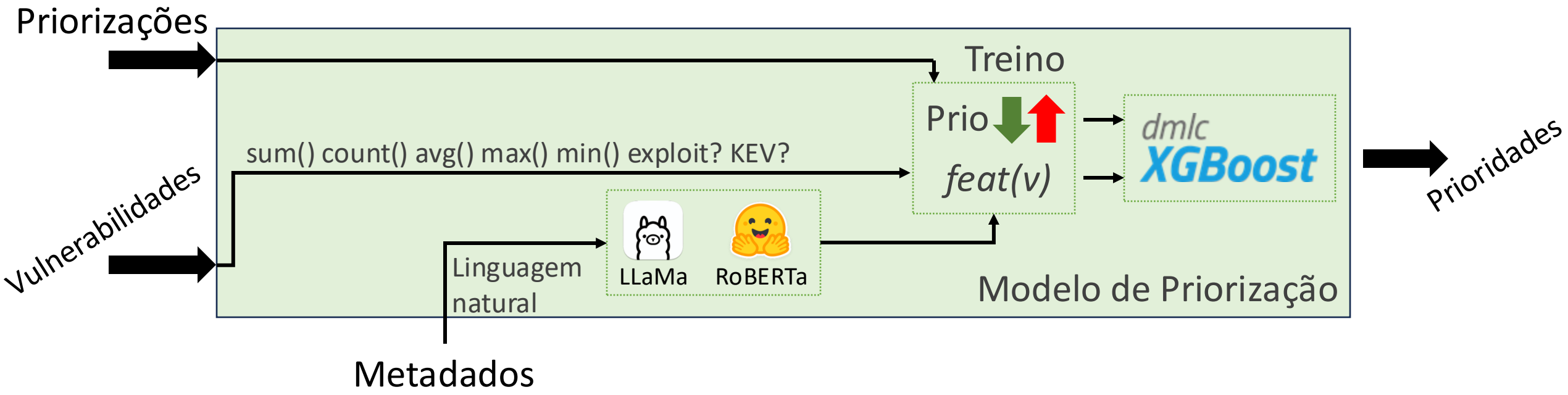
- Obtenção de dados de varreduras de rede
- Análises de vulnerabilidades por
  - Integrantes do projeto
  - Residentes do programa Hackers do Bem

- Pouco realismo
  - Bolsistas e residentes não são responsáveis pela segurança
  - Bolsistas e residentes não atuam em conjunto

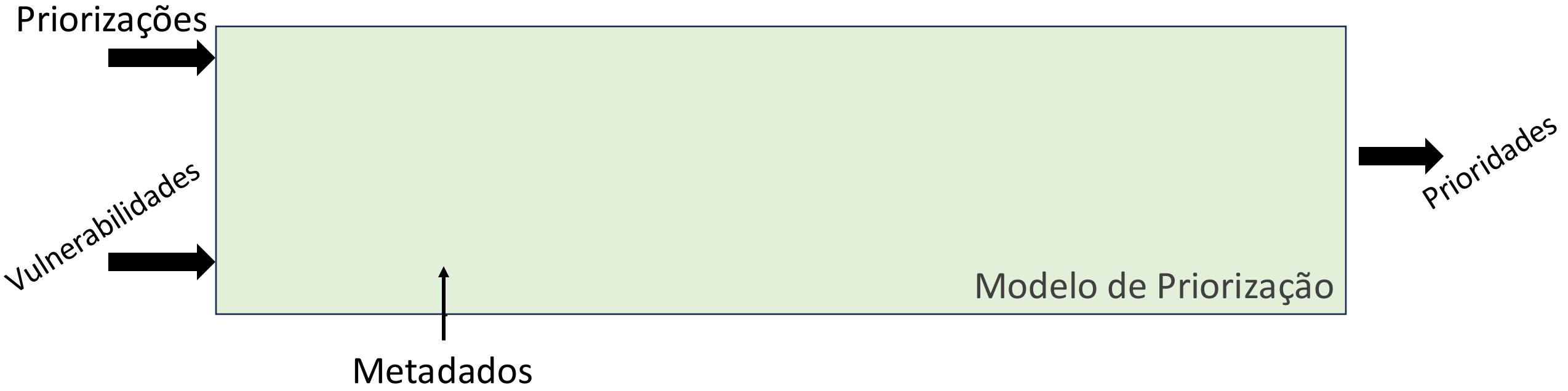
26 Workshop RNP

Priorização de vulnerabilidades

Modelo de priorização de vulnerabilidades

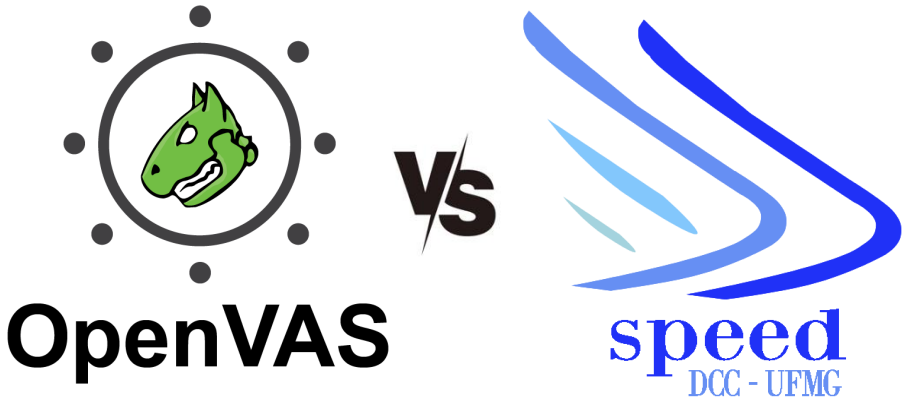


Modelo de priorização de vulnerabilidades



Fatores que impactam a precisão do modelo

- Diversidade das vulnerabilidades
  - Bases de teste balanceadas



32 críticas

19 graves

191 médias

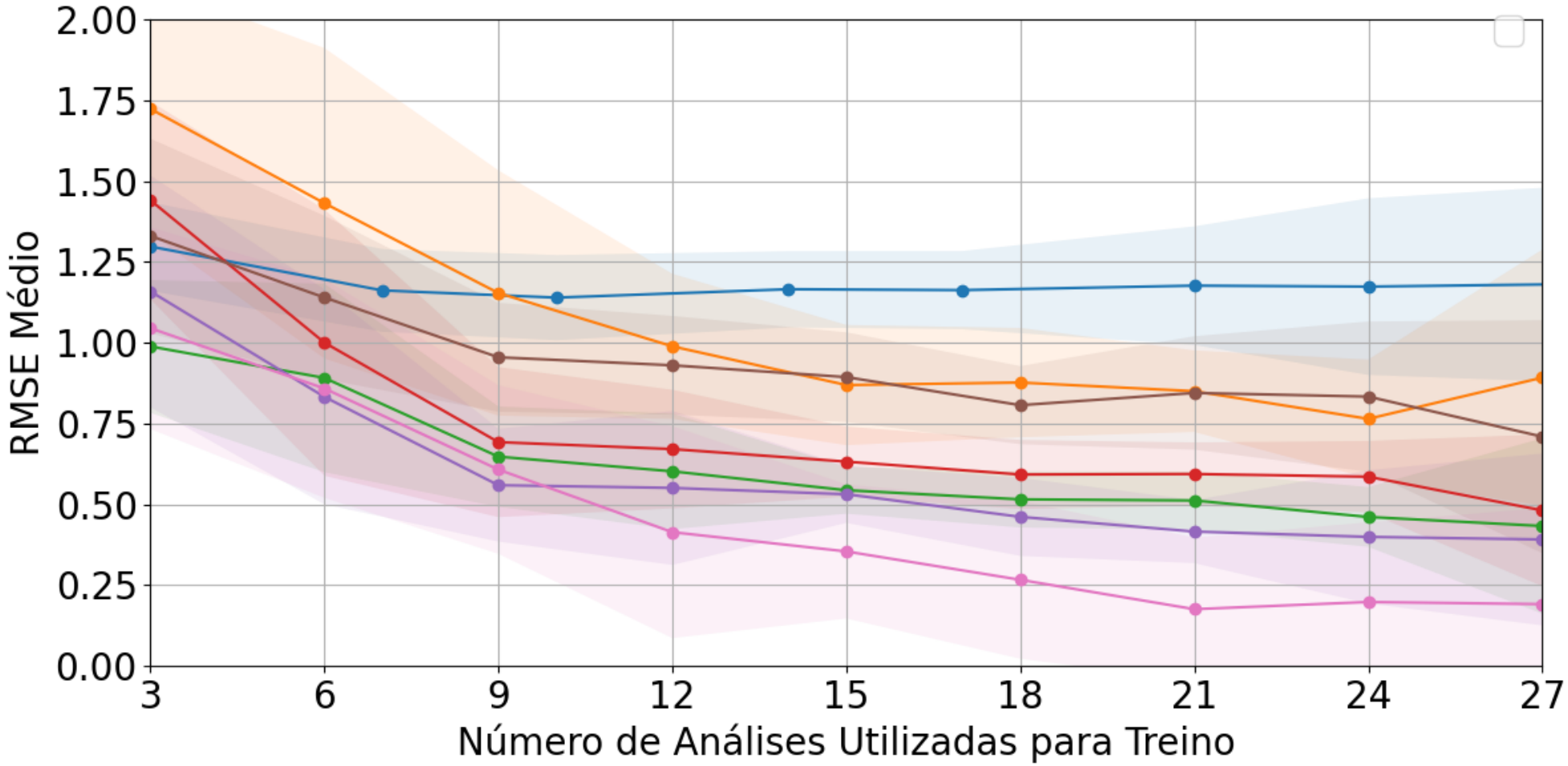
Fatores que impactam a precisão do modelo

