Desenvolvimento de uma Ferramenta de Cibersegurança para Classificação de Malware e Relatório Automático de Ameaças.

Francisco Maia, nº 2024073 | Leonardo Soares, nº 2024076 | Jaquilson Afonso, nº 2024082

Introdução **3**
Informações **4**
Descrição do Produto: 4
Objetivo: 4
Público-alvo: 4
Restrições: 5
Critérios de Sucesso: 5
Comunicação: 6
REQUISITOS **7**
Requisitos e Funcionalidades: 7
Os principais recursos da ferramenta incluem: 7
Como Garantimos a Precisão e Segurança na Análise de Malware: 7
Práticas de Segurança Recomendadas pela Fsociety: 8
REQUISITOS FUNCIONAIS 9
REQUISITOS NÃO FUNCIONAIS 10
RECURSOS **13**
Recursos Humanos (Equipa): 13
Recursos Financeiros:
O financiamento do projeto será obtido através de: 13
Recursos de Software:
Os seguintes softwares e ferramentas serão utilizados no desenvolvimento do CiberShield: 13
Recursos Físicos e Tecnológicos: 14
ANÁLISE DAS NECESSIDADES E PRIORIDADES **15**
Necessidades 15
Prioridades do Projeto 16
LIMITAÇÕES DO PRODUTO **17**
DESIGN **18**
Aplicações Utilizadas **19**
Propriedade Intelectual **20**
Direitos Autorais: 20
Patentes: 20
Marcas Registradas: 20
Segredos Comerciais: 20
Titularidade: 20
Contratos e Acordos: 20
Proteção e Gerenciamento da Propriedade Intelectual **21**
Diagrama UML e casos de uso **22**
Conclusão **23**
Webgrafia **24**

Introdução

Este projeto tem como objetivo criar uma ferramenta online intuitiva para combater malwares e suspeitas dos mesmos. A proposta de uso é instintiva, o utilizador insere informações ou arquivos com suspeita de malícia, e o software analisa, classifica o tipo de malware e gera relatórios detalhados sobre a ameaça detectada. Para garantir que haja precisão e segurança, a ferramenta iria ser desenvolvida com algoritmos de Inteligência Artificial, o que ajuda a identificar certos padrões maliciosos e a aprender com os mesmos, além de integrar e complementar atualizações constantes para acompanhar as novas ameaças cibernéticas, o que permite organizações e indivíduos a se manterem informados sobre ameaças em tempo real e proteger os seus dados de forma eficaz.

Informações

Nome da Empresa: Fsociety
Nome do Produto: CiberShield

Descrição do Produto:

O CiberShield é um software avançado de cibersegurança projetado para classificar de malware e gerar automaticamente relatórios de ameaças. A ferramenta permite que os utilizadores analisem arquivos ou dados suspeitos, a identificar rapidamente potênciais ameaças e a classificar diferentes tipos de malware. Além disso, o programa iria oferecer a possibilidade de personalizar o nível de detalhe dos relatórios, adaptando-se assim às necessidades específicas de cada indivíduo ou organização.

Objetivo:

O objetivo do projeto é fornecer uma solução eficaz, automatizada e precisa para identificar ameaças digitais, o que diretamente contribui para a proteção da privacidade e segurança de dados de utilizadores e organizações. O CiberShield visa otimizar a resposta a ataques cibernéticos e assim fortalecer a defesa contra malwares e outras vulnerabilidades.

Público-alvo:

O público-alvo do projeto inclui empresas, equipas de TI e indivíduos que procuram aprimorar as estratégias de cibersegurança. A ferramenta é ideal para qualquer organização que precise monitorar, identificar e mitigar ameaças digitais de forma rápida e eficaz.

