

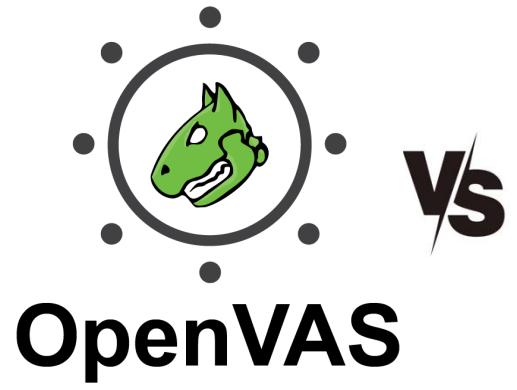
Desafios e soluções para priorização de vulnerabilidades

Ítalo Cunha
Universidade Federal de Minas Gerais

GT-CRI^YO

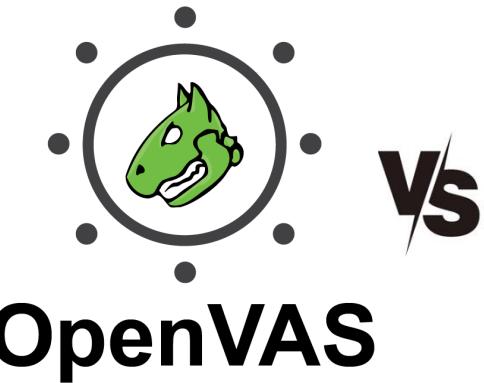
Desafios e soluções para priorização
de vulnerabilidades