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

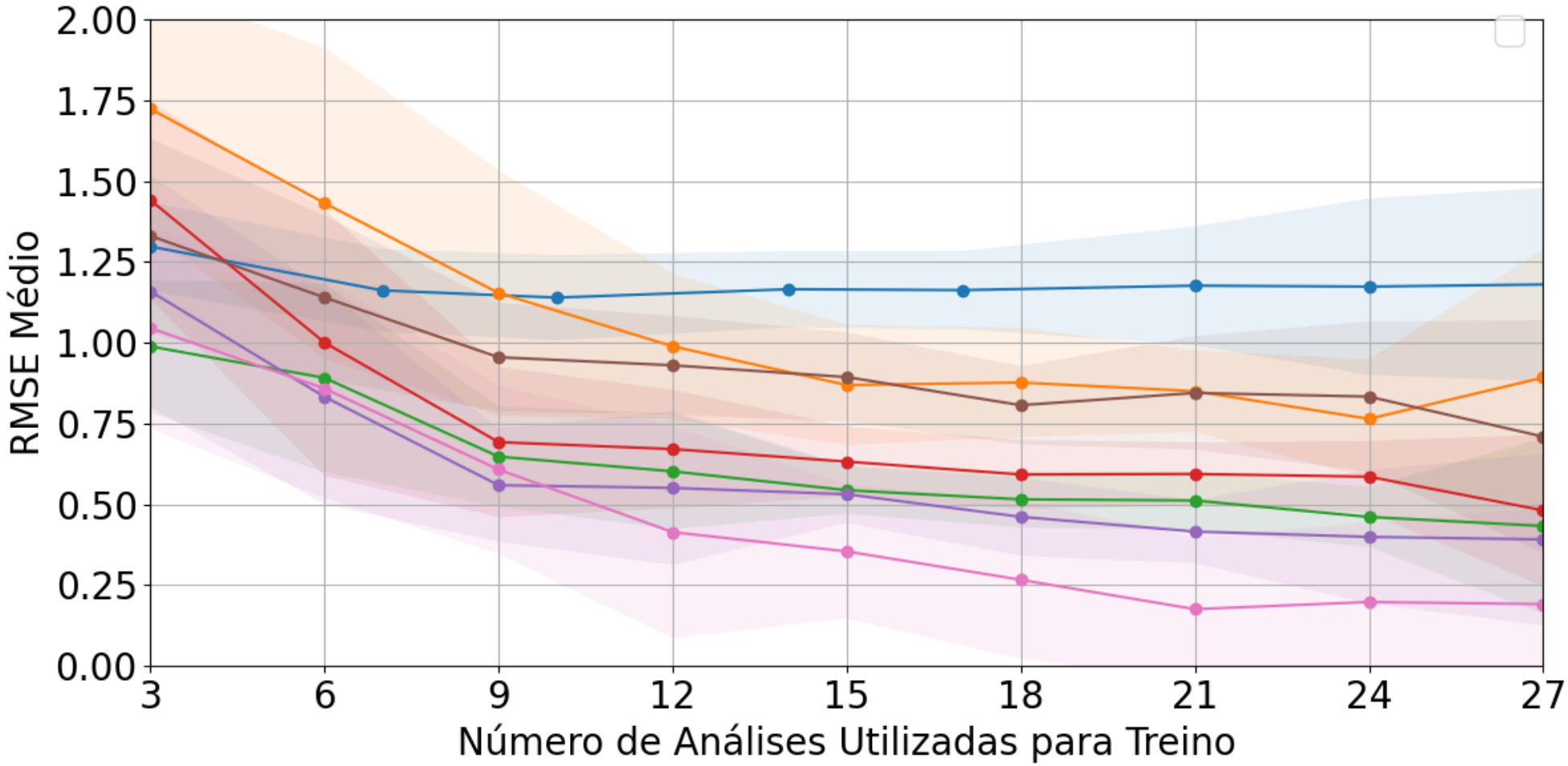
Fatores que impactam a precisão do modelo

- 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”

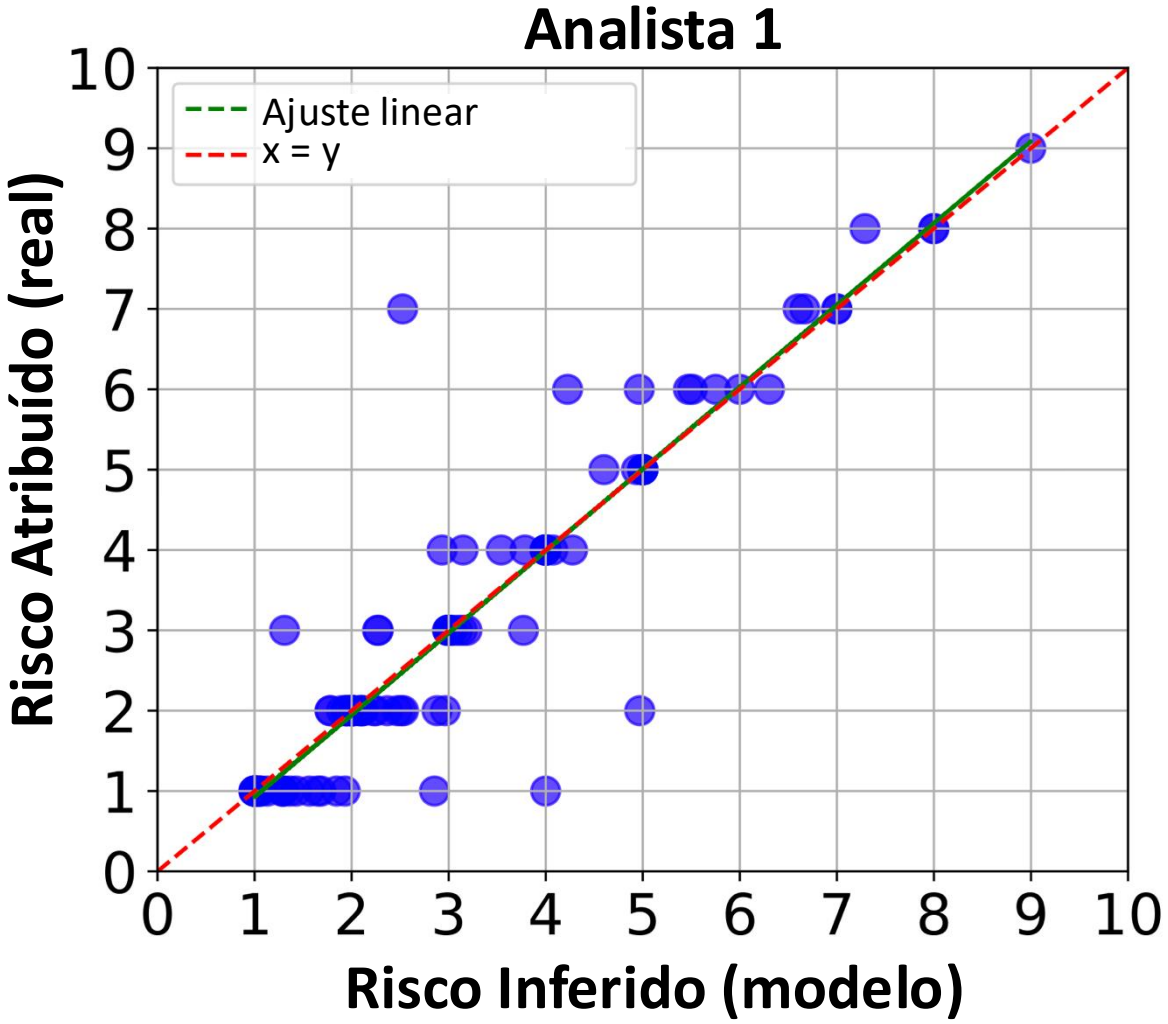
Quantas análises são necessárias para treino?



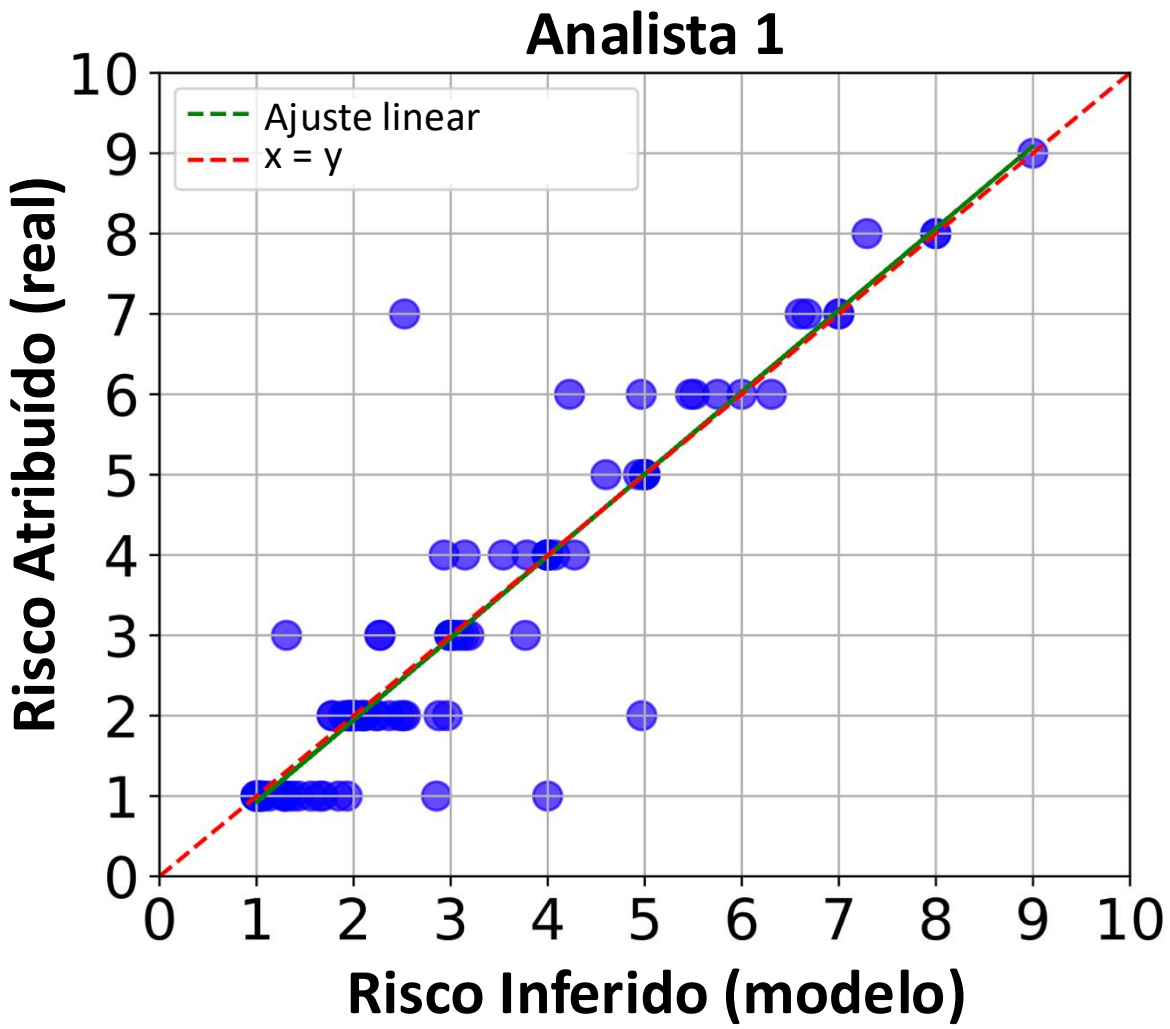
Quantas análises são necessárias para treino?