Restrições:

O cronograma para a conclusão do projeto é de aproximadamente 6 meses, dividido da seguinte forma:

- 5 semanas para o desenvolvimento do script inicial da análise de malware;
- 8 semanas para o desenvolvimento de scripts adicionais e integração dos mesmos e integração de IA ;
- 4 semanas para implementar e executar a plataforma;
- 4 semanas para testes, avaliações e resolução de problemas;
- 2 semanas para a entrega final e os ajustes provenientes de feedback.

O orçamento total do projeto é de 100.000 euros, distribuído entre:

- Membros da Equipa (desenvolvedores, especialistas em cibersegurança, designers);
- Aquisições (softwares de apoio e bibliotecas externas);
- Treino da equipa em novas tecnologias e ameaças decorrentes;
- Equipamento necessário para o desenvolvimento e testes;
- Espaço físico ou virtual para reuniões e colaborações;
- Pesquisa contínua sobre novas ameaças cibernéticas;
- Serviços Profissionais (trabalhadores independentes);
- Viagens, se necessário, para conferências ou reuniões presenciais.
- Marketing e campanhas para divulgação e promoção da plataforma.

Critérios de Sucesso:

O sucesso do projeto será avaliado com base em dois fatores principais:

1. Avaliação Técnica, conduzida por especialistas e o professor, para assim garantir que o software atenda aos padrões de qualidade e segurança esperados;
2. Adesão do utilizador, medida pelo número de acessos e utilização da ferramenta.

O nosso compromisso é fornecer uma solução que contribua para um ambiente online mais seguro e confiável.

Comunicação:

A comunicação entre a equipa de desenvolvimento e os clientes será realizada via e-mail empresarial. Um membro da equipa será responsável por acompanhar os “tickets” e responder a dúvidas,para garantir um suporte contínuo. Os clientes poderão enviar perguntas, reportar problemas ou sugerir melhorias para que o software atenda às expectativas e necessidades tanto dos utilizadores como das empresas, o que por sua vez reforça que o projeto se desenvolve progressivamente ao longo do tempo.

REQUISITOS

Requisitos e Funcionalidades:

A CiberShield tem como objetivo ser uma ferramenta eficaz para a classificação de malware e gerir automaticamente relatórios de ameaças, com o intuito de proporcionar uma interação agradável para o utilizador. Ele pode proporcionar um ambiente e pode submeter newsletters ou acrescentar outras informações para análise, onde o mesmo vai receber dois relatórios detalhados que lhe permitam perceber e combater qualquer tipo de ameaça. A ferramenta, no que diz respeito aos relatórios, embora não otimize as chances máximas possíveis de um relatório, tem uma configuração automática que se adapta a qualquer nível de detalhe para o benefício da empresa.

Os principais recursos da ferramenta incluem:

- Análise automática de malware com IA, para proporcionar uma classificação precisa e rápida;
- Gerar relatórios em tempo real, com opção de exportação em diferentes formatos (PDF, CSV);
- Alertas personalizados sobre novas ameaças detetadas;
- Integração com outras ferramentas de segurança para um ecossistema de proteção mais robusto.

Como Garantimos a Precisão e Segurança na Análise de Malware:

Para garantir a eficácia na detecção de ameaças, o CiberShield segue os seguintes princípios:

- Mecanismos de Análise Avançados: O sistema utiliza algoritmos de “machine learning” e análise comportamental para identificar ameaças, mesmo aquelas que não estão em bancos de dados conhecidos;
- Atualizações Frequentes: O software é constantemente atualizado para reconhecer novos tipos e novas variáveis de malware;
- Classificação Precisa: As ameaças identificadas não são classificadas apenas com base em assinaturas, mas também através de padrões de comportamento suspeitos.

Práticas de Segurança Recomendadas pela Fsociety:

Para complementar o uso do CiberShield e fortalecer a segurança dos dados a nossa empresa recomenda:

- Não confiar em links e anexos suspeitos recebidos por e-mail ou mensagens;
- Proteger os seus dispositivos: manter documentos sensíveis e telas de dispositivos longe de olhares terceiros;
- Evitar o uso de redes Wi-Fi públicas para acessar informações pessoais ou financeiras;
- Instale antivírus e mantenha todos os dispositivos atualizados com as últimas atualizações de segurança.

