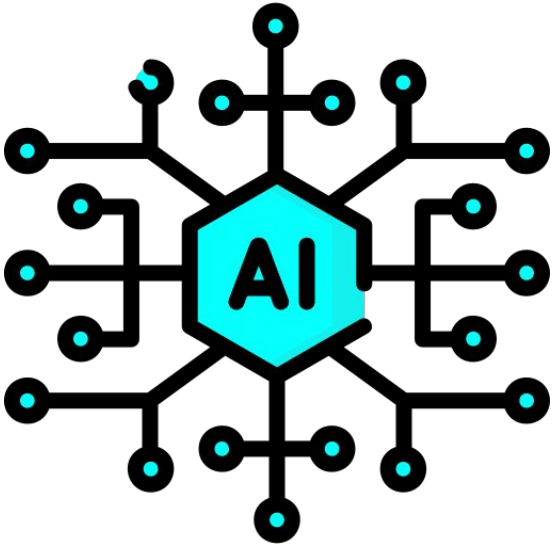
AutoDroid: disponibilizando a ferramenta DroidAugmentor como serviço

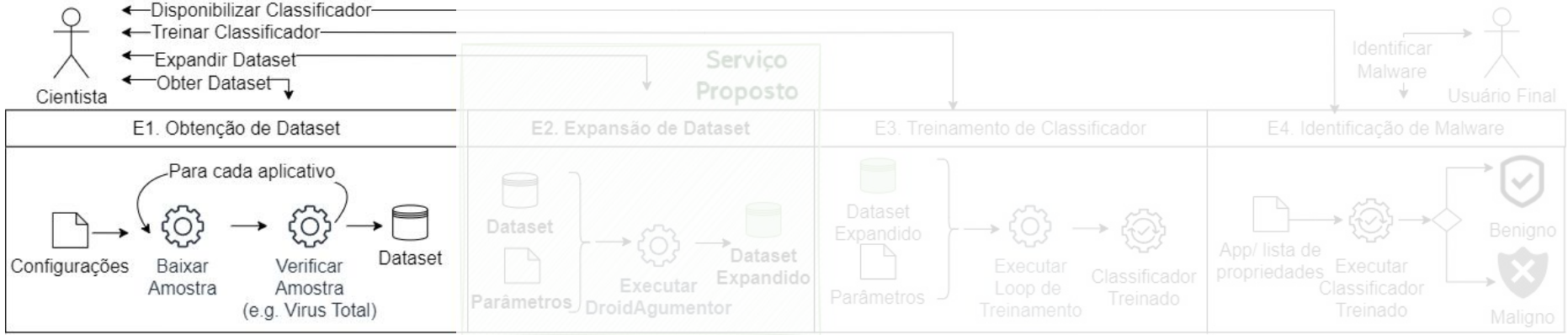
Luiz Felipe Laviola, Kayuã Paim, Diego Kreutz, Rodrigo Mansilha

VII Workshop Regional de Segurança da Informação e de Sistemas Computacionais (WRSeg 2023)


01
10
10
01
10
01

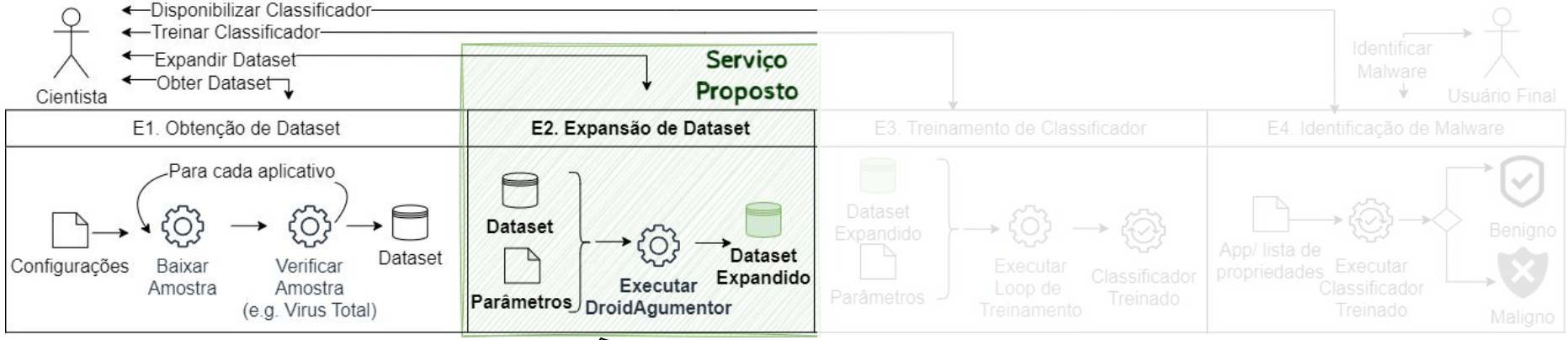

AI

Pipeline de IA para detecção de *malware*



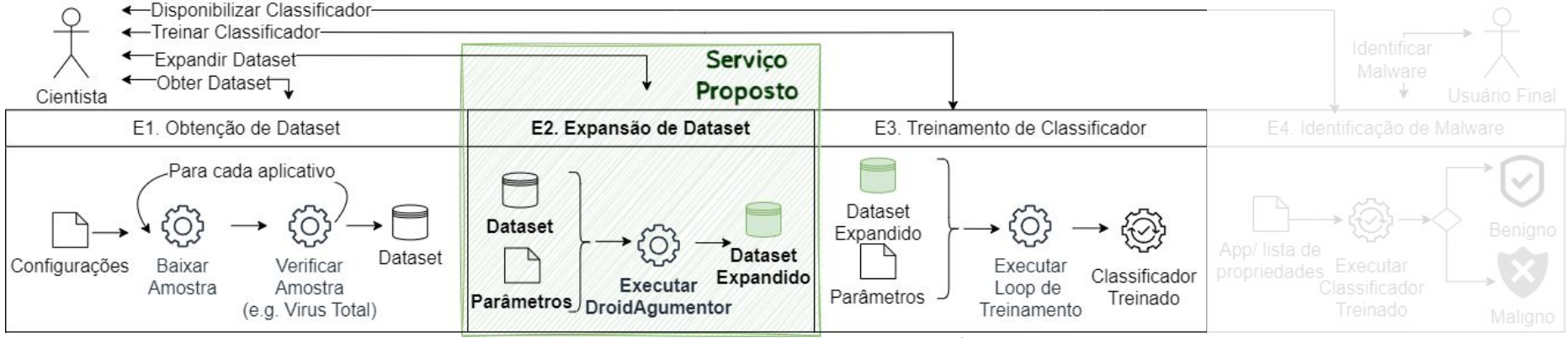
Obtenção de dataset (e.g., ADBuilder, AMGenerator)