Ítalo Cunha
Universidade Federal de Minas Gerais





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



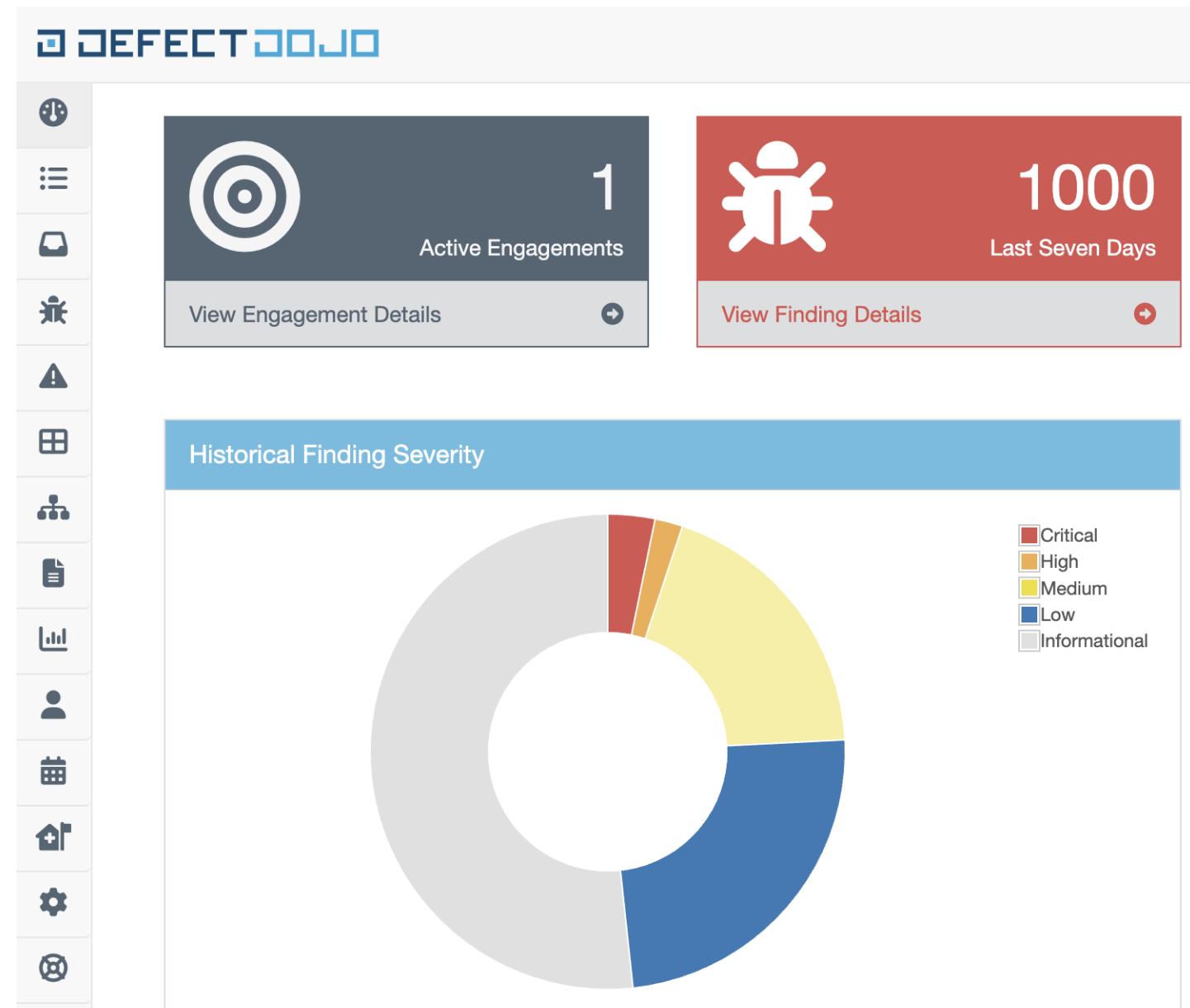
OpenVAS

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

32 críticas

19 graves

191 médias





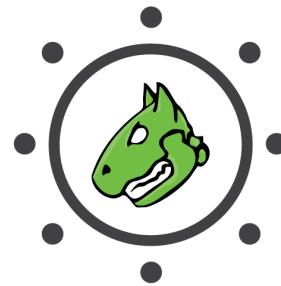
OpenVAS

vs



speed
DCC - 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

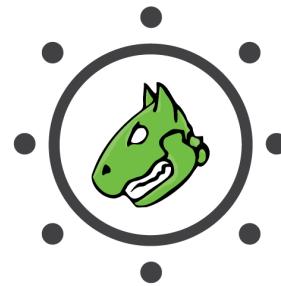


vs



OpenVAS

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	

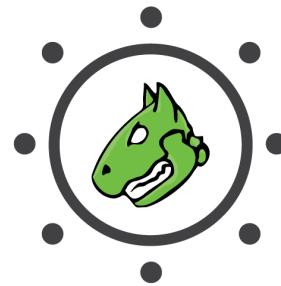


vs



OpenVAS

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	



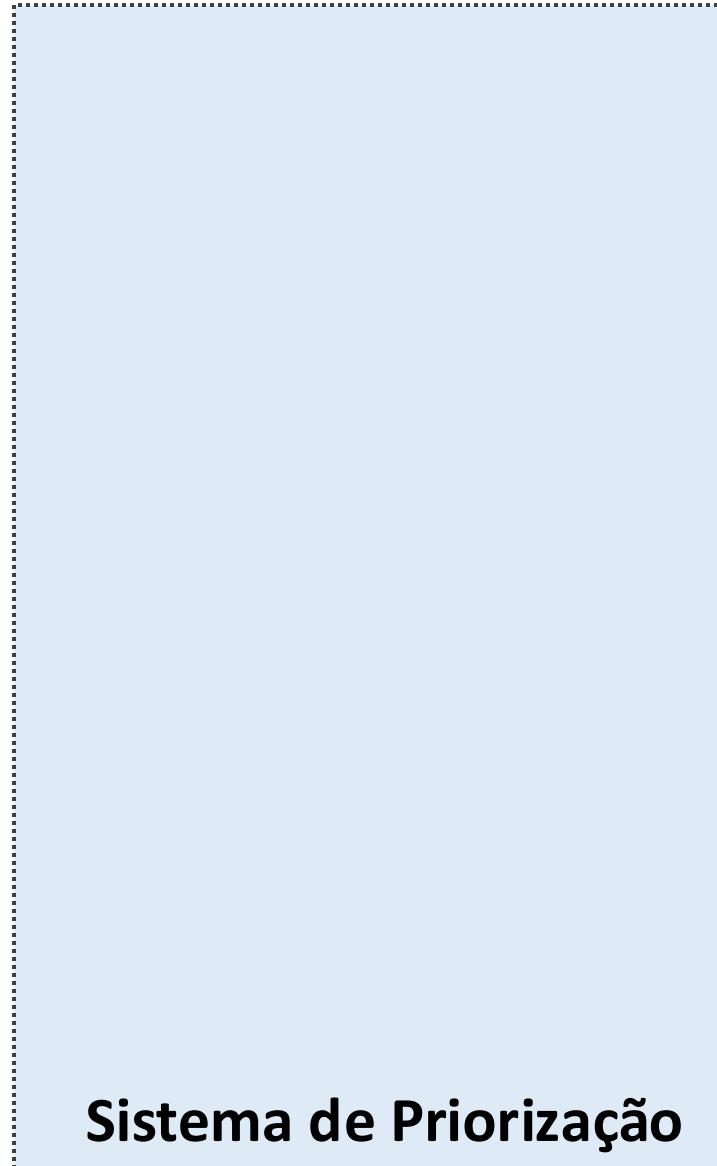
vs



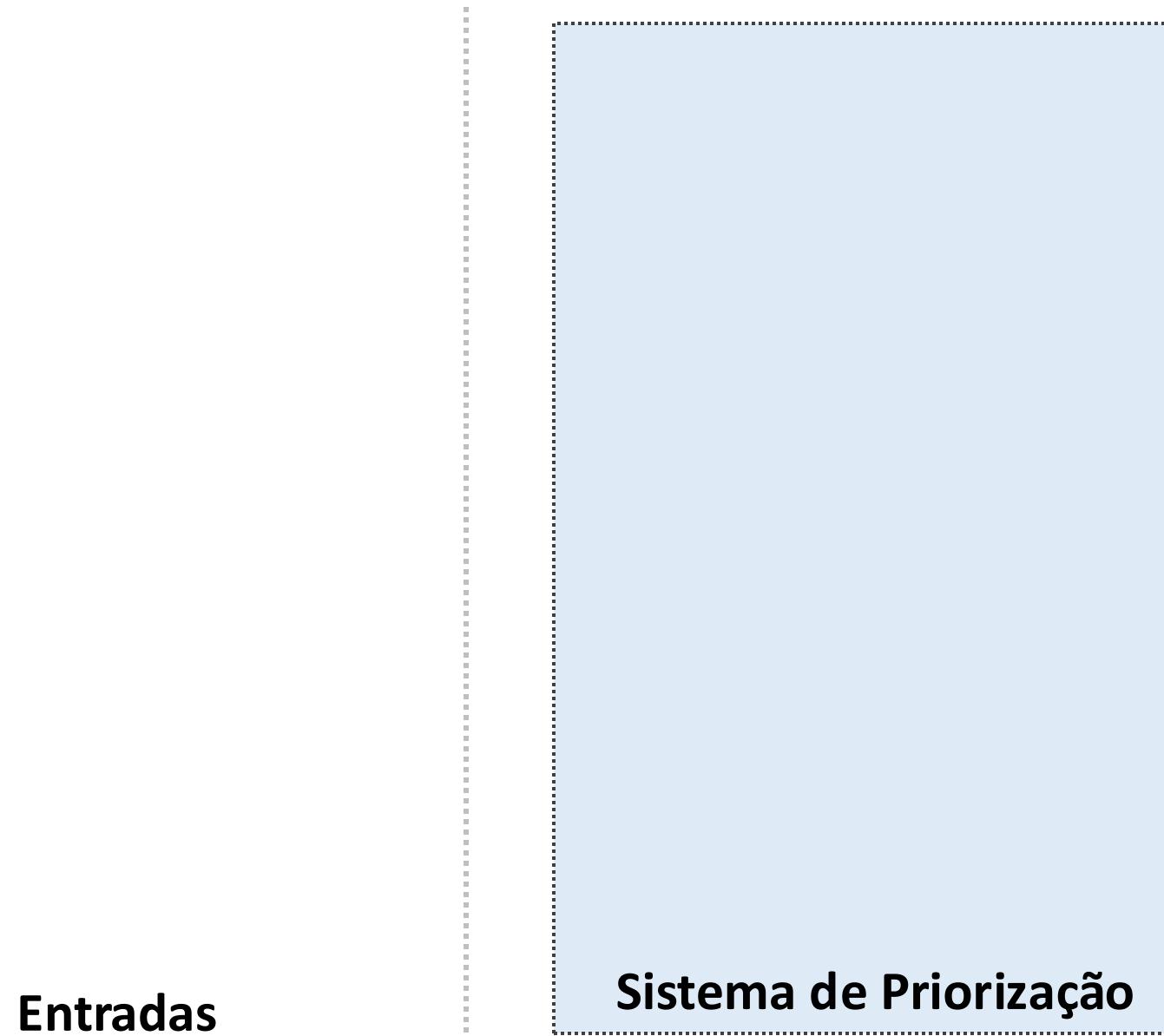
OpenVAS

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



Sistema de priorização de vulnerabilidades



Entradas

Sistema de Priorização

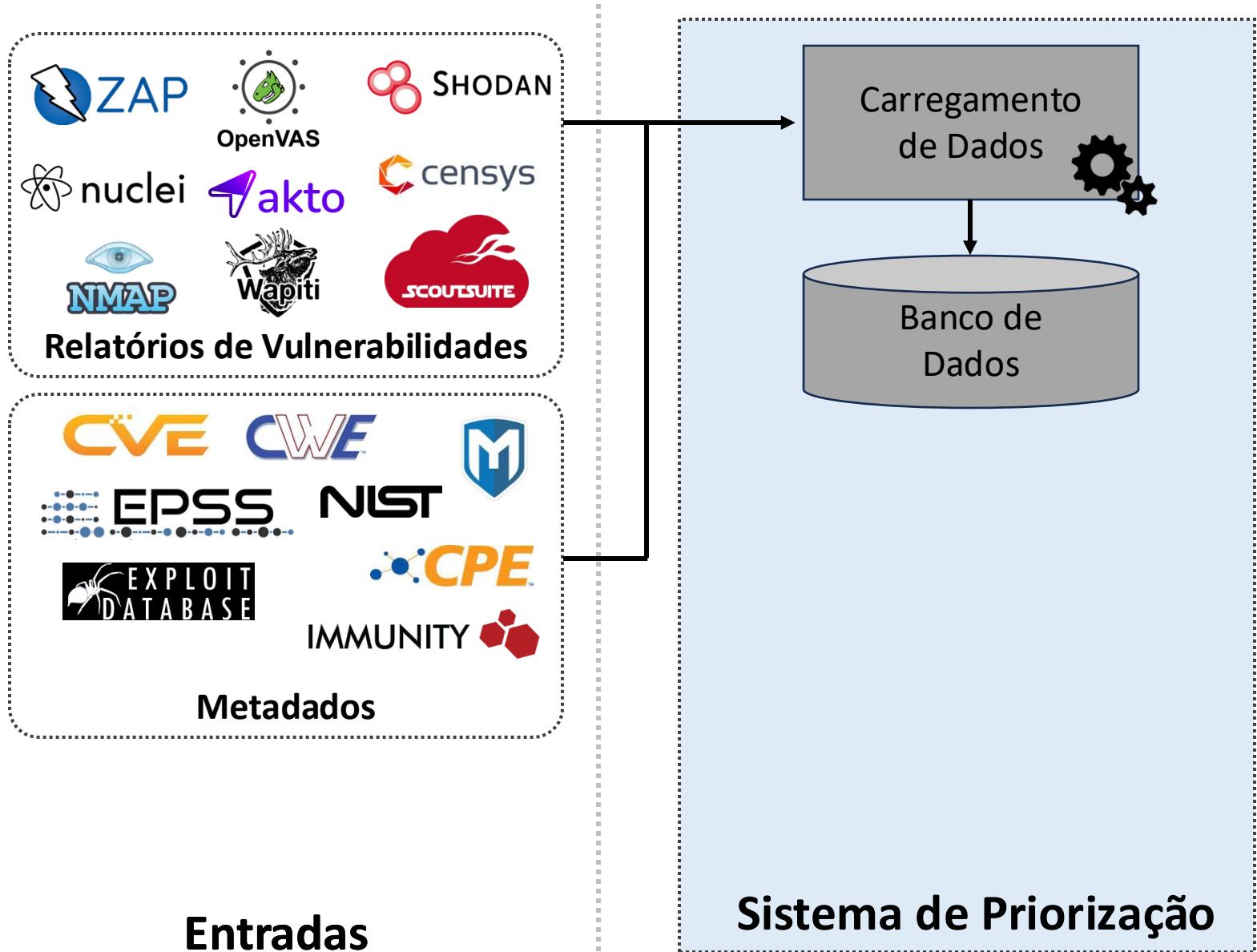
Sistema de priorização de vulnerabilidades



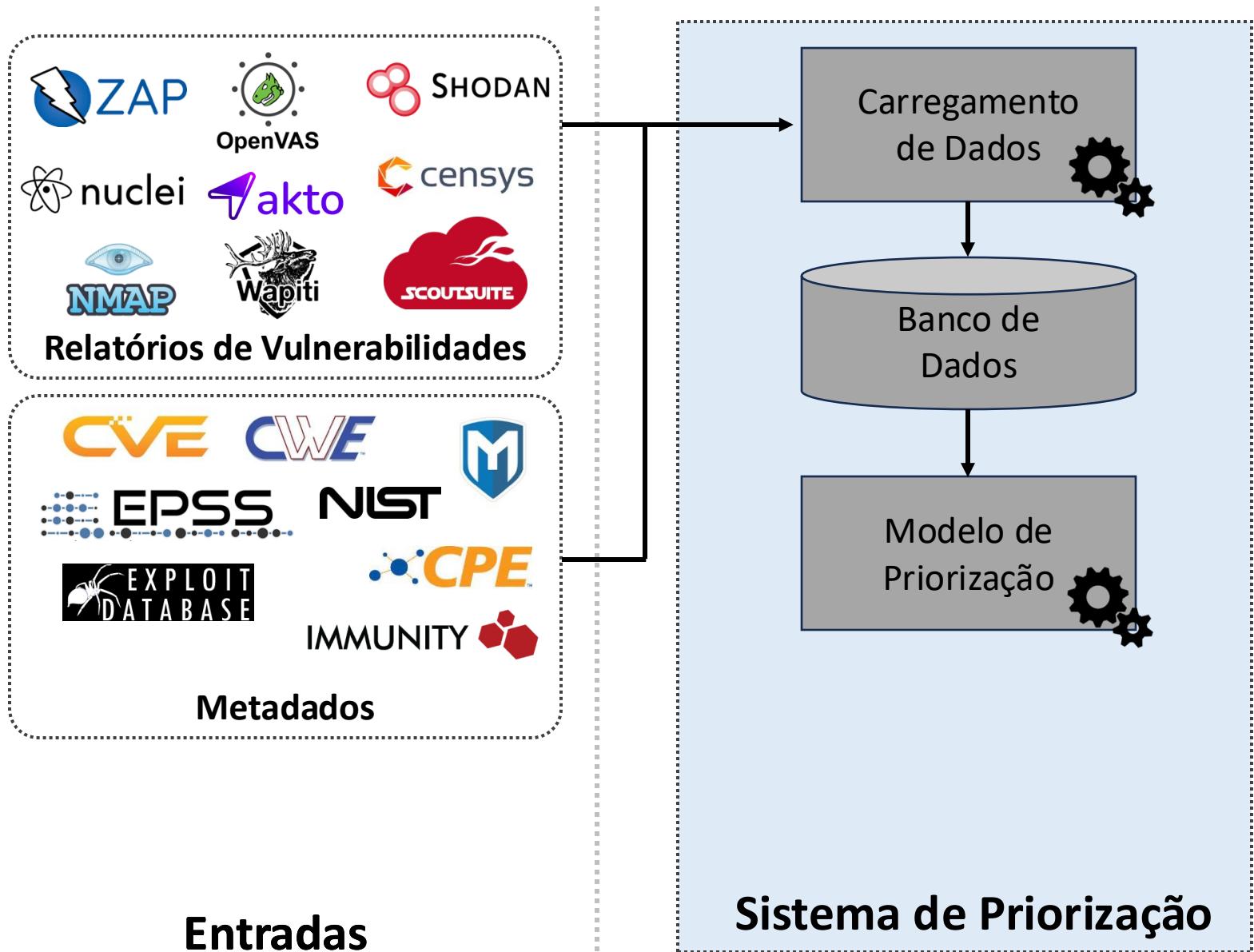
Entradas

Sistema de Priorização

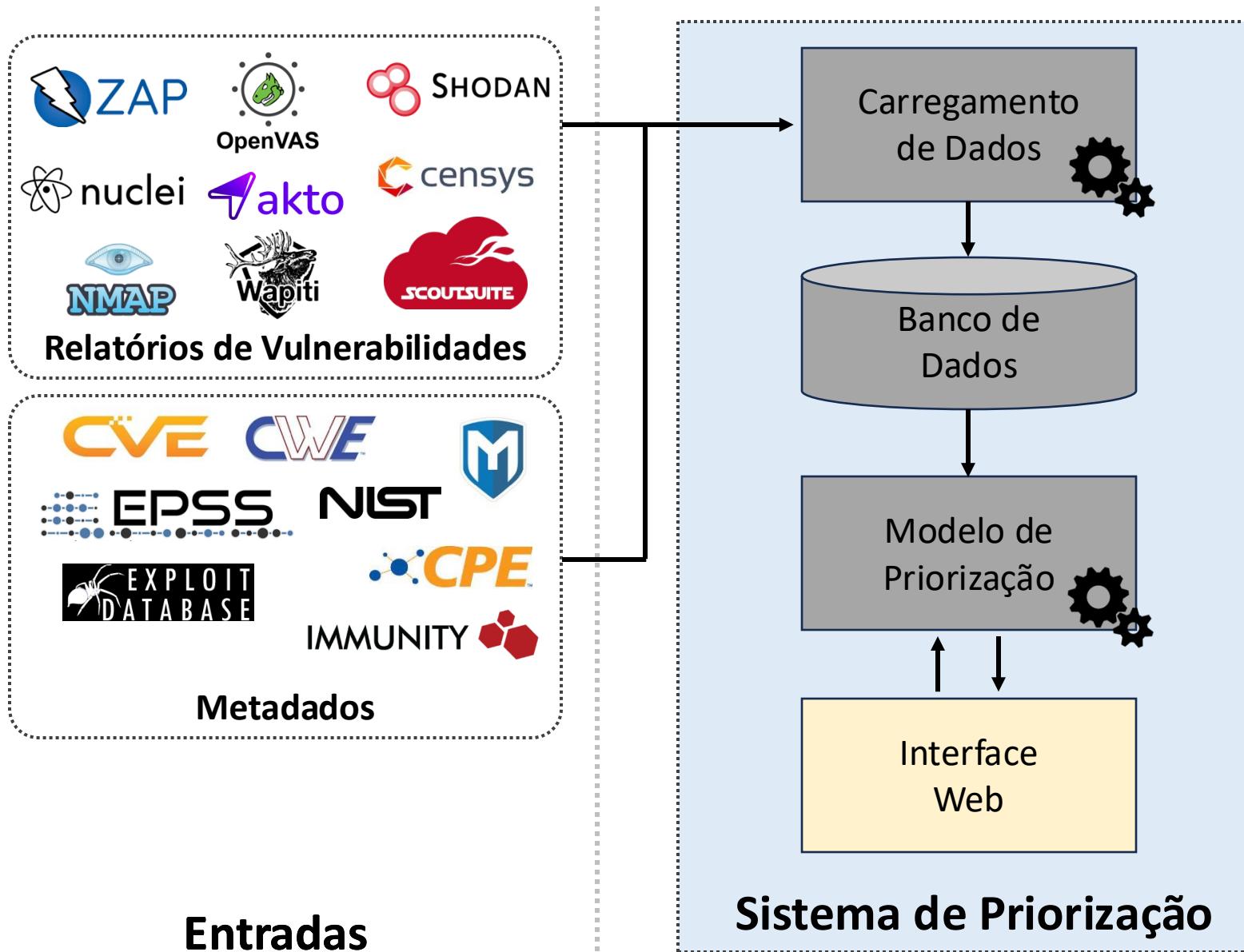
Sistema de priorização de vulnerabilidades