Com essas funcionalidades e boas práticas, o CiberShield garante uma abordagem completa para identificar e prevenir ameaças cibernéticas.

REQUISITOS FUNCIONAIS

1. **Classificação Automática do Malware:**
   O sistema permite que o utilizador carregue arquivos ou insira dados suspeitos para análise. O *CiberShield* utiliza algoritmos de Inteligência Artificial para identificar, classificar e categorizar diferentes tipos de malware, para que seja garantida uma deteção precisa e rápida.

2. **Entrada de Dados pelo Utilizador:**
   O utilizador pode inserir arquivos, links ou dados que considere suspeitos. Além disso, o sistema oferece opções de análise em diferentes níveis, o que permite ao utilizador escolher a abordagem mais adequada à sua necessidade.

3. **Gerar Automaticamente Relatórios de Ameaças:**
   Após a análise, o sistema gera relatórios detalhados que descrevem o tipo de malware identificado, o nível de risco associado e recomendações para mitigar o mesmo. O utilizador pode personalizar o nível de detalhe do relatório conforme as suas necessidades.

4. **Exportar e Compartilhar os Relatórios:**
   Os relatórios gerados podem ser exportados em diferentes formatos, como PDF ou CSV, para facilitar a integração e interação com outras ferramentas de segurança a compartilhar os mesmos com equipas de TI e gestão.

5. **Validar as Ameaças em Tempo Real:**
   O CiberShield fornece feedback instantâneo sobre as ameaças detetadas, com indicadores visuais que mostram o nível de gravidade da ameaça. O sistema também valida a presença de arquivos maliciosos desconhecidos através de análise comportamental.

6. **Interface de Utilizador (UI) Intuitiva:**
   A interface do CiberShield foi desenvolvida para ser simples e intuitiva, permitindo que utilizadores de todos os níveis de experiência consigam realizar análises de forma rápida e eficaz. O dashboard apresenta os resultados de forma clara, com opções de navegação intuitivas.

7. **Histórico e Repetição de Análises:**
   O sistema armazena um histórico das análises realizadas, o que permite que o utilizador consulte relatórios anteriores ou repita a análise de arquivos com os mesmos métodos e parâmetros. Isso facilita o acompanhamento de ameaças recorrentes ou a monitorar arquivos em diferentes momentos.

8. **Alertas e Notificações Personalizadas:**
   Os utilizadores podem configurar o sistema para receber alertas automáticos sobre novas ameaças ou atualizações de segurança. As notificações podem ser enviadas via e-mail ou integradas a outras plataformas de monitoramento.

9. **Integração com Ferramentas de Cibersegurança:**
   O CiberShield pode ser integrado com outras ferramentas de segurança, como firewalls, antivírus e sistemas de monitoramento de rede, para por sua vez permitir uma abordagem de segurança mais completa e unificada.

REQUISITOS NÃO FUNCIONAIS

1. **Desempenho:**
   O CiberShield foi concebido para realizar análises de malware e gerar relatórios de ameaças de forma rápida e eficaz, para minimizar o tempo de resposta mesmo durante a análise de grandes volumes de dados. O objetivo é proporcionar uma experiência fluida e sem interrupções, independentemente da qualidade da conexão com a internet ou da complexidade dos arquivos analisados.

2. **Progresso:**
   O sistema foi projetado para ser progressivo e de aprendizagem, para permitir que o produto se expanda, como a integração com APIs de terceiros, análises mais profundas de ameaças e suporte a um maior volume de dados sem comprometer o desempenho ou a segurança.

3. **Segurança:**
   A segurança é o pilar central do CiberShield. Todos os arquivos analisados são tratados com um alto padrão de confidencialidade, e nenhuma informação sensível é armazenada no servidor após a análise. O sistema utiliza criptografia para proteger a transmissão de dados e segue as melhores práticas para mitigar riscos de “leaks” de dados ou acesso não autorizado.