Pipeline de IA para detecção de *malware*



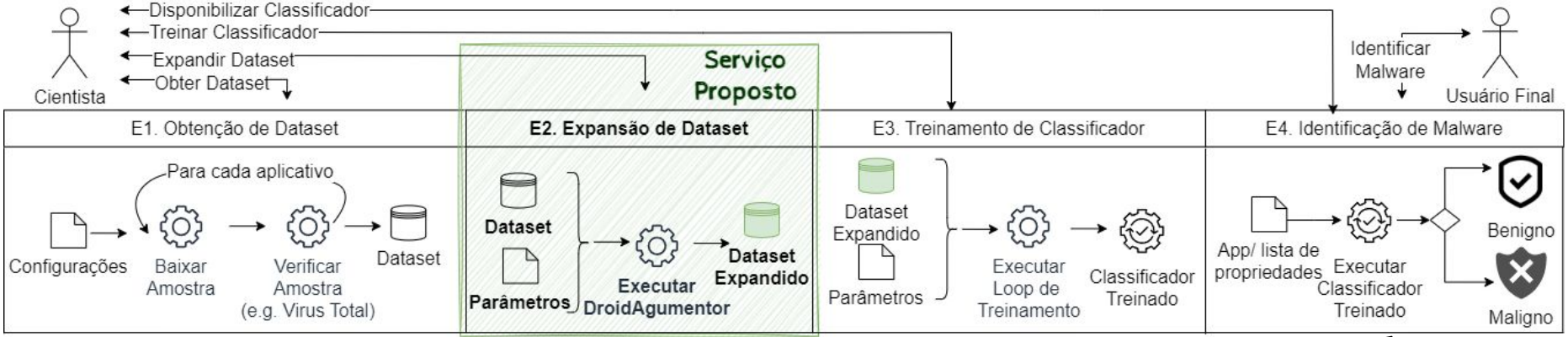
DroidAugmentor

Pipeline de IA para detecção de *malware*



Pipeline convencional de ML, incluindo treinamento dos classificadores

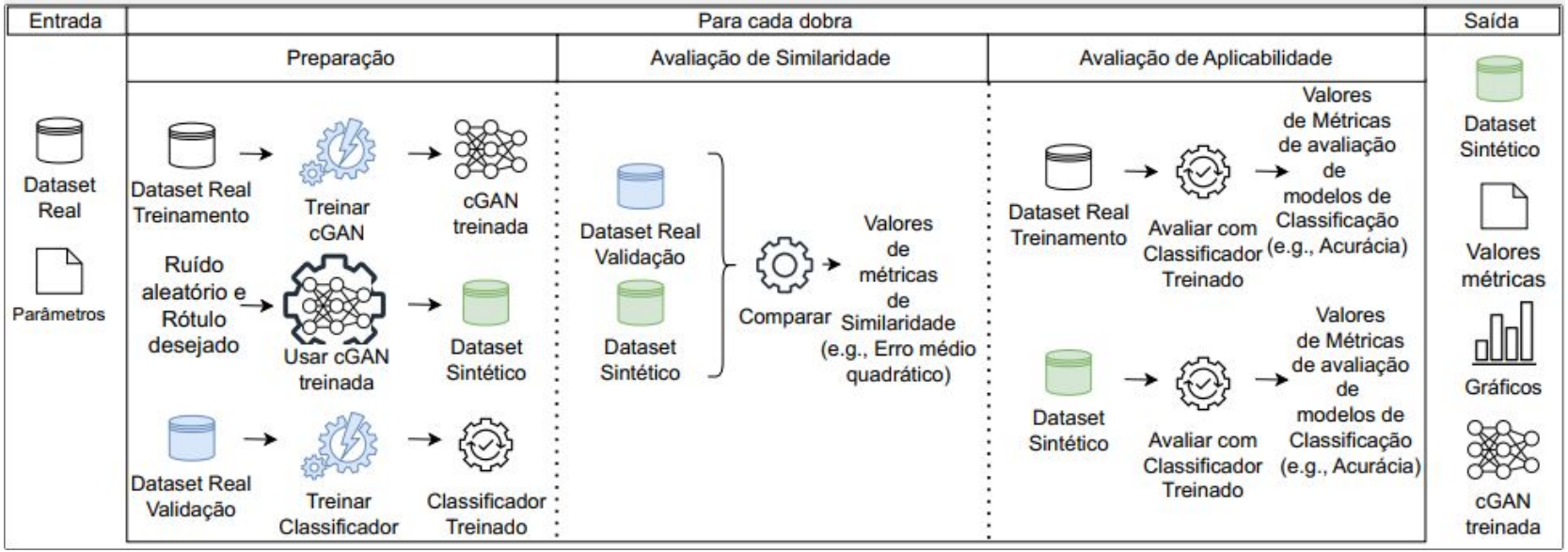
Pipeline de IA para detecção de *malware*



Utilização dos classificadores para detecção de *malwares*

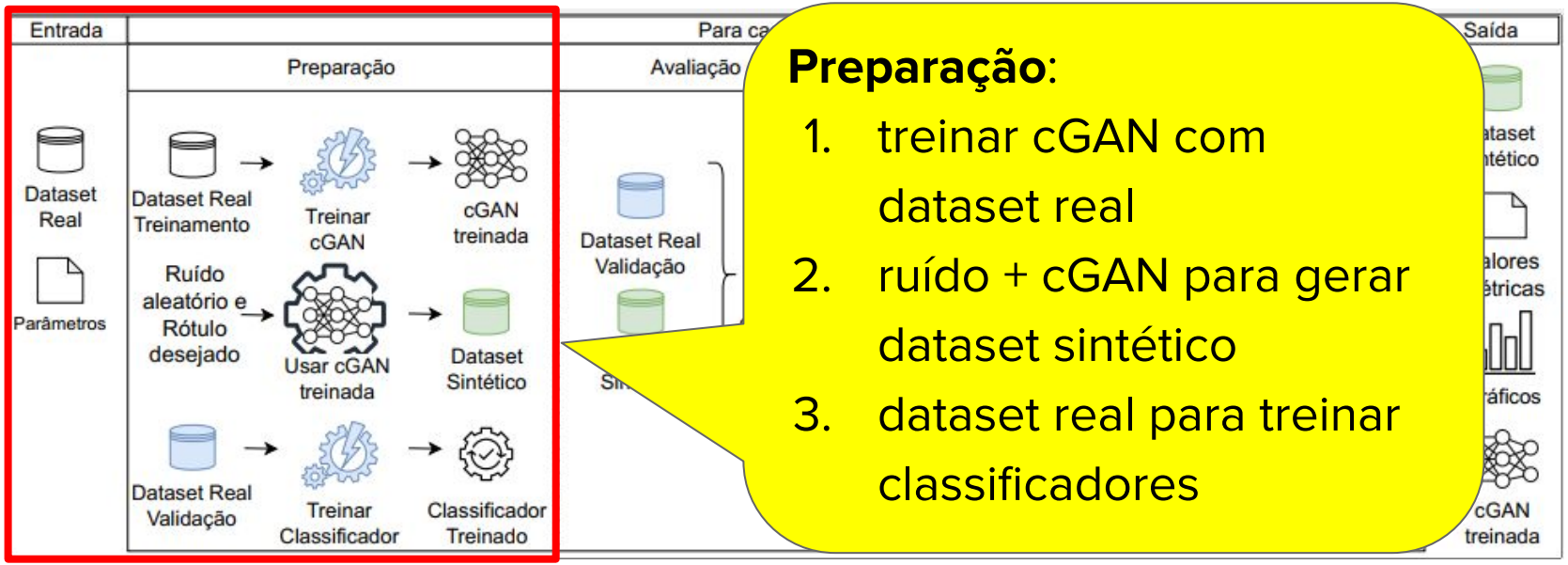
DroidAugmentor

- Ferramenta de código aberto
- Expandir *datasets* de malware



DroidAugmentor

- Ferramenta de código aberto
- Expandir *datasets* de malware

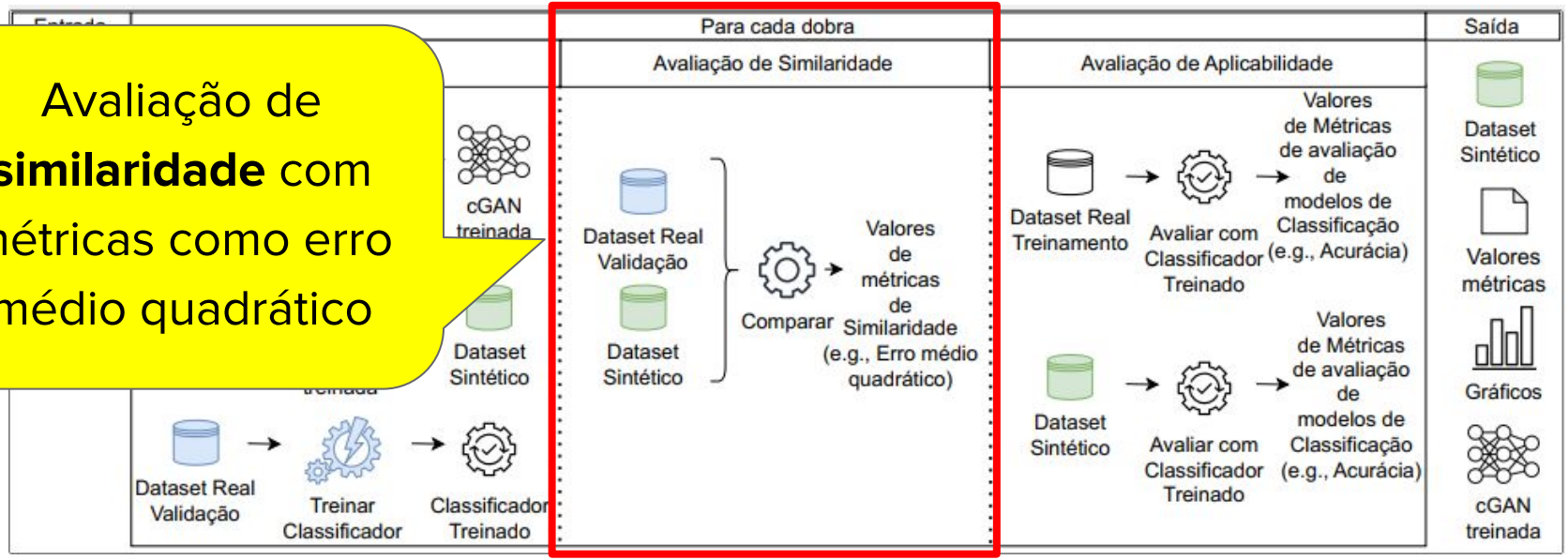


Preparação:

1. treinar cGAN com dataset real
2. ruído + cGAN para gerar dataset sintético
3. dataset real para treinar classificadores