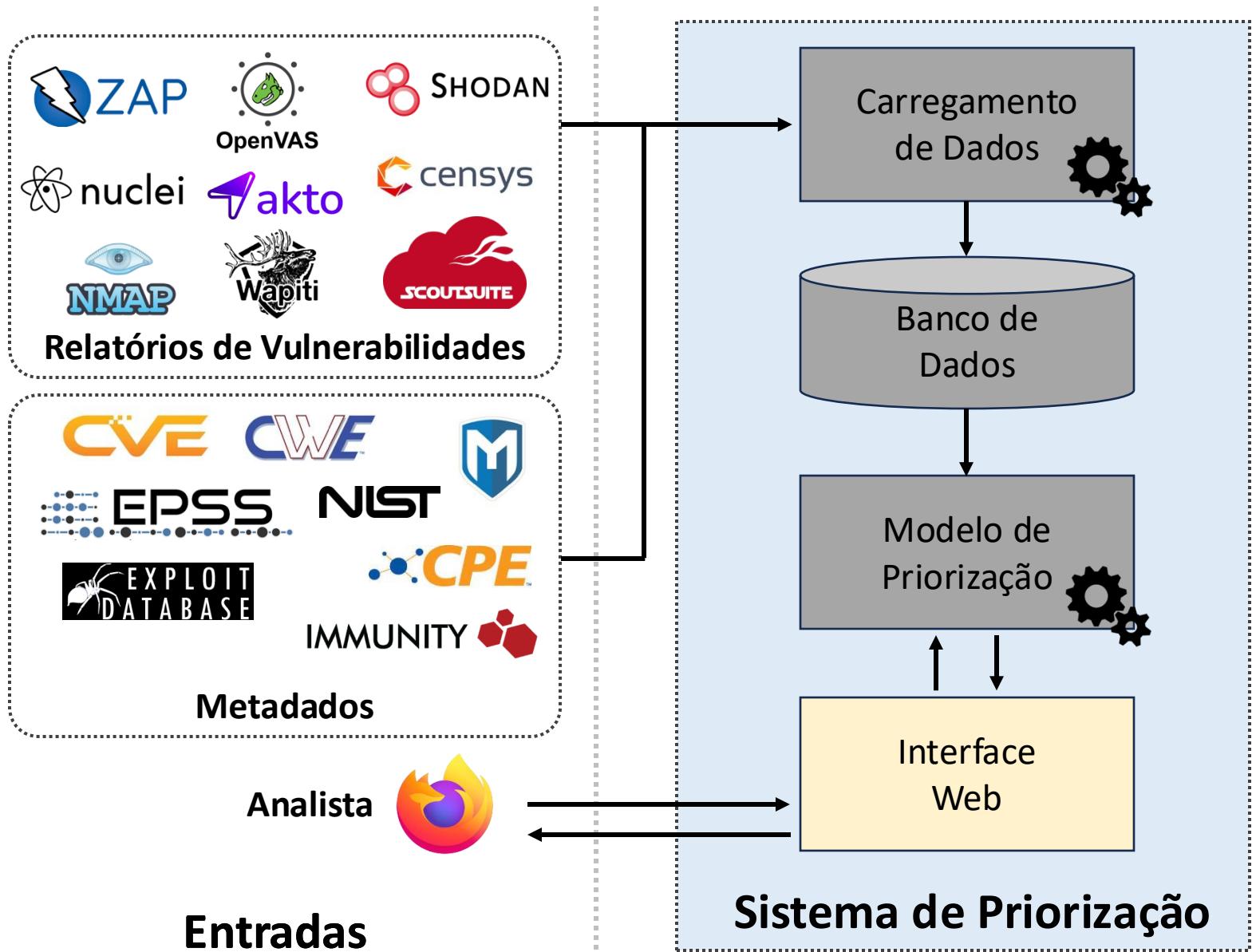
Sistema de priorização de vulnerabilidades



Sistema de priorização de vulnerabilidades



Sistema de priorização de vulnerabilidades



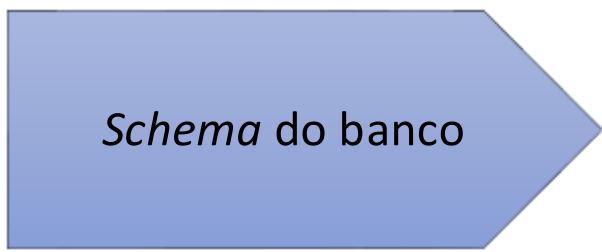
Desafio para priorização: Análises de vulnerabilidades para treino

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

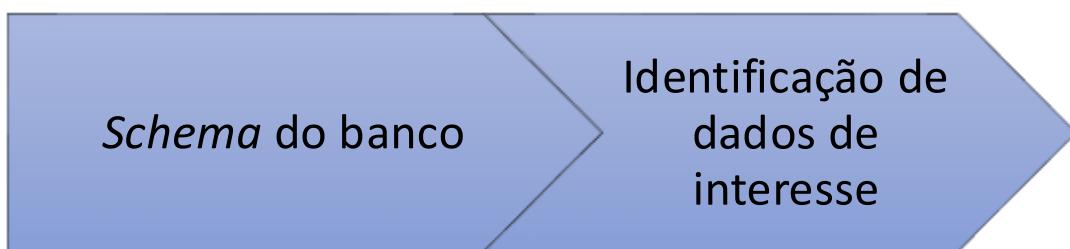
- Controle do risco vs. perda de informações úteis
- Anonimização dos dados específica para o contexto



Schema do banco

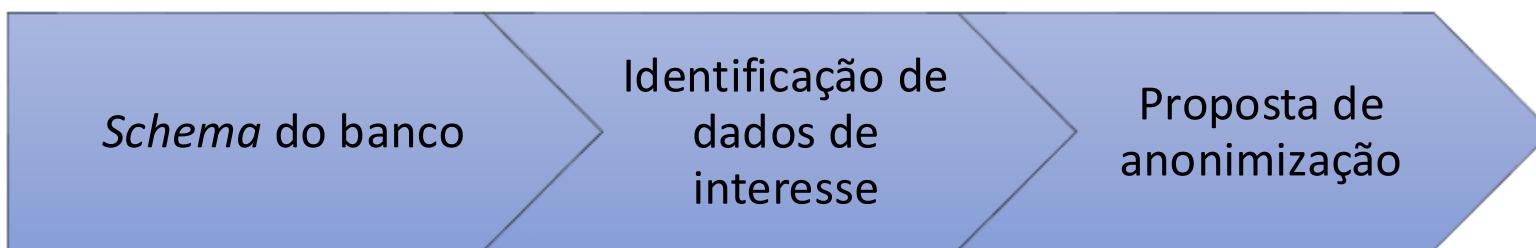
Obtendo bases de dados de sistemas de gerência

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



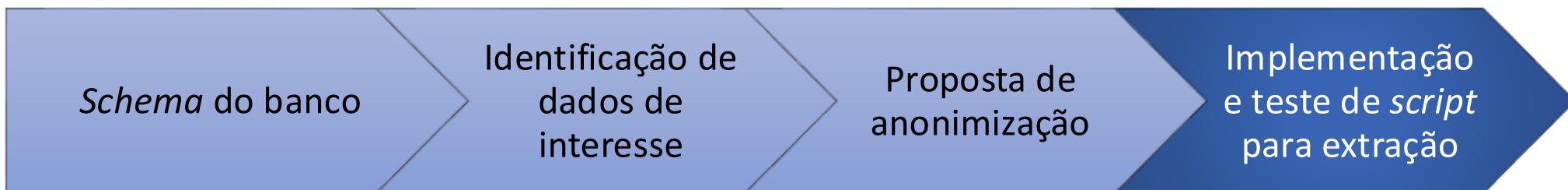
Obtendo bases de dados de sistemas de gerência

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



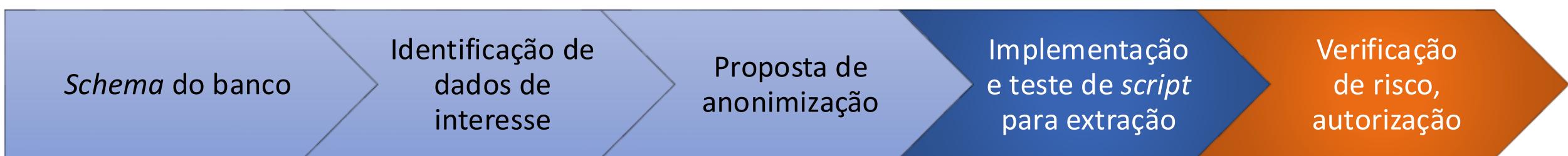
Obtendo bases de dados de sistemas de gerência

- 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

DEFECTDOJO

Search... 🔍 🔔 5 👤

All Findings ⬇️ Filter

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:

<input type="checkbox"/>	Severity	Name	CWE	Vulnerability Id	EPSS Score	EPSS Percentile	Votes
<input type="checkbox"/>	High	Report Default Community Names of the SNMP Agent_ ⋮		CVE-1999-0517	92.33%	99.72%	Nothing selected
<input type="checkbox"/>	High	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS_ ⋮		CVE-2016-2183	40.02%	97.06%	Mild Moderate Severe Critical

Metadados sobre vulnerabilidades

The screenshot shows the DEFECTDOJO application interface. At the top, there is a navigation bar with icons for Home, Issues, Reports, Dashboards, Integrations, and Help. On the right side of the header are a search bar, a notification bell icon with a '5' count, and a user profile dropdown.

The main content area displays a report titled "SSL/TLS: Report Vulnerable Cipher Suites for HTTPS_150.164.23.203_443/tcp". The report was last reviewed today by Admin User (admin), last status updated today, and created today. It includes a "(Re)Import" link and a three-dot menu icon.

A section titled "Metadata" is expanded, containing a note: "* Cards with a black border have a KEV (Known Exploited Vulnerability) associated with them!"

Four cards are listed under the "Metadata" section:

- CVE-2020-29583** (KEV): EPSS 0.94, CVSSv3 9.8. Associated with Privilege Escalation and CWE-522.
- CVE-1999-0502**: EPSS 0.53, CVSS Missing 0.0.
- CVE-2009-3710** (KEV): EPSS 0.03, CVSS Missing 0.0. Associated with Privilege Escalation and Remote Code Execution.
- CVE-2012-4577**: EPSS 0.03, CVSSv2 10.0. Associated with Privilege Escalation and Remote Code Execution. CPE information: Korenix Jetport.

Annotations are present in the bottom left corner pointing to the KEV cards, and in the bottom right corner pointing to the CPE information.

