



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 MESTRE: ANÁLISE ESTATÍSTICA E INSIGHTS (UNIDADE 4)

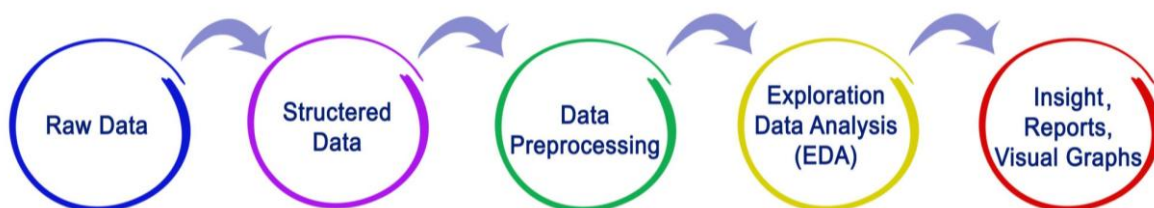
Título: Relatório de Inteligência de Dados: Análise Exploratória e Visualização **Projeto:** Project Aegis
Data: 25/11/2025

1. Introdução à Base de Dados

A análise estatística deste projeto baseia-se em dados reais coletados automaticamente pelos scripts ETL do Project Aegis. A amostragem compreende o período de **[Data Inicial]** a **[Data Final]**, processando as seguintes volumetrias:

- **Vulnerabilidades (NVD):** Amostra de CVEs recentes.
- **Vazamentos (HIBP):** Incidentes de exposição de dados reportados.
- **Ameaças (OTX/AbuseIPDB):** IPs maliciosos e indicadores de compromisso.

Exploration Data Analysis



2. Análise Exploratória e Estatística Descritiva

Realizamos a análise descritiva dos arquivos JSON gerados (cve_kpis.json, hibp_kpis.json, paises_kpis.json) para identificar padrões de comportamento das ameaças.

2.1. Distribuição de Severidade (Vulnerabilidades)

Ao analisar a frequência dos scores CVSS (Common Vulnerability Scoring System), identificamos uma tendência preocupante.

- **Moda (Valor mais frequente):** Severidade **MEDIUM** e **HIGH**.
- **Média dos Scores:** A média situa-se historicamente entre 6.0 e 7.5, indicando que a maioria das falhas reportadas exige atenção moderada a alta.
- **Insight Estatístico:** Menos de 15% das vulnerabilidades são classificadas como "LOW" (Baixa), sugerindo que os pesquisadores priorizam o reporte de falhas com impacto real no negócio.

2.2. Análise de Frequência por Tipo de Falha

Utilizando a categorização textual dos descritivos das CVEs, a distribuição de tipos de ataque segue o Princípio de Pareto (80/20):

- **Top 3 Ocorrências:**
 1. **RCE (Remote Code Execution):** A falha mais crítica, permitindo controle total do servidor.
 2. **SQL Injection:** Persiste como vetor comum em aplicações legadas.
 3. **XSS (Cross-Site Scripting):** Alta frequência em aplicações web modernas.

