



Caros(as) autores(as) dos trabalhos aceitos no SBSeg24,

Esta é uma proposta de template/exemplo de slides para o SBSeg 2024! Você pode modificar e editar livremente. Substitua as logos do template pelas da sua(s) instituição(ões). Adeque o conteúdo ao seu trabalho.

O último slide contém apenas as logos dos patrocinadores, para fins de divulgação e valorização. Você pode removê-lo de sua apresentação.

Sugerimos que você verifique atentamente as instruções para uma boa apresentação no link a seguir.

<https://sbseg2024.ita.br/>

Cordialmente,
Organização do SBSeg 2024



Título do seu Trabalho a ser Apresentado na Trilha Principal ou em um dos Eventos Satélites do SBSeg 2024

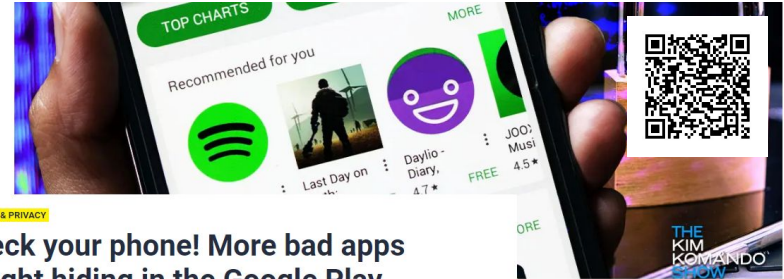


Sugestão: coloque aqui
as logos das instituições
dos co-autores e
agências de fomento ou
outras instituições
financiadoras

Autor1, Autor2, Autor3,
Autor4, Autor5, Autor6, ...

Instituição 1
Instituição 2
Instituição 3

Motivação



SECURITY & PRIVACY

Check your phone! More bad apps caught hiding in the Google Play Store

BY CHARLIE FRIPP; KOMANDO.COM • MARCH 21, 2022 SHARE: [Twitter](#) [Facebook](#) [Pinterest](#)

Crypto malware in patched wallets targeting Android and iOS devices

ESET Research uncovers a sophisticated scheme that distributes trojanized Android and iOS app cryptocurrency wallets



Lukas Stefanko

24 Mar 2022 - 01:30PM



Problema(s)

<i>Dataset</i>	Tempo	# Maliciosos	Threshold	Metadados
MalGenome	2010 - 2012	1.264		Não
DREBIN	2013	5.560	2	Não
PiggyBacking	2016	1.136	1	Não
AMD	2010 - 2016	24.533	28	Não

Tamanho e cobertura

Problema(s)

<i>Dataset</i>	Tempo	# Maliciosos	Threshold	Metadados
MalGenome	2010 - 2012	1.264		Não
DREBIN	2013	5.560	2	Não
PiggyBacking	2016	1.136	1	Não
AMD	2010 - 2016	24.533	28	Não

Ausência de metadados

Problema(s)

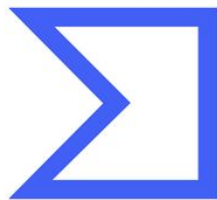
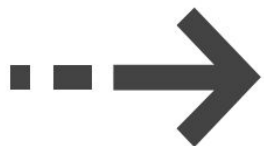
<i>Dataset</i>	Tempo	# Maliciosos	Threshold	Metadados
MalGenome	2010 - 2012	1.264		Não
DREBIN	2013	5.560	2	Não
PiggyBacking	2016	1.136	1	Não
AMD	2010 - 2016	24.533	28	Não

Threshold de detecção

Desafio(s)

SHA256

VT Cache



Relatório

Limitações da rotulação com VirusTotal

Desafio(s)

