1. Declaração do Problema

O problema:	Os Hackers do Mal estão utilizando técnicas de IA (Inteligência Artificial) para realizar “mutações” em malwares, dificultando sua detecção.
Que afeta:	Usuários de computadores e dispositivos móveis, dentre outras tecnologias que possam estar sujeitas a ataque de malware.
Cujo impacto:	Aumento do nível de proliferação de malware: um dos maiores desafios da segurança da informação.
Ganhos ao resolver:	Os Hackers do Bem podem enfrentar esta proliferação de malwares utilizando ferramentas de IA como o DroidAugmentor para que a detecção dos malwares “mutantes” seja amplamente aprimorada.

2 Declaração do Produto

Público-alvo:	Hackers do bem, cientistas, pesquisadores e estudantes da área de IA e Segurança da Informação.
Motivação:	Executar ferramentas tais como a DroidAugmentor pode ser uma tarefa muito complexa e nada escalável, criando uma grande barreira de aprendizagem e utilização da ferramenta.
Produto:	AutoDroid
Benefícios:	Ao oferecer ferramentas como a DroidAugmentor como um serviço, torna sua execução escalável, de fácil aprendizado e com melhor aproveitamento para experimentação.
Alternativas:	
Vantagens:	A AutoDroid fornece um meio escalável e parametrizável para a execução das ferramentas como DroidAugmentor.

3. Papéis e Responsabilidades

Papel	*Responsabilidades*
Engenheiro de Software	Descobrir, especificar, analisar e validar requisitos; Elaborar e documentar o projeto; Implementar o projeto em código; Realizar testes; Implantar o projeto em ambiente produtivo; Monitorar o funcionamento; Evoluir o sistema e projeto como um todo.
Orientadores	Apresentar os desejos e necessidades para o projeto; Auxiliar no entendimento e especificação de requisitos; Utilizar a ferramenta reportando bugs e solicitando as alterações necessárias; Apresentar feedbacks para os Engenheiros de Software; Proceder com as entregas e documentação científica.
Hacker do Bem (cientista)	Utilizar a plataforma; Reportar defeitos e demais problemas na utilização.

4. Ambiente do Usuário

O usuário deverá ter um dispositivo (seja fixo ou móvel) com acesso à internet e com ao menos uma ferramenta de navegação para acessar a versão web do produto ou um cliente de API REST/GraphQL (ex.: curl, httpie, postman, insomnia) previamente instalado em seu dispositivo.

5. Escopo do Produto

Identificador	História de Usuário
RF01	**Como** visitante, **quero** obter informações sobre o Malware Datalab (AutoDroid + DroidAugmentor) na página inicial **para** que eu conheça o projeto, sua motivação e finalidade.
RF02	**Como** visitante, **quero** me autenticar utilizando login social como Google, Apple e Meta **para** acessar a plataforma.
RF03	**Como** Hacker do Bem, **quero** alterar os meus dados cadastrais como nome, e-mail e telefone **para** manter a ficha cadastral atualizada na plataforma.

