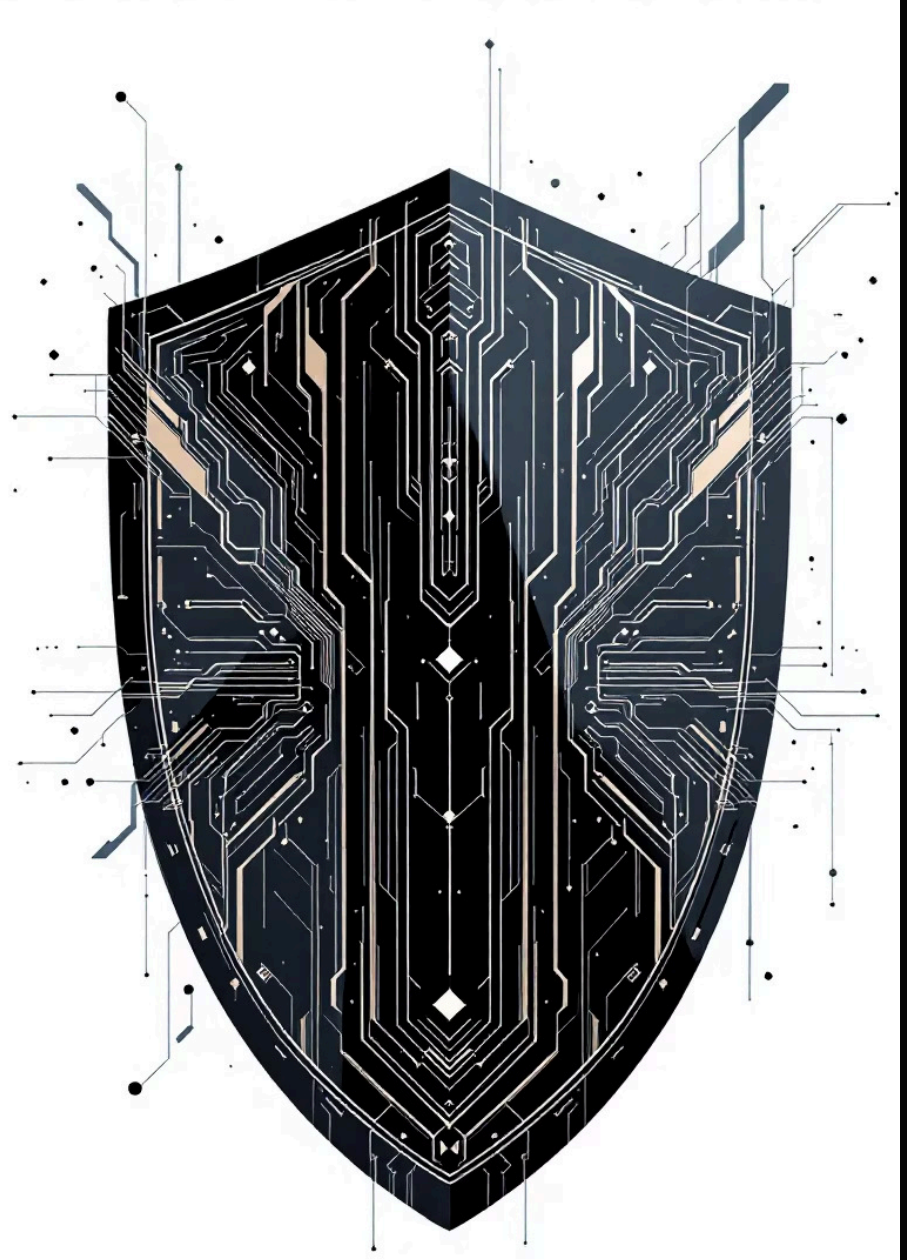
Global Cybersecurity Threats (2015–2024)

Table of Contents



Understanding the Evolving Cyber Threat Landscape

This project delves into global cybersecurity threats from 2015 to 2024, analyzing a comprehensive dataset. Our goal is to extract actionable insights and identify significant trends to better comprehend the ever-changing nature of cyber risks.

Dataset Overview: A Decade of Cyber Incident Data

Our dataset comprises **3,000 detailed entries**, providing a rich source for understanding cyber incidents. Each row captures critical information about specific attacks, enabling a multi-faceted analysis of the threat landscape.

1

Incident Details

Country, Year, Attack Type, Target Industry

2

Impact Metrics

Financial Loss (Million $), Number of Affected Users

3

Threat Vectors

Attack Source, Security Vulnerability Type

4

Response & Resolution

Defense Mechanism Used, Incident Resolution Time (Hours)

Analysis Questions: Uncovering Key Insights

Our investigation is structured around a series of questions, ranging from fundamental inquiries into attack patterns to advanced explorations of correlations and predictive potential.

General Questions

- Most targeted countries and industries?
- Evolution of attacks over time?
- Common attack types and sources?
- Average financial loss per country/attack type?
- Relationship between affected users and financial loss?
- Vulnerabilities contributing most to attacks?
- Impact of defense mechanisms on resolution time?

Advanced Questions

- Relationship between attack type and target industry?
- Financial losses from nation-state attacks?
- Industries most affected by user count?
- Trends in average financial losses over years?
- Effectiveness of defense mechanisms?
- Country-specific attack type vulnerabilities?
- Zero-day vs. weak password resolution times?

