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

Documento de Definição do Problema e Oportunidades Identificadas

1. Introdução

No atual cenário digital, as ameaças cibernéticas se desenvolvem diariamente se tornando cada vez mais complexas, exigindo que profissionais e organizações estejam constantemente atualizados para proteger seus ativos digitais. Contudo, a fragmentação das informações disponíveis sobre riscos e ataques digitais dificulta a compreensão clara desse cenário, comprometendo a capacidade de resposta eficiente.

O **Project Aegis** propõe como solução um Painel de Inteligência de Ameaças que centraliza dados críticos provenientes de diversas fontes públicas e confiáveis. Por meio de um dashboard analítico, o projeto visa coletar, processar e apresentar informações relevantes sobre as ameaças digitais de forma clara, intuitiva e acessível, facilitando a análise e a tomada de decisão dos usuários.

Este documento tem como objetivo definir o problema da fragmentação de informações no contexto da cibersegurança e identificar as oportunidades que o Project Aegis pode explorar para entregar valor significativo aos seus usuários.

2. Descrição do Problema

No cenário atual de cibersegurança, as informações sobre ameaças digitais estão dispersas em múltiplas fontes, muitas vezes fragmentadas e difíceis de serem integradas. Essa fragmentação gera diversos desafios para profissionais e organizações que precisam monitorar e responder a riscos em tempo real.

O principal problema enfrentado é a **falta de centralização e clareza nas informações de inteligência de ameaças**, o que dificulta a compreensão do cenário geral, a identificação de tendências e a priorização de respostas eficazes. Essa dispersão pode levar a atrasos na detecção de ameaças, respostas inadequadas e, consequentemente, a maiores riscos de ataques bem-sucedidos.

Além disso, é comum que dashboards e ferramentas existentes apresentem dados complexos, pouco intuitivos, ou com fontes pouco confiáveis, o que impacta negativamente na tomada de decisão dos usuários.

Impactos do problema:

A situação atual representa dificuldade para o usuário em obter uma visão única e atual das ameaças digitais ocorrentes, gerando um aumento do tempo e esforço para efetuar uma análise e resposta a incidentes. A falta de uma solução centralizada também colabora para a tomada de decisões possivelmente precipitadas, com base em informações

incompletas ou desatualizadas, e portanto resultando em maior exposição a riscos e vulnerabilidades

De acordo com o relatório de CiberSegurança 2025 da BrassCom, o Brasil é o país que mais sofre ataques cibernéticos globalmente. Somente no ano de 2023, foram registradas cerca de 60 bilhões de tentativas de invasões. Já em março de 2025, aproximadamente 38% da população brasileira foi vítima de golpes ou sofreu tentativas de fraude bancária.

source

Quem é afetado:

Profissionais de Cibersegurança — Enfrentam dificuldades para monitorar, analisar e responder rapidamente às ameaças digitais devido à dispersão e complexidade das informações disponíveis. Isso compromete a eficiência e a eficácia do trabalho deles.

Organizações e Empresas — A falta de centralização e clareza nas informações de inteligência de ameaças aumenta o risco de ataques cibernéticos bem-sucedidos, o que pode causar prejuízos financeiros, perda de dados e danos à reputação.

Usuários Finais e Clientes — Indivíduos que utilizam serviços digitais, como bancos e plataformas online, estão vulneráveis a golpes e fraudes, como indicado pelo alto percentual da população brasileira que sofreu tentativas de fraude bancária.

Tomadores de Decisão — Gestores e líderes que dependem de informações confiáveis para planejar estratégias de segurança e resposta a incidentes são prejudicados pela falta de dados centralizados e claros, o que pode levar a decisões erradas ou tardias.

Evidências:

A Brasscom (Associação das Empresas de Tecnologia da Informação e Comunicação) reportou que o Brasil registrou cerca de **60 bilhões de tentativas de ataques cibernéticos** em 2023. source

No primeiro semestre de 2025, conforme o relatório do Fortinet (via laboratório FortiGuard), foram detectadas cerca de **314,8 bilhões de atividades maliciosas** voltadas ao Brasil. source

Segundo o relatório da SOCRadar para o Brasil, foram registrados **372.825 ataques DDoS** no ano de 2023. source

Um relatório da Kaspersky aponta que em 2024 pelo menos **105 organizações brasileiras** foram vítimas de ataques de ransomware, com algumas vítimas sendo

atacadas mais de uma vez, o que evidencia tanto a frequência como a reincidência. source