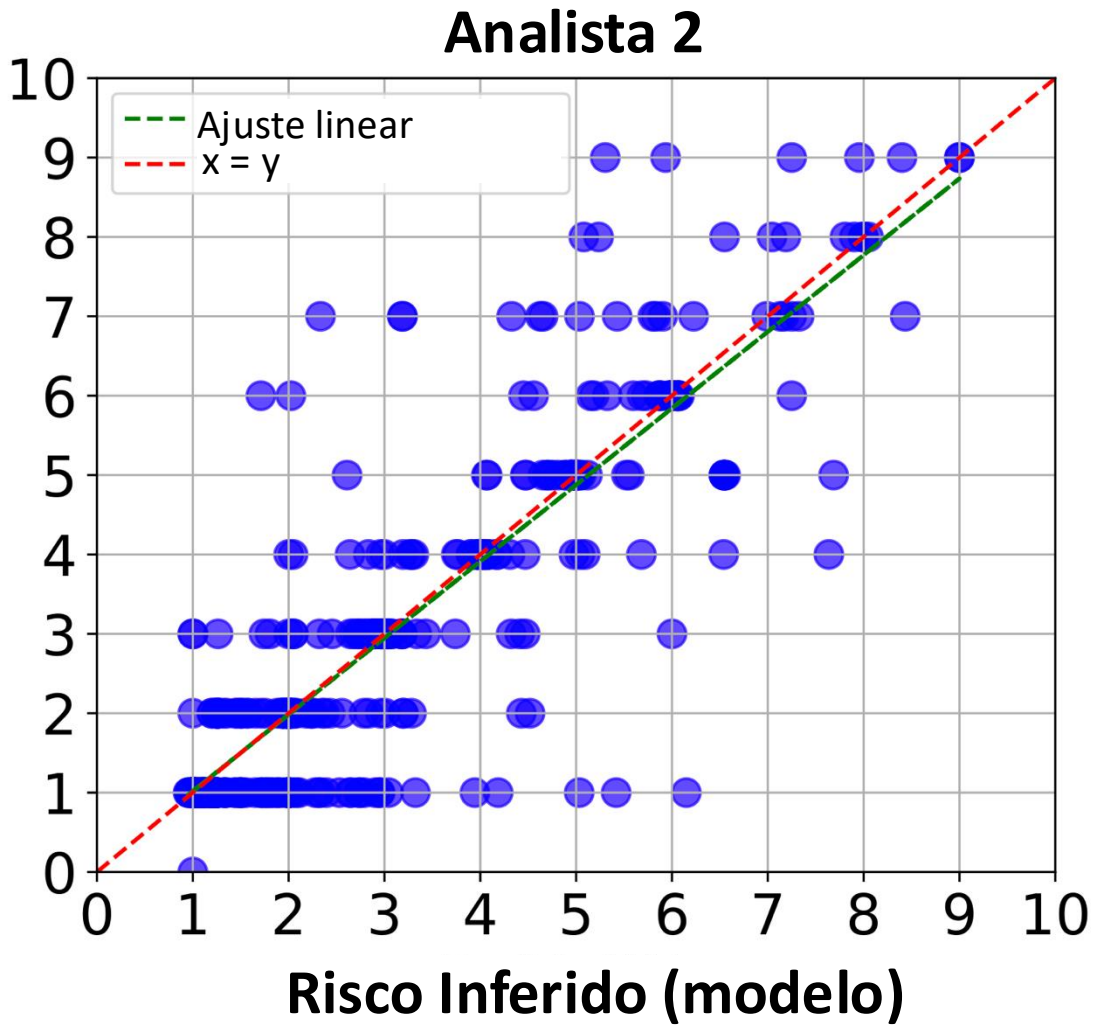


Previsões correlacionadas com os votos



Previsões correlacionadas com os votos





26 Workshop RNP

Aplicações de IA para priorização de vulnerabilidades

Extração de dados de linguagem natural

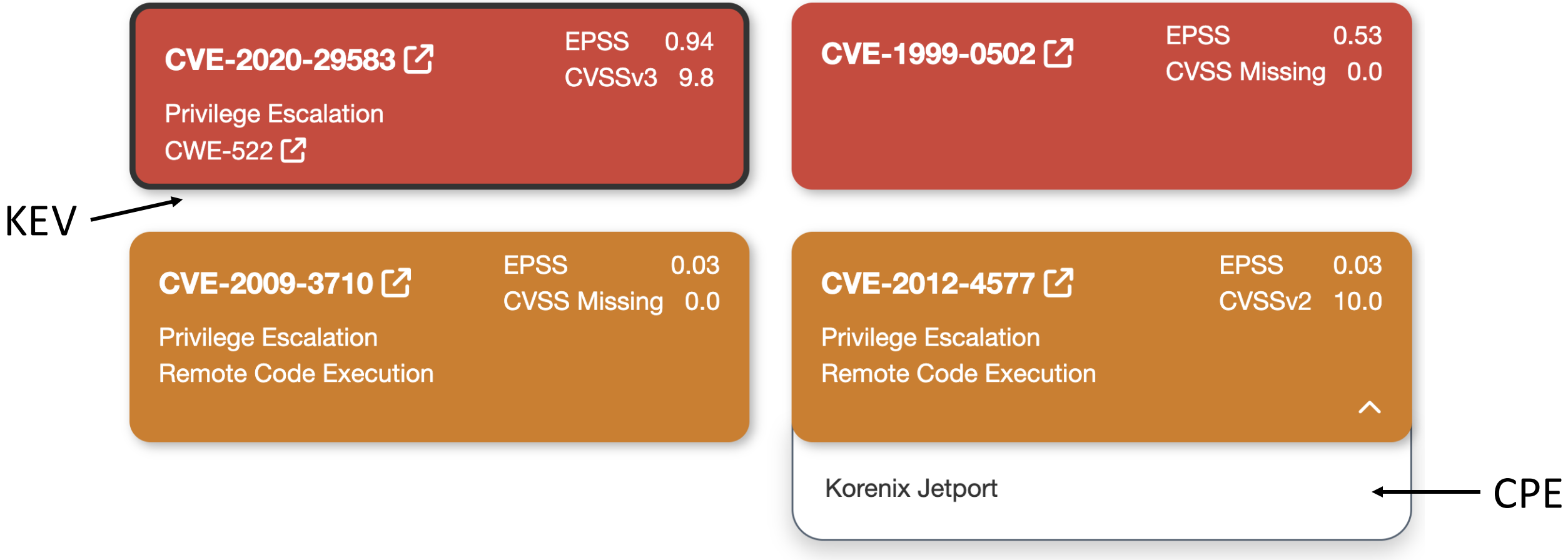
- Muita informação sobre vulnerabilidades em linguagem natural
  - Descrição do CVE, CWE, *exploits*
  - Mensagens de discussão de vulnerabilidades
    - Listas de discussão
    - Fóruns
    - Sistemas de gerência de vulnerabilidades
  - Páginas Web

Extração de dados de linguagem natural

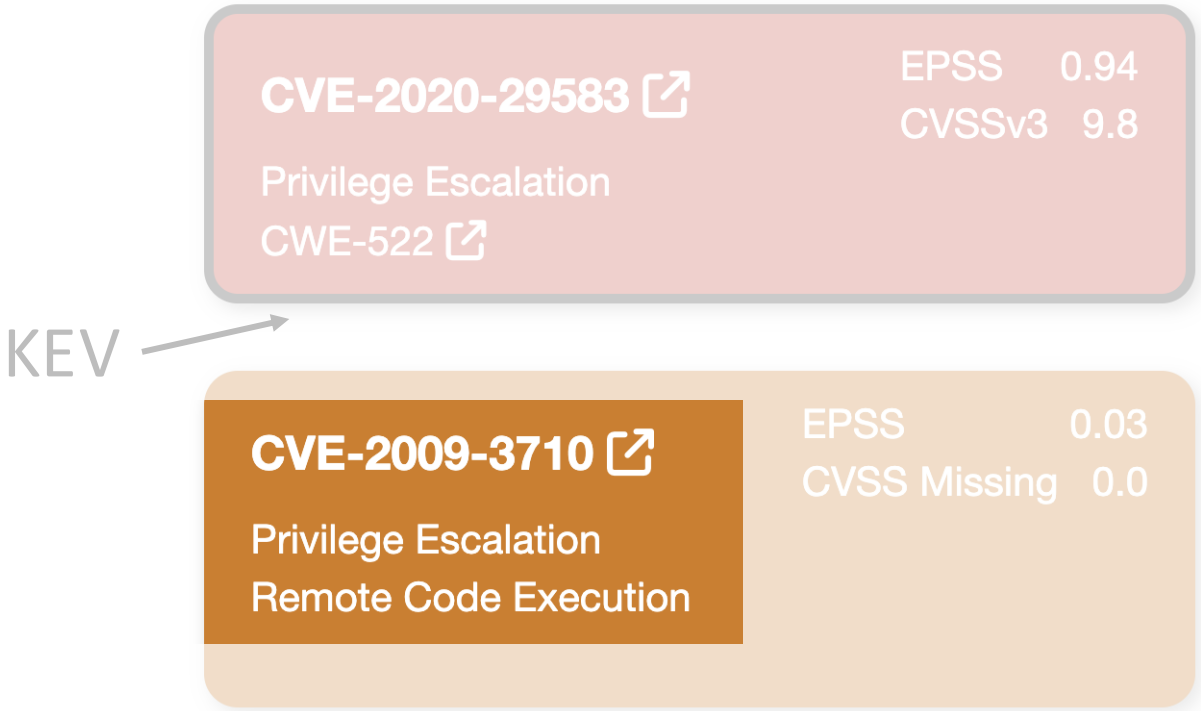
- Muita informação sobre vulnerabilidades em linguagem natural
  - Descrição do CVE, CWE, *exploits*
  - Mensagens de discussão de vulnerabilidades
    - Listas de discussão
    - Fóruns
    - Sistemas de gerência de vulnerabilidades
  - Páginas Web

- Geração de propriedades (*features*) que podem ser usadas como entrada para modelos de IA

Metadados relacionados a vulnerabilidades



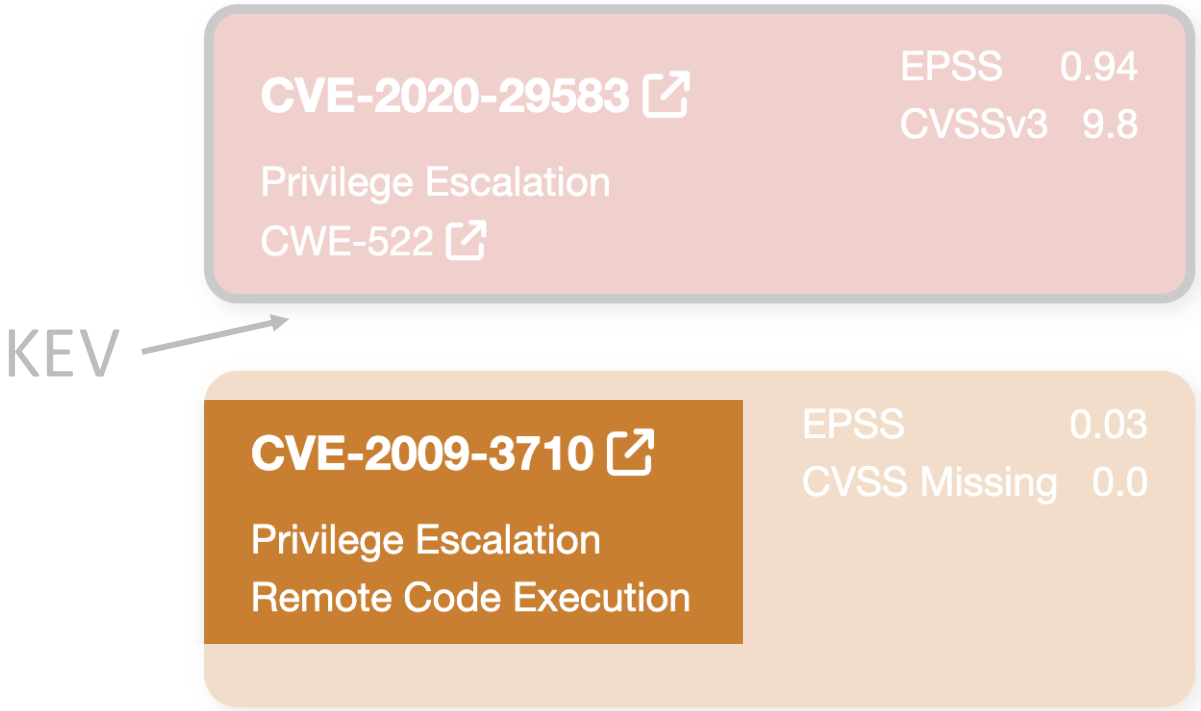
Metadados relacionados a vulnerabilidades



