CENTRO UNIVERSITÁRIO DE BRASÍLIA
CIÊNCIA DA COMPUTAÇÃO

FELIPE BARCELOS DE CARVALHO (RA: 22350044)
MARCOS VINICIUS ROCHA (RA: 22352865)
JOÃO MARCELO GUIMARÃES DOURADO (RA: 22350653)
EDUARDO ARAÚJO UCHOA (RA: 22353207)
DAVI MAIA (RA: 22305561)

PROJECT AEGIS:
PAINEL DE INTELIGÊNCIA DE AMEAÇAS

BRASÍLIA
2025

Backlog inicial com histórias de usuário

História de Usuário 1: Listar e validar fontes confiáveis de CVEs e vazamentos, para que os dados apresentados no dashboard tenham credibilidade.

Critério de Aceitação: Pelo menos 3 fontes principais definidas (ex: NVD, CVE Mitre, Have I Been Pwned).

Prioridade: Alta

História de Usuário 2: Coletar uma amostra de dados dos últimos 6 meses, para que possamos popular o protótipo com informações reais.

Critério de Aceitação: Planilha estruturada contendo: Data, Tipo de Ameaça, Severidade (CVSS), Setor Afetado.

Prioridade: Alta

História de Usuário 3: Categorizar os vetores de ataque na amostra coletada, para que possamos identificar padrões recorrentes.

Critério de Aceitação: Dados classificados por vetor (ex: Phishing, Ransomware, Exploit de vulnerabilidade conhecida).

Prioridade: Média

História de Usuário 4: Visualizar um gráfico de "Ameaças por Severidade" na tela inicial, para que eu possa entender rapidamente o nível de criticidade do cenário atual.

Critério de Aceitação: Protótipo exibe gráfico com divisão clara (Crítico, Alto, Médio, Baixo) baseado nos dados reais coletados.

Prioridade: Alta

História de Usuário 5: Filtrar a visualização por "Setor Afetado" (ex: financeiro, saúde), para que eu possa personalizar a análise para meu contexto.

Critério de Aceitação: Protótipo deve ter a interface de filtros

(dropdowns/checkboxes), mesmo que apenas simule a filtragem em uma ou duas telas de exemplo.

Prioridade: Média

História de Usuário 6: Clicar em um card de ameaça recente para ver detalhes, para que eu entenda o impacto específico daquela vulnerabilidade.

Critério de Aceitação: Tela de "Detalhes da Ameaça" desenhada com campos para: Descrição, CVSS, Data de Divulgação e Medidas de Mitigação recomendadas.

Prioridade: Média

História de Usuário 7: Gerar um relatório de tendências a partir do protótipo, para justificar a necessidade de desenvolvimento completo do Aegis.

Critério de Aceitação: Relatório destacando pelo menos 3 insights descobertos (ex: "Aumento de 20% em ataques ao setor financeiro").

Prioridade: Alta

Backlog do Produto (Refinado)

1. **[Alta] Automação de Coleta CVE:** Como desenvolvedor, quero um script Python que consulte a API do NIST/NVD automaticamente, para não precisar baixar planilhas manualmente.
2. **[Alta] Monitoramento de Vazamentos:** Como usuário, quero visualizar as empresas com vazamentos recentes (HIBP), para saber se preciso trocar senhas.
3. **[Média] Gráfico de Mapa/Países:** Como analista, quero ver a origem dos IPs maliciosos em um gráfico, para identificar países ofensores.
4. **[Crítica] Infraestrutura Serverless:** Como DevOps, quero configurar o GitHub Actions para rodar os scripts todo dia às 06h e 18h, garantindo custo zero de servidor.
5. **[Alta] Segurança de Credenciais:** Como arquiteto, quero usar Variáveis de Ambiente (Secrets) no repositório, para não expor minhas chaves de API no código público.