Blacklist
Visão

Introdução

Este documento organiza as ideias e conceitos explorados na Lean Inception do dia 06 de abril, durante a disciplina de Análise e Projeto de Software. O projeto Blacklist visa desenvolver um MVP (Produto Mínimo Viável) para um software web multicliente e sem fins lucrativos, com o objetivo de diminuir a quantidade de golpes cibernéticos aplicados pelo mundo.

Grupo **Sechura**

Membros do grupo:

- Luiz Gustavo da Costa
- Gustavo Maxwel
- Augusto Estevão
- Henrique Almeida
- Caio Alencar
- Gabriel Santos

Posicionamento

Declaração do problema

O problema de	*falhas de segurança web,*
afeta	*Potencialmente todos os usuários na web,*
cujo impacto é	*Diversos pois podem ser monetários, de reputação, de integridade e etc,*
uma solução de sucesso deveria	*Prevenir que o usuário caia nesses golpes cibernéticos.*

Declaração da visão do software

Para	*usuários de navegadores web,*
Que	*possuem fragilidades de segurança,*
O (nome do produto)	*Blacklist é um software agregado de segurança,*
Que	*reduz riscos, dificultando a invasão do sistema,*
Diferente de	*Avast,*
Nosso produto	*possui mais funcionalidades.*

Descrição das partes interessadas

Resumo das partes interessadas

Nome	**Descrição**	**Responsabilidades**
Usuários Finais	Usuários comuns de navegadores web que desejam proteger seus dispositivos.	• Utiliza o produto • Avaliar a eficácia e usabilidade do software
Desenvolvedores	Equipe responsável pelo desenvolvimento e manutenção do Blacklist.	• Desenvolver e manter o software • Integrar novas funcionalidades e atualizações de segurança • Testar e garantir a qualidade do software
Empresas Parceiras em Potencial	Organizações que podem colaborar ou patrocinar o projeto Blacklist.	• Fornecer feedback e sugestões para melhorias • Participar de testes e validações do software • Colaborar com iniciativas de marketing e divulgação do Blacklist
Administradores de TI	Profissionais responsáveis pela gestão e segurança dos sistemas de TI nas organizações.	• Configurar e administrar o Blacklist nas redes e sistemas corporativos • Monitorar incidentes de segurança e responder a ameaças
Analistas de Segurança	Especialistas em segurança da informação encarregados de avaliar e mitigar riscos cibernéticos.	• Avaliar a eficácia das funcionalidades de segurança do Blacklist • Realizar análises de ameaças e recomendações de melhorias
Auditoria e Conformidade	Departamentos ou profissionais responsáveis pela auditoria e conformidade regulatória.	• Avaliar a conformidade do Blacklist com padrões e regulamentações de segurança • Garantir que o software atenda a requisitos legais e regulatórios

Contexto de negócio

Número de Usuários:

- Variedade de usuários, desde indivíduos preocupados com a segurança de seus dispositivos até grandes organizações empresariais que necessitam proteger seus sistemas e dados sensíveis.

Ciclo de Tarefas:

- Inclui desde a instalação e configuração inicial do Blacklist até a manutenção contínua, monitoramento de ameaças em tempo real, resposta a incidentes de segurança e implementação de melhorias e atualizações.

Ambiente de Trabalho:

- Principalmente em ambientes corporativos, mas também abrangendo usuários domésticos que buscam proteção contra ameaças cibernéticas ao navegar na internet.

Plataformas de Sistema:

- O Blacklist deve ser compatível com uma variedade de plataformas, incluindo diferentes navegadores web (Google Chrome, Mozilla Firefox, Microsoft Edge, etc.) e sistemas operacionais (Windows, macOS, Linux).

Integração com Outros Aplicativos/Sistemas:

- Possibilidade de integração com sistemas de gestão de segurança, firewalls, bancos de dados, APIs de segurança, entre outros, para garantir uma abordagem holística e integrada à segurança cibernética.

Restrições Ambientais:

- Adaptação às diversas restrições ambientais, como acesso móvel, ambientes externos, restrições de rede (Wi-Fi público, VPNs corporativas), garantindo a funcionalidade e segurança em diferentes cenários de uso.