Criação de bases para treino

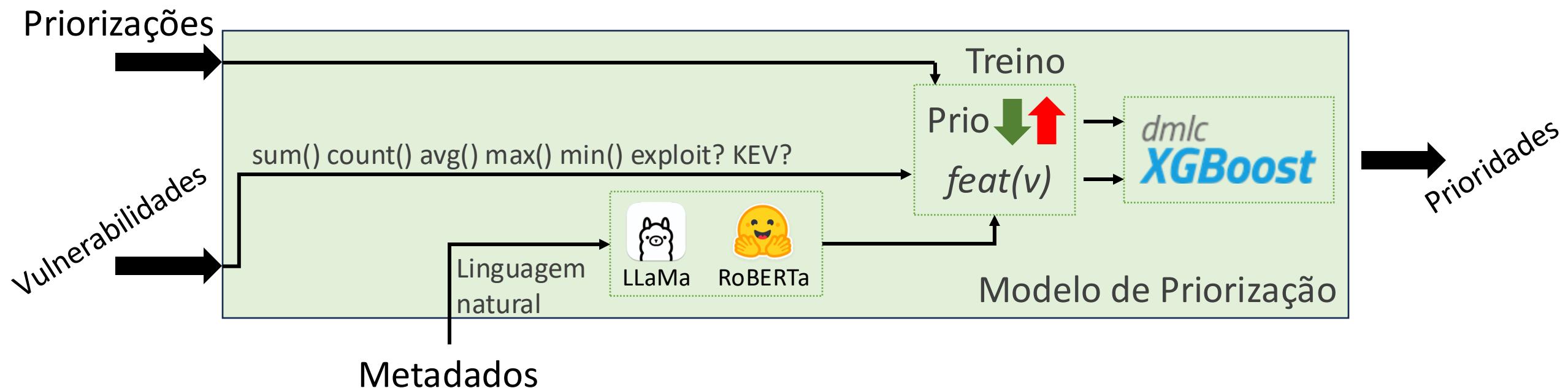
- Obtenção de dados de varreduras de rede
- Análises de vulnerabilidades por
 - Integrantes do projeto
 - Residentes do programa Hackers do Bem

Criação de bases para treino

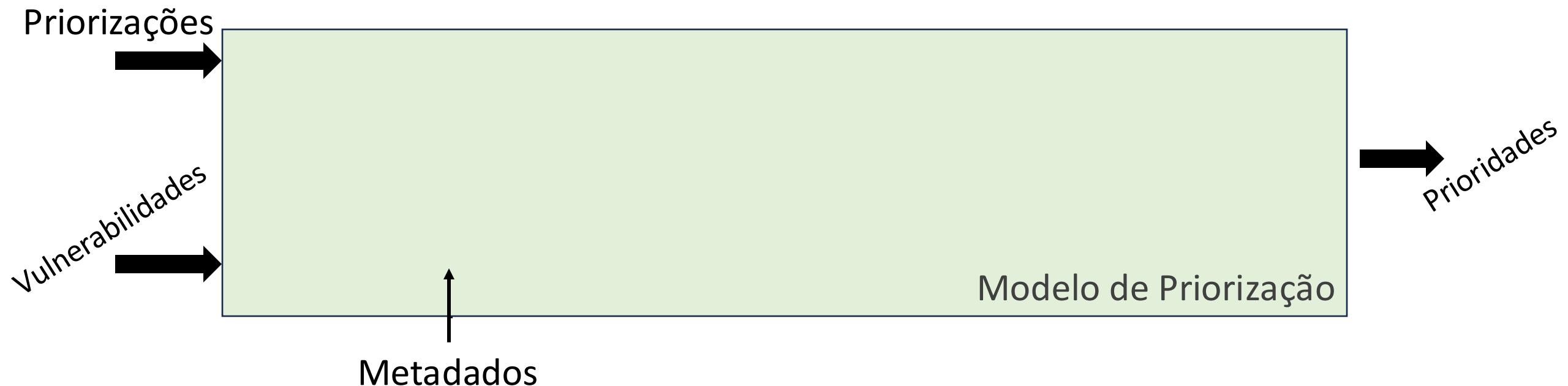
- Obtenção de dados de varreduras de rede
- Análises de vulnerabilidades por
 - Integrantes do projeto
 - Residentes do programa Hackers do Bem
- Pouco realismo
 - Bolsistas e residentes não são responsáveis pela segurança
 - Bolsistas e residentes não atuam em conjunto

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



vs

OpenVAS



32 críticas

19 graves

191 médias

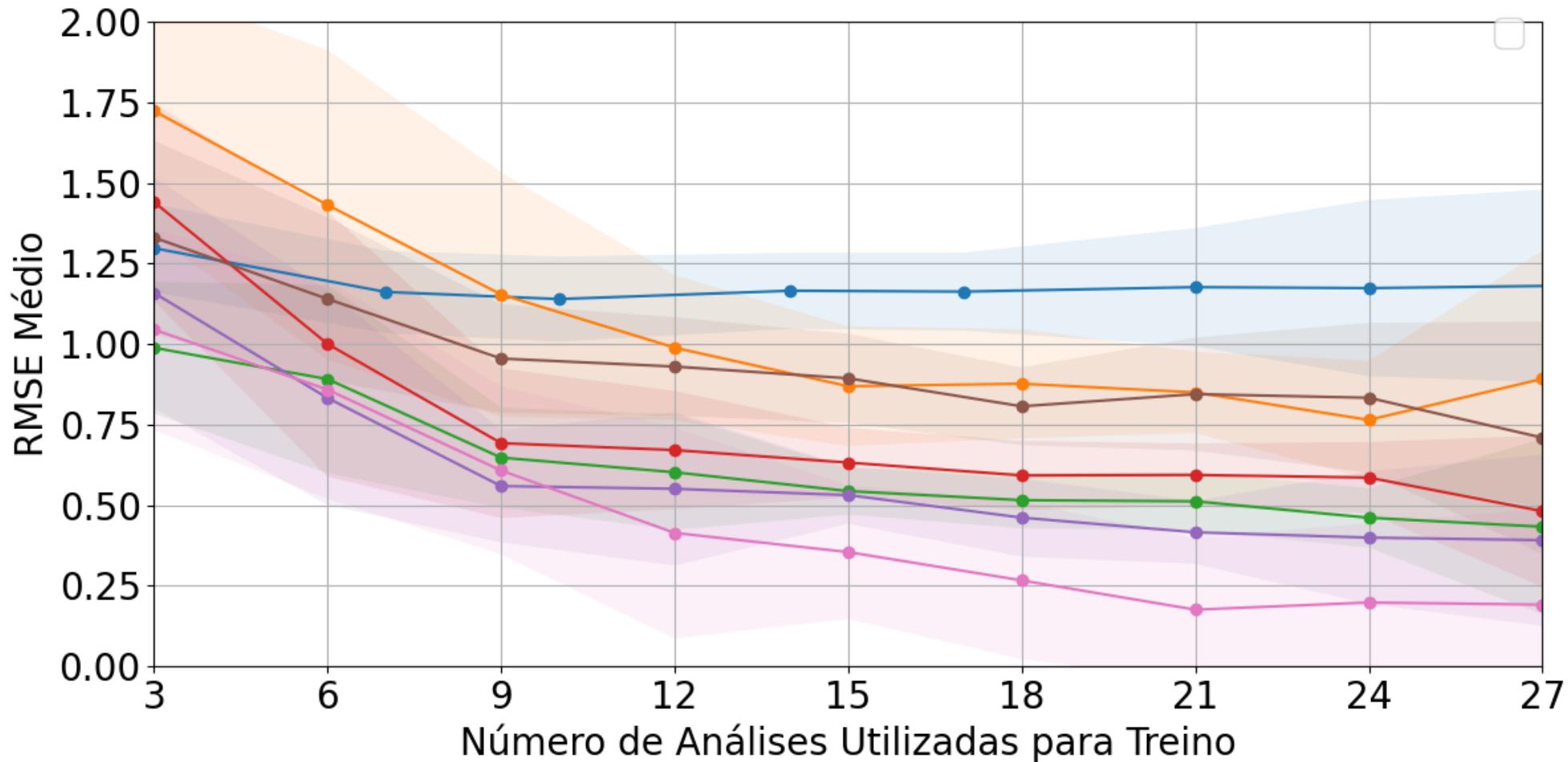
Fatores que impactam a precisão do modelo

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

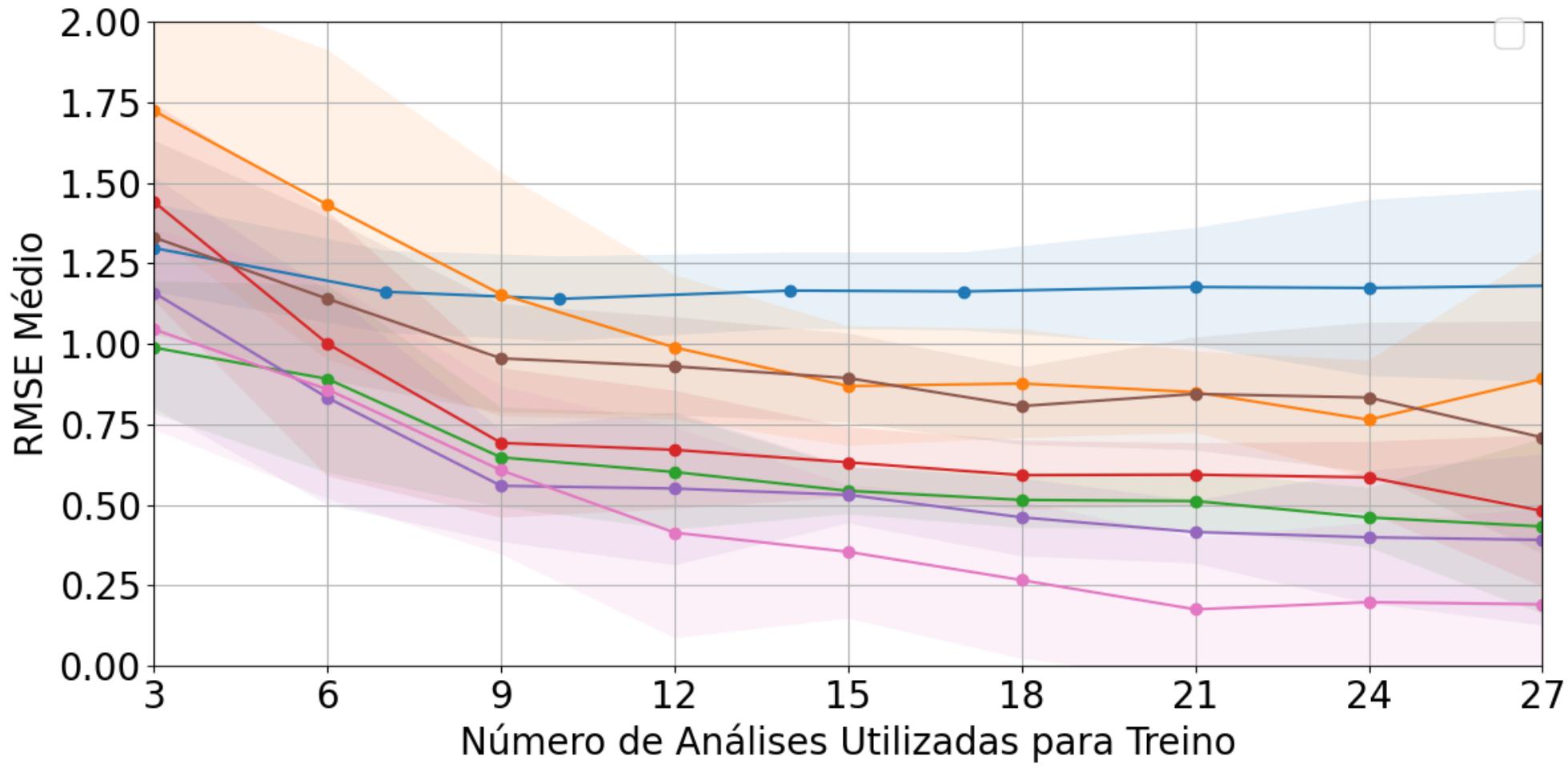
Fatores que impactam a precisão do modelo

- 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”