4. **Privacidade:**
   A privacidade dos utilizadores é uma prioridade. O CiberShield não exige o registro de dados pessoais para a utilização da ferramenta. Todos os dados analisados são processados de forma anônima, para garantir que a confidencialidade e a proteção das informações dos utilizadores seja possível.

5. **Disponibilidade**:
   O CiberShield foi concebido para estar disponível 24/7 e assim garantir que os utilizadores possam acessar a plataforma a qualquer momento. A arquitetura do sistema é robusta e confiável, com mínima necessidade de manutenção para um tempo de atividade constante.

6. **Compatibilidade:**
   O sistema é compatível com os principais navegadores, como Google Chrome, Firefox e Microsoft Edge. Além disso, o CiberShield é totalmente responsivo, garantindo uma experiência consistente tanto em dispositivos móveis quanto em desktops.

Com esses requisitos, o CiberShield garante não só uma análise eficaz de ameaças, mas também uma experiência segura, acessível e adaptável às necessidades dos utilizadores.

RECURSOS

Recursos Humanos (Equipa):

- **Desenvolvedores:** 2-3 profissionais especializados em frontend e backend, responsáveis pela criação da interface e infraestrutura da plataforma;
- **Especialistas em Cibersegurança**: 1-2 profissionais focados na segurança da informação, análise de ameaças e proteção de dados;
- **Designer UX/UI:** 1 profissional para criar uma interface intuitiva e acessível, garantindo uma experiência de utilizador fluida;
- **Gerente de Projeto:** Responsável pela gestão do cronograma, recursos e comunicação entre as equipes;
- **Consultores Externos:** Especialistas em IA e machine learning para auxiliar na implementação dos algoritmos de classificação de malware.

Recursos Financeiros:

O financiamento do projeto será obtido através de:

- Empréstimos bancários para cobertura de custos iniciais;
- Patrocínios de empresas de tecnologia, interessadas em apoiar soluções inovadoras de cibersegurança;
- Investidores privados ou parcerias estratégicas com startups e instituições focadas em segurança digital.

Recursos de Software:

Os seguintes softwares e ferramentas serão utilizados no desenvolvimento do *CiberShield*:

- **Linguagens de Programação:** Python para análise de dados e implementação de IA;
- **Controle de Versão:** GitHub para gerir todo o projeto;
- **Ambientes de Desenvolvimento:** Visual Studio Code para desenvolver do código;
- **Documentação e Colaboração:** Google Docs e Google Forms para documentar o projeto e recolher feedback;
- **Design:** Canva para criar materiais visuais e protótipos da interface;
- **Comunicação da Equipa:** WhatsApp para comunicar entre os membros da equipa;
- **Host e Plataforma Web:** AWS ou Google Cloud para uma infraestrutura de “host” segura.

Recursos Físicos e Tecnológicos:

- Servidores de Alta Performance para processamento de dados e análise de ameaças;
- Computadores e Equipamentos de Teste com configurações avançadas para o desenvolvimento e simulação de ameaças;
- Espaço Físico e/ou Virtual para reuniões e colaboração da equipe.

Esses recursos irão garantir que o CiberShield seja desenvolvido com um alto padrão de qualidade e funcionalidade e a atender às exigências de segurança e desempenho do mercado de cibersegurança.

ANÁLISE DAS NECESSIDADES E PRIORIDADES

Necessidades

1. Monitorizar Ameaças e Detetar Malware

O utilizador necessita de um sistema que permita rastrear e identificar malwares de forma eficiente e em tempo real. A ferramenta deve ser capaz de analisar comportamentos suspeitos, detetar ameaças e fornecer alertas imediatos sobre possíveis infecções.

2. Personalização na Análise de Ameaças

O utilizador deve ter a possibilidade de configurar parâmetros específicos para detetar malwares, como definir listas de domínios suspeitos e escolher quais tipos de ameaças monitorar. Isso assegura uma proteção adaptada às necessidades individuais.

