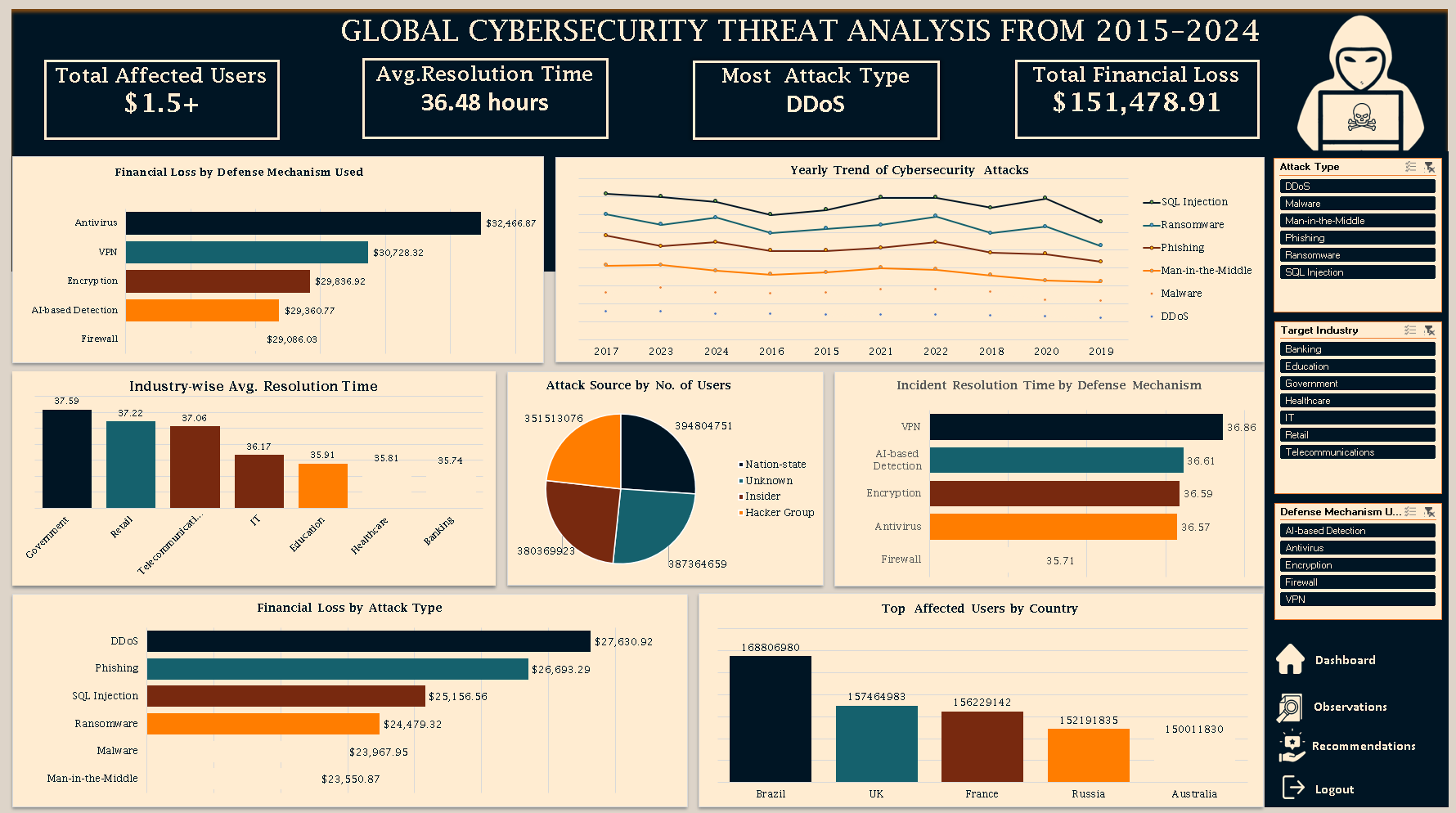
**Technical Report: Global Cybersecurity Threats (2015-2024)**

**1. Outline**

Introduction  
Story of Data  
Data Splitting and Preprocessing  
Pre-Analysis  
In-Analysis  
Post-Analysis and Insights  
Data Visualizations & Charts  
Recommendations and Observations  
Conclusion  
References & Appendices

**2. Introduction**

****

**Objective of the Project:**  
This project analyzes global cybersecurity threats from 2015 to 2024 to understand the impact of different attack types, identify the most affected regions and sectors, and evaluate the effectiveness of defense mechanisms.

**Problem Being Addressed:**  
Cyber threats are increasingly sophisticated and widespread, resulting in substantial financial loss and operational disruption. This analysis aims to identify patterns and insights that can inform more robust cybersecurity strategies.

**Key Datasets and Methodologies:**  
The dataset used combines incident-level data and pivot summaries including financial losses, affected users, and resolution times. Microsoft Excel tools such as Pivot Tables, Filters, and Lookup functions were employed.