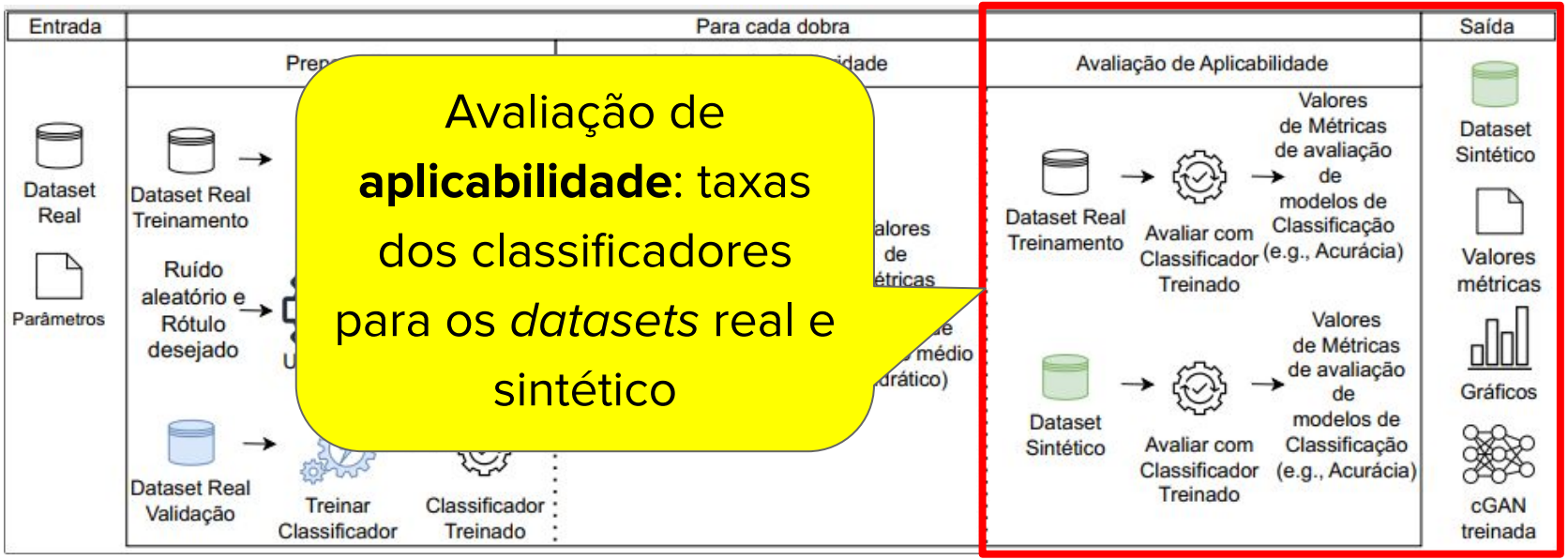
DroidAugmentor

- Ferramenta de código aberto
- Expandir *datasets* de malware



DroidAugmentor

- Ferramenta de código aberto
- Expandir *datasets* de malware



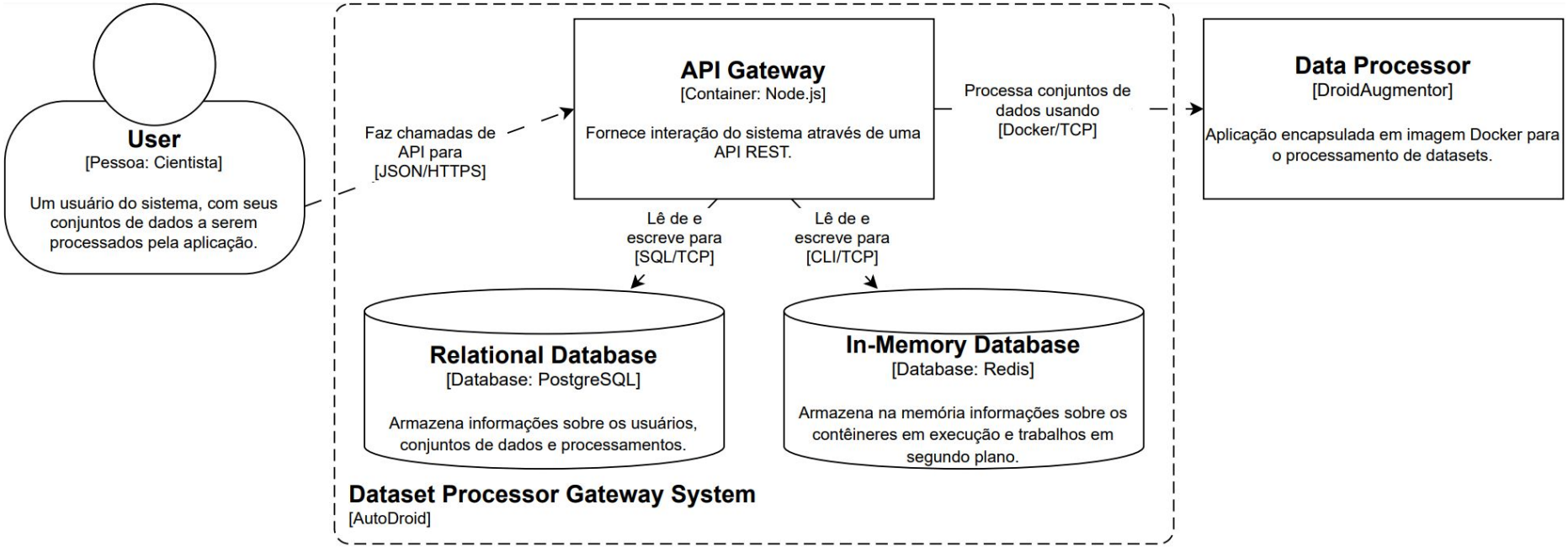
DroidAugmentor

- Requer instalação de múltiplas dependências
- Exige muitos recursos computacionais
- Disponível apenas para o usuário local

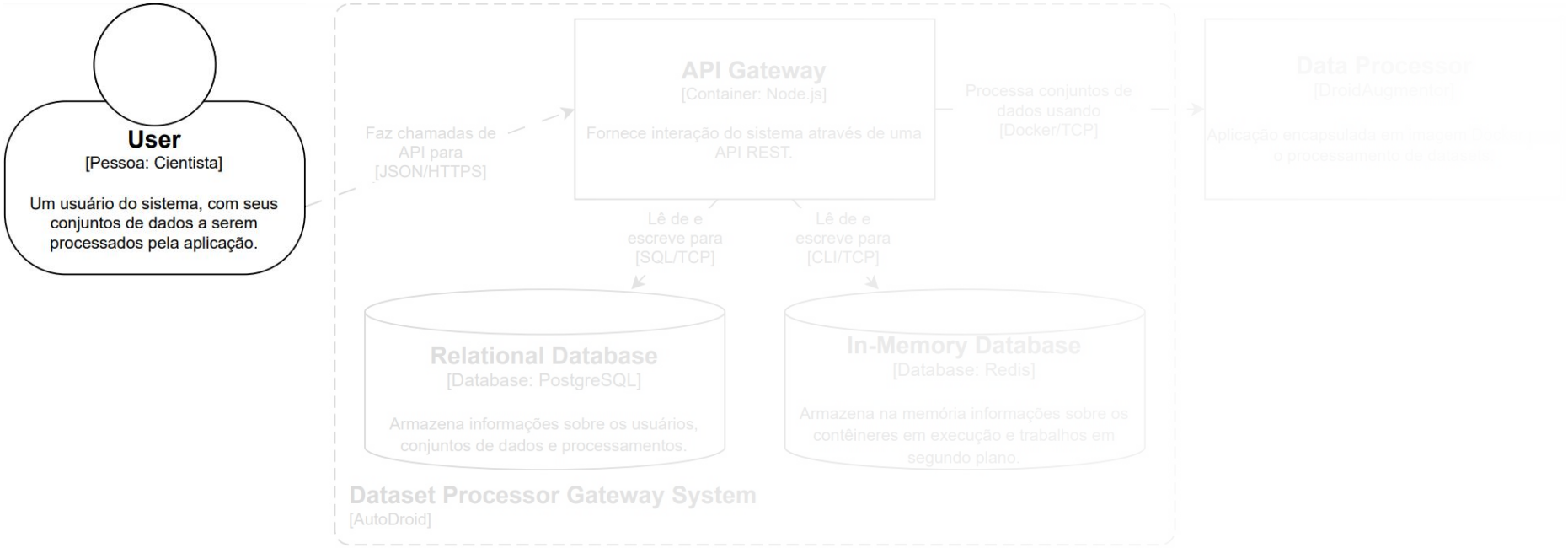
AutoDroid

- Oferece o **DroidAugmentor como serviço**
- Utilização através de API REST
- Software gratuito
- Código *Open Source* (GitHub)
- Desenvolvida em Typescript para Node.js