3. Usabilidade e Facilidade de Uso

O sistema deve ser intuitivo, permitindo que o utilizador configure e visualize relatórios de ameaças de maneira clara e objetiva. A interface deve facilitar a navegação e as informações, para garantir que mesmo utilizadores sem experiência técnica possam utilizá-lo com eficácia.

4. Garantia de Privacidade e Segurança dos Dados

A privacidade do utilizador deve ser uma prioridade. O sistema não deve armazenar ou compartilhar informações sensíveis, para garantir que a análise das ameaças ocorra sempre de forma segura sempre.

Prioridades do Projeto

1. Alta Prioridade

- **Monitorização e Detecção de Malware**

A principal prioridade do projeto é garantir que o sistema identifique e rastreie ameaças de malware com alta precisão, fornecendo alertas em tempo real sobre atividades suspeitas.

- **Facilidade de Uso**

A interface deve ser intuitiva e acessível, permitindo que os utilizadores monitorem ameaças e configurem o sistema sem dificuldades.

- **Personalização da Análise de Ameaças**

Permitir que os utilizadores ajustem os critérios de deteção, definindo listas de domínios suspeitos, níveis de sensibilidade e categorias específicas de malware a serem rastreadas.

2. Média Prioridade

- **Relatórios Detalhados sobre Ameaças**

Embora não seja essencial para o funcionamento básico, a inclusão de relatórios detalhados ajudará os utilizadores a compreender melhor os riscos detectados e tomar medidas preventivas.

- **Compatibilidade Diferentes hardwares**

O sistema deve ser acessível tanto em desktops quanto em dispositivos móveis, para que seja garantida uma experiência consistente para todos os utilizadores. Essa compatibilidade amplia o alcance e a utilidade da ferramenta.

LIMITAÇÕES DO PRODUTO

1. Configuração do Utilizador

O sistema depende das configurações definidas pelo utilizador para rastrear e detectar ameaças de malware. O utilizador pode personalizar listas de domínios suspeitos e ajustar os critérios de análise, mas a eficácia da deteção pode variar conforme as definições aplicadas.

2. Garantia de Privacidade e Segurança

Nenhuma informação sobre as ameaças detectadas ou atividades dos utilizadores é armazenada nos servidores. Os dados são analisados e descartados localmente, garantindo que a confidencialidade e a segurança dos utilizadores sejam preservadas.

3. Acesso via Browser e Internet

O sistema precisa de uma ligação à Internet, visto que é acessado diretamente através de um navegador web. Isso proporciona a liberdade para os usuários, que podem acompanhar e monitorar ameaças a partir de qualquer dispositivo, mas isso também significa que não é possível utilizar o sistema offline.

DESIGN

Cenário de Sucesso Principal

1. Objetivos do Projeto

O principal objetivo do nosso projeto é criar uma interface que seja fácil e agradável de usar para que os usuários possam acompanhar as ameaças relacionadas ao malware de forma eficaz e acessível. O principal objetivo é criar um recurso que facilite o tracking de malware de modo que ele seja simples para qualquer pessoa usar, disponível para qualquer nível de conhecimento técnico. O intuito é dar uma resposta que seja prática para os usuários e que, ao mesmo tempo, seja eficaz e de fácil manuseio na identificação de riscos potenciais.

2. Métricas de Sucesso

O sucesso do nosso projeto é medido pela facilidade e rapidez com que o utilizador consegue monitorar ameaças e identificar potenciais malwares. Para alcançar este sucesso, o design do sistema deve:

- **Análise de Ameaças Simples:**

Durante a fase de monitoramento, o usuário deve ser capaz de ver e responder a ameaças com uma quantidade razoável de facilidade.

- **Eficiência nos Processos:**

As ameaças devem ser processadas em tempo real, pois qualquer atraso pode ser prejudicial ao responder a um ataque.