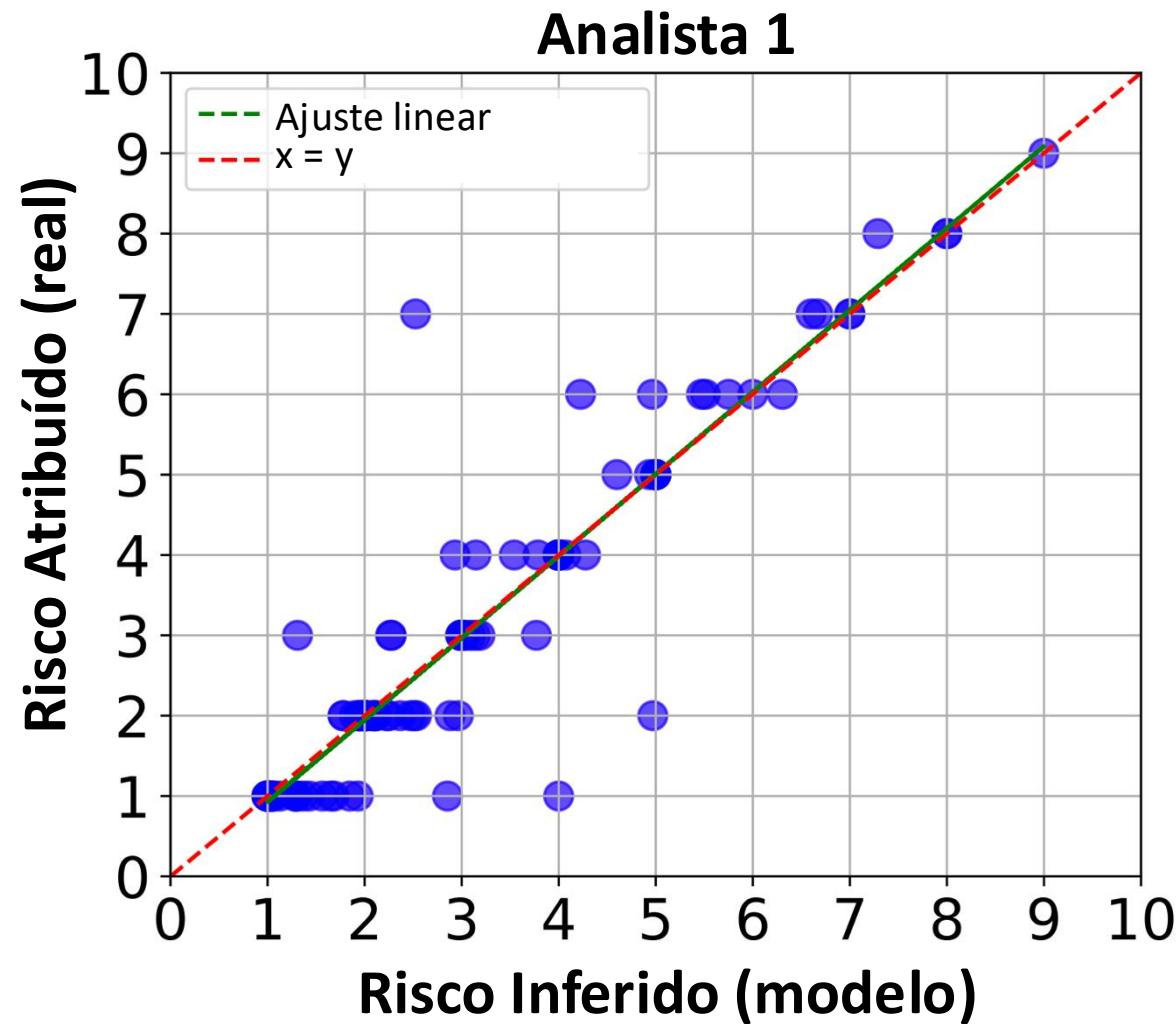
Quantas análises são necessárias para treino?



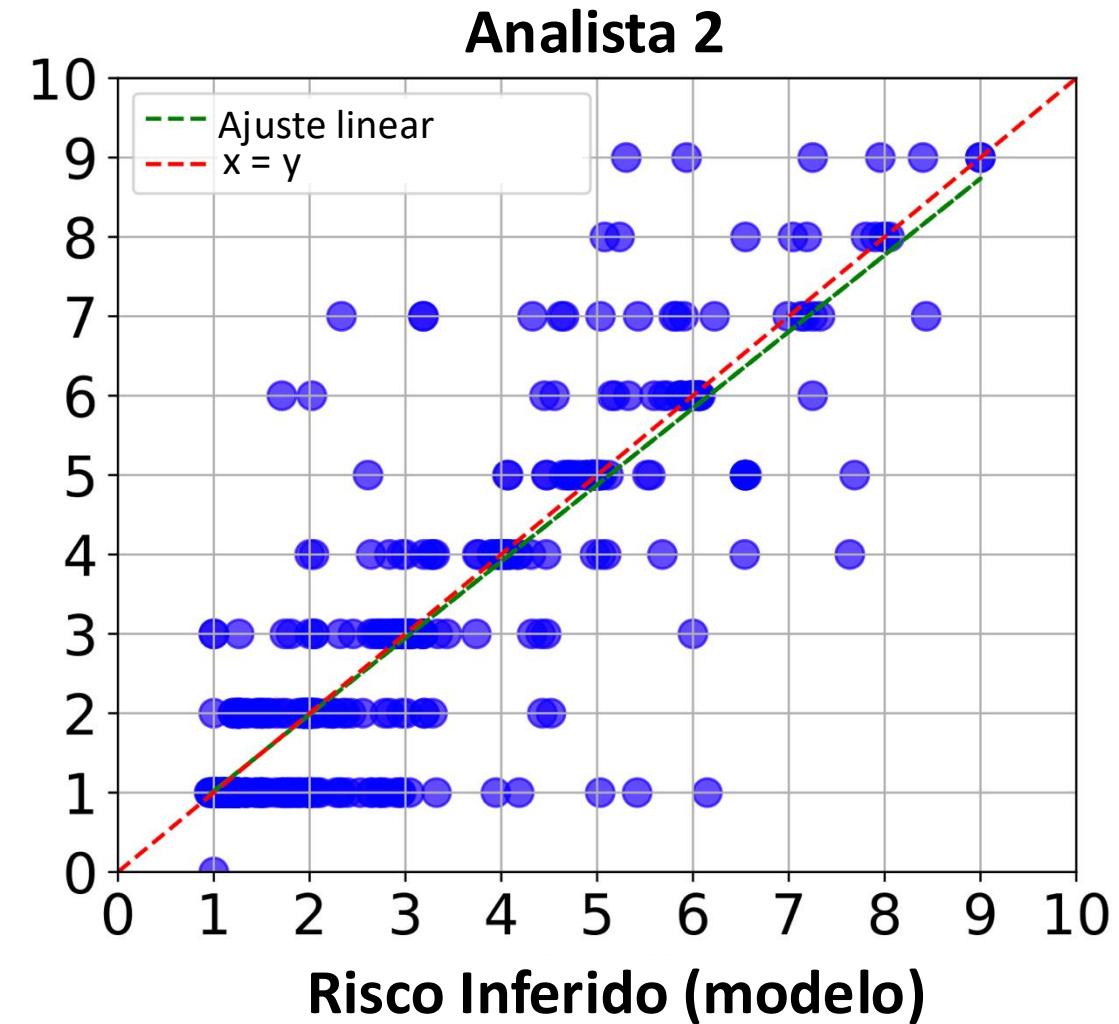
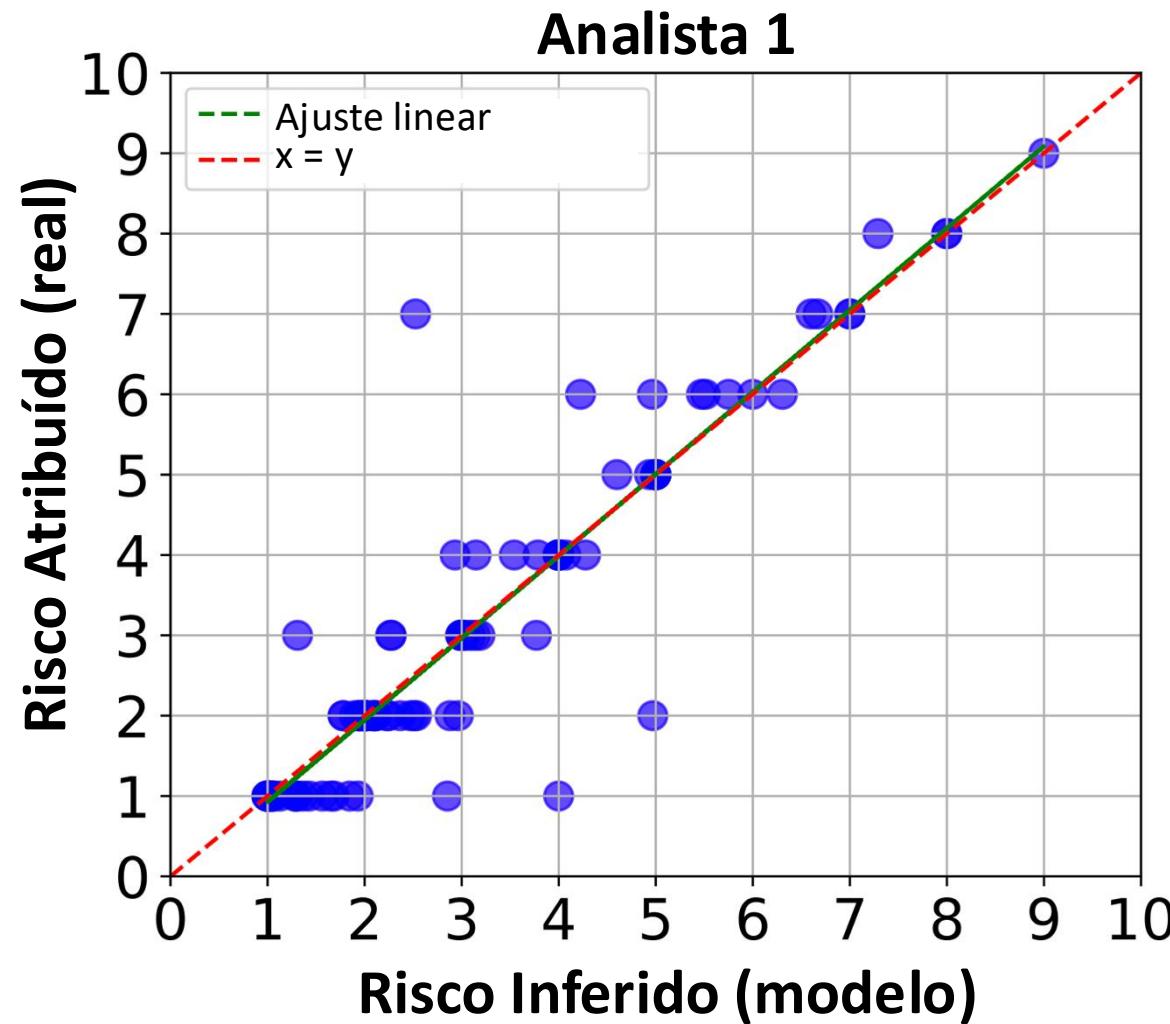
Quantas análises são necessárias para treino?



Previsões correlacionadas com os votos



Previsões correlacionadas com os votos



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

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

KEV



Korenix Jetport



CPE

Metadados relacionados a vulnerabilidades

CVE-2020-29583 ↗

Privilege Escalation

CWE-522 ↗

EPSS 0.94

CVSSv3 9.8

CVE-2009-3710 ↗

Privilege Escalation

Remote Code Execution

EPSS 0.03

CVSS Missing 0.0

KEV →

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

CVE-2020-29583 ↗

Privilege Escalation

CWE-522 ↗

EPSS 0.94

CVSSv3 9.8

CVE-2009-3710 ↗

Privilege Escalation

Remote Code Execution

EPSS 0.03

CVSS Missing 0.0

KEV →

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 gerativos 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)



**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

Desafios e soluções para priorização de vulnerabilidades

Ítalo Cunha
Universidade Federal de Minas Gerais

**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)

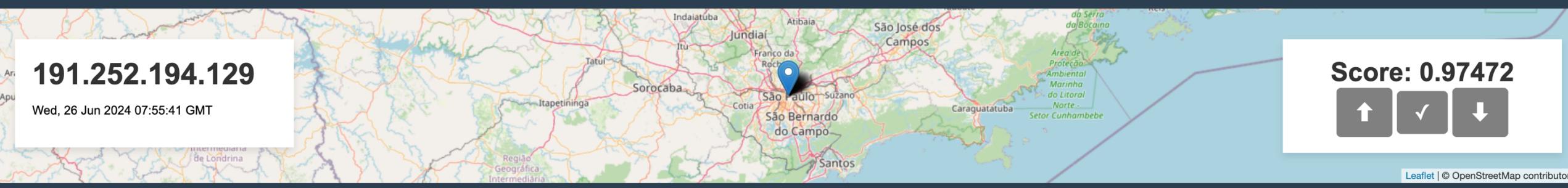


Criação de bases para treino

- 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

DEFECTDOJO

Search... 🔍 🔔 5 👤

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:

<input type="checkbox"/>	Severity	Name	CWE	Vulnerability Id	EPSS Score	EPSS Percentile	Votes
<input type="checkbox"/>	High	Report Default Community Names of the SNMP Agent_ ⋮		CVE-1999-0517	92.33%	99.72%	Nothing selected
<input type="checkbox"/>	High	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS_ ⋮		CVE-2016-2183	40.02%	97.06%	Mild Moderate Severe Critical

Metadados sobre vulnerabilidades

The screenshot shows the DEFECTDOJO application interface. At the top, there is a navigation bar with icons for Home, Issues, Reports, Dashboards, Integrations, and Help. On the right side of the header are a search bar, a notification bell icon with a '5' count, and a user profile icon.

