Global Cybersecurity Threats (2015–2024)

Data Analysis & Power BI Dashboard

Project Objective:

To analyze and visualize global cybersecurity incidents from 2015 to 2024 by identifying patterns in attack types, affected industries, financial losses, and resolution strategies. The goal is to derive actionable insights for cybersecurity readiness and risk mitigation.

Tools & Technologies:

- **Python** (Pandas, Matplotlib/Seaborn)
- **Power BI** (Interactive Dashboard)
- **Jupyter Notebook**
- **CSV Dataset**: `Global_Cybersecurity_Threats_2015-2024.csv`

Dataset Overview: (In details)

- **Rows:** 3000 incidents
- **Columns:** 10 attributes including: which column represents what you have to write
    - Country
    - Year
    - Attack Type
    - Target Industry
    - Financial Loss
    - Number of Affected Users
    - Security Vulnerability Type
    - Defense Mechanism Used
    - Resolution Time (Hours)

Python Data Analysis (Pandas)

Data Cleaning:

- Verified missing values
- Checked duplicates
- Converted and validated data types

Exploratory Data Analysis (EDA):

- Top 10 countries with highest cyberattacks
- Common attack types (Phishing, Ransomware, etc.)
- Most affected industries (IT, Retail, Healthcare)
- Year-wise trends of attacks and financial losses
- Attack Source vs. Vulnerability Type combinations
- Resolution time vs. Attack Type insights

Visuals Created in Python:

- Top 10 countries with most cyberattacks
- Most common attack types
- Industries most targeted
- Correlation (loss vs users vs resolution time)
- Financial loss by attack type (to show distribution & outliers)

Power BI Dashboard (Interactive Reporting)

Key Visuals:

- **KPI Cards** – Total Incidents, Total Loss, Avg. Resolution Time
- **Line Chart** – Year-wise trend of cyberattacks or financial losses
- **Bar Chart** – Attack Types by Frequency
- **Stacked Bar** – Industry vs. Attack Type
- **Pie Chart** – Attack Source (Nation-state, Insider, etc.)
- **Matrix or Table** – Defense Mechanism × Average Resolution Time
- **Slicers** – Filters: Year, Country, Industry, Vulnerability Type
- **Treemap or Donut** – Vulnerability types or Affected User breakdown
- **Map**- Which country have more attack (Visuals Through)

Interactions:

- Drill-through to view detailed incident stats
- Dynamic KPIs: Total Incidents, Total Loss ($), Avg. Resolution Time

Key Insights:

- The highest number of attacks occurred in the USA, India, and China.

- **Ransomware and Phishing** caused the highest financial loss.
- **Retail, IT, and Healthcare** were the most targeted industries.
- **Unpatched software** and **weak passwords** were common vulnerabilities.
- **AI-based Detection** showed lower resolution times compared to traditional firewalls.

Business Recommendations:

- Invest in **AI-driven defense systems**
- Prioritize patch management to reduce vulnerability exposure
- Strengthen cyber awareness in retail and education sectors
- Implement proactive monitoring for high-risk regions

Outcome:

This project demonstrates end-to-end capability in:

- **Data wrangling and analytics using Python**
- **Interactive business intelligence with Power BI**
- **Insightful storytelling for cybersecurity risk management**