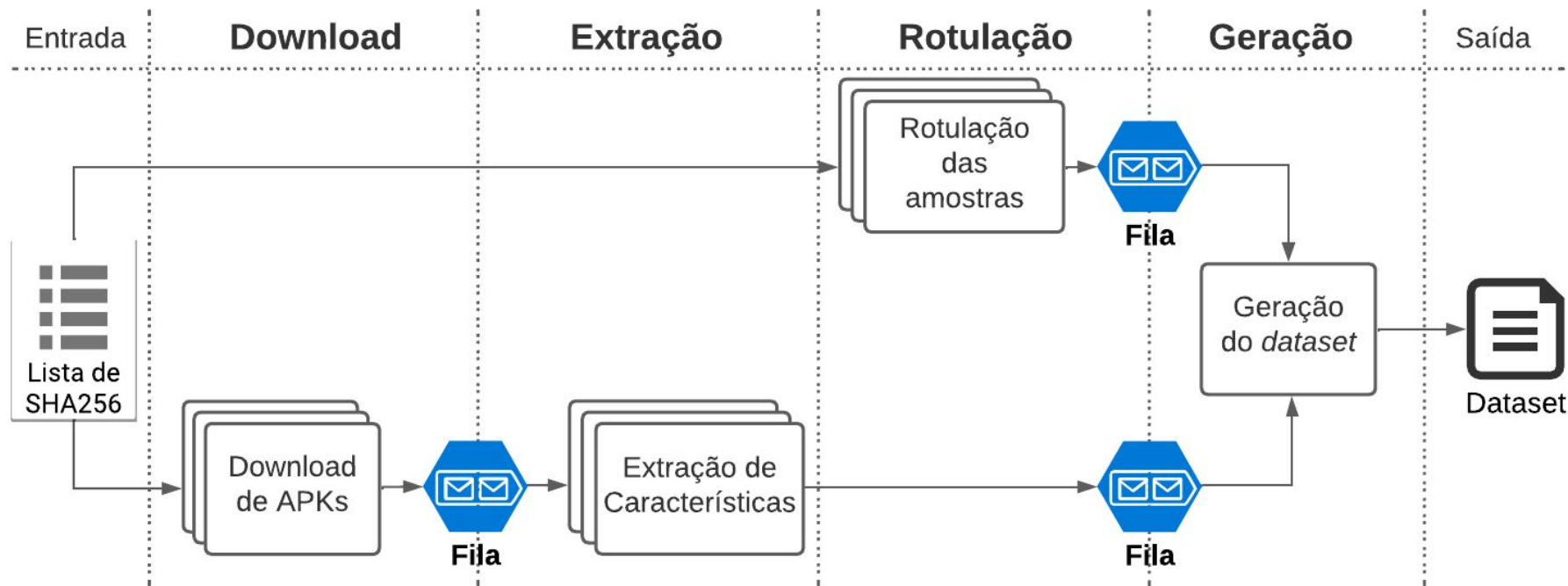
Aplicativo: **Corrida de Fogo de Vento**