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

Metadados relacionados a vulnerabilidades



Inferências de propriedades a partir de descrições textuais usando LLMs

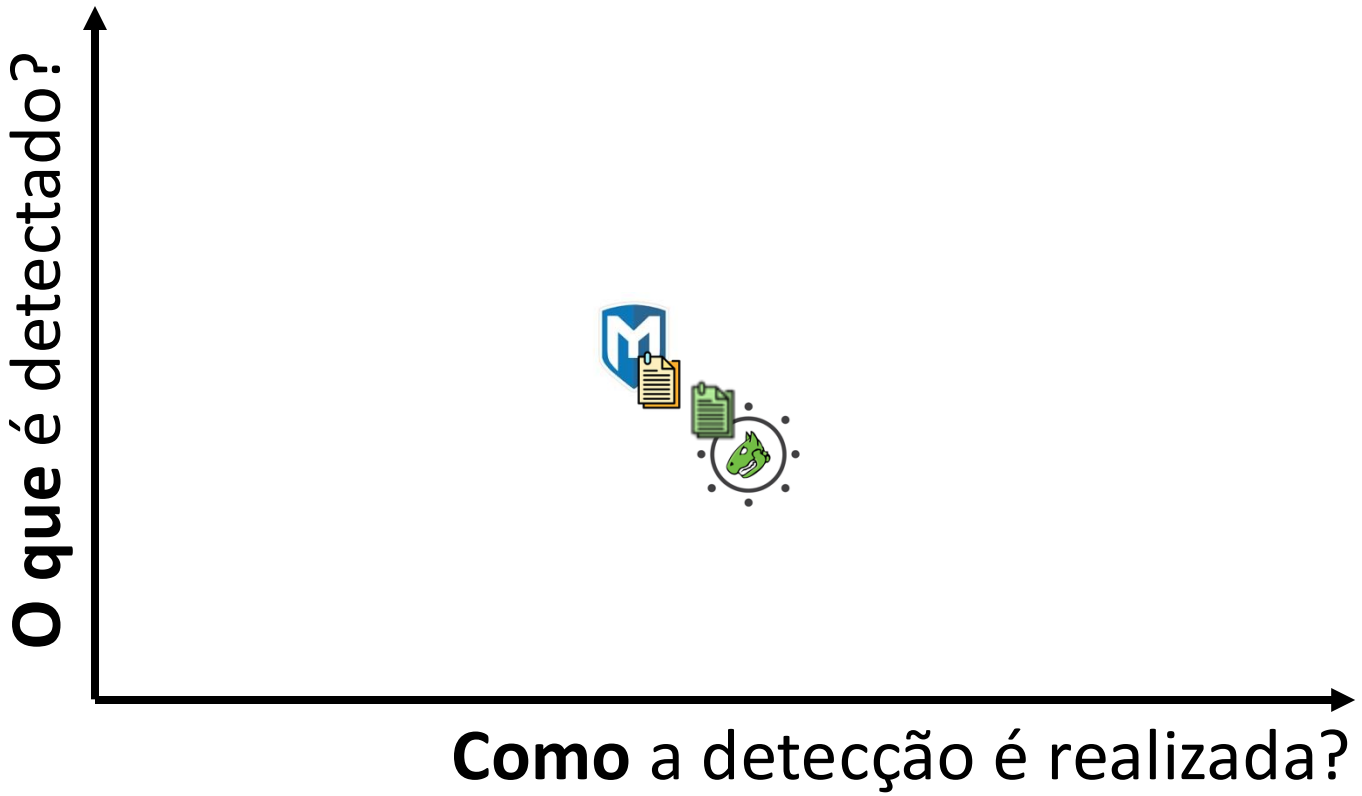
- Descrição do CVE
- Procedimento de mitigação
- Código do *script* de detecção
- Nomes de organização
- Conteúdo de página Web

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 Workshop RNP

Desafios e soluções para priorização de vulnerabilidades

Ítalo Cunha
Universidade Federal de Minas Gerais

26 Workshop RNP

Backup slides

Inferência de risco com dados históricos

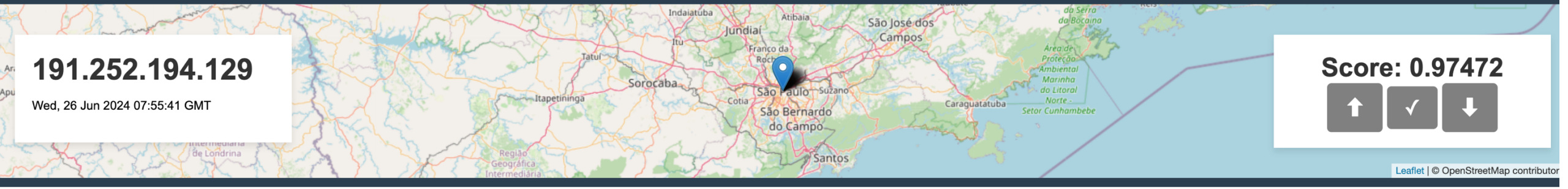
- Inferência de risco usando bases de dados de sistemas de gerência
- Indicadores de risco
  - Tempo de resposta ao incidente
  - Quantidade de analistas envolvidos
  - Número de interações (mensagens)

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

Sistema de gerência de vulnerabilidades do Shodan

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

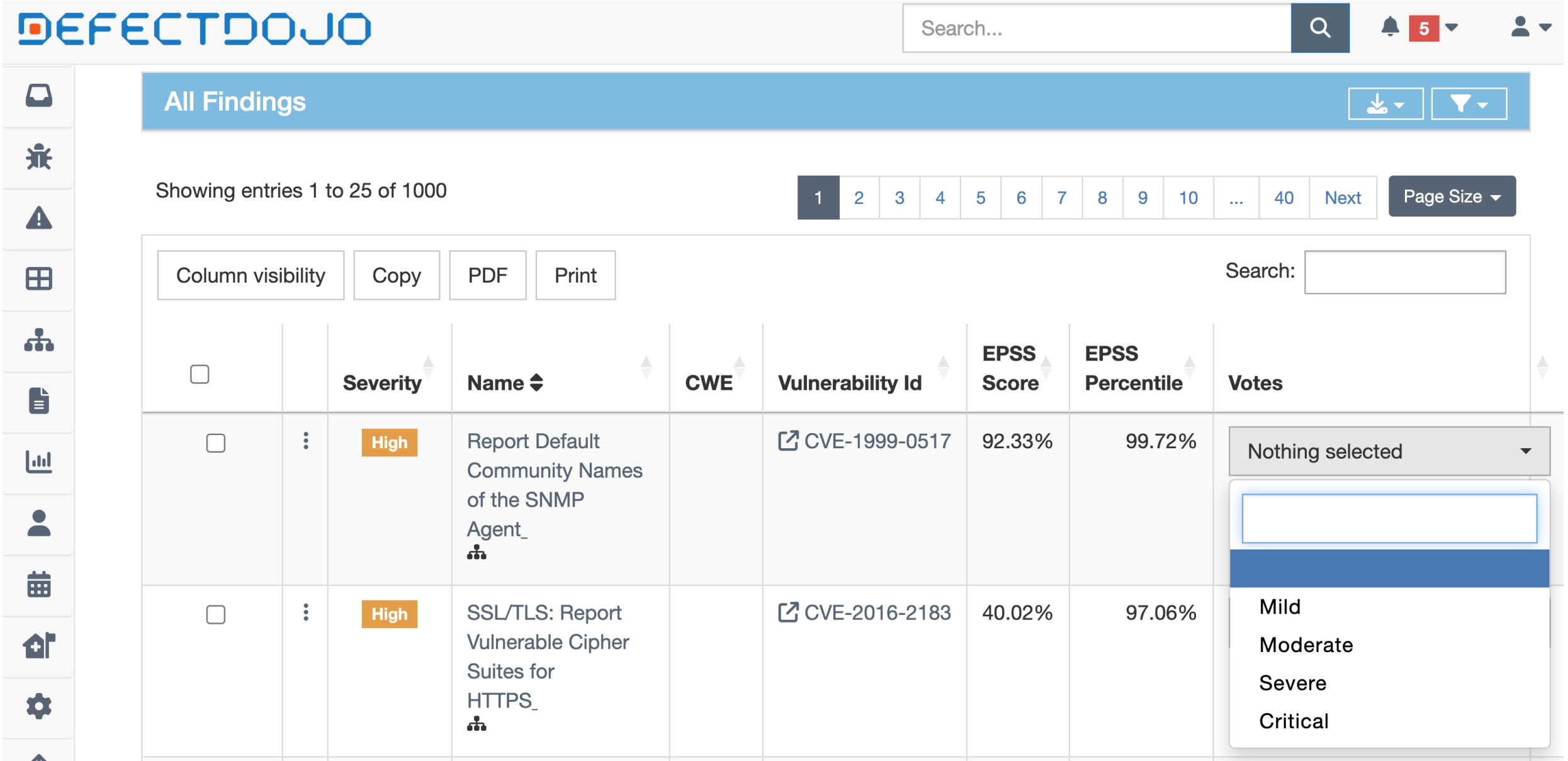
Hostnames:

