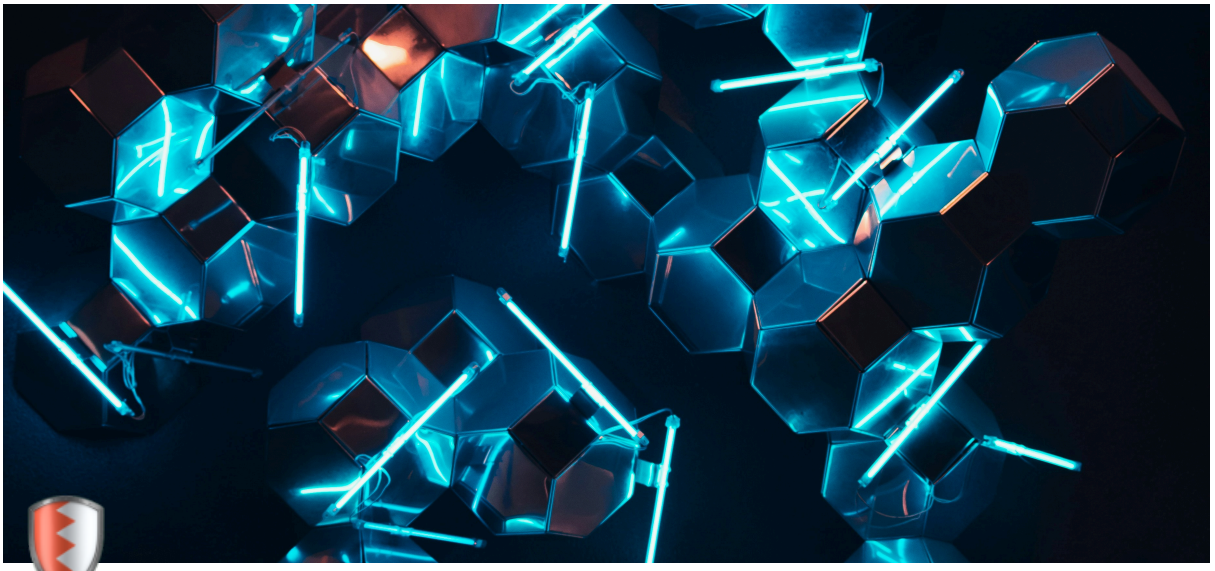


Global Cybersecurity Threats (2015-2024)

1. Background & Overview

1.1 Objective

What is this project about? - This project aims identify which industries and countries are most at risk, examine how **attack frequency** and **severity** have changed over time, and assess the relationship between threat type, data exposure, and **financial impact** using the **EDA analysis**

Through this process, the project not only highlights where **vulnerabilities** persist but also provides **data-driven recommendations** that can inform both policy and practice in digital security.

Who is this project for? - The intended audience for this report includes **cybersecurity professionals**, **data analysts**, **risk managers**, and **business decision-makers** who require a clear understanding of global threat dynamics to strengthen their defense strategies.

Business Questions:

- Which countries or regions are most frequently targeted?
- Which industries experience the highest number of attacks and financial losses?

- What are the most common types of cyber threats between 2015 and 2024?
- How does response time affect the severity and financial outcome of attacks?

1.2 Data Understanding

About the Dataset: The Global Cybersecurity Threats Dataset (2015-2024) contains 3000+ records providing extensive data on cyberattacks, malware types, targeted industries, and affected countries. It is designed for threat intelligence analysis, cybersecurity trend forecasting, and machine learning model development to enhance global digital security.

Dataset summary:

Column Name	Description
Country	Country where the attack occurred
Year	Year of the incident
Threat Type	Type of cybersecurity threat (e.g., Malware, DDoS)
Attack Vector	Method of attack (e.g., Phishing, SQL Injection)
Affected Industry	Industry targeted (e.g., Finance, Healthcare)
Data Breached (GB)	Volume of data compromised
Financial Impact ($M)	Estimated financial loss in millions
Severity Level	Low, Medium, High, Critical
Response Time (Hours)	Time taken to mitigate the attack
Mitigation Strategy	Countermeasures taken

Attack Type summary:

Attack Type	Description
DDoS	DDoS (Distributed Denial of Service) is a cyber attack. It overwhelms a system with traffic from multiple sources. Attackers use botnets to flood the target with traffic. This causes resource exhaustion, making the system unavailable. DDoS attacks can lead to downtime, financial losses, and data breaches.