The main content area displays a report titled "SSL/TLS: Report Vulnerable Cipher Suites for HTTPS_150.164.23.203_443/tcp". The report was last reviewed today by Admin User (admin), last status updated today, and created today. It includes a "(Re)Import" link and a three-dot menu icon.

A section titled "Metadata" is expanded, containing a note: "* Cards with a black border have a KEV (Known Exploited Vulnerability) associated with them!"

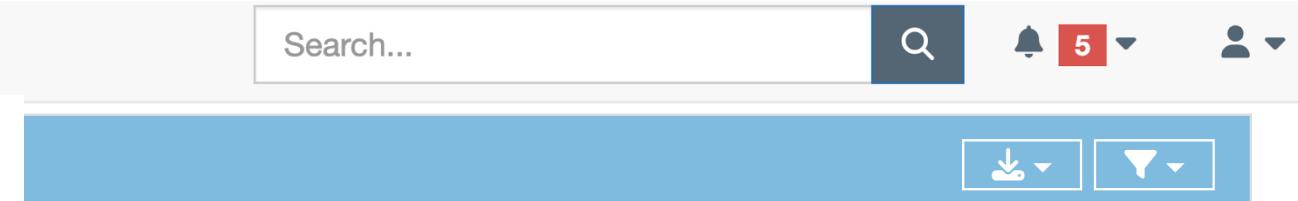
Four cards are listed under the "Metadata" section:

- CVE-2020-29583** (KEV): EPSS 0.94, CVSSv3 9.8. Associated with Privilege Escalation and CWE-522.
- CVE-1999-0502**: EPSS 0.53, CVSS Missing 0.0.
- CVE-2009-3710** (KEV): EPSS 0.03, CVSS Missing 0.0. Associated with Privilege Escalation and Remote Code Execution.
- CVE-2012-4577**: EPSS 0.03, CVSSv2 10.0. Associated with Privilege Escalation and Remote Code Execution. CPE information: Korenix Jetport.

Annotations are present in the bottom left corner pointing to the KEV cards, and in the bottom right corner pointing to the CPE information.

Extensões ao DefectDojo

DEFECTDOJO



The screenshot shows the DefectDojo application interface. At the top, there is a navigation bar with a search bar containing "Search...", a magnifying glass icon, a bell icon with a "5" notification, and a user profile icon. Below the navigation bar is a blue header bar with download and filter icons. The main content area displays a table of vulnerabilities. The table has columns: "Vulnerability Id", "EPSS Score", "EPSS Percentile", and "Votes". The first row shows CVE-1999-0517 with an EPSS Score of 92.33% and Percentile of 99.72%, and a dropdown menu for votes showing "Nothing selected". The second row shows CVE-2016-2183 with an EPSS Score of 40.02% and Percentile of 97.06%, and a dropdown menu for votes showing "Mild", "Moderate", "Severe", and "Critical". A search bar labeled "Search:" is located at the top right of the table area.

Vulnerability Id	EPSS Score	EPSS Percentile	Votes
CVE-1999-0517	92.33%	99.72%	Nothing selected
CVE-2016-2183	40.02%	97.06%	Mild Moderate Severe Critical

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



- Vazamento de dados
- Violação de privacidade



- Desempenho da aplicação
- Funcionamento da infraestrutura



Desenvolvedores

- Corrigir bugs
- Upgrade de sistemas



Sysadmins

- Instalar firewalls
- Reconfiguração de sistemas

Análise de risco

Vulnerabilidade + Ameaça + Impacto

Análise de risco

Vulnerabilidade + 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

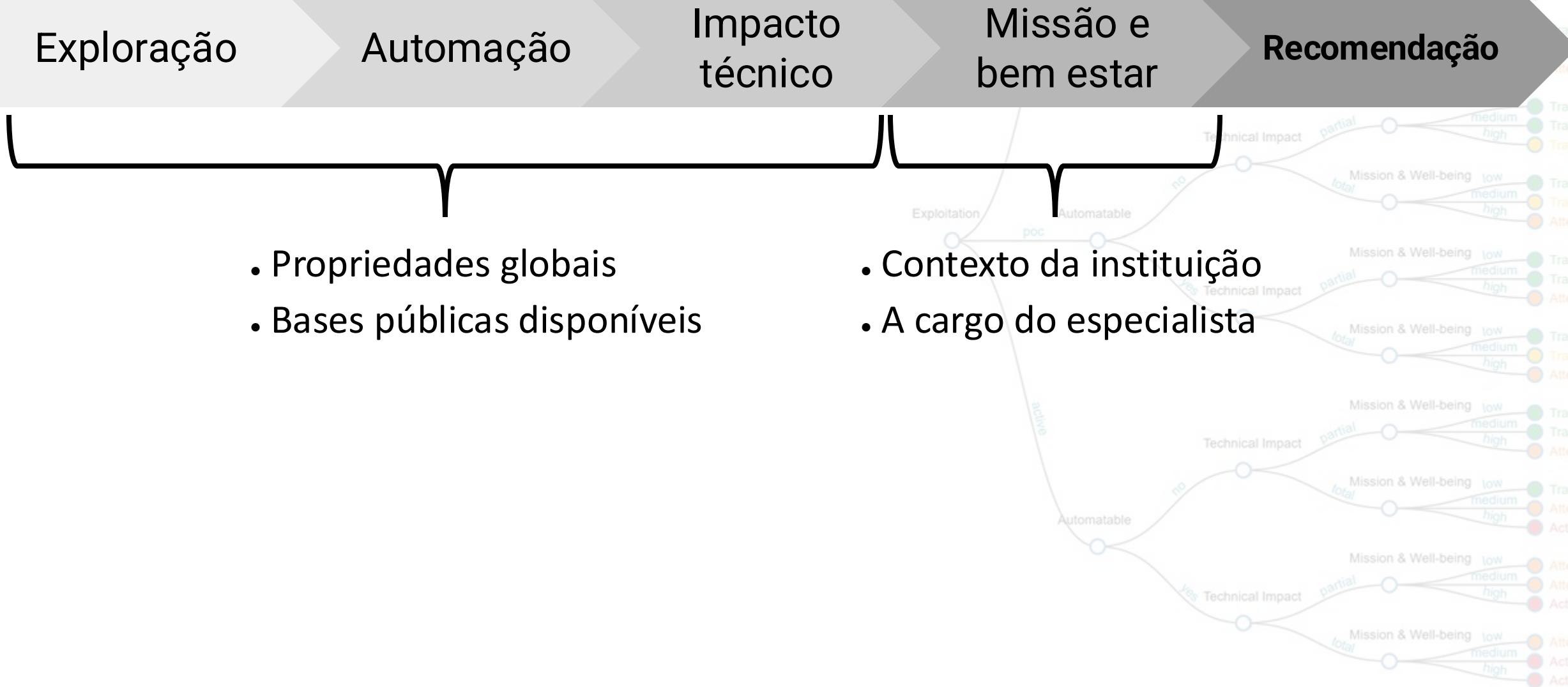
Impacto técnico

Missão e p bem estar

Recomendação



Árvore de decisão do SSVC



Análise de risco

Vulnerabilidade +



Ameaça



Impacto



- Propriedades da vulnerabilidade

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

- Propriedades da empresa
- Propriedades do analista

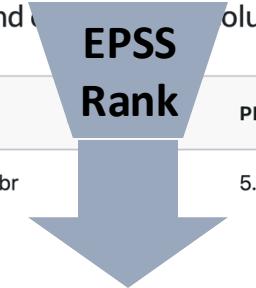
Vibe Check

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 click on the column to check details.


**EPSS
Rank**

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	PRIORITIZER	VOTE
HTTP/1.1	177.191.201.115	443	São Paulo		Algar Telecom	177-191-201-115.xd-	algarnetsuper.com.br	5.7341	<button>Skip</button>
Server: Apache									
Date: Wed, 26 Jun 2024 02:59:26 GMT									
HTTP/1.1	186.208.72.86	443	Maceió		Veloo Net	186-208-72-	veloo.com.br	0.9755	6.1696
Date: Wed, 26 Jun 2024 05:29:34 GMT									
HTTP/1.1	177.184.11.35	443	Rio De Janeiro		Equinix Brasil	localhost.ativacaorj.alo	alog.com.br	0.9755	5.3687
Date: Wed, 26 Jun 2024 18:44:19 GMT									
HTTP/1.1	201.83.152.102	9443	São Paulo		Claro Nxt	c9539866.virtua.com.b	virtua.com.br	0.9755	7.3774
Date: Wed, 26 Jun 2024 23:04:21 GMT									
HTTP/1.1	189.89.181.190	8140	Salvador	Wind	Its Telecommunicacoes	189-89-181-	itsweb.com.br	0.9754	3.9230
Server: Microsoft-IIS/7.5									
Date: Wed, 26 Jun 2024 11:46:39 GMT									



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 the column to check details.

**EPSS
Rank**

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	PRIO	VOTE	Actions
HTTP/1.1	177.191.201.115	443	São Paulo		Algar Telecom	177-191-201-115.xd-dynamic.algarnetsuper.com.br	Provedor núvem	0.9757	5.7341	<button>Skip</button> <button>▼</button>
HTTP/1.1	186.208.72.86	443	Maceió		Veloo Net	186-208-72-86.veloo.com.br	Provedor residencial	0.9755	6.1696	<button>Skip</button> <button>▼</button>
HTTP/1.1	177.184.11.35	443	Rio De Janeiro		Equinix Brasil	localhost.ativacaorj.ag.com.br	Provedor núvem	0.9755	5.3687	<button>Skip</button> <button>▼</button>
HTTP/1.1	201.83.152.102	9443	São Paulo		Claro Nxt	c9539866.virtua.com.br	Provedor residencial	0.9755	7.3774	<button>Skip</button> <button>▼</button>
HTTP/1.1	189.89.181.190	8140	Salvador	Wind	Its Telecommunicacoes	189-89-181-190.STATIC.itsweb.co.br	Provedor núvem	0.9754	3.9230	<button>Skip</button> <button>◀▶</button>

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 the column to check details.

**EPSS
Rank**

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	PRIO	VOTE	
HTTP/1.1	177.191.201.115	443	São Paulo		Algar Telecom	177-191-201-115.xd-dynamic.algarnetsuper.com.br	Provedor nûvem	0.9757	5.7341	<button>Skip</button> ▾
Server: Apache										
Date: Wed, 26 Jun 2024 02:59:26 GMT										
HTTP/1.1	186.208.72.86	443	Maceió		Veloo Net	186-208-72-86.veloo.com.br	Provedor residencial	0.9755	6.1696	<button>Skip</button> ▾
Date: Wed, 26 Jun 2024 05:29:34 GMT										
HTTP/1.1	177.184.11.35	443	Rio De Janeiro		Equinix Brasil	localhost.ativacaorj.ag.com.br	Provedor nûvem	0.9755	5.3687	<button>Skip</button> ▾
Date: Wed, 26 Jun 2024 18:44:19 GMT										
HTTP/1.1	201.83.152.102	9443	São Paulo		Claro Nxt	c9539866.virtua.com.br	Provedor residencial	0.9755	7.3774	<button>Skip</button> ▾
Date: Wed, 26 Jun 2024 23:04:21 GMT					Telecomunicacoes					
HTTP/1.1	189.89.181.190	8140	Salvador	Wind	Its Telecommunicacoes	189-89-181-190.STATIC.itsweb.co.br	Provedor nûvem	0.9754	3.9230	<button>Skip</button> ▾
Server: Microsoft-IIS/7.5				ows						
Date: Wed, 26 Jun 2024 11:46:39 GMT										

**Unusual
ports**


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 the green arrow to check details.