E1965D8D028D9824ACC4F39DE02BA2760C0367598B21ABBD303A8416F08598EC

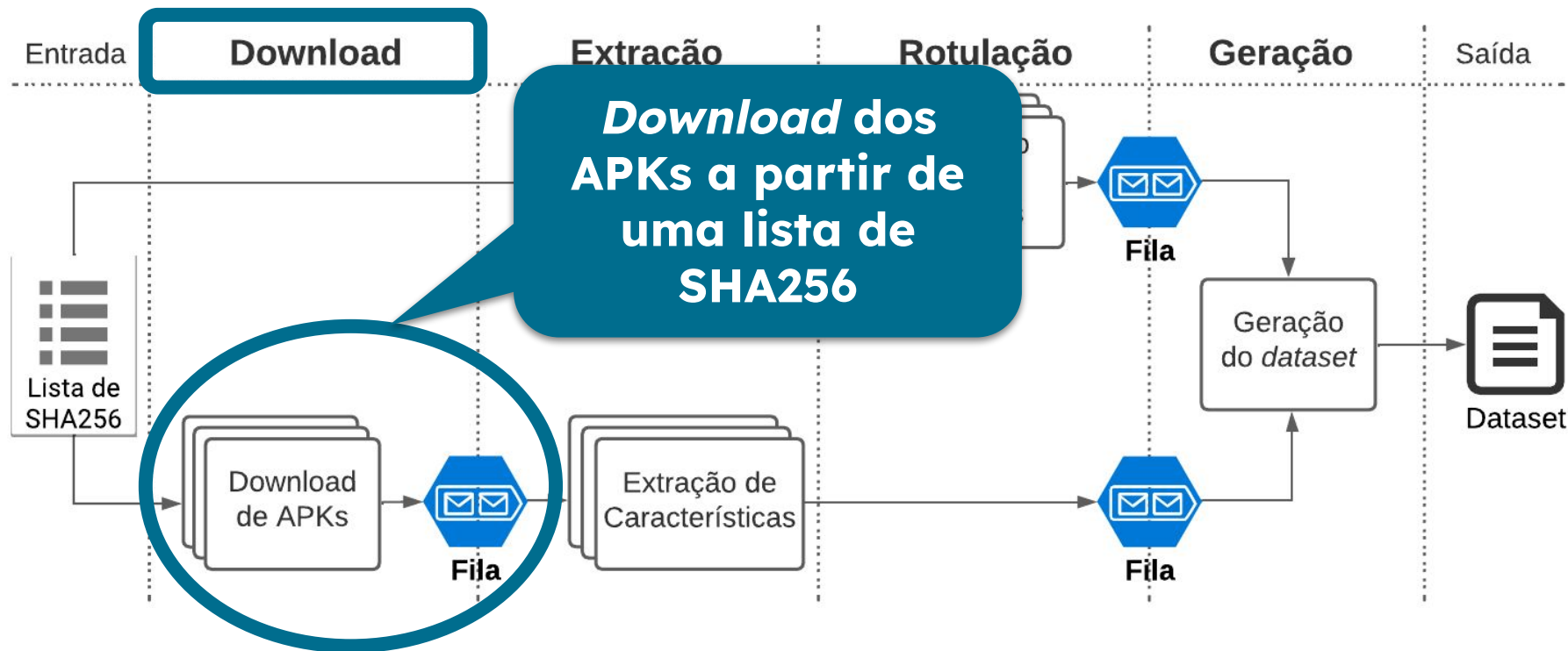
- 27 de Maio de 2014: 1 *Scanner*
- 09 de Junho de 2023: 11 *Scanners*
- 14 de Setembro de 2023: 24 *Scanners*