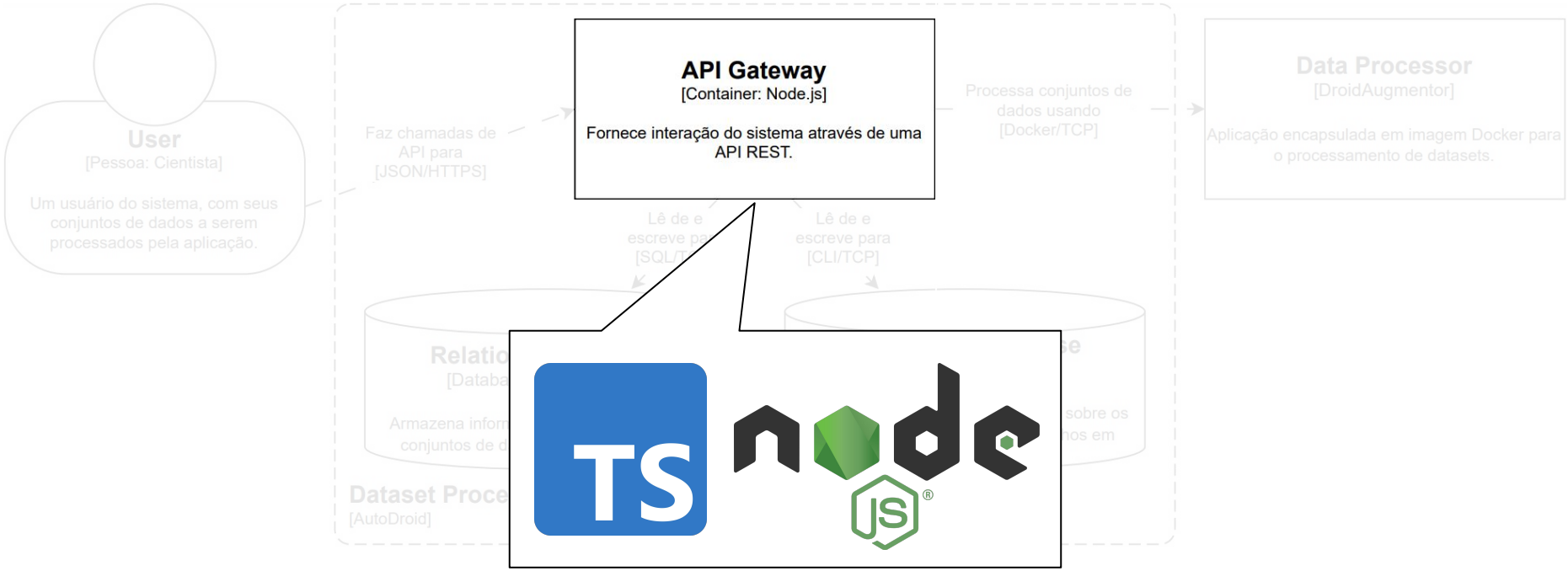
Arquitetura



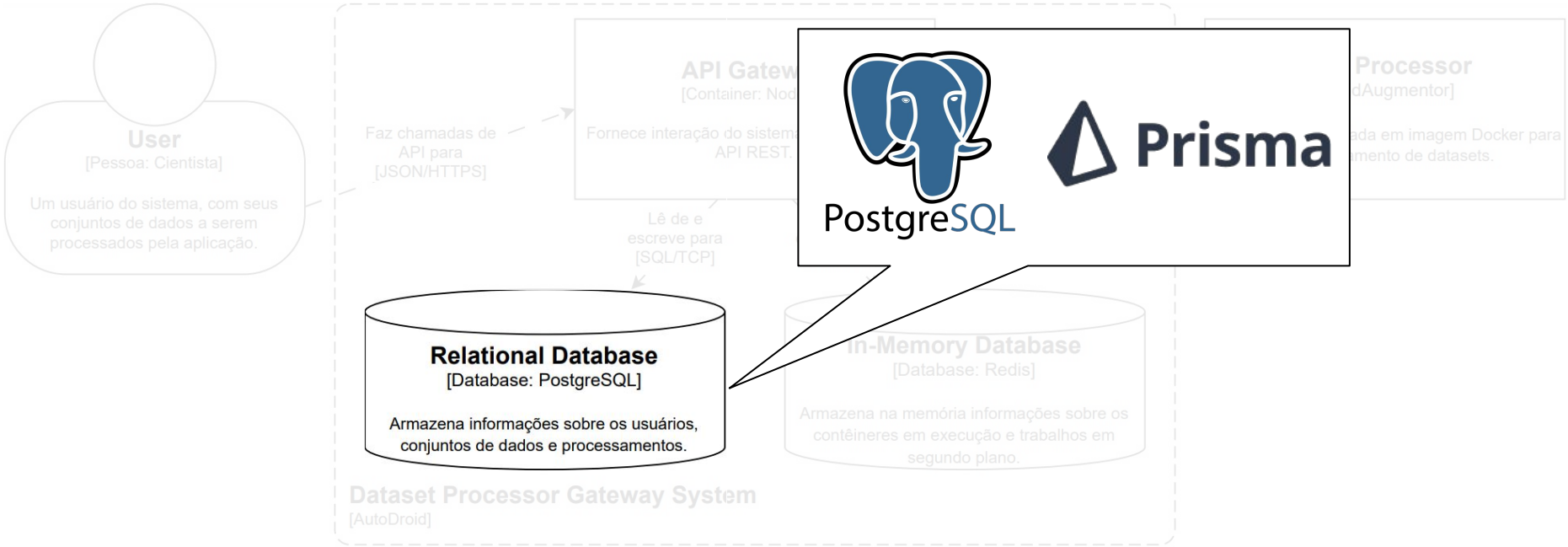
Arquitetura



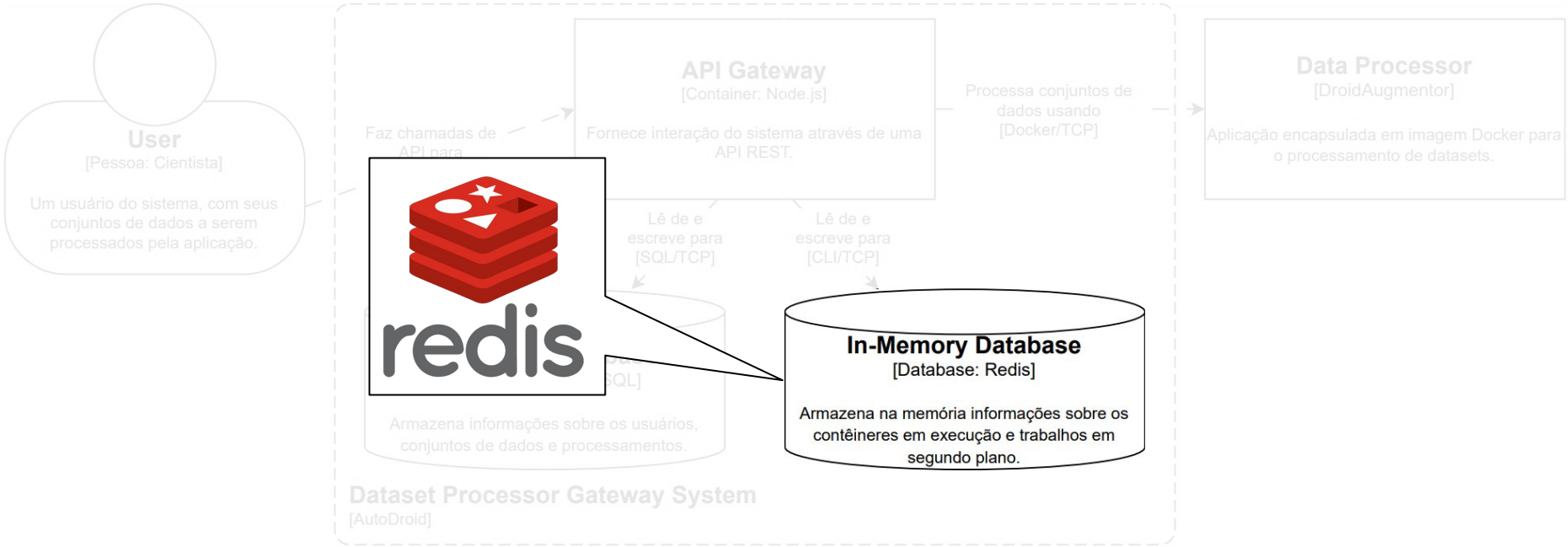
Arquitetura



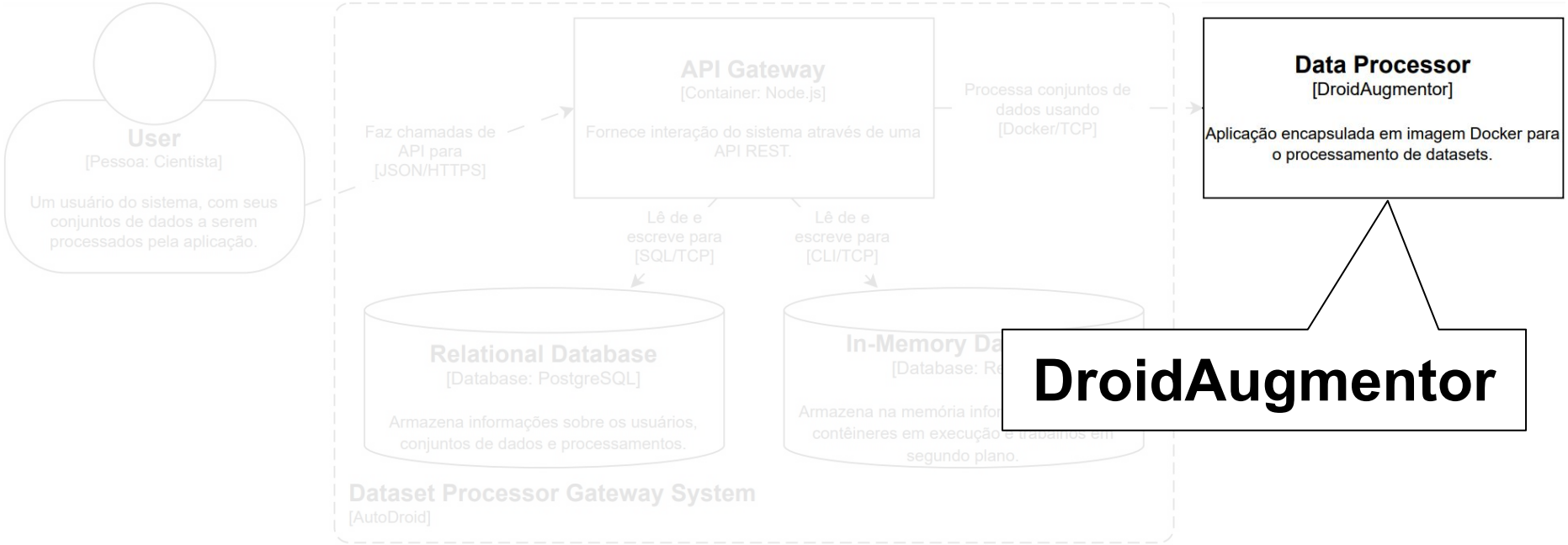
Arquitetura



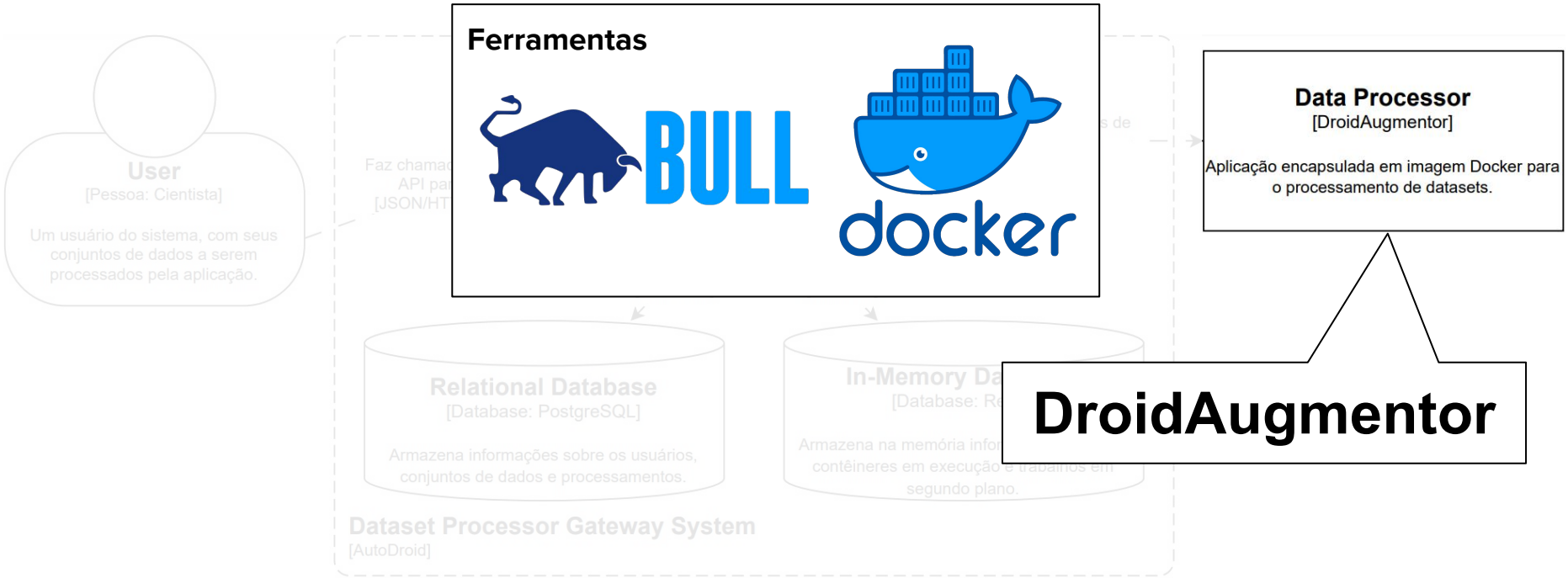
Arquitetura



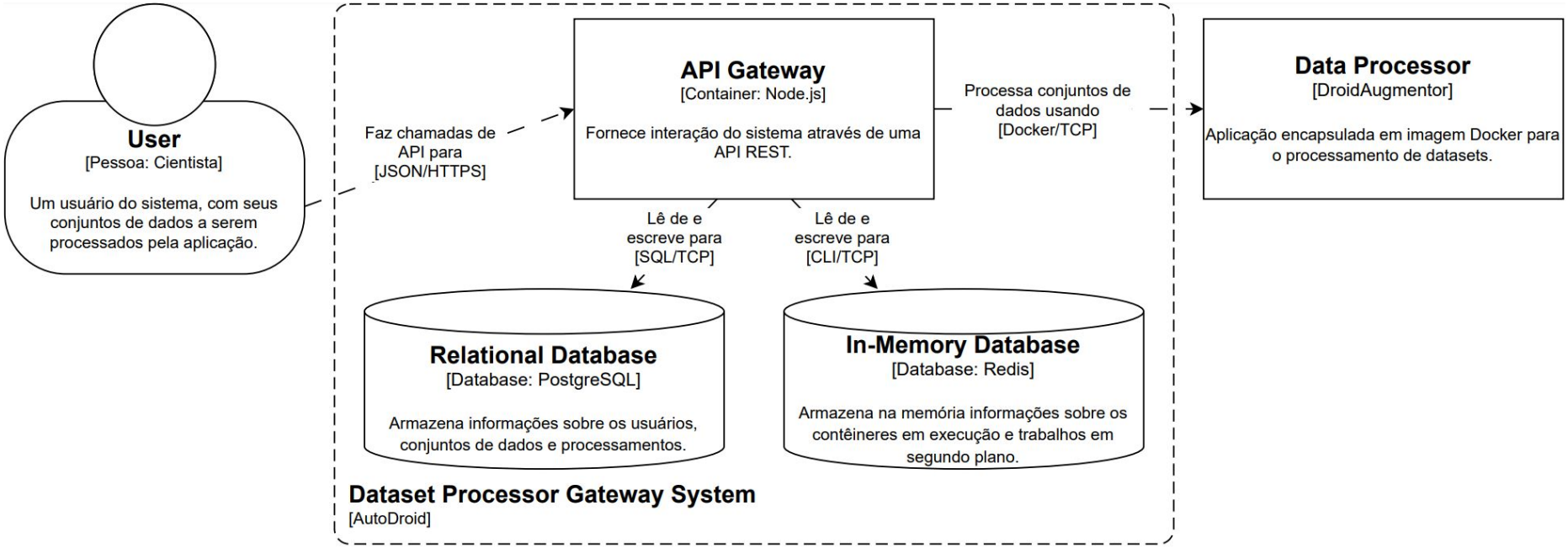
Arquitetura



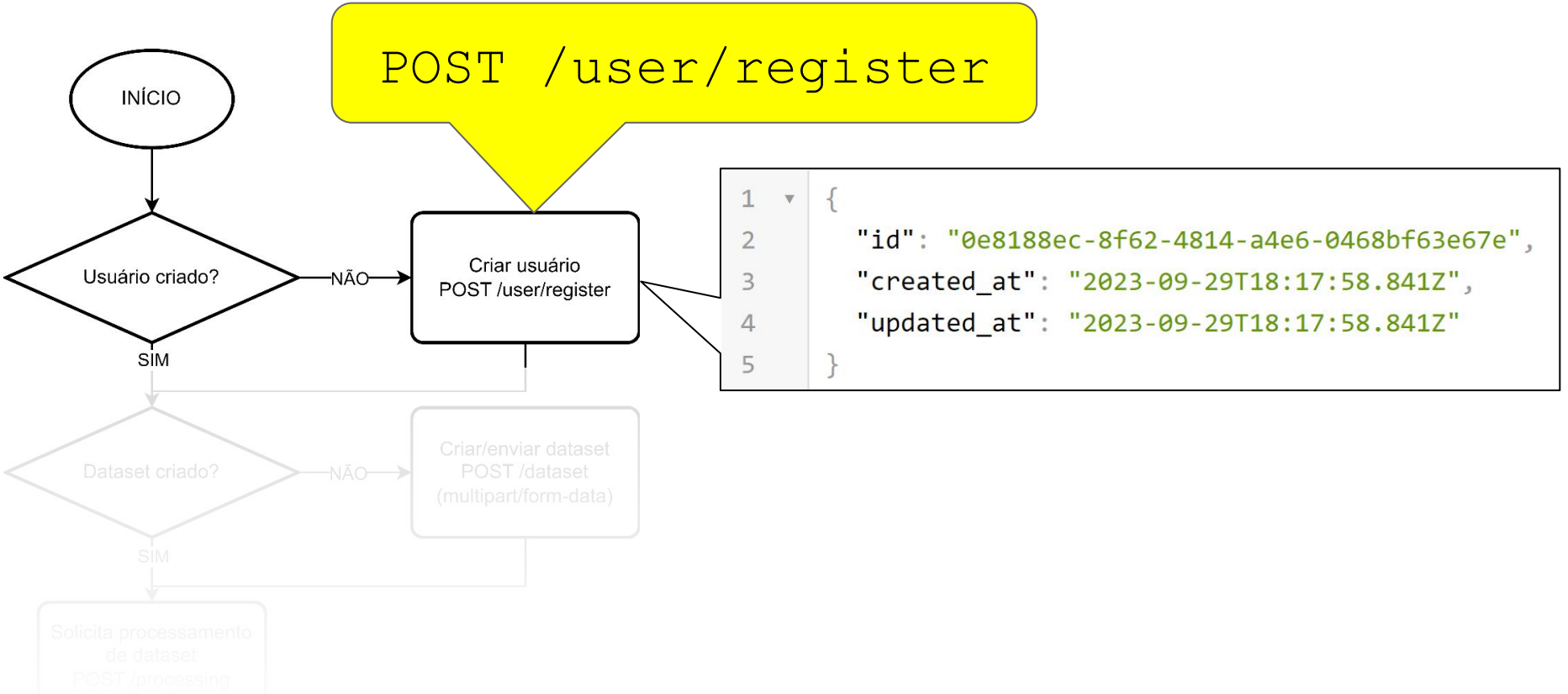
Arquitetura



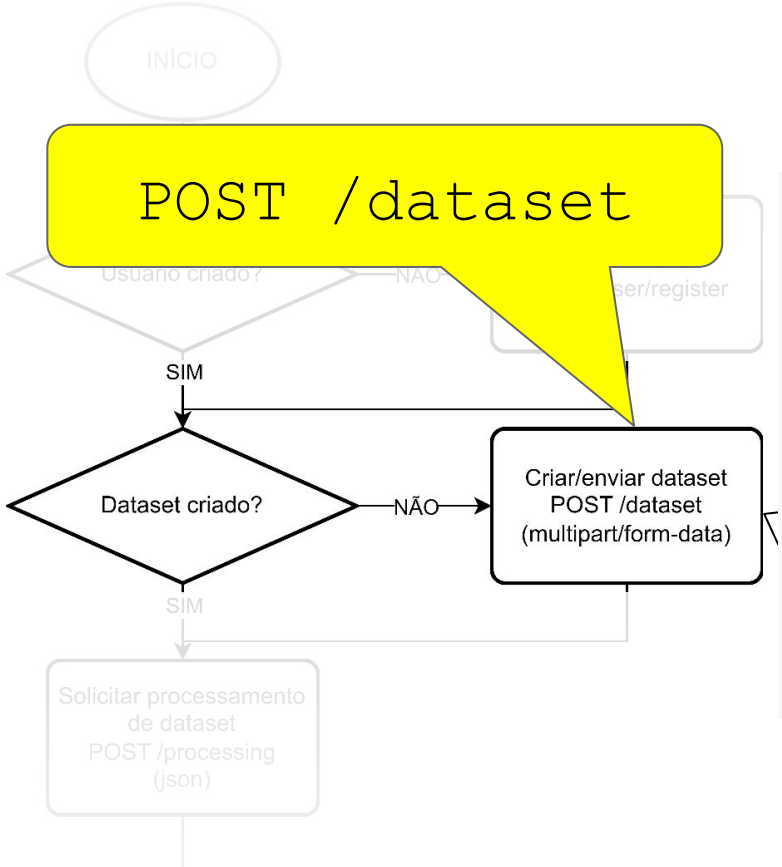
Arquitetura



AutoDroid: *endpoints* da API

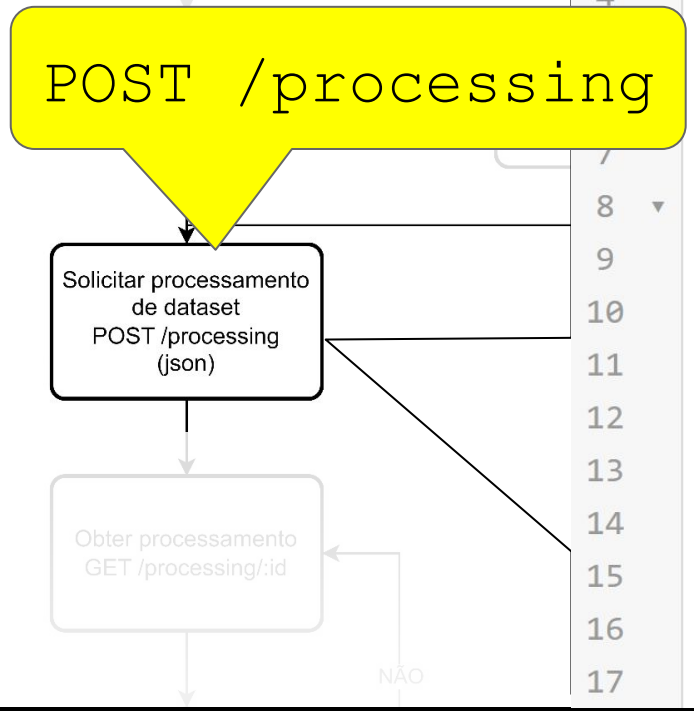


AutoDroid: *endpoints* da API




```
{
  "id": "6f7fcab5-1f12-4a34-a34c-f6a9c97ee8b2",
  "description": "An awesome dataset",
  "user_id": "0e8188ec-8f62-4814-a4e6-0468bf63e67e",
  "user": {↔},
  "file_id": "7c033145-2665-42e3-aae4-d8f987b22be5",
  "file": {
    "id": "7c033145-2665-42e3-aae4-d8f987b22be5",