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

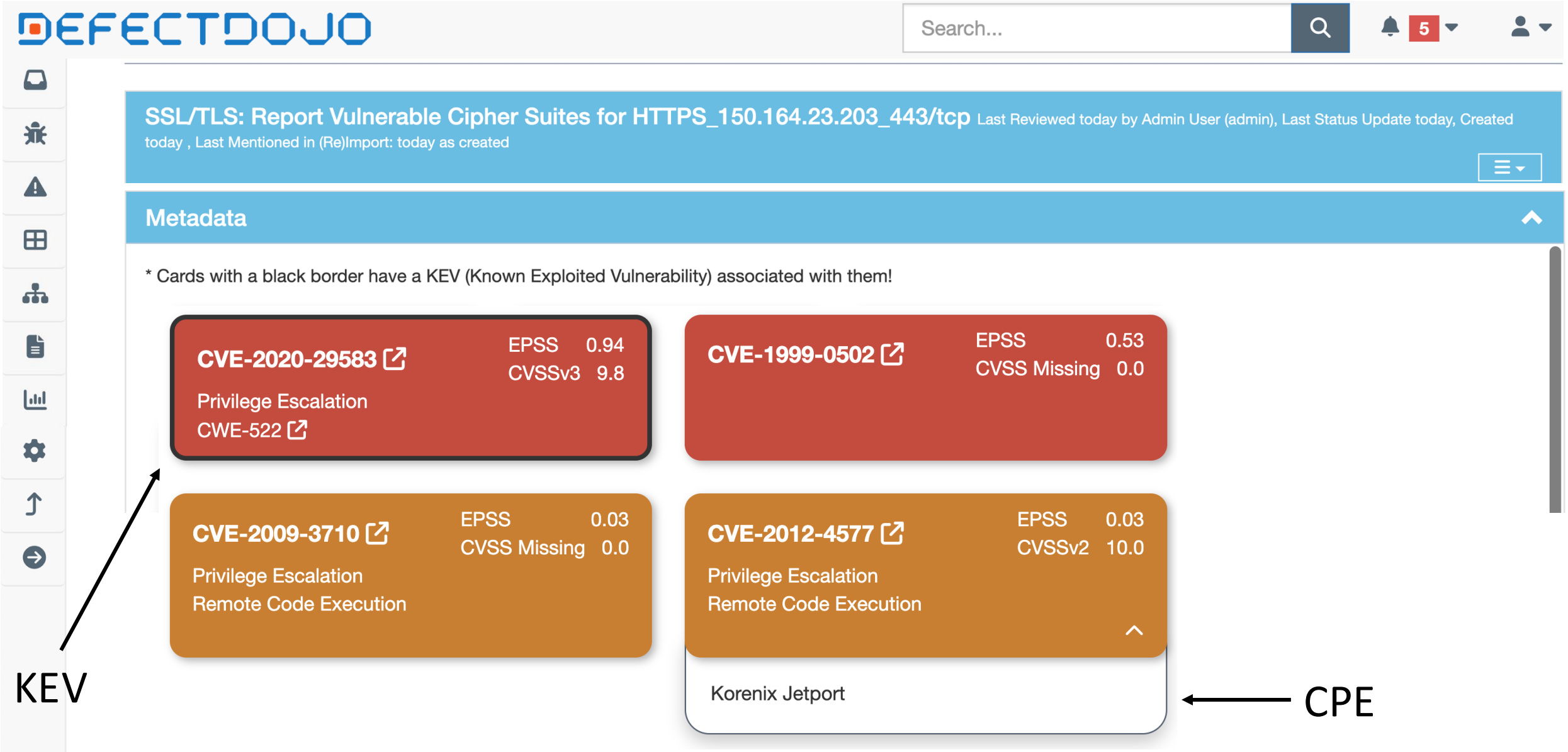
Data

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

Extensões ao DefectDojo



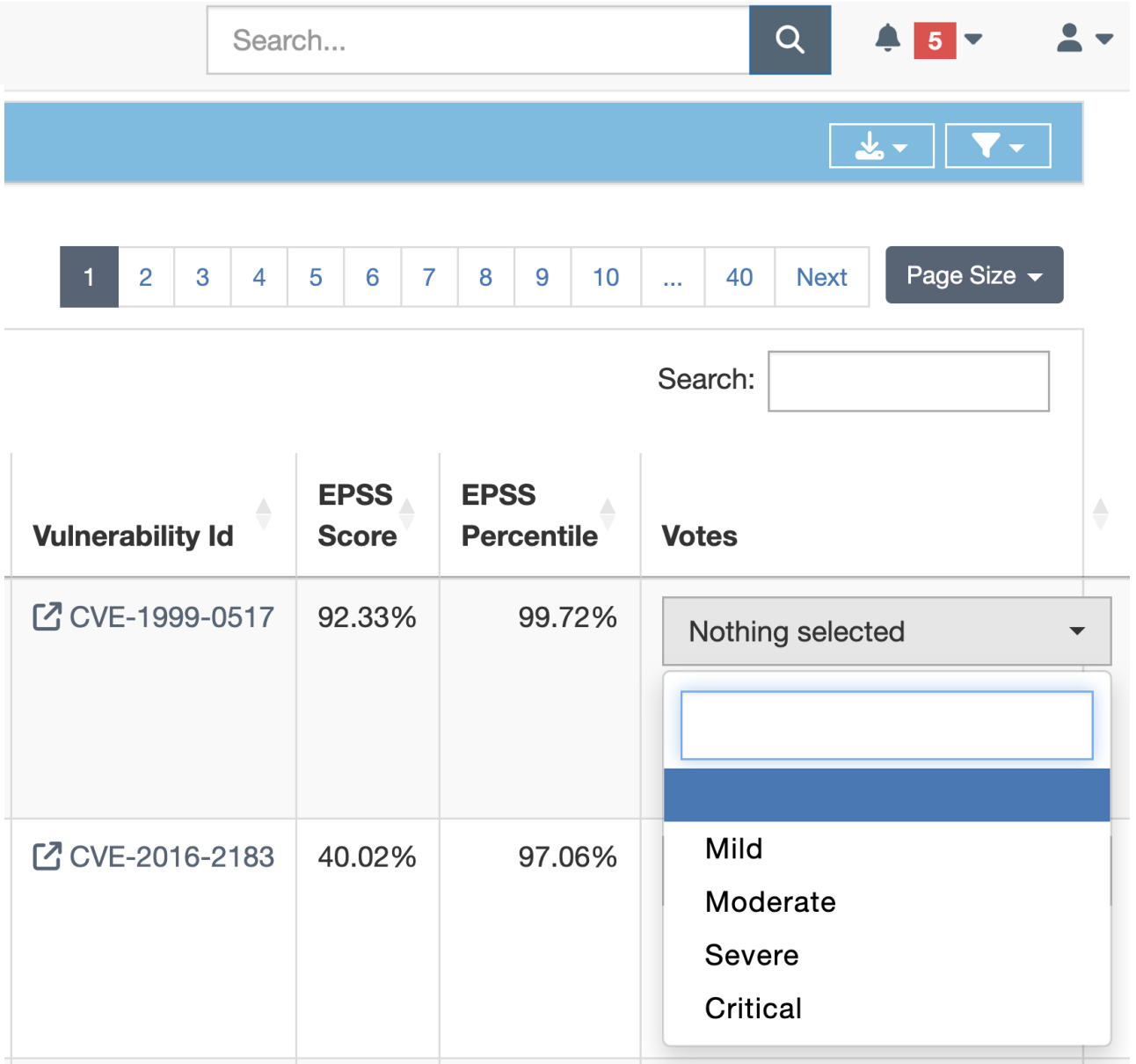
Metadados sobre vulnerabilidades



Extensões ao DefectDojo

Coragem para usar?

- Enviar as mudanças para a versão código aberto *upstream*
- Nenhuma mudança no banco de dados do DefectDojo
  - Versão original é compatível com nossa versão estendida



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 dos dispositivos
  - Bolsistas e residentes não atuam em conjunto

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 dos dispositivos
  - Bolsistas e residentes não atuam em conjunto

- Dados insuficientes

Contexto da empresa

- Vazamento de dados
- Violação de privacidade

- Desempenho da aplicação
- Funcionamento da infraestrutura

Contexto da empresa e analistas de segurança

serasa experian

- Vazamento de dados
- Violação de privacidade

globoplay

- Desempenho da aplicação
- Funcionamento da infraestrutura

Desenvolvedores

- Corrigir bugs
- Upgrade de sistemas

Sysadmins

- Instalar firewalls
- Reconfiguração de sistemas

Análise de risco

Vulnerbldade + Ameaça + Impacto

Análise de risco

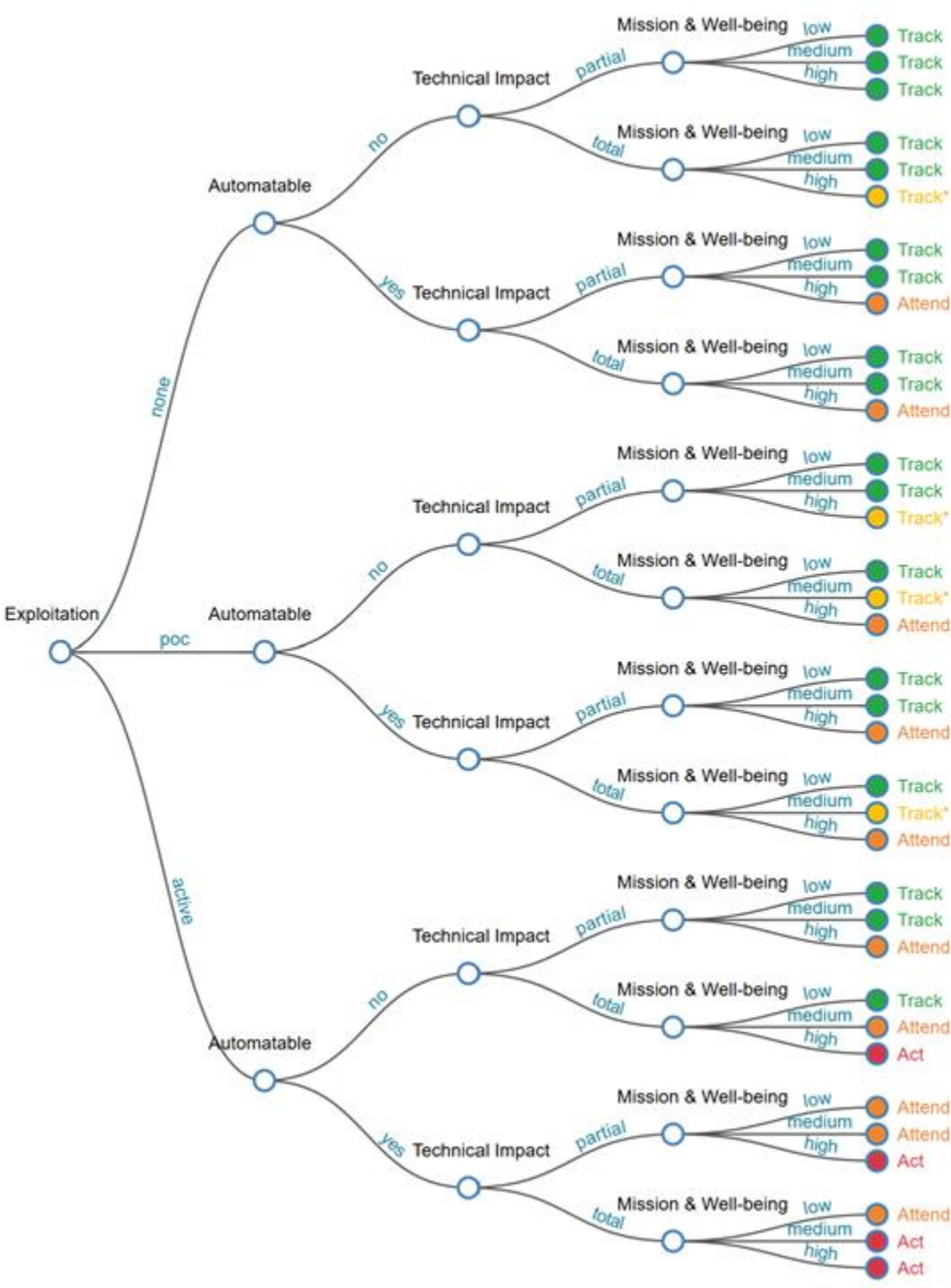
Vulnerbldade + **Ameaça** **+** **Impacto**