O Brasil participou com cerca de 41,78 % de todos os ataques DDoS na América Latina no primeiro semestre de 2023 — ou seja, quase metade dos incidentes regionais foram no Brasil. source

---

3. Análise das Causas

A fragmentação das informações de inteligência de ameaças no campo da cibersegurança decorre de um conjunto de causas interligadas, tanto estruturais quanto operacionais, que comprometem a capacidade das organizações de compreender e reagir de forma eficaz ao cenário de riscos digitais. Entre as causas principais, destaca-se a **falta de integração entre as diversas fontes de dados de segurança disponíveis**. As informações sobre ameaças cibernéticas são disseminadas por múltiplas origens, como feeds de inteligência, relatórios de empresas especializadas, bancos de dados de vulnerabilidades e comunidades técnicas, cada uma utilizando formatos e métricas próprios. Isso dificulta a consolidação das informações e a construção de uma visão unificada das ameaças em curso.

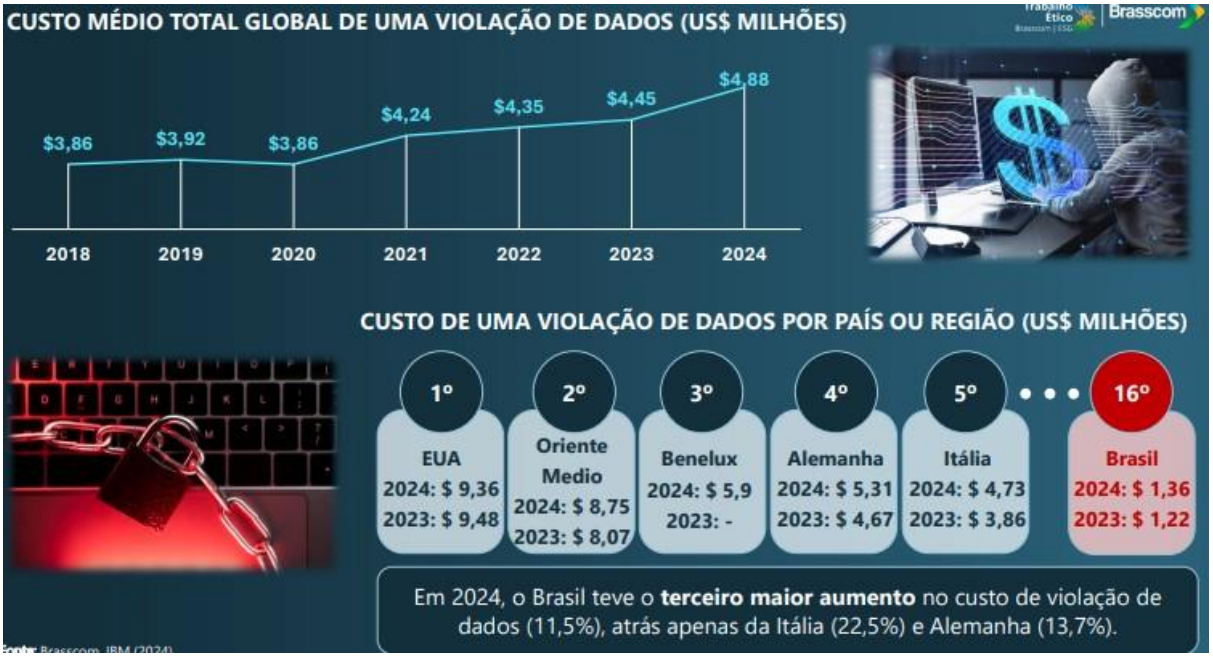
Outro fator relevante é a ausência de plataformas unificadas e acessíveis que centralizem a coleta, o processamento e a visualização desses dados. As soluções existentes são, em sua maioria, proprietárias e de alto custo, voltadas a grandes corporações, o que impede que profissionais independentes e pequenas empresas tenham acesso a sistemas de inteligência de ameaças integrados. Soma-se a isso o crescimento exponencial do volume e da complexidade dos dados gerados diariamente, tornando inviável o monitoramento manual de todas as fontes.

Entre as causas secundárias, observa-se a carência de profissionais especializados em inteligência de ameaças, um problema global que se manifesta de forma acentuada no Brasil. Mesmo quando os dados estão disponíveis, a falta de especialistas capazes de interpretá-los e transformá-los em ações estratégicas limita a efetividade das respostas. Muitas empresas ainda dependem de fontes públicas de dados incompletas ou desatualizadas, o que leva à tomada de decisões baseadas em informações imprecisas.