Phishing	Phishing is a cybercrime where attackers, posing as legitimate entities, use fraudulent emails, text messages, or phone calls to trick individuals into revealing sensitive information like passwords, financial details, or personal data.
SQL Injection	Structured Query Language (SQL) injection is an attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code.
Ransomware	Ransomware is malware that encrypts files or locks devices. Attackers demand a ransom for decryption or unlock codes. Types include crypto-ransomware, locker ransomware, and doxware. Consequences include data loss, financial loss, and reputational damage. Prevention involves backups, software updates, antivirus software, and employee education.
Malware	Malware is malicious software that harms or exploits devices. Types include viruses, worms, trojans, ransomware, and spyware. Malware attacks can steal data, disrupt systems, or demand ransom. Attacks often occur through phishing, downloads, or vulnerabilities. Prevention involves antivirus software, updates, and safe computing practices.
Man-in-the-Middle	man-in-the-middle (MITM) attack is a cyberattack where an attacker intercepts and potentially alters communication between two parties, pretending to be one of them to steal sensitive information or disrupt the conversation.

Security Vulnerability Type summary:

Security Vulnerability Type	Description
Unpatched Software	Occurs when systems or applications are not updated with the latest security patches, leaving known vulnerabilities exploitable by attackers. Regular patch management is essential to mitigate this risk.
Weak Passwords	Refers to easily guessable or reused passwords that allow unauthorized access to systems. Implementing strong password policies and multi-factor authentication can reduce this vulnerability.
Social Engineering	Involves manipulating individuals into revealing confidential information or granting access. Common examples include phishing, baiting, and pretexting attacks.

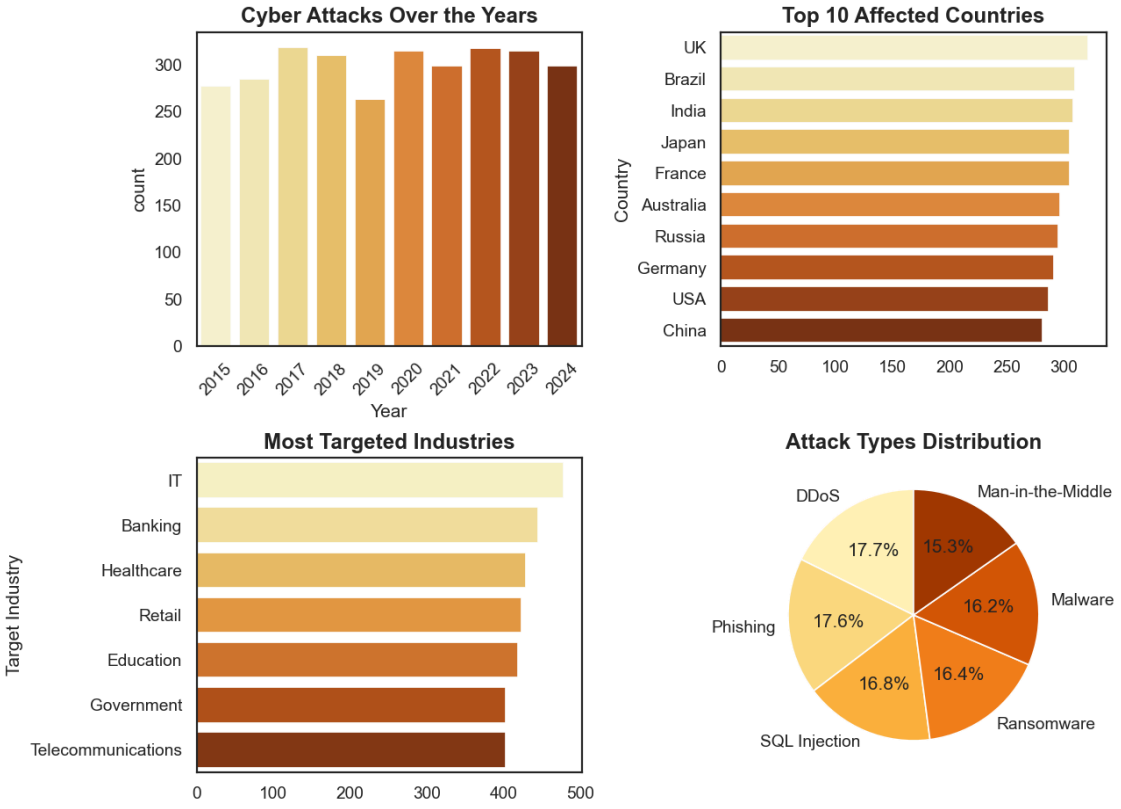
Zero-day	A newly discovered software flaw unknown to the vendor or the public. Since no patch exists yet, attackers exploit it before developers can release a fix. Early threat detection and network segmentation help minimize impact.