- Propriedades da vulnerabilidade

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

- Impacto na missão
- Impacto operacional

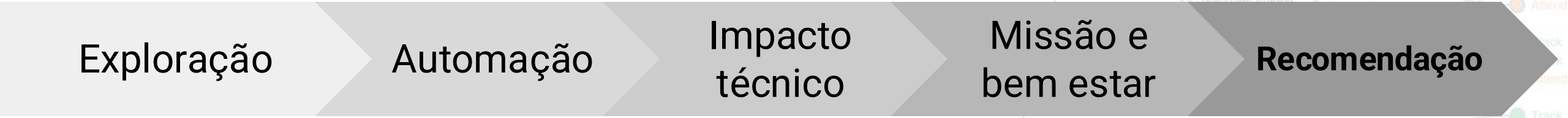
Árvore de decisão do SSVC



Árvore de decisão do SSVC

Exploração → Automação → Impacto técnico → Missão e bem estar → **Recomendação**

Árvore de decisão do SSVC



- Propriedades globais
- Bases públicas disponíveis

- Contexto da instituição
- A cargo do especialista

Análise de risco

Vulnerbldade +

- Propriedades da vulnerabilidade

Ameaça

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

+

Impacto

- Propriedades da empresa
- Propriedades do analista

Vibe Check

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 olumn to check details.

EPSS Rank

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS		PRIO	VOTE
HTTP/1.1 Server: Apache Date: Wed, 26 Jun 2024 02:59:26 GMT	177.191.201.115	443	São Paulo		Algar Telecom	177-191-201-115.xd-dynamic.algarnetsuper.com.br	algarnetsuper.com.br		5.7341	Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 05:29:34 GMT	186.208.72.86	443	Maceió		Veloo Net	186-208-72-86.veloo.com.br	veloo.com.br	0.9755	6.1696	Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 18:44:19 GMT	177.184.11.35	443	Rio De Janeiro		Equinix Brasil	localhost.ativacaorj.alog.com.br	alog.com.br	0.9755	5.3687	Skip
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 11:46:39 GMT	189.89.181.190	8140	Salvador	Windows	Its Telecomunicacoes	189-89-181-190.STATIC.itsweb.com.br	itsweb.com.br	0.9754	3.9230	Skip

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 olumn to check details.

EPSS Rank

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS		PRIO	VOTE
HTTP/1.1 Server: Apache Date: Wed, 26 Jun 2024 02:59:26 GMT	177.191.201.115	443	São Paulo		Algar Telecom	177-191-201-115.xd-dynamic.algarnetsupe com.br	Provedor núvem	0.9757	5.7341	Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 05:29:34 GMT	186.208.72.86	443	Maceió		Veloo Net	186-208-72-86.veloo.com.br	Provedor residencial	0.9755	6.1696	Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 18:44:19 GMT	177.184.11.35	443	Rio De Janeiro		Equinix Brasil	localhost.ativacaorj.al g.com.br	Provedor núvem	0.9755	5.3687	Skip
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 r	Provedor residencial	0.9755	7.3774	Skip
HTTP/1.1 Server: Microsoft-IIS/7.5 Date: Wed, 26 Jun 2024 11:46:39 GMT	189.89.181.190	8140	Salvador	Wind ows	Its Telecomunicacoes	189-89-181-190.STATIC.itsweb.co .br	Provedor núvem	0.9754	3.9230	Skip

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 olumn to check details.

EPSS Rank

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS		PRIO	VOTE
HTTP/1.1 Server: Apache Date: Wed, 26 Jun 2024 02:59:26 GMT	177.191.201.115	443	São Paulo		Algar Telecom	177-191-201-115.xd-dynamic.algarnetsupe com.br		0.9757	5.7341	Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 05:29:34 GMT	186.208.72.86	443	Maceió		Veloo Net	186-208-72-86.veloo.com.br		0.9755	6.1696	Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 18:44:19 GMT	177.184.11.35	443	Rio De Janeiro		Equinix Brasil	localhost.ativacaorj.al g.com.br		0.9755	5.3687	Skip
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 r		0.9755	7.3774	Skip
HTTP/1.1 Server: Microsoft-IIS/7.5 Date: Wed, 26 Jun 2024 11:46:39 GMT	189.89.181.190	8140	Salvador	Wind ows	Its Telecomunicacoes	189-89-181-190.STATIC.itsweb.co .br		0.9754	3.9230	Skip

Provedor núvem

Provedor residencial

Provedor núvem

Provedor residencial

Provedor núvem

Unusual ports

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 ... heck details.

Prio

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	E... ↓		VOTE
HTTP/1.1 Server: Apache Date: Wed, 26 Jun 2024 02:59:26 GMT	177.191.201.115	443	São Paulo		Algar Telecom	177-191-201-115.xd-dynamic.algarnetsuper.com.br	algarnetsuper.com.br	0.9757		Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 05:29:34 GMT	186.208.72.86	443	Maceió		Veloo Net	186-208-72-86.veloo.com.br	veloo.com.br	0.9755	6.1696	Skip
HTTP/1.1 Date: Wed, 26 Jun 2024 18:44:19 GMT	177.184.11.35	443	Rio De Janeiro		Equinix Brasil	localhost.ativacaorj.alog.com.br	alog.com.br	0.9755	5.3687	Skip
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 11:46:39 GMT	189.89.181.190	8140	Salvador	Windows	Its Telecomunicacoes	189-89-181-190.STATIC.itsweb.com.br	itsweb.com.br	0.9754	3.9230	Skip

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 [illegible] heck details.

Prio

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	EPSS		VOTE
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 23:20:32 GMT	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	gov.br	0.9747	8.4260	9
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 10:54:49 GMT	187.191.100.136	443	São Paulo		Claranet Technology	unisuam.edu.br	gov.br	0.9747	8.2722	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 07:50:51 GMT	191.252.194.129	443	São Paulo		Locaweb Servicos De Internet	vps16051.publiccloud.com.br,fertipraxis.com.br,www.fertipraxis.com.br	publiccloud.com.br,fertipraxis.com.br	0.9747	8.1484	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ 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	gov.br	0.9735	7.5451	Skip
HTTP/1.1 Server: nginx Date: Wed, 26 Jun 2024 19:23:36 GMT	150.162.2.10	443	Florianópolis		Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br	gov.br	0.9556	7.5354	Skip

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 [illegible]heck details.

Prio

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	EPSS		VOTE
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 23:20:32 GMT	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	gov.br	0.9747	8.4260	9
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 10:54:49 GMT	187.191.100.136	443	São Paulo		Claranet Technology	unisuam.edu.br	gov.br	0.9747	8.2722	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 07:50:51 GMT	191.252.194.129	443	São Paulo		Locaweb Servicos Internet			0.9747	8.1484	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ 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	gov.br	0.9735	7.5451	Skip
HTTP/1.1 Server: nginx Date: Wed, 26 Jun 2024 19:23:36 GMT	150.162.2.10	443	Florianópolis		Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br	gov.br	0.9556	7.5354	Skip

Laboratório clínico

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 [illegible]neck details.

Prio

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	EPSS		VOTE
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 23:20:32 GMT	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	gov.br	0.9747	8.4260	9
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 10:54:49 GMT	187.191.100.136	443	São Paulo		Claranet Technology	unisuam.edu.br	gov.br	0.9747	8.2722	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 07:50:51 GMT	191.252.194.129	443	São Paulo					0.9747	8.1484	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ 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	gov.br	0.9735	7.5451	Skip
HTTP/1.1 Server: nginx Date: Wed, 26 Jun 2024 19:23:36 GMT	150.162.2.10	443	Florianópolis		Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br	gov.br	0.9556	7.5354	Skip

Provedor núvem

Laboratório clínico

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 [illegible]neck details.

Prio

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	EPSS		VOTE
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 23:20:32 GMT	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	gov.br	0.9747	8.4260	9
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 10:54:49 GMT	187.191.100.136	443	São Paulo		Claranet Technology	unisuam.edu.br	gov.br	0.9747	8.2722	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ Date: Wed, 26 Jun 2024 07:50:51 GMT	191.252.194.129	443	São Paulo					0.9747	8.1484	Skip
HTTP/1.1 Server: Apache/2.4.6 (CentOS) OpenSSL/ 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	gov.br	0.9735	7.5451	Skip
HTTP/1.1 Server: nginx Date: Wed, 26 Jun 2024 19:23:36 GMT	150.162.2.10	443	Florianópolis		Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br	gov.br	0.9556	7.5354	Skip

Provedor núvem

Laboratório clínico

Port 443

Identificação de vulnerabilidades relacionadas

Varredura por ShellShock utilizando vetores de ataque distintos

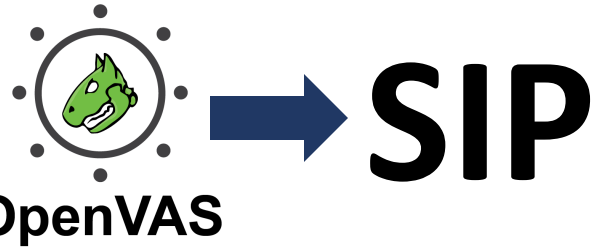
Identificação de vulnerabilidades relacionadas