    "filename": "087ded2b-e62a-4483-a703-dea4c9517413:1696011517165.csv",
    "mime_type": "text/csv",
    "extension": "csv",
    "size": 59685
  }
}
```

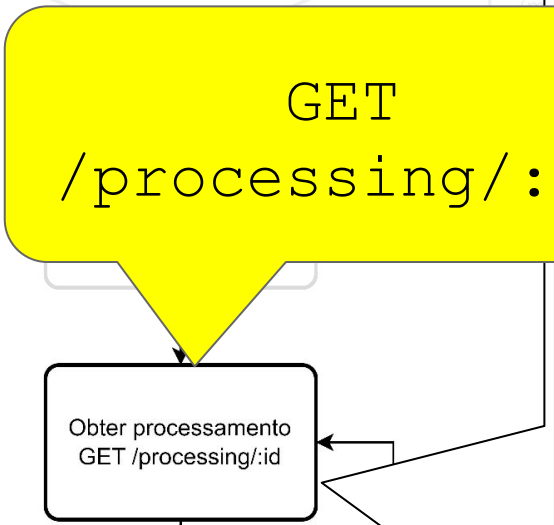
AutoDroid: *endpoints* da API




```
{
  "id": "31eca735-0d8b-4dfc-95c5-4d40ead36b2e",
  "dataset_id": "6f7fcab5-1f12-4a34-a34c-f6a9c97ee8b2",
  "started_at": null,
  "finished_at": null,
  "retries": 0,
  "processor": "droidaugmentor",
  "params": {
    "verbosity": "20",
    "number_epochs": "1000",
    "training_algorithm": "Adam",
    "dense_layer_sizes_d": "256",
    "dense_layer_sizes_g": "256"
  },
  "status": "PENDING",
  "status_description": "Processing requested and is now pendi
}
```

AutoDroid: *endpoints* da API

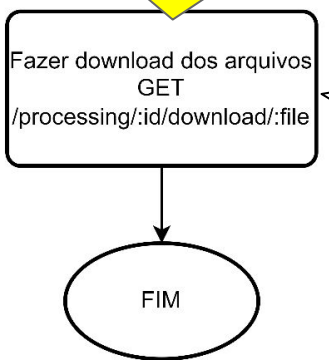
GET
/processing/:id



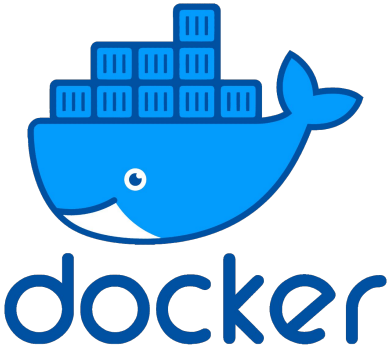

```
{
  "processor": "droidaugmentor",
  "started_at": null,
  "finished_at": null,
  "retries": 1,
  "destination": "storage/processing",
  "status": "PROCESSING",
  "status_description": "Processing",
  "created_at": "2023-09-13T13:30:49.165Z",
  "updated_at": "2023-09-13T13:31:03.178Z",
  "files": [↔]
}
```

AutoDroid: *endpoints* da API

GET
/processing/:id
/download/:file




```
{
  "processor": "droidaugmentor",
  "retries": 1,
  "destination": "storage/processing",
  "status": "SUCCEEDED",
  "status_description": "Succeeded",
  "files": [
    "AdaBoost_Real.pdf",
    "AdaBoost_Synthetic.pdf",
    "Comparison_Real_Synthetic.pdf",
    "DecisionTree_Real.pdf",
    "DecisionTree_Synthetic.pdf",
    "logging.log",
    "models_saved"
  ]
}
```



Plataforma de código aberto que **simplifica** o desenvolvimento, o **empacotamento** e a **execução** de aplicativos em contêineres virtualizados.