Visão geral do produto

Necessidades e funcionalidades

[Evite os detalhes técnicos. Mantenha as descrições das funcionalidades em um nível geral. Concentre-se nas funcionalidades necessárias e por que (não como) elas devem ser desenvolvidas. Necessidade tem relação com o problema, o negócio. Funcionalidade é da solução, ou seja, do software. Capture a prioridade das partes interessadas e informe o membro do grupo responsável pela funcionalidade.]

Necessidade	**Funcionalidade**	**Prioridade**	**Responsável**
Análise de E-mails Suspeitos	Analisar cabeçalhos de e-mails para detecção de possíveis ameaças. Verificar a autenticidade de e-mails pessoais e corporativos. Manter uma lista atualizada de e-mails suspeitos. Verificar o conteúdo do e-mail recebido Checar links suspeitos	Alta	
Segurança na Navegação Web	Identificar e alertar sobre sites falsos ou maliciosos. Garantir uma navegação segura por meio de bloqueios proativos.	Alta	
Verificação de Credibilidade de Informações	Utilizar técnicas de IA para verificar a veracidade de notícias e informações. Apresentar selos de verificação de fontes confiáveis.	Média	
Monitoramento e Relatórios de Segurança	Monitorar atividades suspeitas em tempo real. Gerar relatórios detalhados sobre incidentes e tendências de segurança.	Média	
Integração e Colaboração com Parceiros	Facilitar a integração com sistemas de segurança existentes. Permitir colaboração e compartilhamento de informações com empresas parceiras.	Baixa	

Requisitos não funcionais preliminares

Nesta fase preliminar, foram identificados os seguintes requisitos não funcionais, que serão detalhados e refinados ao longo do processo de desenvolvimento do Blacklist:

Padrões Aplicáveis, Hardware e Requisitos de Plataforma

- O Blacklist deverá seguir os padrões de segurança cibernética reconhecidos internacionalmente, como ISO/IEC 27001 e NIST Cybersecurity Framework.
- Quanto ao hardware, o sistema deve ser capaz de rodar em ambientes de servidor web comum, sem a necessidade de hardware especializado.
- Os requisitos de plataforma incluem suporte para navegadores web modernos, como Chrome, Firefox, Edge e Safari, em suas versões mais recentes.

Requisitos de Desempenho

- Tempo de resposta: O sistema deve responder às solicitações dos usuários em um tempo médio de X segundos, para garantir uma experiência ágil.
- Capacidade de processamento: O Blacklist deve suportar um número estimado de X usuários simultâneos, sem degradação significativa no desempenho.
- Escalabilidade: O sistema deve ser dimensionável para lidar com um aumento de X% no volume de dados e tráfego, conforme necessário.

Requisitos Ambientais

- O software deve ser desenvolvido levando em consideração questões ambientais, como consumo de energia e impacto ambiental mínimo durante sua operação.
- Considerações de acessibilidade devem ser incluídas, garantindo que o Blacklist seja utilizável por pessoas com diferentes capacidades e necessidades.

Qualidade e Robustez

- O sistema deve demonstrar alta robustez, resistindo a ataques de segurança conhecidos e mantendo a integridade dos dados mesmo em situações adversas.
- A tolerância a falhas deve ser implementada, garantindo que o Blacklist seja capaz de se recuperar automaticamente de falhas de hardware ou software.

Usabilidade

- A interface do usuário deve ser intuitiva e amigável, com elementos de design que facilitem a navegação e compreensão das funcionalidades do sistema.
- A documentação do usuário, incluindo manuais, guias de uso e ajuda online, deve estar disponível e ser de fácil acesso para os usuários.

Documentação e Embalagem

- Todos os requisitos do Blacklist devem ser documentados de forma clara e precisa, incluindo manuais do usuário, guias de instalação e requisitos de configuração.
- O produto final deve ser adequadamente embalado e rotulado, seguindo as normas de embalagem e rotulagem relevantes para software de segurança cibernética.

Requisito não funcional	**Prioridade**
Padrões Aplicáveis, Hardware e Plataforma	Baixa
Desempenho	Alta
Robustez	Alta
Tolerância a Falhas	Alta
Usabilidade	Alta
Acessibilidade	Média
Qualidade e Confiabilidade	Alta

Documentação e Embalagem	Baixa
Segurança	Alta
Ambientais	Baixa