As limitações orçamentárias também exercem papel significativo, sobretudo entre pequenas e médias empresas que não dispõem de recursos financeiros para investir em soluções robustas de monitoramento. Finalmente, a ausência de uma cultura organizacional voltada à inteligência de ameaças contribui para a manutenção de uma postura predominantemente reativa diante de incidentes de segurança, em vez de uma abordagem preventiva baseada na análise contínua de tendências.

Dessa forma, o conjunto dessas causas justifica a relevância do **Project Aegis**, que propõe a criação de um painel de inteligência de ameaças centralizado, acessível e padronizado, capaz de integrar múltiplas fontes de dados, oferecer visualização contextualizada e democratizar o acesso à informação estratégica em cibersegurança. Essa solução busca mitigar os efeitos da fragmentação informacional e aprimorar a capacidade de análise e tomada de decisão dos profissionais e organizações diante do cenário crescente de ameaças digitais.


BRASIL É UM DOS MAIORES ALVOS DE ATAQUES CIBERNÉTICOS NO MUNDO
Brasil sofreu 60 bilhões de tentativas de ataques cibernéticos em 2023, enquanto em 2022 registrou um total de 103 bilhões
Em 2023, o montante de tentativas de ataques direcionados à América Latina foi de 200 bilhões, 14,5% do total global nesse ano
93% dos líderes cibernéticos e 86% dos líderes empresariais acreditam que a instabilidade geopolítica pode desencadear um evento cibernético de grande escala nos próximos dois anos. (WEF, 2024)
Fonte: Brasscom, FortiGuard Labs (Fortinet), WEF, NetScout


CUSTO MÉDIO TOTAL GLOBAL DE UMA VIOLAÇÃO DE DADOS (US$ MILHÕES)
Brasscom
$3,86
$3,92
$3,86
$4,24
$4,35
$4,45
$4,88
2018
2019
2020
2021
2022
2023
2024
CUSTO DE UMA VIOLAÇÃO DE DADOS POR PAÍS OU REGIÃO (US$ MILHÕES)
1º EUA 2024: $ 9,36 2023: $ 9,48
2º Oriente Medio 2024: $ 8,75 2023: $ 8,07
3º Benelux 2024: $ 5,9 2023: -
4º Alemanha 2024: $ 5,31 2023: $ 4,67
5º Itália 2024: $ 4,73 2023: $ 3,86
16º Brasil 2024: $ 1,36 2023: $ 1,22
Em 2024, o Brasil teve o terceiro maior aumento no custo de violação de dados (11,5%), atrás apenas da Itália (22,5%) e Alemanha (13,7%).

4. Oportunidades Identificadas

A crescente digitalização da economia global, impulsionada pela transformação digital, tem ampliado significativamente o espectro de riscos cibernéticos enfrentados por organizações públicas e privadas. Entretanto, esse cenário também cria um terreno fértil para o surgimento de novas oportunidades no campo da cibersegurança, especialmente no desenvolvimento de soluções inovadoras voltadas à inteligência de ameaças e à proteção digital.

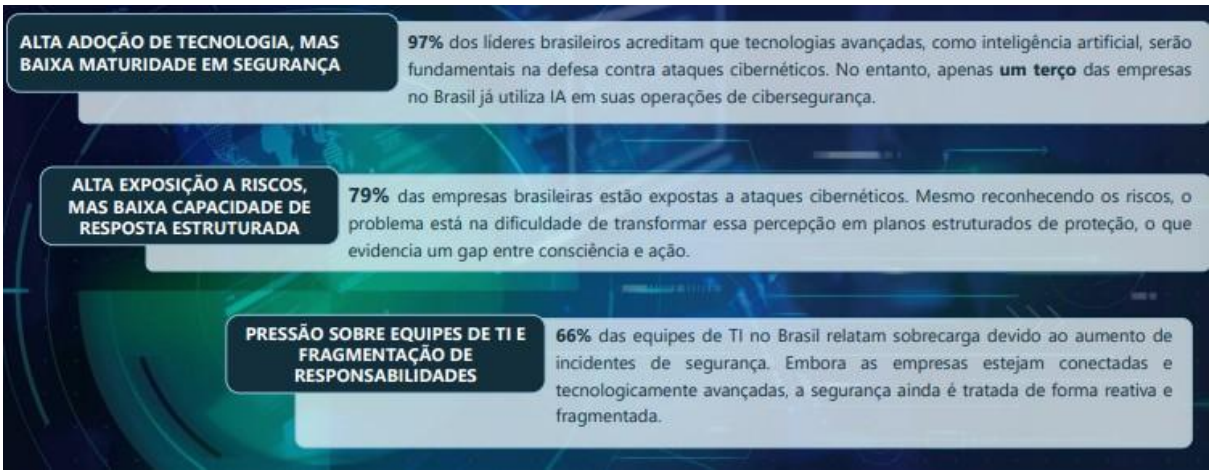
De acordo com o **Relatório de Cibersegurança 2025 da Brasscom**, o aumento expressivo dos investimentos em segurança digital representa uma oportunidade concreta para o setor de Tecnologia da Informação. À medida que empresas e governos intensificam seus esforços para mitigar riscos e fortalecer sua postura de segurança, observa-se uma crescente demanda por serviços especializados, plataformas analíticas e ferramentas de monitoramento avançado. Essa expansão do mercado cria espaço para o desenvolvimento de produtos tecnológicos, capazes de combinar automação, integração de dados e usabilidade, características que se alinham à proposta do **Project Aegis**.