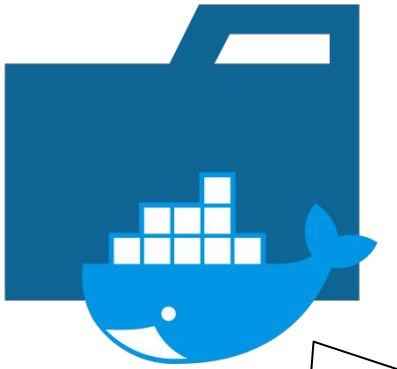
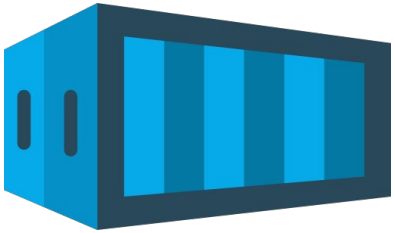
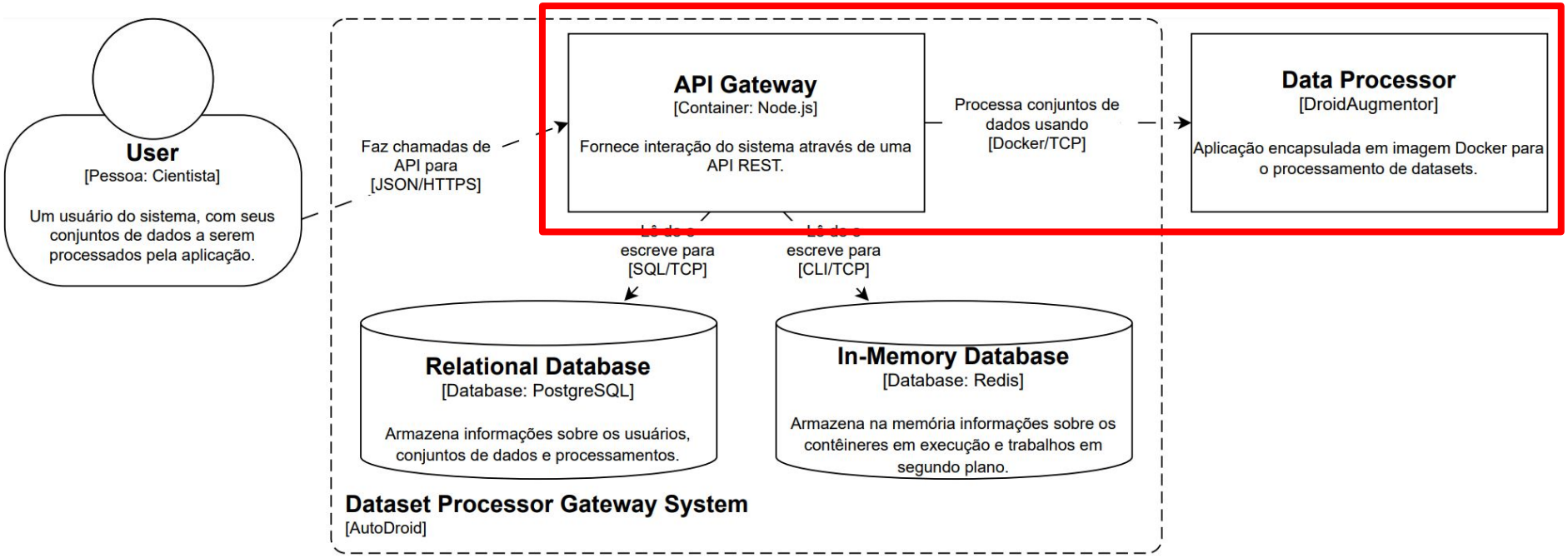


Imagem: contém os recursos, ferramentas e código necessário para executar um aplicativo ou serviço.

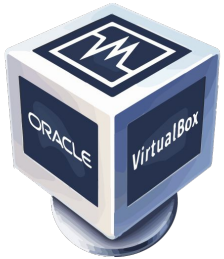


Container: instância em tempo de execução de uma imagem Docker, que facilita o isolamento e execução de um aplicativo em diferentes ambientes.

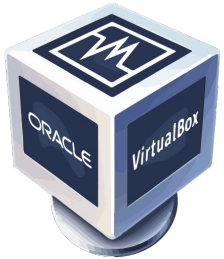
Implementação (Docker in Docker)



