Title: Analysis of Global Cybersecurity Threats Trends (2015-2024)

Team name: Cyber**Insights**

Member name: Vandan Amin, Chaker Baloch, Aiden Wise

Logo:

1. Introduction to the Dataset

Source

The dataset used for this analysis is derived from the "Global Cybersecurity Threats (2015-2024)" dataset hosted on Kaggle, curated by Atharva Soundankar. This comprehensive dataset aggregates data on cyber incidents from diverse sources, including organizations, governmental cybersecurity agencies, independent security researchers, and global threat intelligence reports. Its extensive coverage ensures representation from multiple countries and industries, providing an in-depth and wide-ranging view of cybersecurity incidents globally.

Purpose

The primary purpose of this dataset is to facilitate detailed analysis and understanding of cybersecurity threats over a decade (2015-2024). By providing granular details on types of threats, attack methods, impacted industries, financial implications, severity levels, and geographical distribution, this dataset enables robust threat intelligence analysis, cybersecurity trend forecasting, and the development of predictive models. This supports enhanced global cybersecurity measures and proactive threat mitigation strategies.

2. Dataset Description

Incident_ID

Type: Numerical
Length/Range: Unique identifier (1 - 100,000+)

Date

Type: Date
Length/Range: 01-01-2015 to 12-31-2024

Threat_Type

Type: Categorical
Length/Range: Malware, Phishing, Ransomware, DDoS, Data Breach

Severity

Type: Categorical
Length/Range: Low, Medium, High, Critical

Industry

Type: Categorical
Length/Range: Finance, Healthcare, Government, Technology, Education, Others

Country

Type: Text/Categorical
Length/Range: Global (various countries worldwide)

Impact

Type: Text

Length/Range: Descriptive text explaining the effect or impact of the cybersecurity threat

Resolution_Status

Type**:** Categorical
Length/Range: Resolved, Unresolved, Mitigated, Investigating

3. Potential Significance and Insights

1. **Trend Analysis**
   By examining cybersecurity threats from 2015 to 2024, we can uncover important trends and patterns, such as increases in specific attack methods like ransomware or phishing. This information allows cybersecurity professionals to better anticipate threats and develop proactive strategies to protect organizations.

2. **Industry Vulnerability**
   Understanding which industries face the highest risks and most severe impacts from cyber threats helps businesses and organizations tailor their security measures. By identifying sectors frequently targeted, such as finance or healthcare, we can recommend stronger, customized cybersecurity approaches.

3. **Geographical Insights**
   Analyzing cybersecurity incidents by location provides valuable insights into regional vulnerabilities. Recognizing patterns where certain countries or regions experience more frequent or severe attacks can enhance international collaboration, improve cybersecurity policies, and inform targeted educational and preventive measures.