Dados defasados

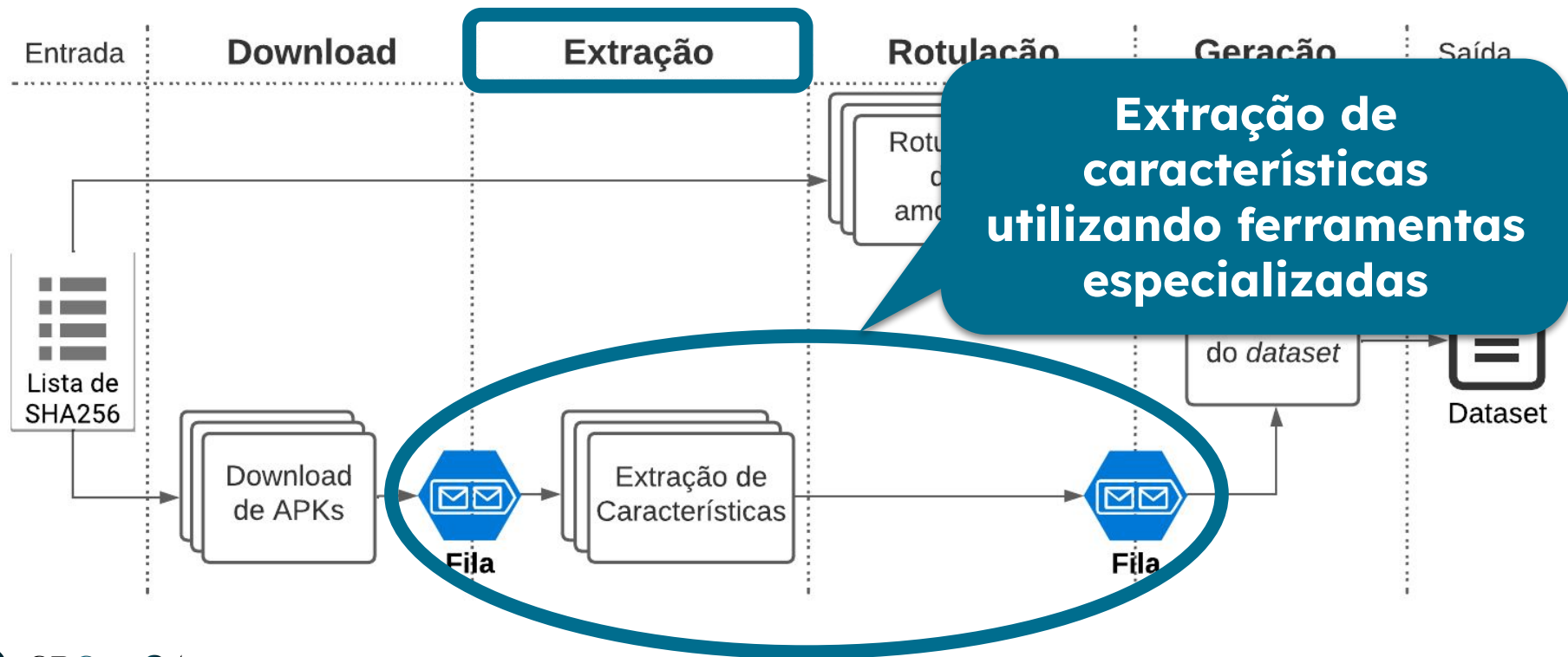
Solução Proposta



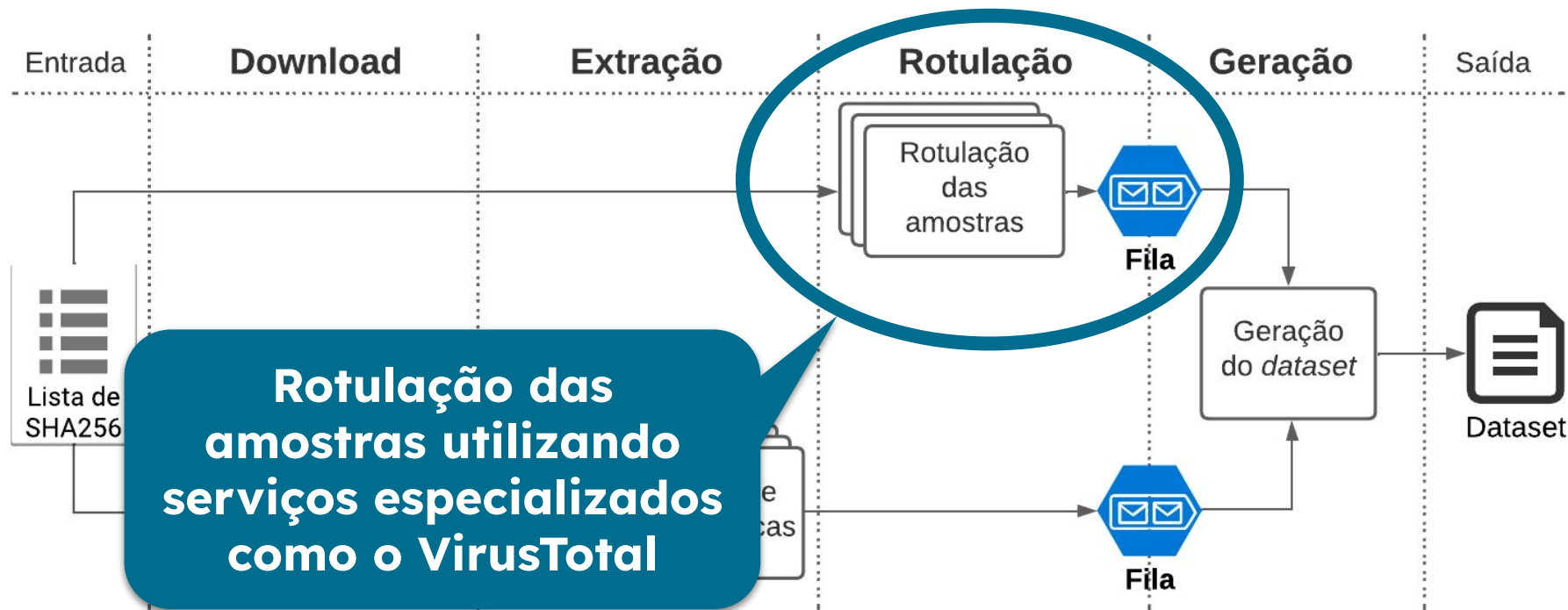
Solução Proposta



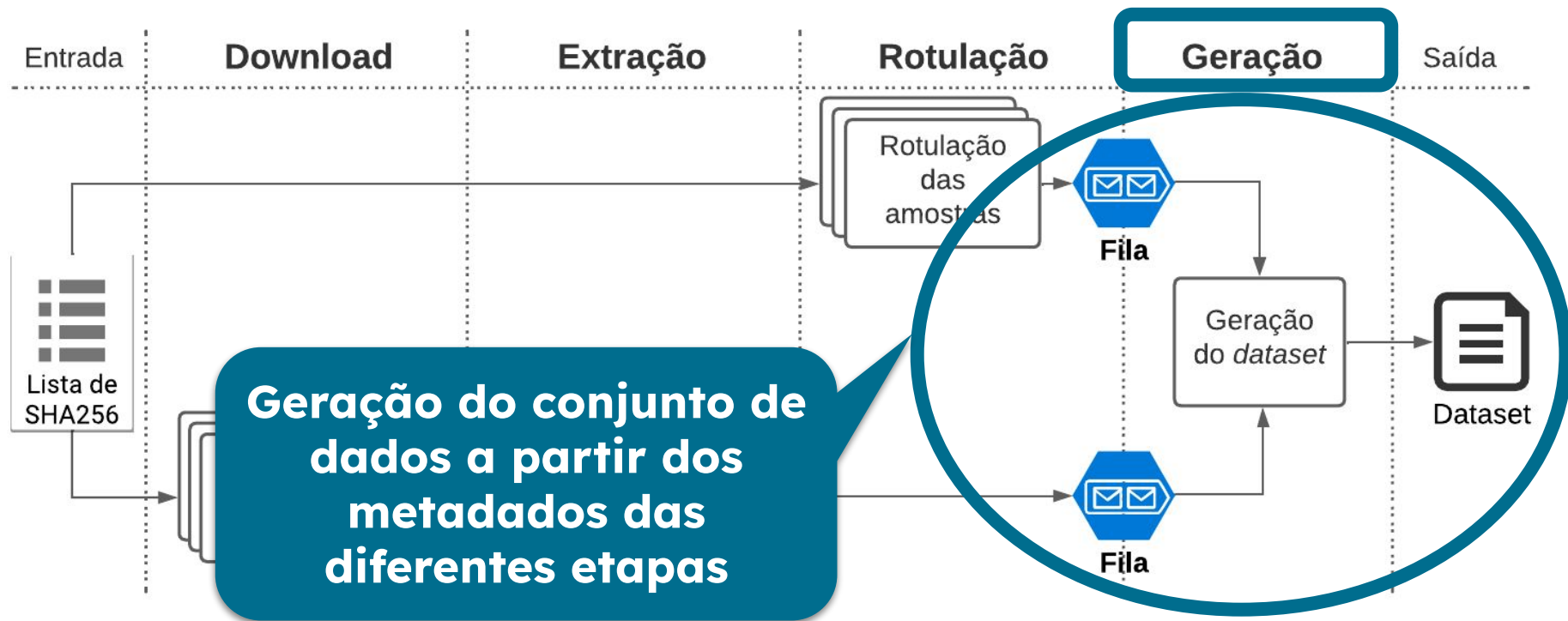
Solução Proposta



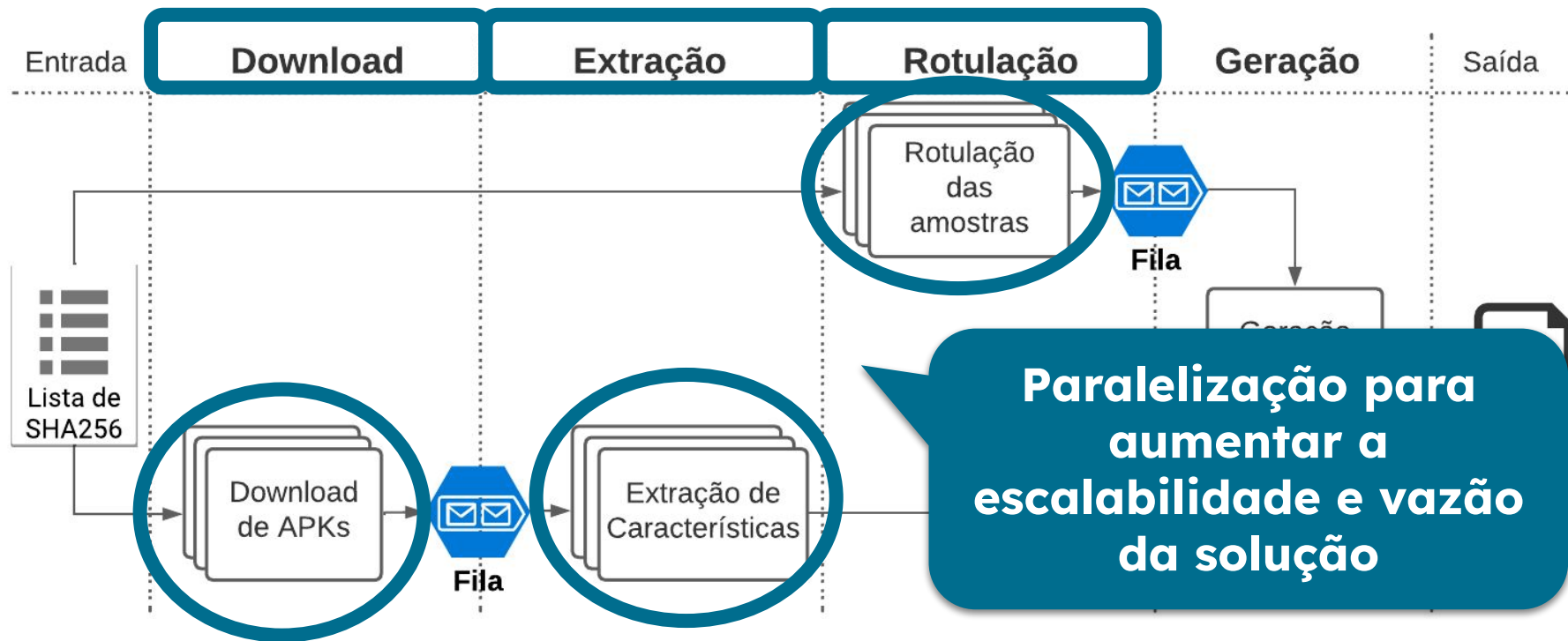
Solução Proposta



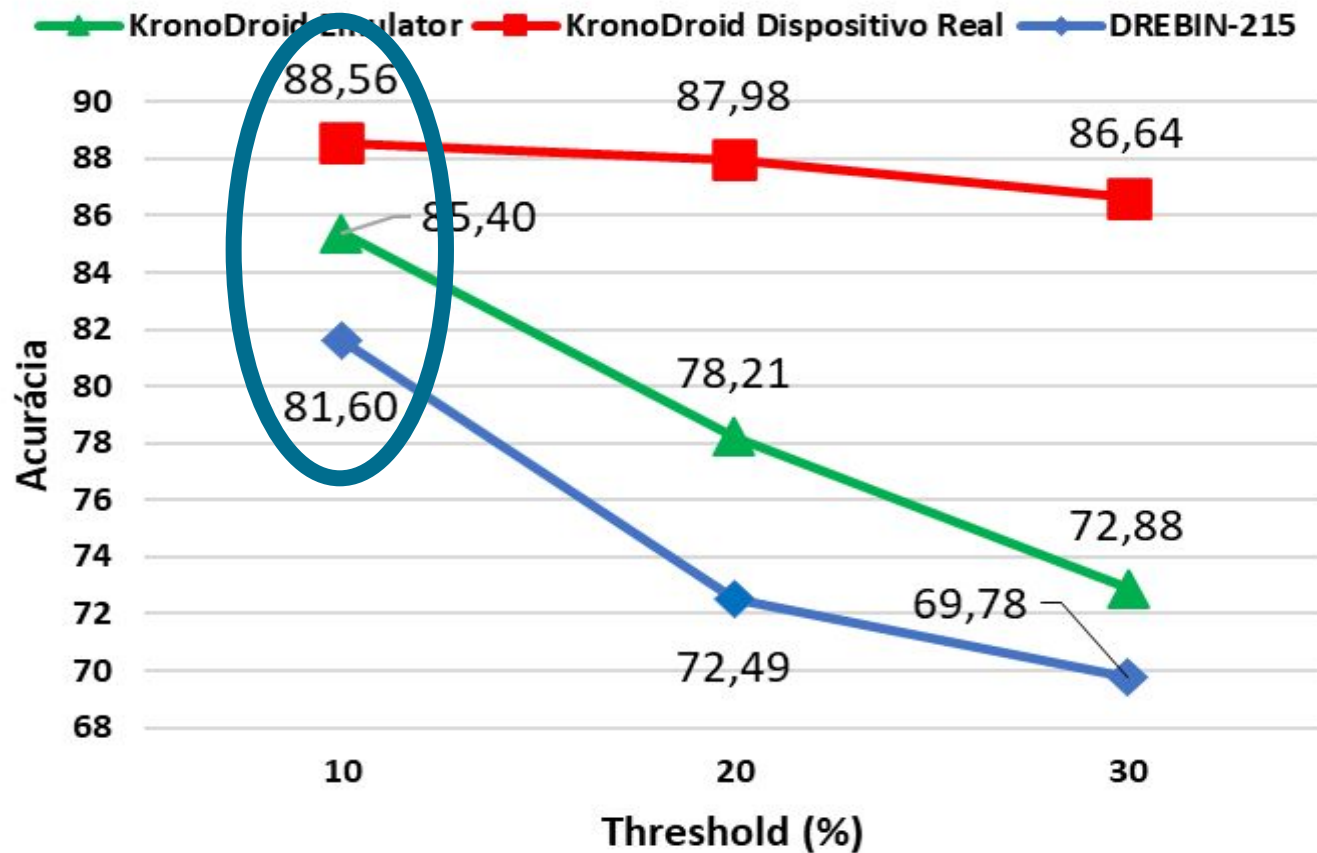