**3. Story of Data**

**Data Source:**  
The data is likely from compiled global incident reports, organizational disclosures, and cybersecurity surveys.

**Data Collection Process:**  
Data appears to be aggregated from internal systems and public threat intelligence feeds, structured into Excel sheets.

**Data Structure:**

* Rows: Each row in the core dataset represents a single cybersecurity incident.
* Columns: Country, Year, Attack Type, Target Industry, Financial Loss, Affected Users, Attack Source, Vulnerability Type, Defense Mechanism, Resolution Time.

**Important Features and Their Significance:**

* **Attack Type:** Determines threat variety.
* **Financial Loss:** Quantifies business impact.
* **Defense Mechanism:** Indicates mitigation success.
* **Resolution Time:** Measures incident response efficiency.

**Data Limitations or Biases:**

* Some sheets had incomplete headers.
* Possible underreporting or inconsistencies in country-level data.

**4. Data Splitting and Preprocessing**

**Data Cleaning:**  
Minor formatting adjustments and removal of blank rows.

**Handling Missing Values:**  
Rows with missing key fields were excluded from the core analysis.

**Data Transformations:**  
Aggregated values by country, attack type, and defense mechanism using pivot tables.

**Data Splitting:**

* Dependent: Financial Loss, Affected Users
* Independent: Country, Attack Type, Defense, Year

**Industry Context:**  
This dataset falls under the **Cybersecurity and IT risk management** industry.

**Stakeholders:**

* CISO/IT Security Teams
* Senior Executives
* Government Cybersecurity Agencies

**Value to the Industry:**  
Provides decision-makers with evidence to prioritize threat response and allocate resources effectively.

**5. Pre-Analysis**

**Identify Key Trends:**

* DDoS and Ransomware appear frequently across years.
* Developing countries like Brazil and India show high user impact.

**Potential Correlations:**

* Unpatched Software correlates with high financial loss.
* Nation-state attacks lead to large-scale user impact.

**Initial Insights:**  
Some defense mechanisms like Antivirus are associated with higher losses, indicating misalignment in threat-defense pairing.

**6. In-Analysis**

**Unconfirmed Insights:**

* VPN and MFA tend to reduce resolution times.
* Government and IT sectors report the fastest resolution.

**Recommendations:**

* Reevaluate investments in Antivirus alone.
* Promote patch management and password hygiene.

**Analysis Techniques Used in Excel:**

* Pivot Tables for aggregation.
* Conditional Formatting to highlight high-impact cells.
* LOOKUP functions for resolution mapping.

**7. Post-Analysis and Insights**

**Key Findings:**

* DDoS caused over $27 billion in damages.
* Brazil had the highest number of affected users (168M).
* Nation-state attacks affected nearly 400 million users.
* Antivirus was associated with $32 billion in losses.

**Comparison with Initial Findings:**  
Initial assumptions about Antivirus effectiveness were disproven. Resolution times also showed unexpected results with VPNs outperforming Firewalls.

**8. Data Visualizations & Charts**

**Charts and Graphs:**

* Bar Chart: Financial Loss by Attack Type
* Pie Chart: Affected Users by Country
* Line Graph: Yearly Trends by Attack Type
* Bar Chart: Avg. Resolution Time by Defense

**Dashboard:**  
Includes consolidated metrics: Total Loss, Top Countries, Effective Defenses, and Incident Volume Trends.

**Explanation of Visualizations:**

* Bar chart shows DDoS leading in financial damage.
* Pie chart highlights Brazil and India as major user loss centers.
* Line graph illustrates rise of Ransomware post-2018.
* Defense bar chart demonstrates effectiveness of MFA and VPN.

**9. Recommendations and Observations**

**Actionable Insights:**

* Enforce regular software patching.
* Prioritize MFA and VPN deployment.
* Strengthen cyber hygiene training.

**Optimizations or Business Decisions:**

* Reallocate budget from legacy tools like Antivirus to modern EDR solutions.
* Focus defense in high-incident regions.

**Unexpected Outcomes:**

* MFA outperformed Antivirus in both cost and resolution.
* Nation-state actors remain the most dangerous, often bypassing traditional defenses.

**10. Conclusion**

**Key Learnings:**

* Attack type and defense mismatches lead to higher losses.
* Data-driven defense strategy is essential.

**Limitations:**

* Missing headers in some summary sheets.
* No metadata on sample completeness or reporting scope.

**Future Research:**

* Incorporate real-time data feeds.
* Analyze individual incident narratives and attacker profiles.

**11. References & Appendices**

**References:**

* Internal Excel file: Global\_Cybersecurity\_Threats\_2015–2024 Task 21A.xlsx

**Appendices:**

* Raw Pivot Tables from Excel
* Dashboard Visuals
* Formula Snippets: =VLOOKUP(), =IFERROR(), Pivot Configurations