🛡️Visão do Produto: Project Aegis

1. Visão Geral

- Para: Profissionais de TI, analistas de segurança e pequenas/médias empresas
- Que: Se sentem sobrecarregados com o volume de notícias e dados de segurança dispersos pela internet, dificultando a compreensão do real cenário de ameaças.
- O: Project Aegis
- É uma: Plataforma de inteligência de ameaças cibernéticas
- Que: Agrega, correlaciona e visualiza dados de fontes públicas confiáveis em um painel único e intuitivo.
- Diferente de: Feeds de dados brutos (como listas de CVEs) e soluções corporativas complexas e caras,
- Nosso produto: Democratiza o acesso à inteligência de ameaças, traduzindo dados complexos em insights claros e acionáveis para uma tomada de decisão mais rápida e eficaz.

---

2. O Problema

No cenário atual, a informação sobre cibersegurança é abundante, mas fragmentada e caótica. Profissionais e empresas enfrentam os seguintes desafios:

- **Sobrecarga de Informação:** São bombardeados diariamente com notícias sobre vazamentos, novas vulnerabilidades (CVEs) e malwares em dezenas de sites, blogs e redes sociais.
- **Falta de Contexto:** Os dados são desconexos. Uma lista de CVEs não informa qual malware está explorando ativamente aquela falha. Uma notícia sobre um vazamento não se conecta facilmente aos vetores de ataque utilizados.
- **Alto Custo de Ferramentas:** As soluções de ponta que fazem essa centralização são extremamente caras, deixando estudantes, pesquisadores e, principalmente, pequenas e médias empresas sem acesso a inteligência de qualidade.
- **Ação Reativa e Lenta:** A necessidade de "juntar as peças" manualmente consome um tempo precioso, atrasando a implementação de medidas de proteção e tornando as respostas a incidentes mais lentas.

---

3. O Público-Alvo

Nosso foco inicial é atender a dois perfis principais:

- Persona 1: O Analista de Segurança (Júnior a Pleno) / Estudante
    - **Objetivos:** Manter-se atualizado sobre as últimas tendências, entender a relevância de novas vulnerabilidades, gerar relatórios e aprofundar seu conhecimento prático.

    - **Frustrações:** Perder tempo compilando dados de várias fontes, dificuldade em visualizar o "quadro geral" das ameaças e falta de ferramentas acessíveis para análise.
- Persona 2: O Gestor de TI em uma Pequena/Média Empresa (PME)
    - **Objetivos:** Proteger a infraestrutura da empresa com recursos limitados, tomar decisões informadas sobre onde investir em segurança e justificar esses investimentos para a diretoria.
    - **Frustrações:** Não é um especialista em cibersegurança, não tem tempo para pesquisas aprofundadas e precisa de informações diretas e acionáveis, não de dados técnicos brutos.

---

4. A Solução: Project Aegis

O Project Aegis é um painel analítico (dashboard) projetado para ser o **ponto central de inteligência de ameaças**. Nossa solução irá:

1. **Coletar:** Monitorar e extrair dados de fontes públicas e confiáveis (ex: MITRE para CVEs, notícias de portais especializados em segurança, feeds de IOCs - Indicadores de Comprometimento).
2. **Processar:** Estruturar e correlacionar esses dados, conectando uma vulnerabilidade a um tipo de malware ou um vazamento de dados a um setor industrial específico.
3. **Visualizar:** Apresentar as informações em um dashboard interativo, com gráficos e mapas que revelam padrões, tendências e os riscos mais iminentes de forma clara e compreensível.

Em essência, transformamos o ruído de dados em um sinal claro de inteligência.

---

5. Principais Funcionalidades (Visão de Longo Prazo)

Para entregar o valor principal, o Aegis se concentrará em:

- **Dashboard Centralizado e Interativo:** Uma visão "em uma única tela" das ameaças mais relevantes, setores mais atacados, tipos de malware em ascensão e as vulnerabilidades mais críticas do momento.
- **Feed de Ameaças Agregado:** Uma linha do tempo unificada com as últimas notícias sobre vazamentos, divulgação de CVEs e análises de malware, tudo em um só lugar.
- **Busca e Filtros Avançados:** Permitir que o usuário pesquise por uma ameaça específica (ex: "Log4j") ou filtre a visualização por setor, país ou período de tempo.
- **Sistema de Alertas Personalizados:** (Funcionalidade futura) Capacidade do usuário de configurar alertas para ser notificado sobre ameaças relacionadas a tecnologias ou setores de seu interesse.

---

6. Análise de Concorrência e Diferenciais

Concorrente / Alternativa	Pontos Fortes	Pontos Fracos (Nossa Oportunidade)
Feeds Públicos e Notícias	Gratuito, fonte primária da informação.	Dados brutos, sem contexto, alta sobrecarga manual, desconexos.
Soluções Corporativas (Ex: Mandiant)	Análise extremamente profunda, inteligência proprietária.	Custo proibitivo para PMEs e usuários individuais, complexidade elevada.

Nosso Diferencial Competitivo: O Project Aegis se posiciona exatamente no meio. Oferecemos a **simplicidade** e a **acessibilidade** dos feeds públicos com o poder da **contextualização** e **visualização** das ferramentas caras, focando em ser a melhor solução para quem precisa de inteligência acionável sem complexidade ou alto custo.

---

7. Objetivos de Negócio (Alinhados à Fase do Projeto)

- Fase 1 (Protótipo/MVP):
  - **Validar a hipótese** de que a centralização e visualização de dados de ameaças gera valor para nosso público-alvo.
  - **Construir um protótipo funcional** que sirva como prova de conceito para definir os requisitos da solução final.
  - **Ser a base para o desenvolvimento** do Projeto Integrador, demonstrando a viabilidade técnica e a relevância da solução.
- Longo Prazo (Visão Futura):
  - Tornar-se uma ferramenta de referência para a comunidade de segurança no Brasil.
  - Criar uma base de usuários engajada para, potencialmente, explorar um modelo *freemium* com funcionalidades avançadas para empresas.

---

8. Referências Bibliográficas:

BROWN, Andrew. Data Breaches: The Cyber Security Handbook. Stroud: Amberley Publishing, 2020. 208 p.

Disponível em: https://www.amberley-books.com/data-breaches.html.

CONSELHO ON FOREIGN RELATIONS. Cyber Operations Tracker. New York, 2025. Disponível em: https://www.cfr.org/cyber-operations/.

GOOGLE. Gemini: [Fonte de Pesquisa para encontrar artigos referentes a vazamentos de dados]. Disponível em: https://gemini.google.com/