Prio

VOTE

[Skip](#) ▾

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	E... ↓	VOTE
HTTP/1.1	177.191.201.115	443	São Paulo		Algar Telecom	177-191-201-115.xd- dynamic.algarnetsuper. com.br	algarnetsuper.com.br	0.9757	Skip ▾
	Server: Apache								
	Date: Wed, 26 Jun 2024 02:59:26 GMT								
HTTP/1.1	186.208.72.86	443	Maceió		Veloo Net	186-208-72- 86.veloo.com.br	veloo.com.br	0.9755	6.1696
	Date: Wed, 26 Jun 2024 05:29:34 GMT								Skip ▾
HTTP/1.1	177.184.11.35	443	Rio De Janeiro		Equinix Brasil	localhost.ativacaorj.alo g.com.br	alog.com.br	0.9755	5.3687
	Date: Wed, 26 Jun 2024 18:44:19 GMT								Skip ▾
HTTP/1.1	201.83.152.102	9443	São Paulo		Claro Nxt	c9539866.virtua.com.b r	virtua.com.br	0.9755	7.3774
	Date: Wed, 26 Jun 2024 23:04:21 GMT				Telecomunicacoes				Skip ▾
HTTP/1.1	189.89.181.190	8140	Salvador	Wind	Its Telecommunicacoes	189-89-181- ows	itsweb.com.br	0.9754	3.9230
	Server: Microsoft-IIS/7.5					190.STATIC.itsweb.com .br			Skip ▾
	Date: Wed, 26 Jun 2024 11:46:39 GMT								

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 the green button to check details.

Prio

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	EPSS	VOTE
HTTP/1.1	201.49.165.149	443	Cuiabá		Centro De Proc De Dados Do Estado De Mato Grosso	www.sac.mti.mt.gov.br,s ac.mti.mt.gov.br	gov.br	0.9747	8.4260
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2 OpenSSL/3.0.2		Date: Wed, 26 Jun 2024 23:20:32 GMT						9 ▾
HTTP/1.1	187.191.100.136	443	São Paulo		Claranet Technology	unisuam.edu.br	gov.br	0.9747	8.2722
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2 OpenSSL/3.0.2		Date: Wed, 26 Jun 2024 10:54:49 GMT						Skip ▾
HTTP/1.1	191.252.194.129	443	São Paulo		Locaweb Servicos De Internet	vps16051.publiccloud.c om.br,fertipraxis.com.b r,www.fertipraxis.com.br	publiccloud.com.br,ferti praxis.com.br	0.9747	8.1484
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2 OpenSSL/3.0.2		Date: Wed, 26 Jun 2024 07:50:51 GMT						Skip ▾
HTTP/1.1	200.130.18.51	443	Brasília		Rede Nacional De Ensino E Pesquisa	capes.gov.br,sdiold.cap es.gov.br	gov.br	0.9735	7.5451
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2 OpenSSL/3.0.2		Date: Wed, 26 Jun 2024 19:48:46 GMT						Skip ▾
HTTP/1.1	150.162.2.10	443	Florianópolis		Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br	gov.br	0.9556	7.5354
	Server: nginx		Date: Wed, 26 Jun 2024 19:23:36 GMT						◀ ▶

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 them to check details.

Prio

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	EPSS	VOTE
HTTP/1.1	201.49.165.149	443	Cuiabá		Centro De Proc De Dados Do Estado De Mato Grosso	www.sac.mti.mt.gov.br,s ac.mti.mt.gov.br	gov.br	0.9747	8.4260
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2 OpenSSL/3.0.2								9
	Date: Wed, 26 Jun 2024 23:20:32 GMT								
HTTP/1.1	187.191.100.136	443	São Paulo		Claranet Technology	unisuam.edu.br	gov.br	0.9747	8.2722
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2 OpenSSL/3.0.2								Skip
	Date: Wed, 26 Jun 2024 10:54:49 GMT								
HTTP/1.1	191.252.194.129	443	São Paulo		Locaweb Servicos Internet	Laboratório clínico		0.9747	8.1484
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2 OpenSSL/3.0.2								Skip
	Date: Wed, 26 Jun 2024 07:50:51 GMT								
HTTP/1.1	200.130.18.51	443	Brasília		Rede Nacional De Ensino E Pesquisa	capes.gov.br,sdiold.cap es.gov.br	gov.br	0.9735	7.5451
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2 OpenSSL/3.0.2								Skip
	Date: Wed, 26 Jun 2024 19:48:46 GMT								
HTTP/1.1	150.162.2.10	443	Florianópolis		Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br	gov.br	0.9556	7.5354
	Server: nginx								Skip
	Date: Wed, 26 Jun 2024 19:23:36 GMT								

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 them to check details.

Prio

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	EPSS	VOTE
HTTP/1.1	201.49.165.149	443	Cuiabá		Centro De Proc De Dados Do Estado De Mato Grosso	www.sac.mti.mt.gov.br,s ac.mti.mt.gov.br		0.9747	8.4260
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2								<button>9</button>
	Date: Wed, 26 Jun 2024 23:20:32 GMT								
HTTP/1.1	187.191.100.136	443	São Paulo		Claranet Technology	unisuam.edu.br		0.9747	8.2722
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2								<button>Skip</button>
	Date: Wed, 26 Jun 2024 10:54:49 GMT								
HTTP/1.1	191.252.194.129	443	São Paulo		Provedor núvem	Laboratório clínico		0.9747	8.1484
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2								<button>Skip</button>
	Date: Wed, 26 Jun 2024 07:50:51 GMT								
HTTP/1.1	200.130.18.51	443	Brasília		Rede Nacional De Ensino E Pesquisa	capes.gov.br,sdiold.cap es.gov.br		0.9735	7.5451
	Server: Apache/2.4.6 (CentOS) OpenSSL/3.0.2								<button>Skip</button>
	Date: Wed, 26 Jun 2024 19:48:46 GMT								
HTTP/1.1	150.162.2.10	443	Florianópolis		Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br		0.9556	7.5354
	Server: nginx								<button>Skip</button>
	Date: Wed, 26 Jun 2024 19:23:36 GMT								

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 them to check details.

Prio

SERVICE	IP	PORT	CITY	OS	ORGANIZATION	HOSTNAMES	DOMAINS	EPSS	VOTE
HTTP/1.1	201.49.165.149	443	Cuiabá		Centro De Proc De Dados Do Estado De Mato Grosso	www.sac.mti.mt.gov.br,s ac.mti.mt.gov.br		0.9747	8.4260
HTTP/1.1	187.191.100.136	443	São Paulo		Claranet Technology	unisuam.edu.br		0.9747	8.2722
HTTP/1.1	191.252.194.129	443	São Paulo		Provedor núvem	Laboratório clínico		0.9747	8.1484
HTTP/1.1	200.130.18.51	443	Brasília		Rede Nacional De Ensino E Pesquisa	capes.gov.br,sdiold.cap es.gov.br		0.9735	7.5451
HTTP/1.1	150.162.2.10	443	Florianópolis		Universidade Federal De Santa Catarina	ufsc.br,paginas.ufsc.br		0.9556	7.5354

Port
443



Identificação de vulnerabilidades relacionadas

**Varredura por ShellShock utilizando
vetores de ataque distintos**

Identificação de vulnerabilidades relacionadas

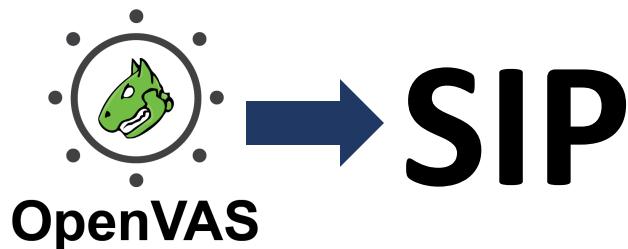
**Varredura por ShellShock utilizando
vetores de ataque distintos**



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**



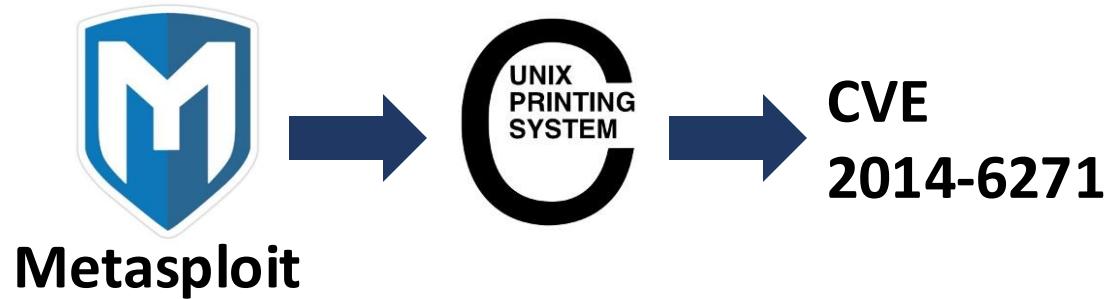
Identificação de vulnerabilidades relacionadas

**Varredura por ShellShock utilizando
vetores de ataque distintos**



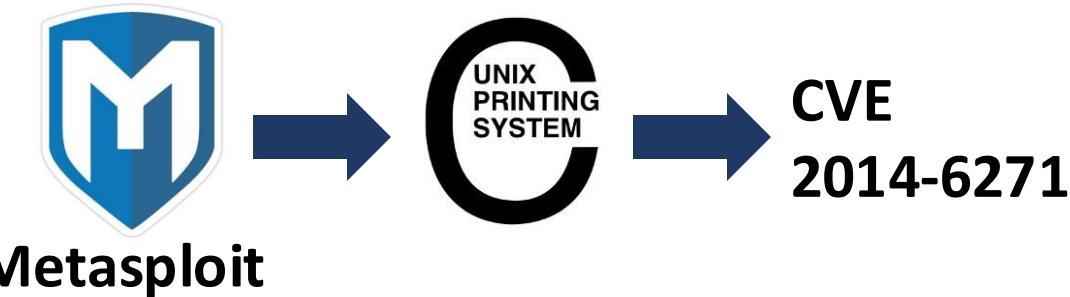
Identificação de vulnerabilidades relacionadas

**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



Varredura por versão 1 do protocolo SSH



Metasploit

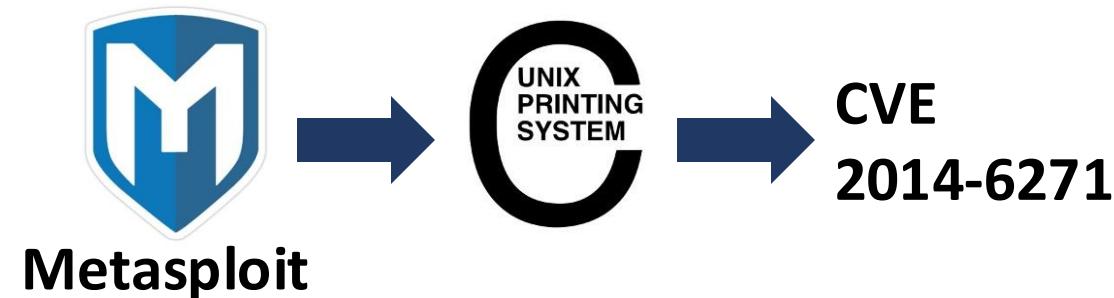
Identificar o mesmo CVE não implica que scripts são equivalentes

Identificação de vulnerabilidades relacionadas

Varredura por ShellShock utilizando vetores de ataque distintos



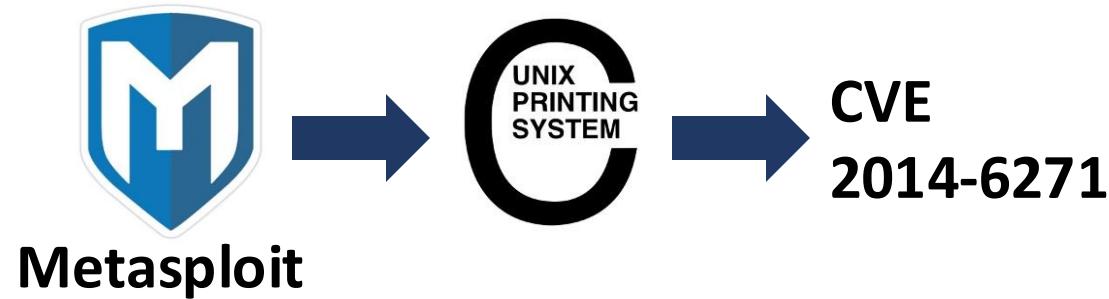
Varredura por versão 1 do protocolo SSH



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



Search...