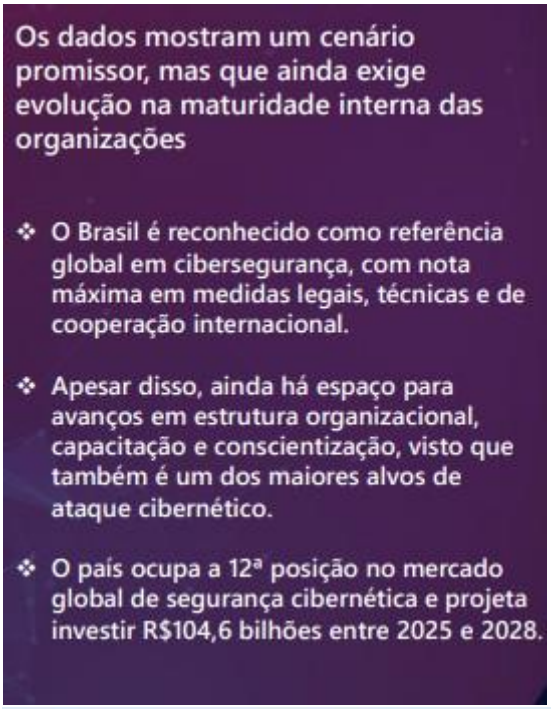
Além do aspecto econômico, o Brasil apresenta um contexto estratégico singular na América Latina. O país é o único da região a alcançar alta pontuação em maturidade de cibersegurança e figura entre os dois únicos do continente americano classificados no **Tier 1** da nova metodologia adotada pela quinta edição do **Global Cybersecurity Index (GCI)**, elaborado pela **União Internacional das Telecomunicações (UIT)**. Essa posição de destaque reflete o comprometimento nacional com a **Agenda Global de Segurança Cibernética**, evidenciando o potencial do país como referência regional em políticas, iniciativas e soluções tecnológicas voltadas à proteção digital.

Entretanto, o mesmo relatório do GCI identifica que, entre os cinco pilares que compõem o índice, o Brasil ainda possui oportunidades de avanço em dois aspectos fundamentais: **estruturas organizacionais** e **capacitação em cibersegurança**. O primeiro pilar relaciona-se ao fortalecimento da governança institucional e da coordenação entre entidades públicas, privadas e acadêmicas, enquanto o segundo envolve a promoção de programas de formação, conscientização e desenvolvimento de competências digitais. Nesse sentido, projetos que contribuam para a difusão do conhecimento, o aprimoramento das práticas de análise de ameaças e a democratização do acesso à informação técnica têm grande potencial de impacto positivo.

Diante desse panorama, o **Project Aegis** posiciona-se como uma iniciativa alinhada às tendências globais e às necessidades nacionais. Ao propor a criação de um painel centralizado de inteligência de ameaças, o projeto não apenas responde ao problema da fragmentação de informações, mas também explora uma oportunidade de mercado em expansão, associando inovação tecnológica, acessibilidade e valor estratégico. Além disso, a plataforma pode servir como ferramenta de apoio à formação profissional, ao

oferecer uma interface didática e baseada em dados reais, fortalecendo o ecossistema de cibersegurança brasileiro.





---

5. Conclusão

- Resumo dos principais pontos.
-
- A ser desenvolvido…