Solução Proposta



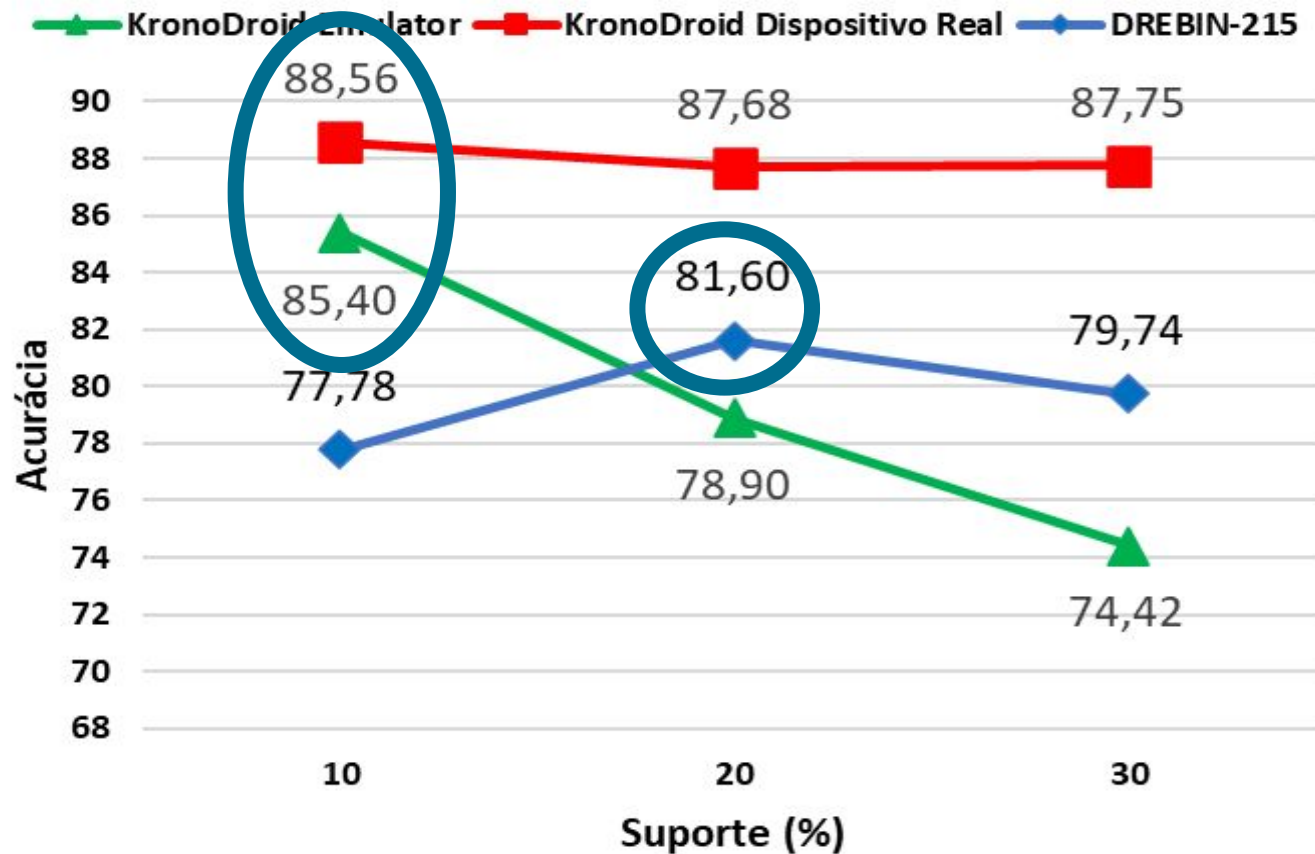
Solução Proposta



Avaliação



Avaliação



Avaliação

<i>Dataset</i>	<i>Recall</i>	<i>MCC</i>	<i>ROC AUC</i>	<i># Car.</i>	<i>% R.</i>
Adroit	69.89	0.72	83.28	18	89.22
Androcrawl	86.51	0.90	93.01	16	88.73
<u>Defensedroid</u>	89.23	0.84	92.11	289	89.96
Drebin-215	91.56	0.88	93.91	23	89.35
KronoDroid	95.93	0.91	95.66	30	89.55

Avaliação



Considerações finais

- Conjuntos de dados atualizados e realistas
- Resultados influenciados dos modelos
 - *Dataset* é determinante
- Outras restrições além dos dados
- Realidade *versus* mundo ideal

Trabalhos futuros

- Estudar mais a fundo as métricas
- Analisar outros modelos
- Criar mais conjuntos de dados atualizados
- Explorar a explicabilidade dos modelos
- Investigar conjuntos de dados contaminados

Obrigado!

- Autor(es)
- Contato(s)



Sugestão:
adicione as
logos das
agências de
fomento,
empresas
financiadoras,
etc.





Patrocinadores do SBSeg 2024!

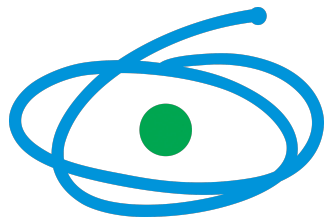
nie.br

egi.br

Google



Tempest



CAPES



SiDi



BugHunt



C . E . S . A . R



FACULDADE
IBPTech