5



All Problems



Redução de 1000 vulnerabilidades para 39 grupos

Page Size ▾

Column visibility

Copy

PDF

Print

Search:

Name	Severity	SLA	Findings Count	Total Script IDs
SSL/TLS: Report Weak Cipher Suites_	Medium	90	170	1
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection_	Medium	90	133	1
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS_	High	30	133	1
SSL/TLS: Certificate Expired	Medium	90	107	1
Report Default Community Names of the SNMP Agent_	High	30	97	1
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection_	Medium	90	65	1

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

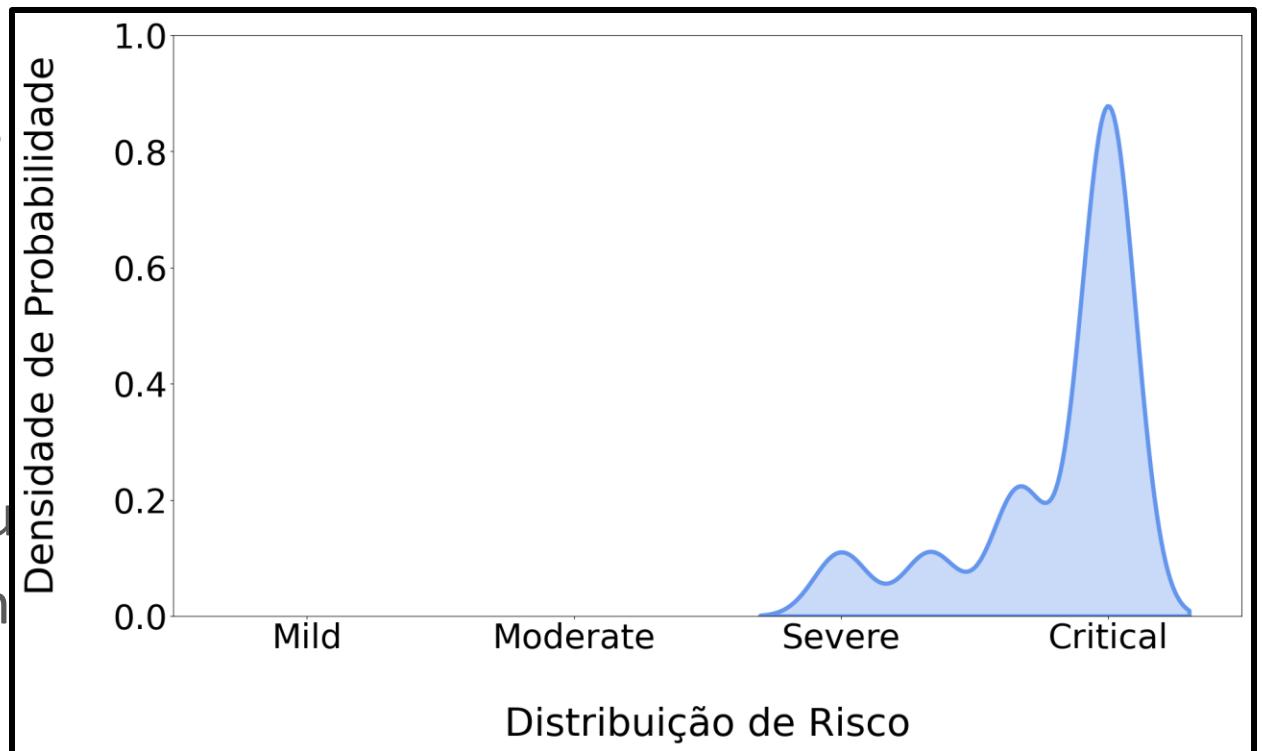
<https://appglassfish.reitoria.uni.edu.br>

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

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

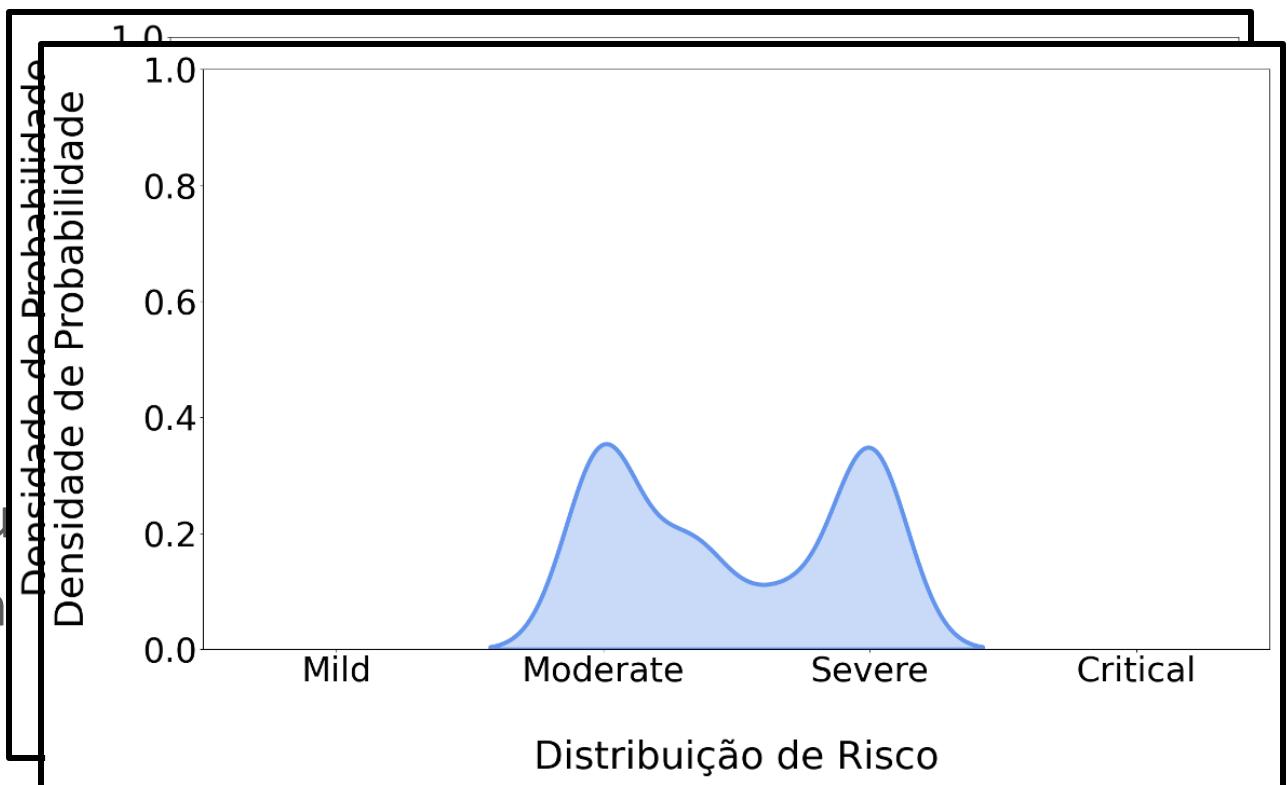
Fatores que impactam a precisão do modelo

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



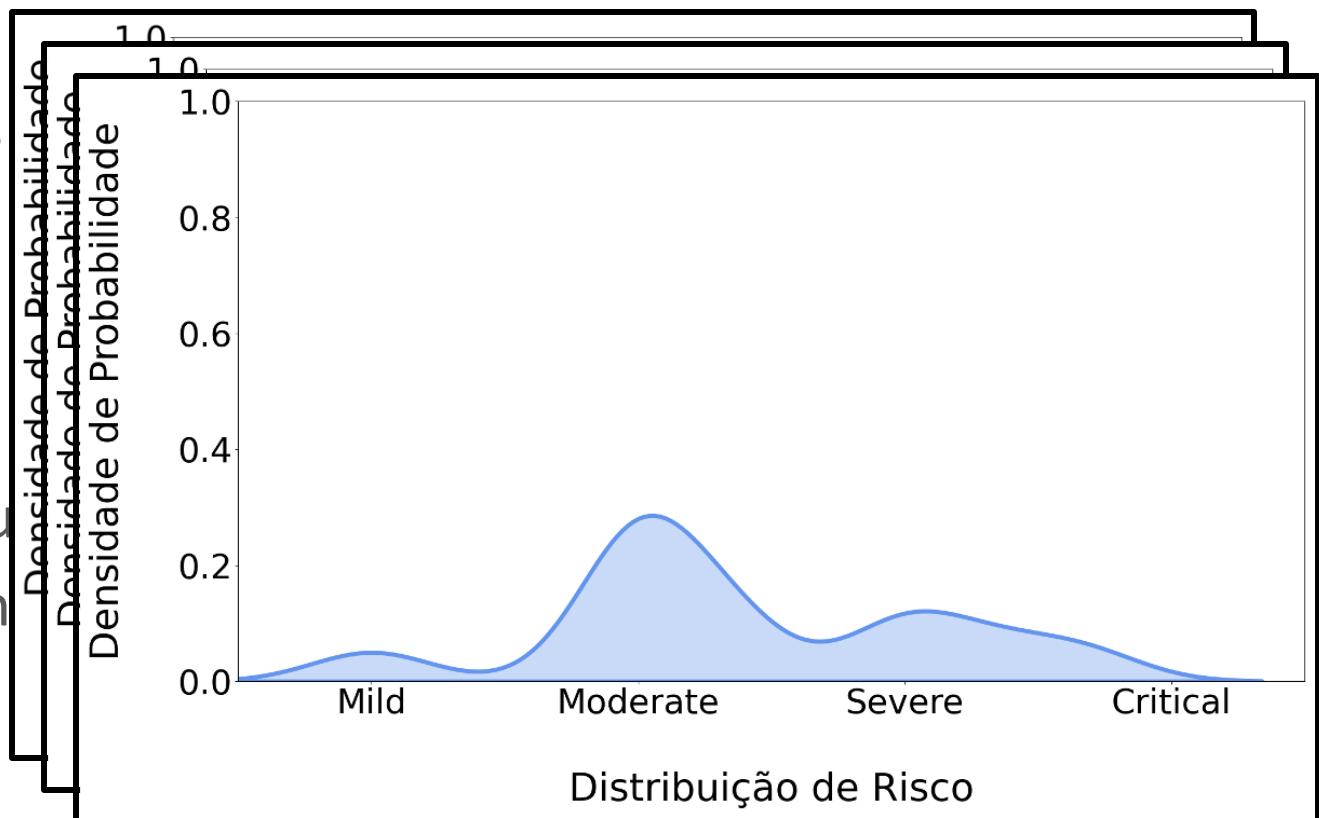
Fatores que impactam a precisão do modelo

- Diversidade das vulnerabilidades
 - Bases de teste balanceadas
- Perfil do analista
 - Grave para um, moderado para outro
 - 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 outro
 - 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*