RF04	**Como** Hacker do Bem, **quero** fechar todas minhas sessões na plataforma **para** manter minha conta segura em caso de atividade suspeita.
RF05	**Como** Hacker do Bem, **quero** finalizar minha sessão no dispositivo corrente **para** garantir minha segurança, especialmente em dispositivos de uso público.
	DO DATASET
RF06	**Como** Hacker do Bem, **quero** realizar o upload de um arquivo dataset, informando opcionalmente uma lista de tags alfanumérica de classificação e uma descrição opcional **para** utilizá-lo posteriormente em um processo.
RF07	**Como** Hacker do Bem, **quero** listar os datasets públicos ou de minha propriedade (privados) **para** posterior utilização.
RF08	**Como** Hacker do Bem, **quero** visualizar um dataset público ou de minha propriedade (privados) **para** conhecimento próprio.
RF09	**Como** Hacker do Bem, **quero** alterar as tags e a descrição do meu dataset **para** utilizá-lo com informações atualizadas.
RF10	**Como** Hacker do Bem, **quero** apagar um dataset **para** que este não esteja mais disponível em minha conta.
RF11	**Como** Hacker do Bem, **quero** tornar um dataset público **para** que possa ser utilizado por outros Hackers do Bem.
	DA APLICAÇÃO
RF12	**Como** Hacker do Bem, **quero** listar as aplicações públicas **para** conhecimento próprio e listagem de opções disponíveis.
RF13	**Como** Hacker do Bem, **quero** visualizar uma aplicação **para** conhecimento próprio.
RF14	**Como** Hacker do Bem, **quero** listar os processos realizados por uma aplicação específica pública **para** análise dos resultados.
	DO PROCESSO
RF15	**Como** Hacker do Bem, **quero** solicitar a execução assíncrona de uma ferramenta (processador) especificando os parâmetros solicitados, e, caso obrigatório na referida ferramenta, a seleção de um dataset **para** que seja feito o experimento desejado.
RF16	**Como** Hacker do Bem, **quero** listar os processos públicos ou solicitados por mim (privados) **para** conhecimento próprio.
RF17	**Como** Hacker do Bem, **quero** visualizar um processo público ou solicitado por mim (privado) **para** que eu veja o andamento e resultados.
RF18	**Como** Hacker do Bem, **quero** realizar o download dos artefatos de saída do processo **para** que sejam analisados os resultados.
RF19	**Como** Hacker do Bem, **quero** solicitar que um resultado de processo seja mantido até uma data escolhida por mim **para** que estes estejam disponíveis por mais tempo.
RF20	**Como** Hacker do Bem, **quero** tornar um processo público **para** que outros Hackers do Bem possam acessá-los.
RF21	**Como** Hacker do Bem, **quero** alterar um processo meu para que seja privado novamente **para** que outros Hackers do Bem não possam mais acessá-los.
RF22	**Como** Hacker do Bem, **quero** apagar um processo **para** organização.
	DO DATASET (ADMINISTRADOR)
RF23	**Como** administrador, **quero** listar todos os datasets, sejam públicos ou privados, **para** exercer poder moderador e analítico.
RF24	**Como** administrador, **quero** visualizar os detalhes de qualquer dataset **para** exercer poder moderador e analítico.
RF25	**Como** administrador, **quero** alterar as tags e descrição de qualquer dataset **para** exercer poder moderador.
RF26	**Como** administrador, **quero** apagar qualquer dataset inclusive com seus respectivos arquivos **para** exercer poder moderador.
RF27	**Como** administrador, **quero** aprovar ou rejeitar solicitações para tornar um dataset público **para** exercer poder moderador.
	DA APLICAÇÃO (ADMINISTRADOR)
RF28	**Como** administrador, **quero** cadastrar uma nova aplicação, especificando a imagem no Docker Hub, os parâmetros possíveis e necessários, além de descrições para cada parâmetro e para a aplicação em si juntamente com o tipo de mime type do dataset caso seja necessário **para** que seja utilizada em novos experimentos.

RF29	**Como** administrador, **quero** listar todas as aplicações, sejam públicas ou privadas, **para** exercer poder moderador e analítico.
RF30	**Como** administrador, **quero** visualizar os detalhes de qualquer aplicação **para** exercer poder moderador e analítico.
RF31	**Como** administrador, **quero** alterar os dados de qualquer aplicação **para** manter os parâmetros atualizados, tanto como as descrições.
RF32	**Como** administrador, **quero** apagar qualquer aplicação **para** exercer poder moderador.
RF33	**Como** administrador, **quero** tornar uma aplicação pública **para** que possa ser utilizada pelos Hackers do Bem.
	DO PROCESSO (ADMINISTRADOR)
RF34	**Como** administrador, **quero** listar todos os processos, sejam públicos ou privados, **para** exercer poder moderador e analítico.
RF35	**Como** administrador, **quero** visualizar os detalhes de qualquer processo **para** exercer poder moderador e analítico.
RF36	**Como** administrador, **quero** alterar as tags e descrição de qualquer processo **para** exercer poder moderador.
RF37	**Como** administrador, **quero** apagar quaisquer processos **para** exercer poder moderador.
	DO WORKER (ADMINISTRADOR)
RF38	**Como** administrador, **quero** registrar novos workers **para** que sejam utilizados para receber trabalhos.
RF39	**Como** administrador, **quero** listar todos os workers **para** monitoramento e controle.
RF40	**Como** administrador, **quero** visualizar um worker juntamente com seus detalhes e trabalhos exercidos por ela **para** monitoramento e controle.
RF41	**Como** administrador, **quero** alterar os dados de um worker **para** controle.
RF42	**Como** administrador, **quero** visualizar a situação dos workers e seus trabalhos que estão sendo executados em tempo real **para** monitoramento e controle.
RF43	**Como** administrador, **quero** remover uma máquina **para** controle.