Methodology: A Rigorous Analytical Approach

To derive meaningful insights, we employed a systematic methodology encompassing data preparation, exploratory analysis, and advanced statistical techniques.

Data Cleaning

Handling missing values, encoding categorical features, and formatting columns for consistency.

Exploratory Data Analysis (EDA)

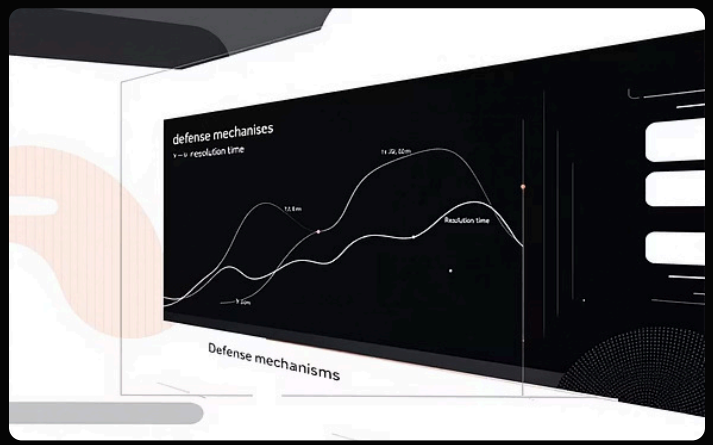
Descriptive statistics, distribution analysis, and uncovering initial relationships within the dataset.

Correlation & Hypothesis Testing

Identifying patterns between key metrics and comparing losses across different attack types and countries.

Visualizing the Cyber Landscape

A range of visualizations will be used to present complex data in an accessible and intuitive manner, highlighting critical trends and relationships.



Key Findings: Critical Insights into Cyber Threats

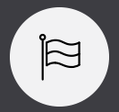
Our analysis has yielded several significant findings that illuminate the current state and evolution of global cybersecurity threats.

High-Target Regions

USA, India, and Brazil consistently experience a high volume of cyberattacks.

Rising Financial Losses

Financial damages have escalated, particularly during major ransomware campaigns.



Nation-State Impact

Attacks originating from nation-states are correlated with higher financial losses.

Vulnerable Industries

Healthcare and Finance sectors remain prime targets for cyber adversaries.

Resolution Challenges

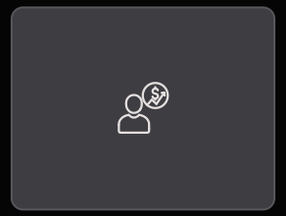
Zero-day exploits significantly prolong incident resolution times compared to weaker password attacks.

Effective Defenses

MFA and Advanced Firewalls are crucial in mitigating both financial and resolution impacts.

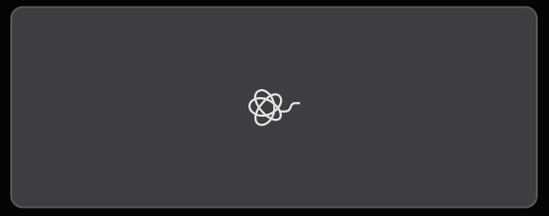
Future Work: Advancing Cybersecurity Intelligence

Building upon these findings, our future endeavors aim to develop proactive and predictive capabilities to enhance global cybersecurity resilience.



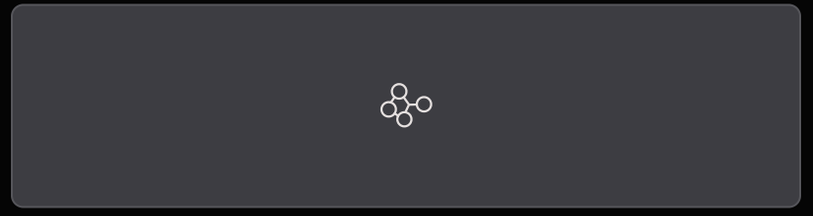
Predictive Models

Forecasting attack likelihood by industry and country.



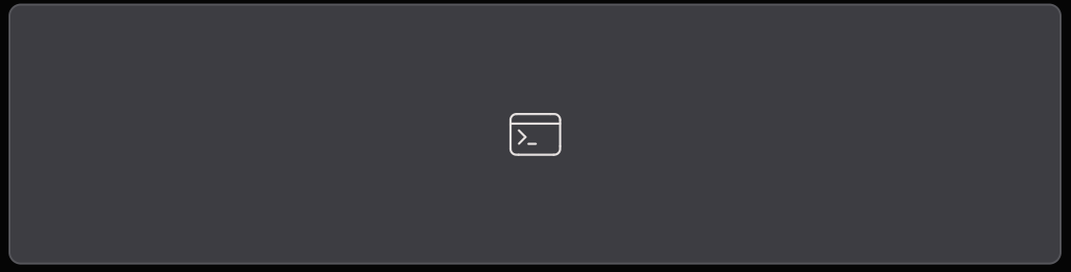
Anomaly Detection

Developing systems for early identification of unusual attack patterns.



Clustering Techniques

Grouping countries and industries with similar threat profiles.



Interactive Dashboard

Creating real-time threat monitoring platforms for actionable intelligence.