Varredura por ShellShock utilizando vetores de ataque distintos

OpenVAS

Identificação de vulnerabilidades relacionadas

Varredura por ShellShock utilizando vetores de ataque distintos

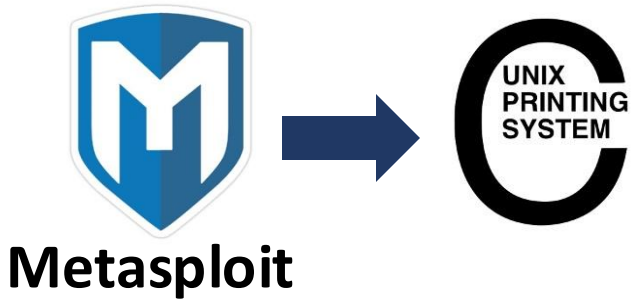


Identificação de vulnerabilidades relacionadas

Varredura por ShellShock utilizando vetores de ataque distintos

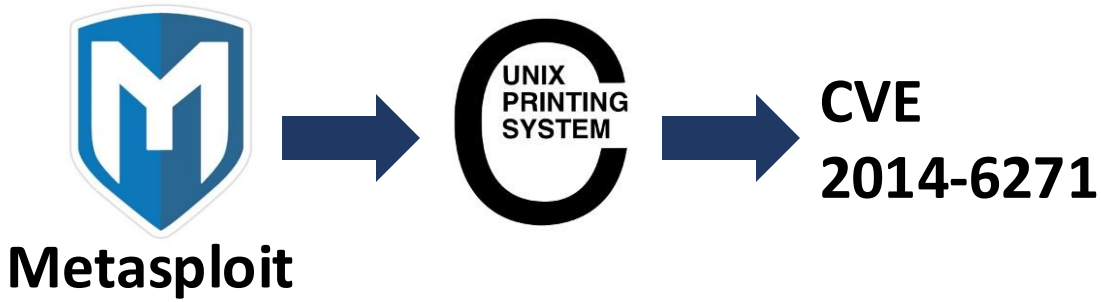
Identificação de vulnerabilidades relacionadas

Varredura por ShellShock utilizando vetores de ataque distintos



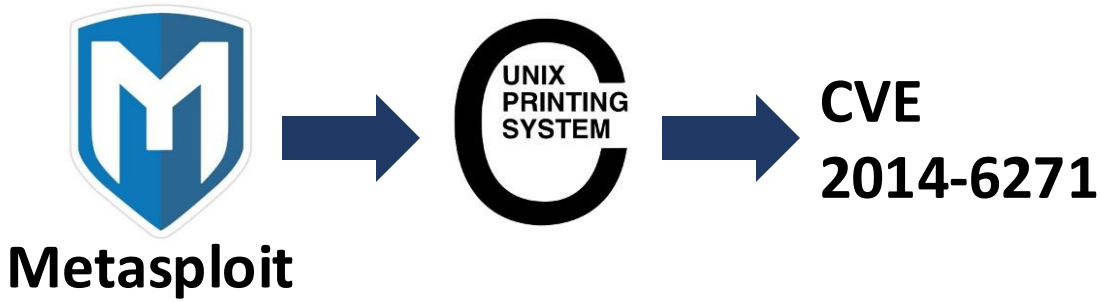
Identificação de vulnerabilidades relacionadas

Varredura por ShellShock utilizando vetores de ataque distintos



Identificação de vulnerabilidades relacionadas

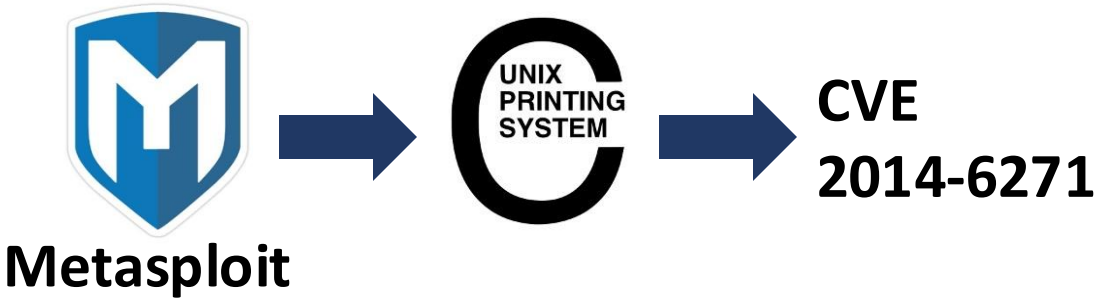
Varredura por ShellShock utilizando vetores de ataque distintos



Identificar o mesmo CVE não implica que scripts são equivalentes

Identificação de vulnerabilidades relacionadas

Varredura por ShellShock utilizando vetores de ataque distintos



Identificar o mesmo CVE não implica que scripts são equivalentes

Varredura por versão 1 do protocolo SSH

Identificação de vulnerabilidades relacionadas

Varredura por ShellShock utilizando vetores de ataque distintos

OpenVAS → **SIP** → **CVE 2014-6271**

Metasploit → 

→ **CVE 2014-6271**

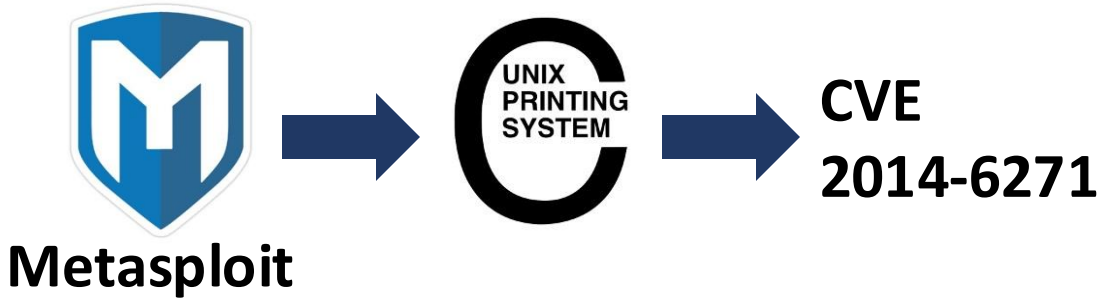
Varredura por versão 1 do protocolo SSH

OpenVAS → **Regex no *banner*** → **CVEs 2001-0361 2001-0572 2001-1473**

Identificar o mesmo CVE não implica que scripts são equivalentes

Identificação de vulnerabilidades relacionadas

Varredura por ShellShock utilizando vetores de ataque distintos

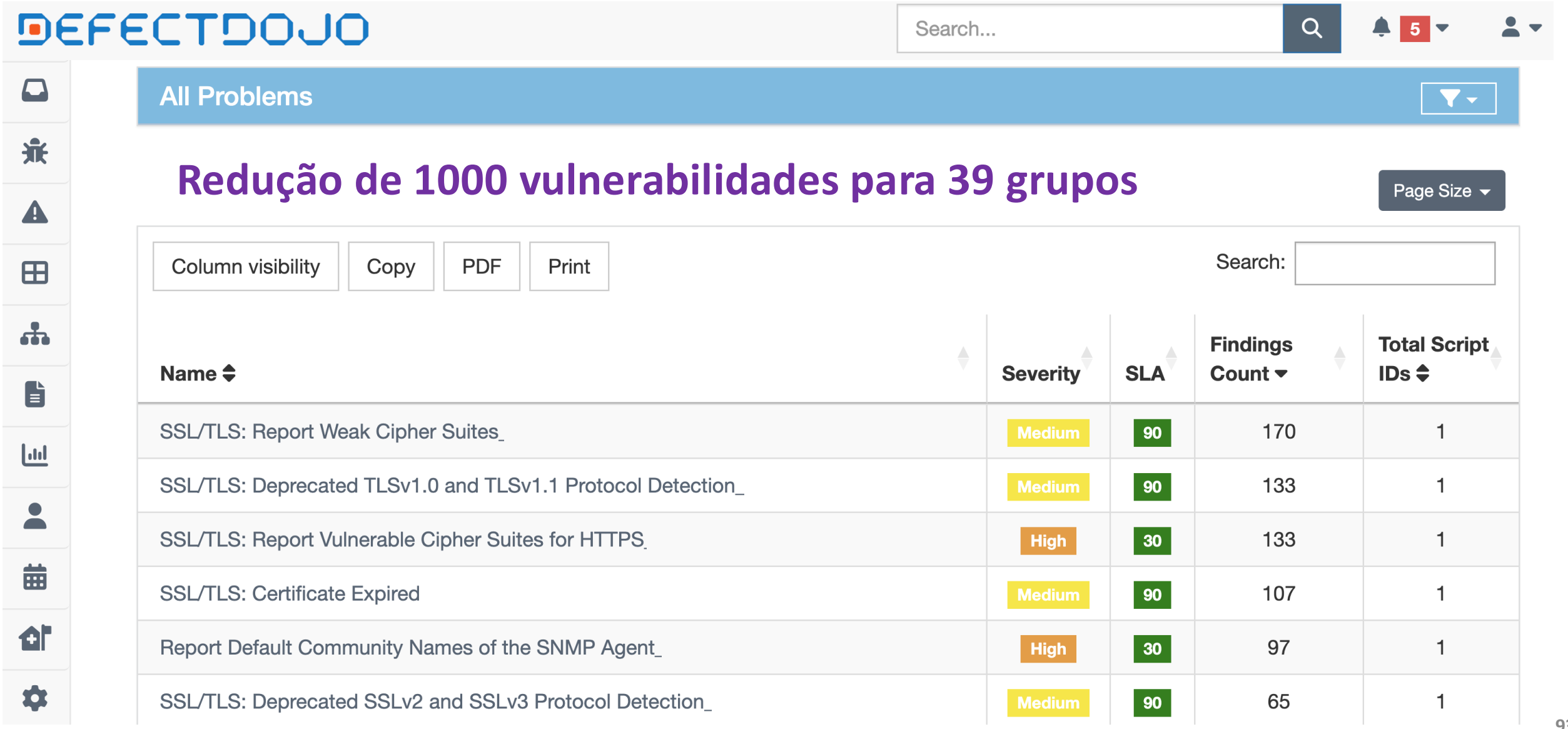


Identificar o mesmo CVE não implica que scripts são equivalentes

Varredura por versão 1 do protocolo SSH

Identificar CVEs diferentes não implica que scripts são complementares

Agrupamento de vulnerabilidades



Anonimização específica para o contexto

- Anonimização de nomes de domínio

https://appglassfish.reitoria.uni.edu.br

https://appglassfish.dcomp.uni.edu.br

https://apptest.lab.dcomp.uni.edu.br

Anonimização específica para o contexto

- Anonimização de nomes de domínio
- Identificação de palavras chaves
  - Manual + modelos de linguagem

https://appglassfish.reitoria.uni.edu.br

https://appglassfish.dcomp.uni.edu.br

https://apptest.lab.dcomp.uni.edu.br

- Tipos e Modelos de Dispositivos
- Fabricantes
- Protocolos
- Serviços, aplicações e ferramentas – app
- Frameworks – glassfish
- Contexto – test, lab
- Provedores de Nuvem
- Departamentos e Unidades
- Sistemas Operacionais

Anonimização específica para o contexto

- Anonimização de nomes de domínio
- Identificação de palavras chaves
  - Manual + modelos de linguagem
  - Importante não comprometer a identidade dos dispositivos

https://appglassfish.reitoria.uni.edu.br

https://appglassfish.dcomp.uni.edu.br

https://apptest.lab.dcomp.uni.edu.br

- Tipos e Modelos de Dispositivos
- Fabricantes
- Protocolos
- Serviços, aplicações e ferramentas – app
- Frameworks – glassfish
- Contexto – test, lab
- Provedores de Nuvem
- Departamentos e Unidades
- Sistemas Operacionais