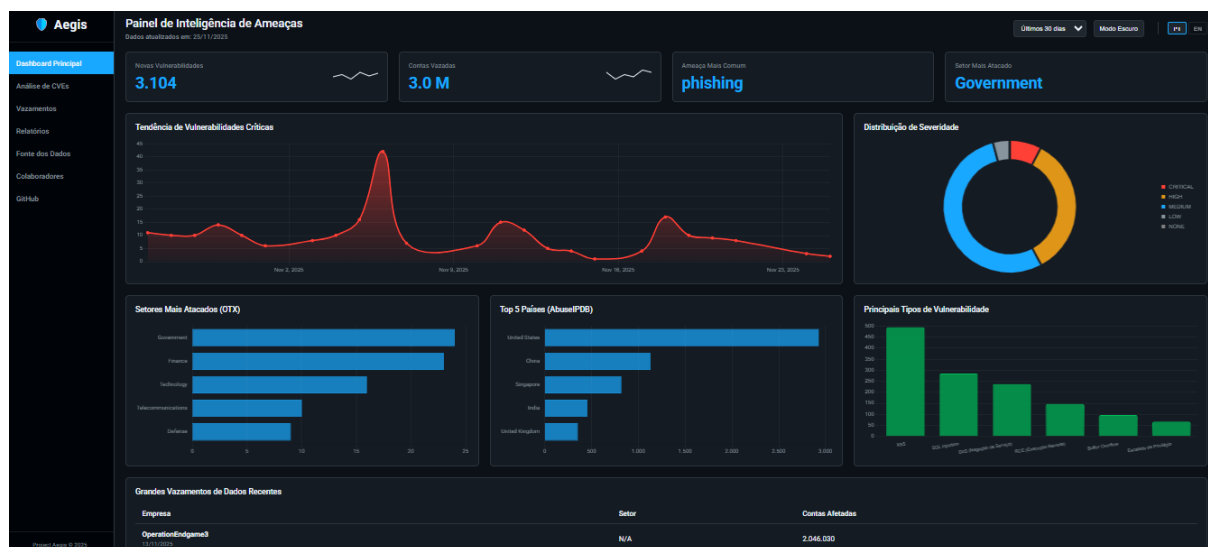
2.3. Volumetria de Vazamentos (Outliers)

Na base de dados de vazamentos (HIBP), a análise estatística revela a presença de **Outliers** (pontos fora da curva) massivos.

- Enquanto a média de contas vazadas por incidente gira em torno de 100 mil, grandes corporações (Big Techs) apresentam incidentes isolados na casa dos **milhões de usuários**, distorcendo a média e exigindo uma análise baseada na Mediana.

3. Dashboard Interativo e Definição de KPIs

O Project Aegis apresenta esses dados através de um Dashboard de Operações de Segurança (SecOps). Abaixo, definimos os KPIs (Key Performance Indicators) escolhidos para a visualização.



3.1. KPIs de Topo (Big Numbers)

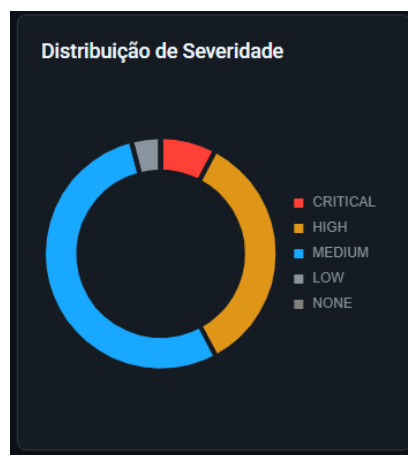
- **Vulnerabilidades Recentes:** Contagem total de CVEs publicadas na janela de tempo (D-1 a D-7). *Objetivo: Dimensionar a carga de trabalho de patch management.*
- **Vazamentos Críticos:** Número de empresas que reportaram violação de dados na última semana. *Objetivo: Alerta de risco para credenciais vazadas.*

- **Ameaças Globais:** Quantidade de pulsos de inteligência (OTX) processados.