6 Premissas e Restrições

Identificador	Requisito Não Funcional
RNF01	A interface web da aplicação e as mensagens de retorno do servidor devem estar disponíveis pelo menos nos seguintes idiomas: Português, Inglês.
RNF02	A aplicação deve poder ser utilizada através de clientes HTTP.
RNF03	A interface web da aplicação deve ter um design CSS responsivo em pelo menos 3 níveis (desktop, tablet e celulares).
RNF04	O servidor deve expor uma API RESTful.
RNF05	O servidor deve expor uma API GraphQL.
RNF06	A aplicação WEB e todas API's expostas deverão utilizar o protocolo HTTPS.
RNF07	O AutoDroid (backend) deve ser stateless, estando preparado para escalar horizontalmente.
RNF08	Todas as verificações de token para autenticação devem verificar a revogação do mesmo previamente.
RNF09	Um administrador pode atuar também como um Hacker do Bem, herdando todas suas permissões enquanto usuário do sistema, acrescido dos poderes de administrador.
RNF10	A aplicação deve garantir a segurança dos métodos através dos níveis de acesso entre visitante, Hacker do Bem e administrador.
RNF11	A autenticação deverá ser feita através do serviço Firebase Authentication.
RNF12	O usuário ao se autenticar com múltiplos provedores de login, a conta deve permanecer a mesma por endereço de e-mail ao invés de múltiplas contas a cada provedor diferente.
RNF13	A interface web da aplicação deve ter aspectos didáticos para ensino e compreensão das ferramentas e da abordagem de IA como solução do problema.
	DO DATASET

RNF14	O dataset sempre será definido como privado inicialmente, apenas o Hacker do Bem que o enviou e administradores poderão ter acesso a este.
RNF15	O dataset não deverá se tornar público imediatamente, este será enfileirado para aprovação dos administradores uma vez registrada a intenção por parte do usuário de torná-lo público.
RNF16	Uma vez declarada a intenção de tornar um dataset público, esta ação não poderá ser desfeita e o dataset não poderá mais ser alterado ou excluído pelo Hacker do Bem que o enviou, pois passará a compor a plataforma como domínio e propriedade do Malware Datalab.
RNF17	Apenas administradores poderão realizar mudanças ou exclusões em datasets públicos.
RNF18	Um dataset público não se tornará privado do Hacker do Bem que o submeteu novamente.
RNF19	O envio de um dataset deve sempre conter um e apenas um arquivo.
RNF20	O envio de um dataset deverá respeitar os mime types suportados pelos processadores (aplicações) disponíveis.
RNF21	O backend deve registrar o resumo criptográfico do dataset (SHA-256).
	DA APLICAÇÃO
RNF22	Apenas administradores poderão adicionar, modificar ou excluir aplicações.
	DO PROCESSO
RNF23	Os processos devem ser executados pelo worker.
RNF24	Os processos sempre são criados privados.
RNF25	Os processos devem ser excluídos automaticamente após 30 dias.
	DO WORKER
RNF26	O worker deverá obrigatoriamente ter o sistema operacional Linux instalado, juntamente com o systemd operacional, além de estar com o Docker, docker compose e Node.js previamente instalados.
RNF27	Deverá ser fornecido um script de setup de ambiente para ser executado no worker.
RNF28	O worker deverá se comunicar com o backend preferencialmente por WebSocket ou através da estratégia de long-polling HTTPS.
RNF29	O worker deverá enviar para o backend suas características como memória, cpu, gpu dentre outros.
RNF30	O servidor deverá registrar os dados de telemetria e de ambiente enviados pelo worker.
RNF31	O worker deverá utilizar arquivos JSON para sua configuração na máquina local.
RNF32	O worker deverá enviar os arquivos gerados pelo processo para o servidor e apagá-los em seguida na máquina local.
RNF33	O worker deverá ser excluído após 7 dias se comunicar com o backend.
RNF34	O worker deverá constantemente informar ao servidor seu status e o andamento de seus processos.