

**Desenvolvimento de uma Ferramenta de Cibersegurança para Classificação de**

**Malware e Relatório Automático de Ameaças.**

**Descrição do Projeto**

O RansomTracker é uma ferramenta avançada preparada para rastrear sites de fraude usados por grupos de ransomware. O projeto tem como objetivo mostrar uma visão abrangente e em tempo real das atividades criminosas na internet, usando AI como ferramenta de complementação do software, permitindo que organizações e indivíduos se mantenham informados sobre ameaças em tempo real e protejam os seus dados de forma eficaz.

**Objetivos do Projeto**

- Monitorar continuamente as atividades de ransomware;

- Fornecer informações atualizadas sobre ameaças em tempo real;

- Ajudar organizações e indivíduos a protegerem seus dados;

- Combate em tempo real de ameaças de malware e ransomware.

- Criar relatórios completos do malware.

- Software de aprendizagem como objetivo conseguir-se adaptar e combater novos malwares.

**Cronograma**

**Pesquisa e Planejamento (1 mês)**

- Pesquisa sobre ransomware e tendências atuais;

- Análise de mercado para identificar concorrentes e necessidades do público-alvo;

- Definição de requisitos do sistema.

- Pesquisa sobre membros e profissionais necessários.

-Informar sobre custos e gestão necessária para a Start-Up.

**Desenvolvimento da Plataforma (1 ano)**

- Criação do sistema de rastreamento (backend e frontend);

- Desenvolvimento de feeds de dados e análises de risco;

- Implementação de funcionalidades de alerta e notificação.

- Implementação de AI para criar reports e aprendizagem com malware.

**Testes e Validações (1 mês)**

- Testes de funcionalidade: garantir que todas as funções executam conforme o esperado;

- Testes de segurança: avaliar vulnerabilidades e diminuir os riscos.

**Lançamento (1 mês) e Feedback (indefinido)**

- Lançamento da plataforma ao público;

- Recolha de feedback dos utilizadores para melhorias futuras.

**Recursos Necessários**

**Equipe:**

- Desenvolvedores: 2-3 (para frontend e backend);

- Especialistas em cibersegurança:1-2 (para garantir a segurança da plataforma);

- Designer UX/UI: 1 (para criar uma interface interativa).

**Orçamento:**

- Pessoal: Salários da equipa;

- Infraestrutura: Servidores, serviços de nuvem, ferramentas de desenvolvimento;

- Marketing: Campanhas para divulgação da plataforma.

**Aplicações Utilizadas**

**Frontend:**

- React ou Angular para construção de interfaces interativas;

- Bootstrap ou Tailwind CSS para design responsivo.

(escolher um)

**Backend:**

- Node.js ou Django para a criação do servidor e API;

- Express.js (se usar Node.js) para administrar as rotas.

(escolher um)

**Base de Dados:**

- MongoDB ou PostgreSQL para armazenar os dados de rastreamento e de análise.

(escolher um)

**Análise de Dados:**

- Python com bibliotecas como Pandas e NumPy para análise de dados;

- Elasticsearch para procurar e analisar grandes quantidades de dados.

**Segurança:**

- OWASP ZAP ou Burp Suite para testes de segurança.

- SSL/TLS para criptografar a comunicação entre clientes e servidores.

(escolher um)

**Monitoramento e Manutenção:**

- Grafana e Prometheus para monitoramento do desempenho da aplicação;

- Sentry para rastreamento de erros em tempo real.

**Propriedade Intelectual**

**Direitos Autorais:**

- Protegem o código-fonte e a documentação do RansomTracker, 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 RansomTracker 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**

**Registro de Direitos:**

- Registar direitos autorais, patentes e marcas para proteção legal.

**Monitoramento:**

- Implementar um sistema para monitorar o uso não autorizado da propriedade intelectual.

**Educação da Equipe:**

- Treinar a equipe sobre a importância da propriedade intelectual e as melhores práticas de proteção.

- normas e ética, (desenvolver)

**Licenças de Software:**

- Decidir sobre o tipo de licença a ser utilizada (open-source ou proprietária).

(escolher e aprofundar como obter a mesma)

**Parcerias e Colaborações:**

- Definir claramente os termos de uso da propriedade intelectual em colaborações.

uml classes