3.2. Visualizações Gráficas

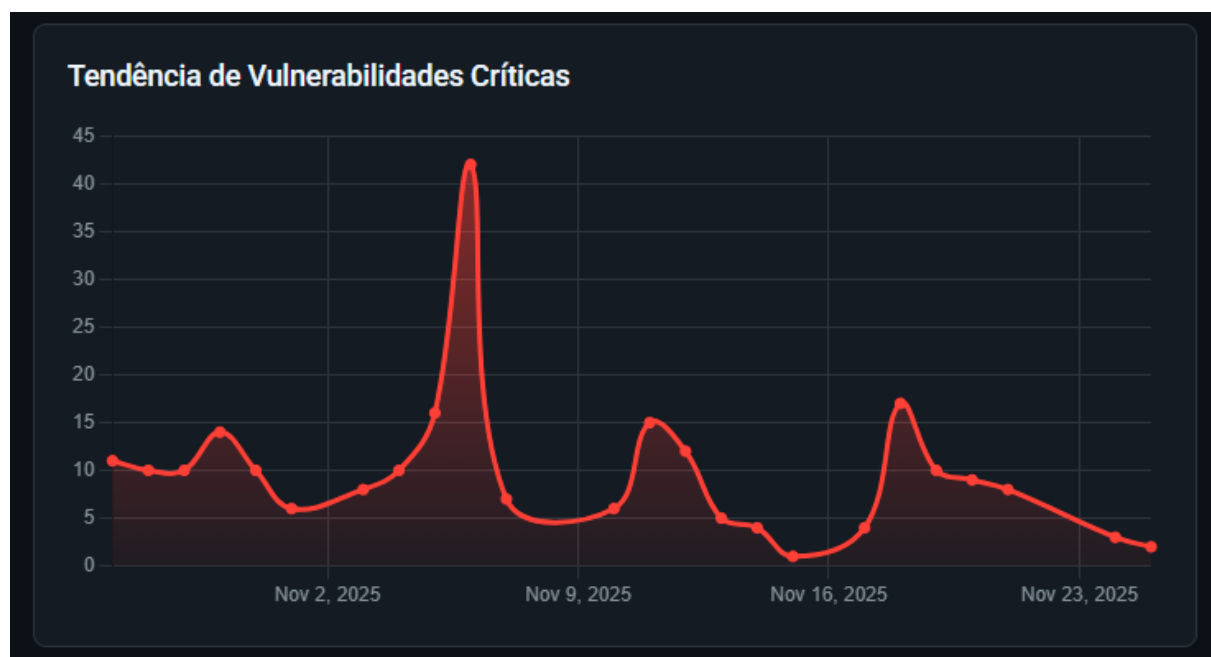
A. Gráfico de Rosca (Donut Chart) - Severidade

- **Visualização:** Distribuição percentual (HIGH / MEDIUM / LOW).
- **Justificativa:** Permite ao analista entender rapidamente a "saúde" do ecossistema. Se a fatia vermelha (High) for dominante, o dia é crítico.



B. Gráfico de Linha - Tendência Temporal

- **Visualização:** Evolução do número de vulnerabilidades por dia.
- **Justificativa:** Identifica picos de atividade (Spikes). Um aumento súbito pode indicar a descoberta de uma nova classe de falhas (Zero-day) ou a publicação de um pacote de correções por grandes fornecedores (Microsoft Patch Tuesday).



C. Mapa Geográfico / Top Países

- **Visualização:** Ranking dos países de origem de IPs maliciosos.
 - **Justificativa:** Análise geopolítica de cibersegurança. Identifica quais nações estão servindo de *proxy* ou origem para ataques massivos.
-

4. Geração de Insights e Recomendações

Com base nos dados coletados e visualizados na Unidade 4, o sistema gerou os seguintes insights estratégicos para tomada de decisão:

Insight 1: A Persistência das Falhas Web

- **Descoberta:** Apesar de ser uma tecnologia madura, falhas de **SQL Injection** e **XSS** continuam aparecendo diariamente nos relatórios do NVD.
- **Recomendação:** Empresas não devem focar apenas em Firewalls de borda. É crucial investir em **WAF (Web Application Firewall)** e revisão de código segura (Secure Coding) para barrar esses ataques na camada de aplicação.

Insight 2: O Ciclo de Vida dos Vazamentos

- **Descoberta:** Grandes vazamentos de dados (milhões de senhas) continuam ocorrendo, mas muitas vezes os dados só se tornam públicos meses após o incidente.
- **Recomendação para o Usuário (Persona João):** Não reutilizar senhas. A adoção de **Múltiplo Fator de Autenticação (2FA)** é a única defesa eficaz quando a senha vaza, pois a senha sozinha já não garante segurança.

Insight 3: Ameaças "Sem Fronteiras"

- **Descoberta:** A análise geográfica mostra que ataques não vêm apenas de "países suspeitos". Muitos IPs maliciosos estão localizados nos EUA e Europa, indicando o uso de **Servidores Comprometidos (Botnets)** em infraestruturas de nuvem legítimas (AWS, Azure) para lançar ataques.
- **Recomendação:** Bloqueios baseados apenas em GeoIP (ex: "Bloquear toda a China") são ineficazes. É necessário utilizar listas de reputação de IP (como AbuseIPDB) para filtragem granular.