Before processing further analysis with data tools like Power BI or Python, the Pandas package is used to assess the data quality in the datasets. The detailed steps are compacted in

Python data assessment and preparation process

2. Preliminary Exploratory Data Analysis

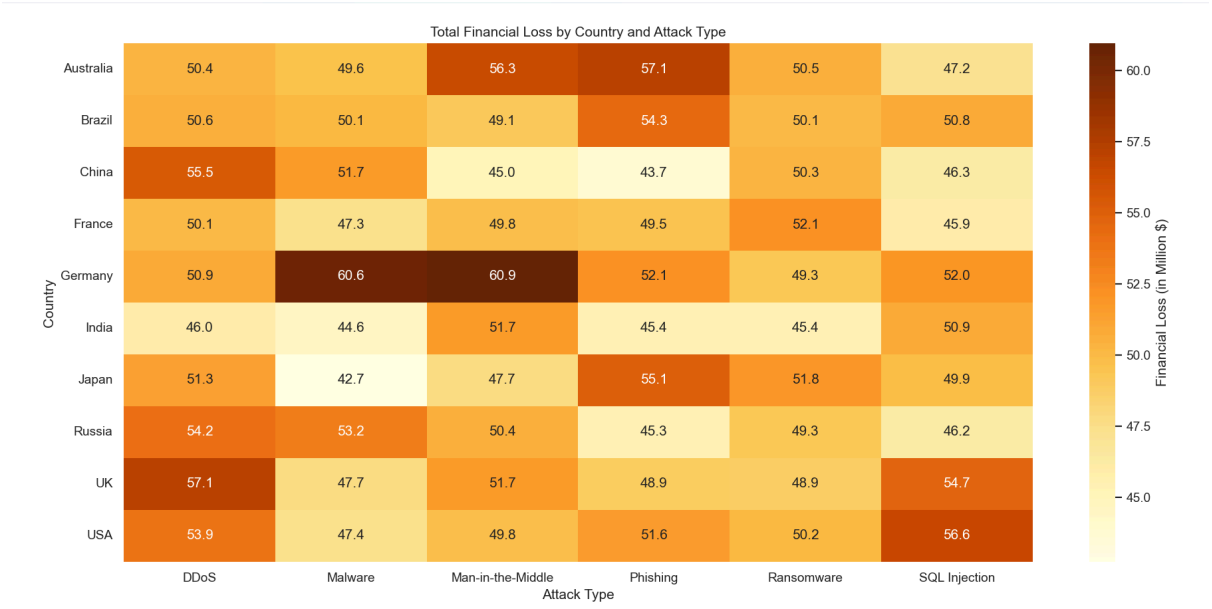
By utilizing some matplotlib and seaborn visualizations, we can extract some ideas and insights for the further analysis and illustration



Several patterns figured out after executing an amount of visualizations:

- **IT Industry** is the most targeted sector by a significant margin (478 incidents). This is likely because of the high value of its data and its central role in digital infrastructure

- **UK, Brazil** and **India** show the **highest number of incidents (**321, 310 and 308 incidents respectively), it is remarkable that these three nations are in three distinguished continents in the world, this indicates that cyber-crime attacks are not evenly distributed geographically, they attack in global reach.



This heatmap indicates several insights that illustrate better financial loss for

- Germany stands out with the highest financial losses, particularly from **Malware** ($60.6M) and **Man-in-the-Middle** attacks ($60.9M), suggesting an extreme severe vulnerability for German security system to these threats.
- Across multiple economic powers like the USA, UK, and Russia, **DDoS** and **SQL Injection** attacks consistently result in high financial losses (generally over $50M). This indicates these are highly disruptive and expensive threats globally.

3. In-dept Exploratory Data Analysis

3.1 Metrics Analysis

Before visualizing the illustrations and exploiting the business insights from Power BI, the metrics summary will be provided, assisting analysts for a better understanding of the dashboard.

3.1.1 YoY Attack Growth %

$$\text{Attack Growth Rate (\%)} = \frac{Attacks_t - Attacks_{t-1}}{Attacks_{t-1}} \times 100\%$$

Meaning: Measures how fast cyberattacks are increasing year over year. **t** refers to the year the attack occured.

Example: If 2023 had 90 attacks and 2024 had 120 → Growth Rate = (120−90)/90 × 100% = 33.3%.

Measure in DAX function:

```
YoY Attack Growth Rate (%) =
VAR CurrentYear = MAX(CyberAttackData[Year])
VAR PrevYear = CurrentYear - 1
VAR Attacks_Current =
    CALCULATE(COUNTROWS('CyberAttackData'), CyberAttackData[Year] = CurrentYear)
VAR Attacks_Previous =
    CALCULATE(COUNTROWS(CyberAttackData), CyberAttackData[Year] = PrevYear)
RETURN
DIVIDE(Attacks_Current - Attacks_Previous,Attacks_Current)*100
```

3.1.2 Average Financial Loss per Attack

$$\text{Average Financial Loss per Attack} = \frac{\text{Total Financial Loss}}{\text{Number of Attacks}}$$

Meaning: Shows the average financial damage caused by each cyberattack.