- **Satisfação do Utilizador:**

A métrica que mais importa é a satisfação do usuário em relação às metas. Se a ferramenta atende às expectativas do usuário em usabilidade e contexto de ameaça, então o projeto atingiu seus objetivos mais importantes.

Se esses critérios forem cumpridos, podemos considerar que o projeto foi bem-sucedido, oferecendo uma solução que combina segurança e usabilidade de forma eficiente.

Aplicações Utilizadas

1. **Frontend**
    - **React** para a construção de interfaces interativas e dinâmicas.
    - **Tailwind CSS** para um design responsivo e eficiente.
2. **Backend**
    - **Node.js** para a criação do servidor e da API.
    - **Express.js** para gerenciar rotas e estruturação do backend.
3. **Base de Dados**
    - **MongoDB** para armazenar dados de rastreamento e análise, garantindo escalabilidade e flexibilidade na manipulação de dados.
4. **Análise de Dados**
    - **Python**, utilizando bibliotecas como **Pandas e NumPy**, para análise e processamento de dados.
    - **Elasticsearch** para indexação e busca eficiente em grandes volumes de dados.
5. **Segurança**
    - **OWASP ZAP** para testes de segurança e identificação de vulnerabilidades.
    - **SSL/TLS** para criptografar a comunicação entre clientes e servidores, garantindo proteção contra ataques cibernéticos.
6. **Monitoramento e Manutenção**
    - **Grafana e Prometheus** para monitoramento do desempenho da aplicação e coleta de métricas.
    - **Sentry** para rastreamento de erros em tempo real, facilitando a detecção e resolução de problemas.

Propriedade Intelectual

Direitos Autorais:

- Protegem o código-fonte e a documentação do CiberShield, garantindo o controle sobre o uso e distribuição.

Patentes:

- Avaliar a possibilidade de patentear inovações tecnológicas desenvolvidas durante o projeto.

Marcas Registradas:

- Registrar o nome CiberShield e logotipos para proteger a identidade da marca.

Segredos Comerciais:

- Proteger algoritmos, métodos de rastreamento e dados sensíveis, assegurando uma vantagem competitiva.

Estrutura de Propriedade Intelectual

Titularidade:

- Definir a empresa como a proprietária da propriedade intelectual criada durante o projeto.

Contratos e Acordos:

- Estabelecer NDAs com a equipa e parceiros;
- Incluir cláusulas nos contratos de trabalho para garantir que a propriedade intelectual pertença à empresa.

Proteção e Gerenciamento da Propriedade Intelectual

1. **Registro de Direitos**
    - Realizar o registro de direitos autorais, patentes e marcas para garantir proteção legal contra uso indevido.

2. **Monitoramento**
    - Implementar um sistema eficaz para rastrear e detectar o uso não autorizado da propriedade intelectual, prevenindo violações e garantindo conformidade legal.

