📊 1. Frequência de Ataques

Tipo de Ataque	Ocorrências
DDoS	531
Phishing	529
SQL Injection	503
Ransomware	493
Malware	485

🔎 **Interpretação:**

- A base é bem equilibrada, com pequena variação entre os tipos de ataque.

📈 2. Visão Geral da Base

Contém estatísticas agregadas (mínimo, máximo, média, etc.) para os atributos da base completa.

Atributo	Mínimo	Máximo	Média	Mediana
Ano (Year)	2015	2024	2019.57	2020
Prejuízo Financeiro ($M)	0.5	99.98	50.49	49.91
Nº Usuários Afetados	424	1,000,000+	~504 mil	~496 mil
Tempo de Resolução (horas)	1	98	36.48	35

📌 **Insights:**

- A base cobre eventos entre 2015 e 2024.
- Os prejuízos são altos em média (~50 milhões).
- Muitos usuários afetados por ataque (~500 mil).
- O tempo de resposta gira em torno de 36h.

🧠 3. Detalhes por Tipo de Ataque

Exemplos:

- **DDoS**: média de $52M em perdas, 499 mil usuários afetados, tempo médio de resolução: 35h.
- **Malware**: média de $49M, 508 mil usuários afetados, 37h para resolver.
- **Man-in-the-Middle**: $51M, 520 mil usuários, 36h.

📌 **Insights:**

- Os diferentes tipos de ataque têm impacto similar.
- O tempo de resolução varia pouco entre eles (~35–37h).
- Pode haver correlação entre tipo de ataque e severidade (bons preditores para classificação).

🤖 **4. Avaliação Inicial dos Algoritmos**

Métrica	Random Forest	XGBoost
Acurácia	19.0%	17.1%
Precisão (macro)	18.8%	17.0%
Recall (macro)	18.8%	17.1%
F1-Score (macro)	18.6%	17.0%

📌 **Interpretação:**

- Baixa performance geral no teste simplificado.
- **Random Forest** teve desempenho ligeiramente melhor em todas as métricas.

🔁 **5. Validação Cruzada**

Métrica	Random Forest	XGBoost
Acurácia	16.2%	16.6%
Precisão (macro)	15.9%	16.8%
Recall (macro)	15.9%	16.6%
F1-Score (macro)	**15.7%**	**16.6%** ✅

📌 **Conclusão:**

- Apesar de perder no teste simplificado, o **XGBoost** teve desempenho mais consistente na validação cruzada e foi superior no **F1-Score**.
- O XGBoost deve ser considerado o **algoritmo vencedor**.