Anonimização específica para o contexto

- Anonimização de nomes de domínio
- Identificação de palavras chaves
  - Manual + modelos de linguagem
  - Importante não comprometer a identidade dos dispositivos
- Como capturar relações de risco?
  - Reitoria > departamento de computação

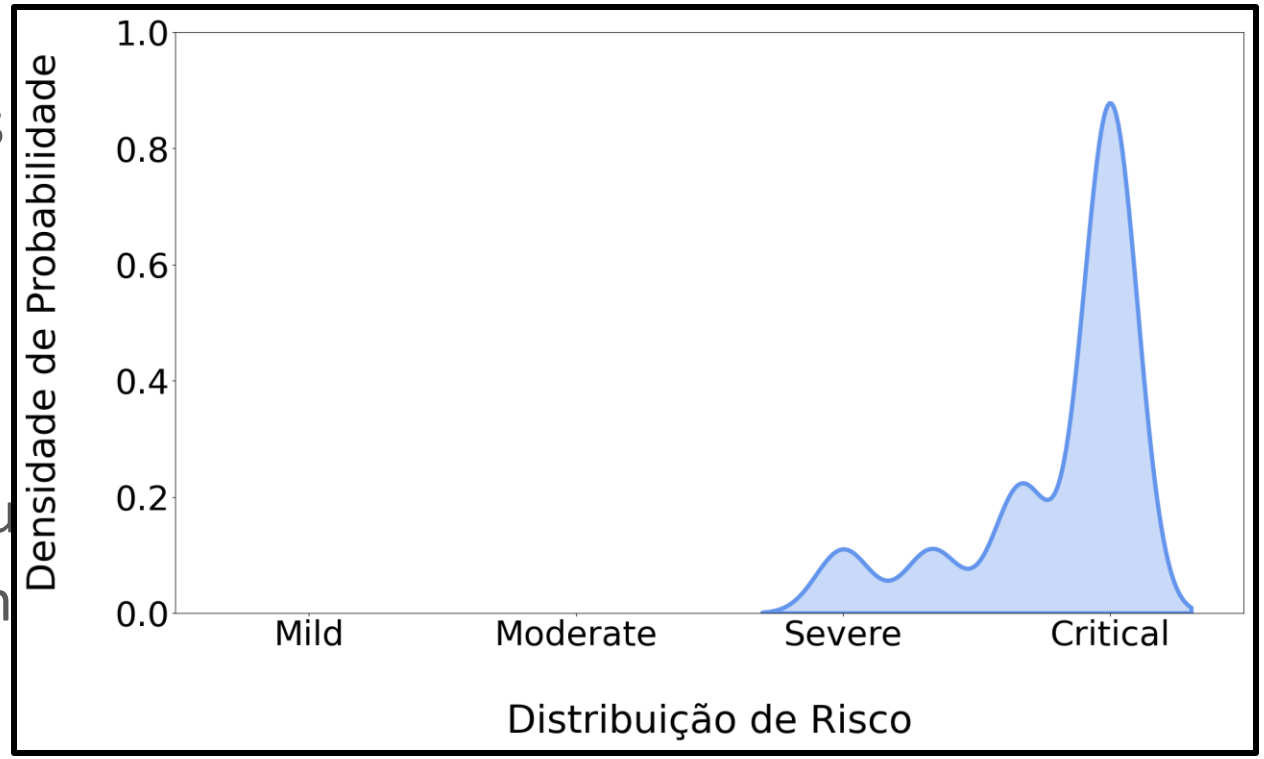
https://appglassfish.reitoria.uni.edu.br

https://appglassfish.dcomp.uni.edu.br

https://apptest.lab.dcomp.uni.edu.br

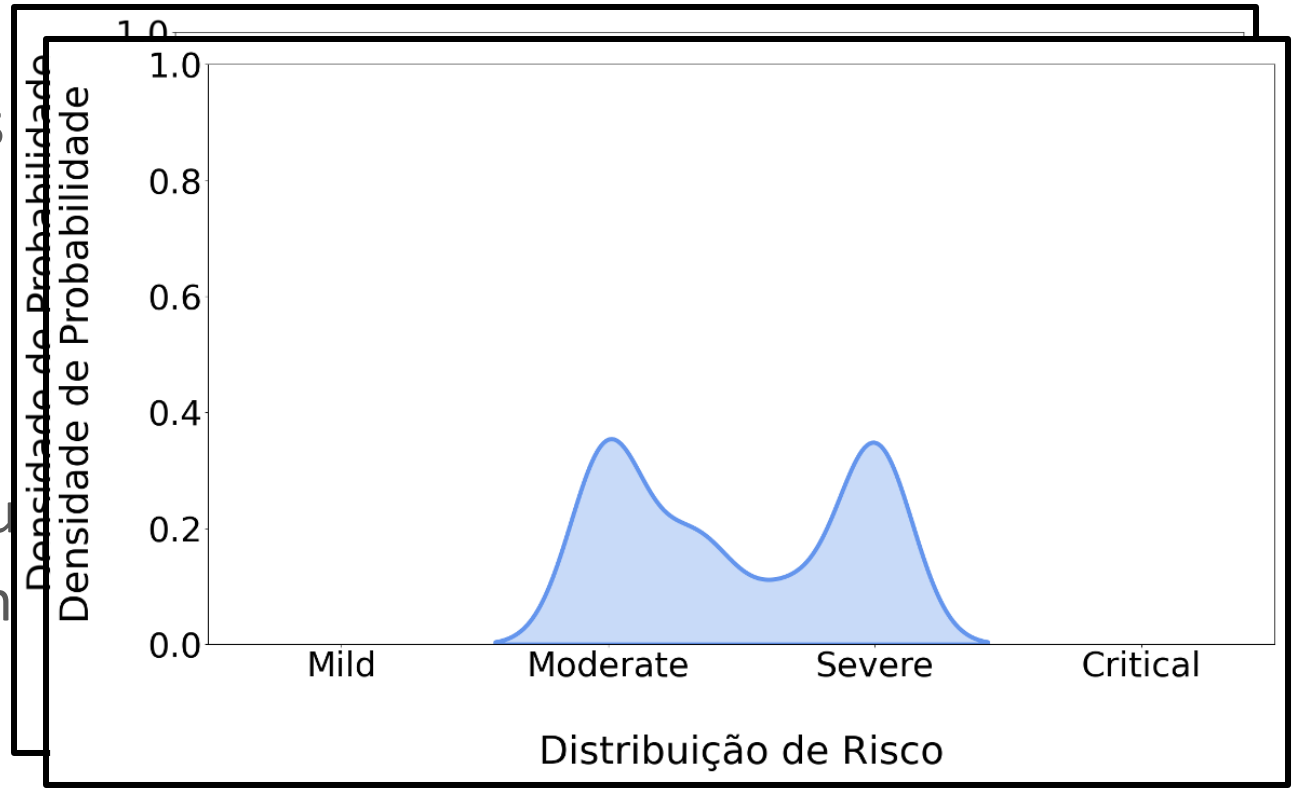
Fatores que impactam a precisão do modelo

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



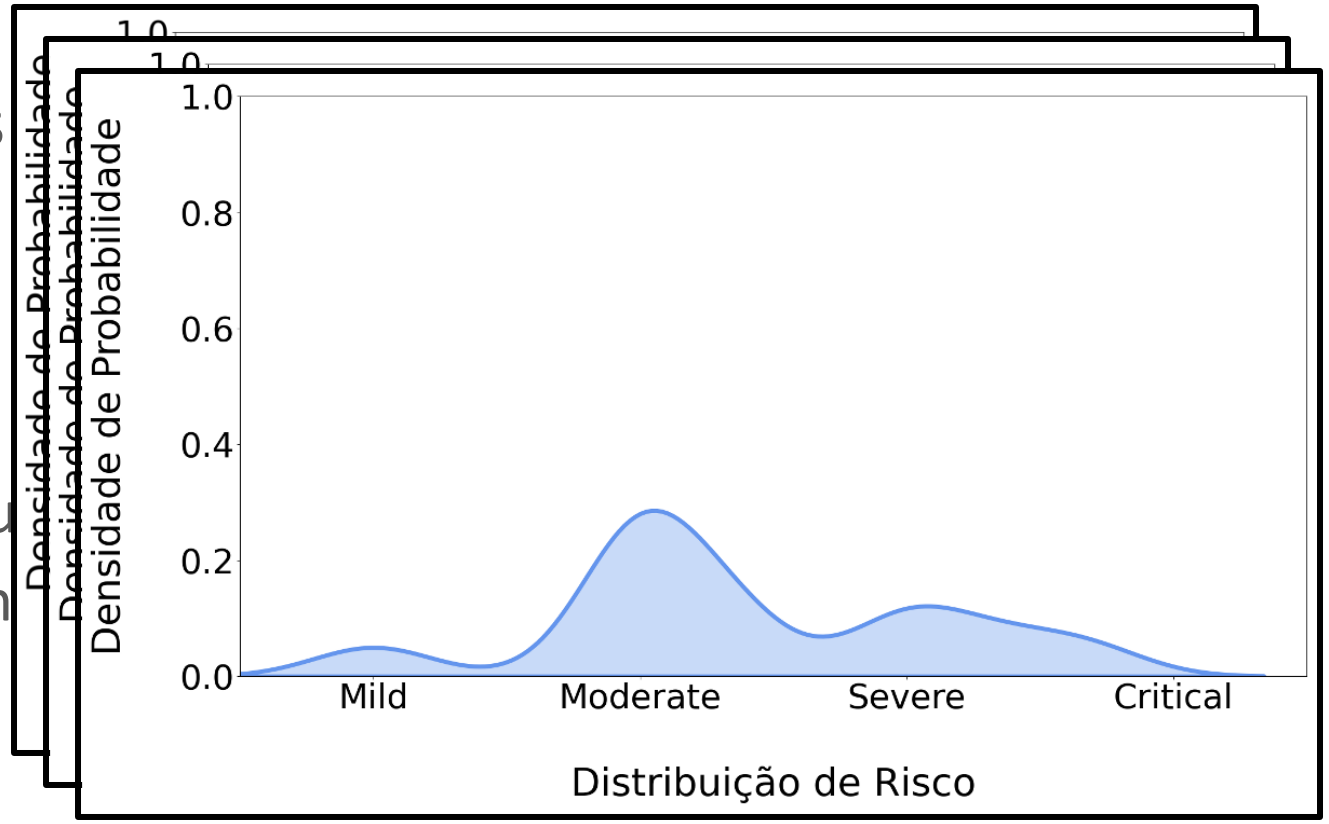
Fatores que impactam a precisão do modelo

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



Fatores que impactam a precisão do modelo

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



Informações sobre vulnerabilidades são sensíveis

- Dispositivos vulneráveis podem ser alvo de ataques
- Risco real
  - Dano material
  - Prejuízo financeiro
  - Impacto social

Informações sobre vulnerabilidades são sensíveis

- Dispositivos vulneráveis podem ser alvo de ataques
- Risco real
  - Dano material
  - Prejuízo financeiro
  - Impacto social

nuclear.X.Y.Z.br

Remote desktop
sem senha