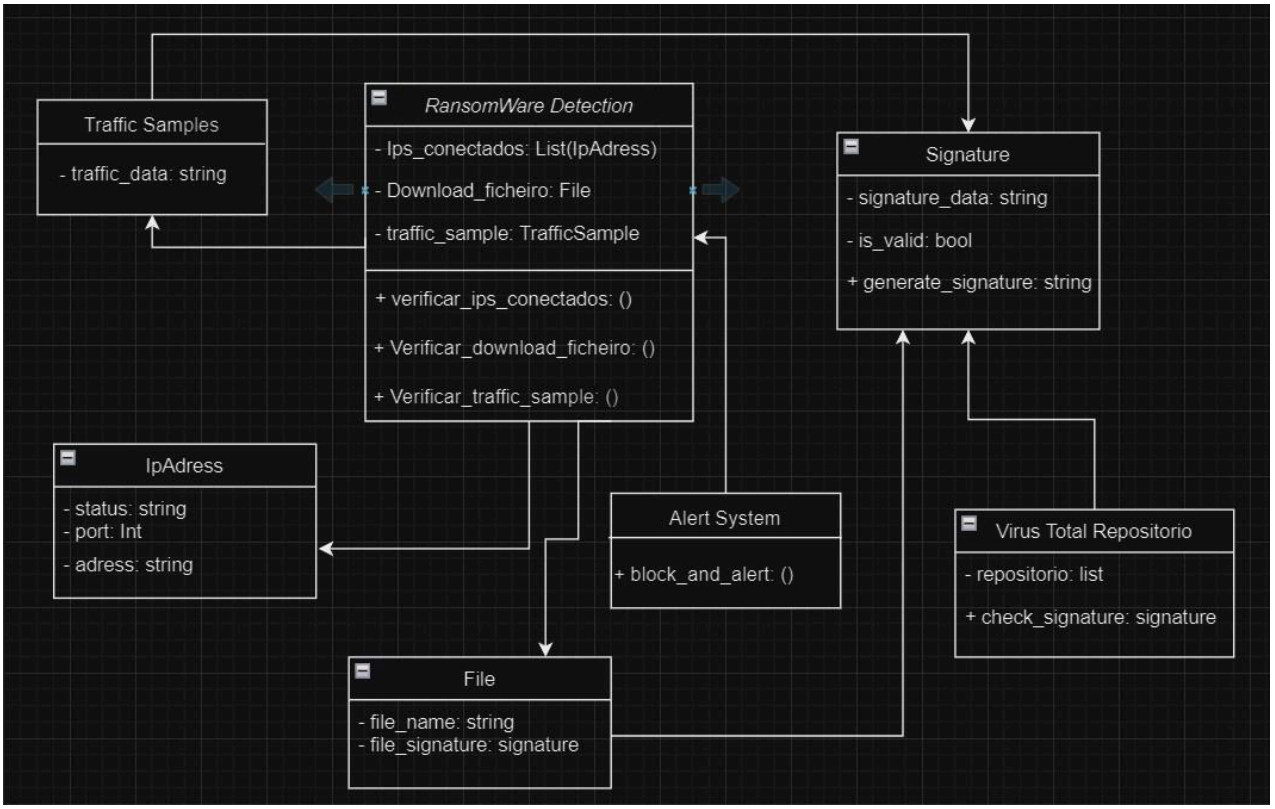
3. **Educação da Equipa**
    - Capacitar a equipa sobre a importância da proteção da propriedade intelectual e as melhores práticas para garantir sua segurança.
    - Desenvolver normas éticas e diretrizes internas para assegurar a conformidade com regulamentações e boas práticas.