HOST

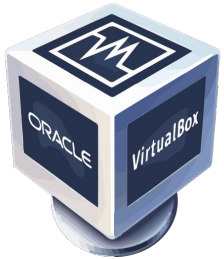


HOST



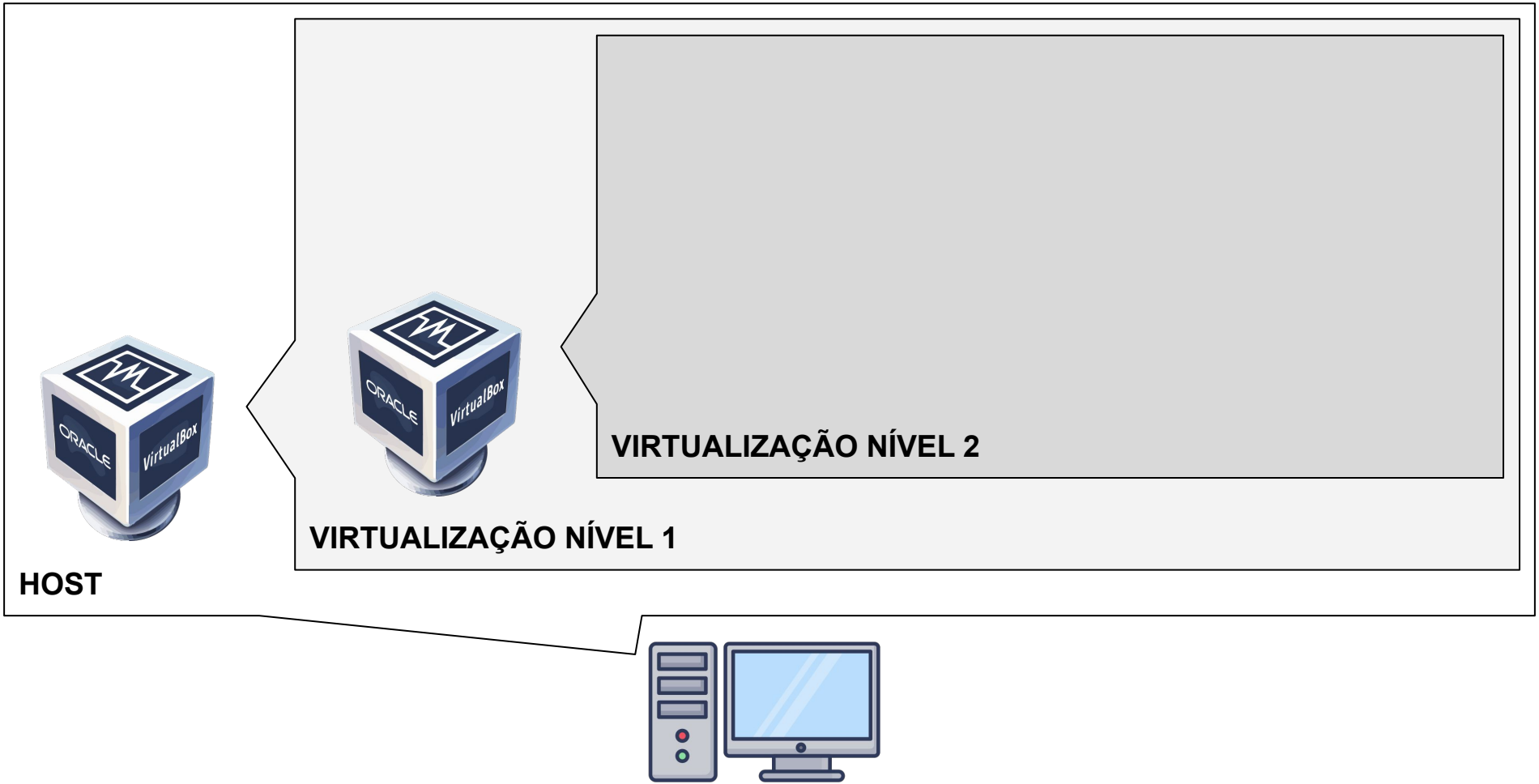
VIRTUALIZAÇÃO NÍVEL 1

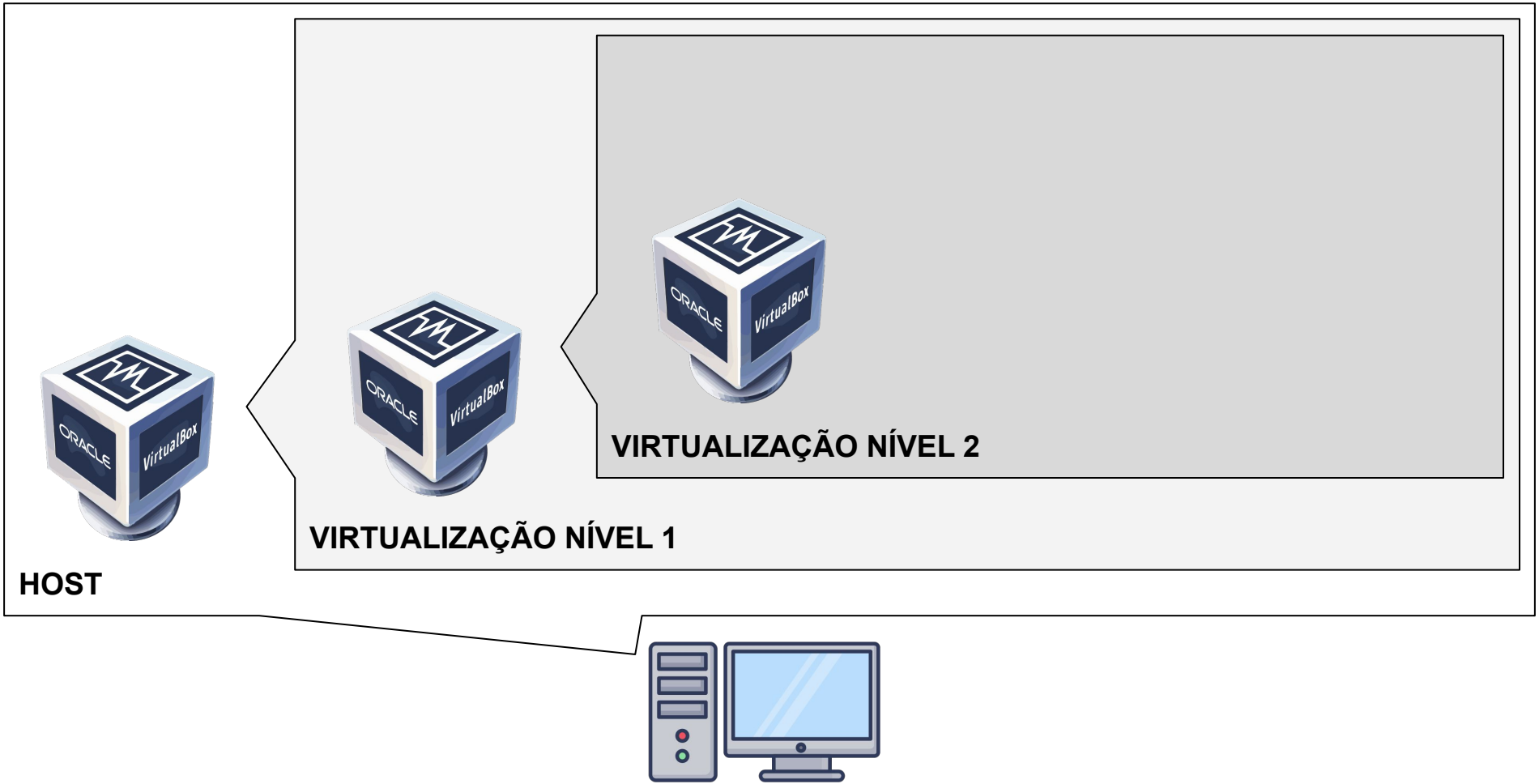
HOST



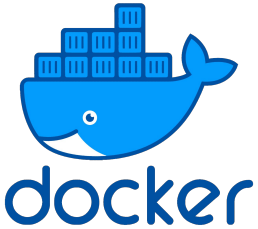
VIRTUALIZAÇÃO NÍVEL 1

HOST

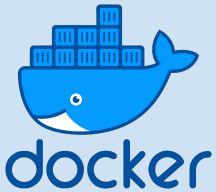

VIRTUALIZAÇÃO NÍVEL 2
VIRTUALIZAÇÃO NÍVEL 1
HOST


VIRTUALIZAÇÃO NÍVEL 2
VIRTUALIZAÇÃO NÍVEL 1
HOST

DroidAugmentor



HOST



CONTAINER DOCKER (Executando o Docker dentro do container) (DinD)

CONTAINER: SGBD

PostgreSQL

CONTAINER: REDIS

redis

CONTAINER: API REST

node

DinD JOB #1
DroidAugmentor

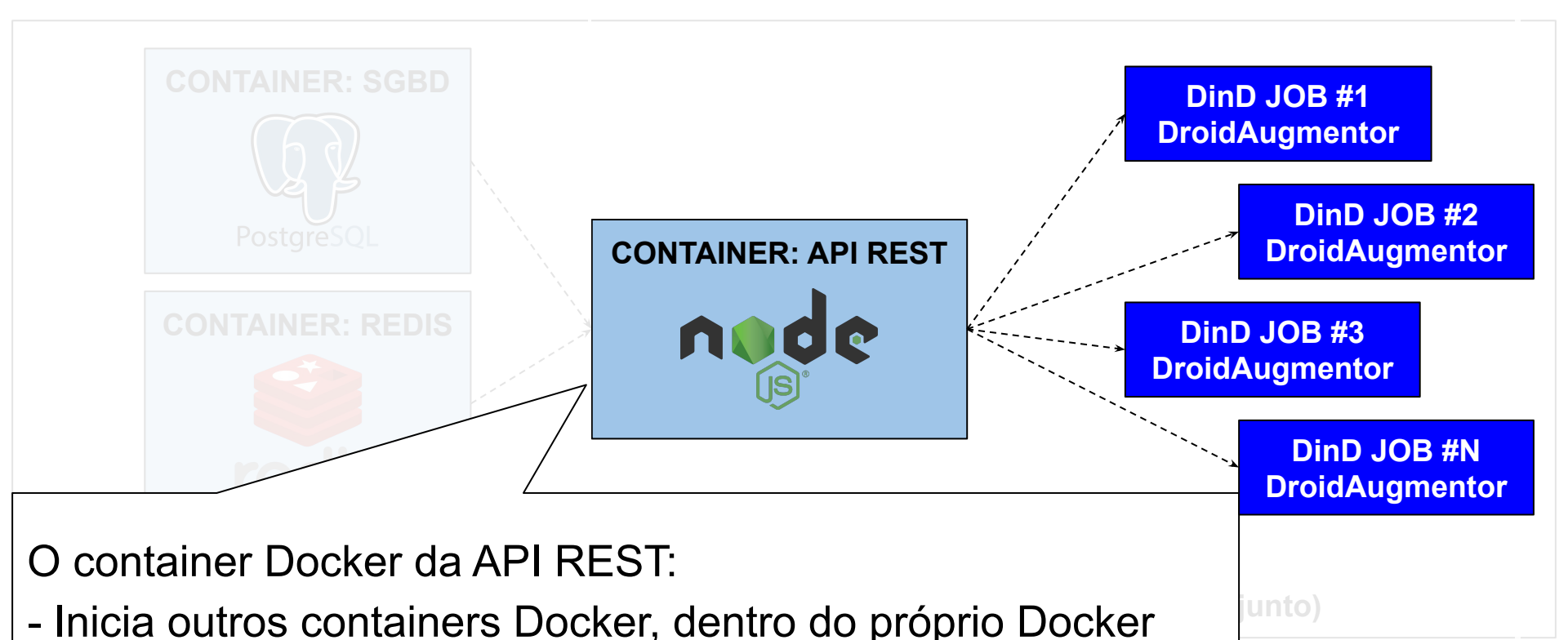
DinD JOB #2
DroidAugmentor

DinD JOB #3
DroidAugmentor

DinD JOB #N
DroidAugmentor

docker

AMBIENTE COM DOCKER-COMPOSE (Múltiplos contêineres em conjunto)



O container Docker da API REST:

- Inicia outros containers Docker, dentro do próprio Docker
- Controla todo o fluxo de vida de cada container criado
- Salva os arquivos durante e ao fim da execução

Níveis de instalação e esforço

Nível 1: Instalar/executar **localmente** o DroidAugmentor **manualmente**, com todas as dependências e configurações necessárias.

Nível 2: Executar a imagem do DroidAugmentor no **Docker localmente**.

Nível 3: Instalar e executar **localmente** o AutoDroid **manualmente**, com todas as dependências e configurações.

Nível 4: Executar o DroidAugmentor através do **Docker Compose** servindo todo o ambiente.

Níveis de instalação e esforço

	Exec.	Modo	Esforço Instalação	Único usuário (recomendação)	Múltiplos usuários (recomendação)
Nível 1 DroidAugmentor	Manual	Aplicação	Alto	Não recomendado	Não recomendado
Nível 2 DroidAugmentor	Docker	Aplicação	Baixo	Recomendado	Não recomendado
Nível 3 AutoDroid	Manual	Serviço	Alto	Neutro	Neutro
Nível 4 AutoDroid	Docker	Serviço	Baixo	Não recomendado	Recomendado

Níveis de instalação e esforço

	Exec.	Modo	Esforço Instalação	Único usuário (recomendação)	Múltiplos usuários (recomendação)
Nível 1 DroidAugmentor	Manual	Aplicação	Alto	Não recomendado	Não recomendado
Nível 2 DroidAugmentor	Docker	Aplicação	Baixo	Recomendado	Não recomendado
Nível 3 AutoDroid	Manual	Serviço	Alto	Neutro	Neutro
Nível 4 AutoDroid	Docker	Serviço	Baixo	Não recomendado	Recomendado

Níveis de instalação e esforço

	Exec.	Modo	Esforço Instalação	Único usuário (recomendação)	Múltiplos usuários (recomendação)
Nível 1 DroidAugmentor	Manual	Aplicação	Alto	Não recomendado	Não recomendado
Nível 2 DroidAugmentor	Docker	Aplicação	Baixo	Recomendado	Não recomendado
Nível 3 AutoDroid	Manual	Serviço	Alto	Neutro	Neutro
Nível 4 AutoDroid	Docker	Serviço	Baixo	Não recomendado	Recomendado

Níveis de instalação e esforço

	Exec.	Modo	Esforço Instalação	Único usuário (recomendação)	Múltiplos usuários (recomendação)
Nível 1 DroidAugmentor	Manual	Aplicação	Alto	Não recomendado	Não recomendado
Nível 2 DroidAugmentor	Docker	Aplicação	Baixo	Recomendado	Não recomendado
Nível 3 AutoDroid	Manual	Serviço	Alto	Neutro	Neutro
Nível 4 AutoDroid	Docker	Serviço	Baixo	Não recomendado	Recomendado

Considerações finais

- AutoDroid disponibiliza o DroidAugmentor como serviço
- Docker facilita o processo de implantação das ferramentas
- AutoDroid oferece gerenciamento de datasets e resultados de processamentos
- AutoDroid pode ser muito útil na pipeline de IA para detecção de *malware*

Trabalhos futuros

- Testes de desempenho do Docker versus DinD
- Auto escalabilidade do serviço, em particular o DataProcessor
- Armazenamento escalável de *datasets* e resultados da DroidAugmentor
- Desenvolvimento de interface *front-end*, criando um *hub* de experimentação e análise
- Avaliação e adição de mecanismos de segurança

Obrigado!

Envie suas perguntas!

https://app.sli.do/

#1703377

AutoDroid: disponibilizando a ferramenta DroidAugmentor como serviço

Luiz Felipe Laviola, Kayuã Paim, Diego Kreutz, Rodrigo Mansilha

AutoDroid

https://github.com/luizfelipelaviola/autodroid