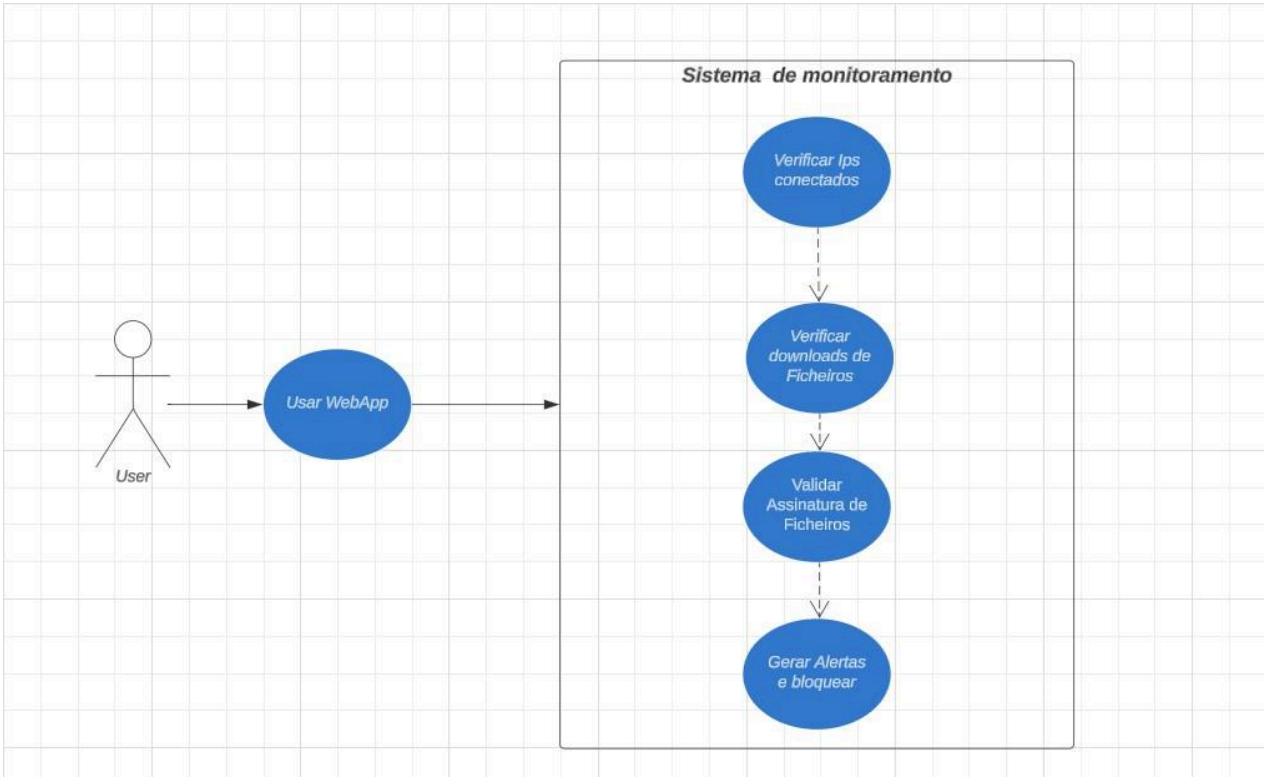
4. **Licenciamento de Software**
    - Definir o tipo de licença a ser adotada (open-source ou proprietária), considerando as vantagens e desafios de cada modelo.
    - Pesquisar e seguir os procedimentos necessários para obtenção da licença escolhida.

5. **Parcerias e Colaborações**

Estabelecer termos claros para o uso da propriedade intelectual em colaborações e parcerias, garantindo a proteção dos direitos e a definição de responsabilidades entre as partes envolvidas.

Diagrama UML e casos de uso





Conclusão

Esta ferramenta é eficaz para a detecção e classificação de malware. Através da implementação de algoritmos AI e técnicas avançadas de análise de ameaças, a plataforma garante uma abordagem automatizada e precisa na identificação de riscos digitais.

Ao longo do projeto, foram consideradas as necessidades dos utilizadores, com o final de priorizar a facilidade de uso, a personalização e a privacidade dos dados. A escolha das tecnologias, como React, Node.js, MongoDB e Elasticsearch, assegurou um desempenho eficiente, permitindo que as empresas e indivíduos utilizem esta ferramenta de maneira confiável e segura (sendo que não está desenvolvido o programa das a estrutura base foi toda pensada e considerada).

Apesar das limitações, como a necessidade da conexão à internet e a dependência das configurações do utilizador, o CiberShield é uma solução inovadora no combate às ameaças cibernéticas. Com atualizações contínuas e integração e interação com outras ferramentas de segurança, com a pretensão de evoluir para acompanhar o cenário dinâmico das ciberameaças.

O sucesso do projeto será medido pela sua aceitação no mercado, usabilidade e impacto na mitigação de ataques digitais. O CiberShield tem potencial para se tornar uma referência na proteção contra malwares e outras vulnerabilidades digitais.

Webgrafia

Link do Github (Todos os documentos encontram-se no Github como Doc, powerpoint inicial e diagramas, etc…) (Todas as informações encontram-se no repositório do trabalho do Github)

https://github.com/Fsociety4ev3r/Fsociety