Example: Total loss = $500M, Attacks = 250 → Avg. Loss = 500 / 250 = $2M per attack

Measure in DAX function:

```
Average Loss per Attack ($M) =
    DIVIDE(SUM(CyberAttackData[Financial Loss (in Million $)]),COUNTROWS(CyberAttackData))
```

3.1.3 Mean Time to Resolve

$$\text{MTTR} = \frac{\sum_{i=1}^{n} \text{Incident Resolution Time}_i}{\text{Number of Incidents}}$$

Meaning: Indicates the average time required to resolve incidents.

Example:

Total resolution time = 1000 hours for 200 incidents→ MTTR = 1000 / 200 = 5 hours per incidents

Measure in DAX function:

```
MTTR (Hours) =
    AVERAGE(CyberAttackData[Incident Resolution Time (in Hours)])
```

3.1.4 Loss Efficiency Ratio

$$\text{Loss Efficiency Ratio} = \frac{\text{Financial Loss (in \$M)}}{\text{Incident Resolution Time (in Hours)}}$$

Meaning: Evaluates financial loss relative to the time taken to handle incidents.

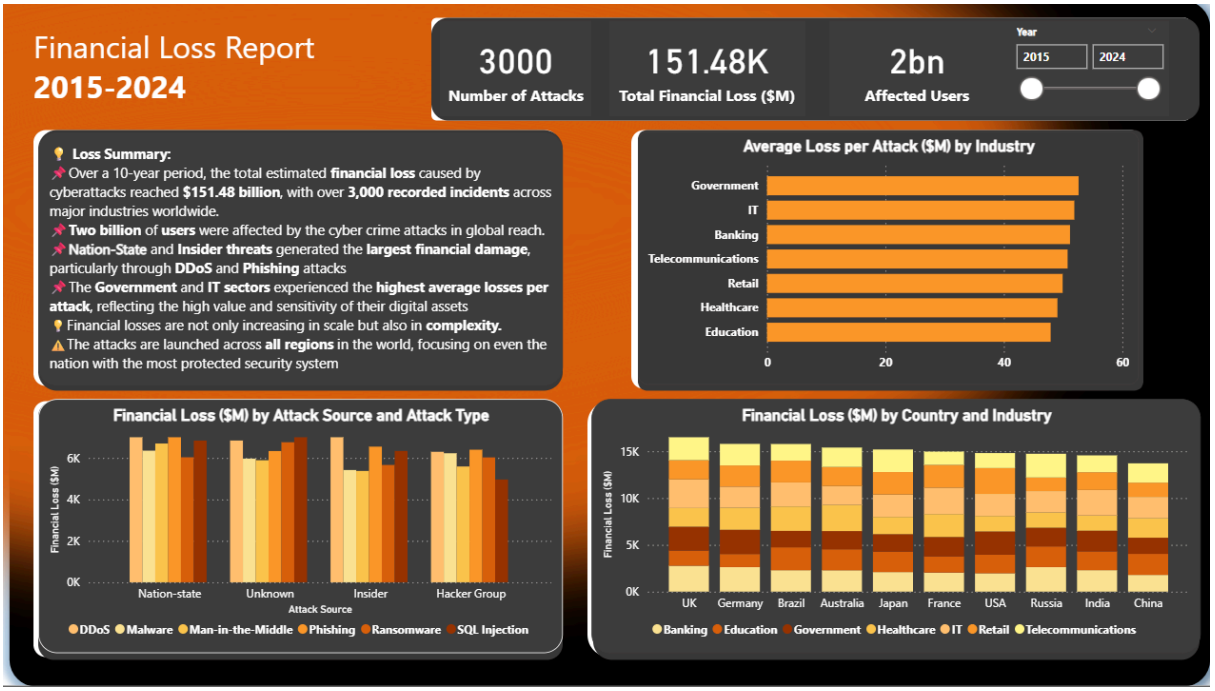
Example: $50M loss over 200 hours → Ratio = 50 / 200 = 0.25 M/hour

Measure in DAX function:

```
Loss Efficiency Ratio =
    DIVIDE(
        SUM(CyberAttackData[Financial Loss (in Million $)]),
        SUM(CyberAttackData[Incident Resolution Time (in Hours)]))
```

3.2 Dashboard Visualizations and In-dept analysis:

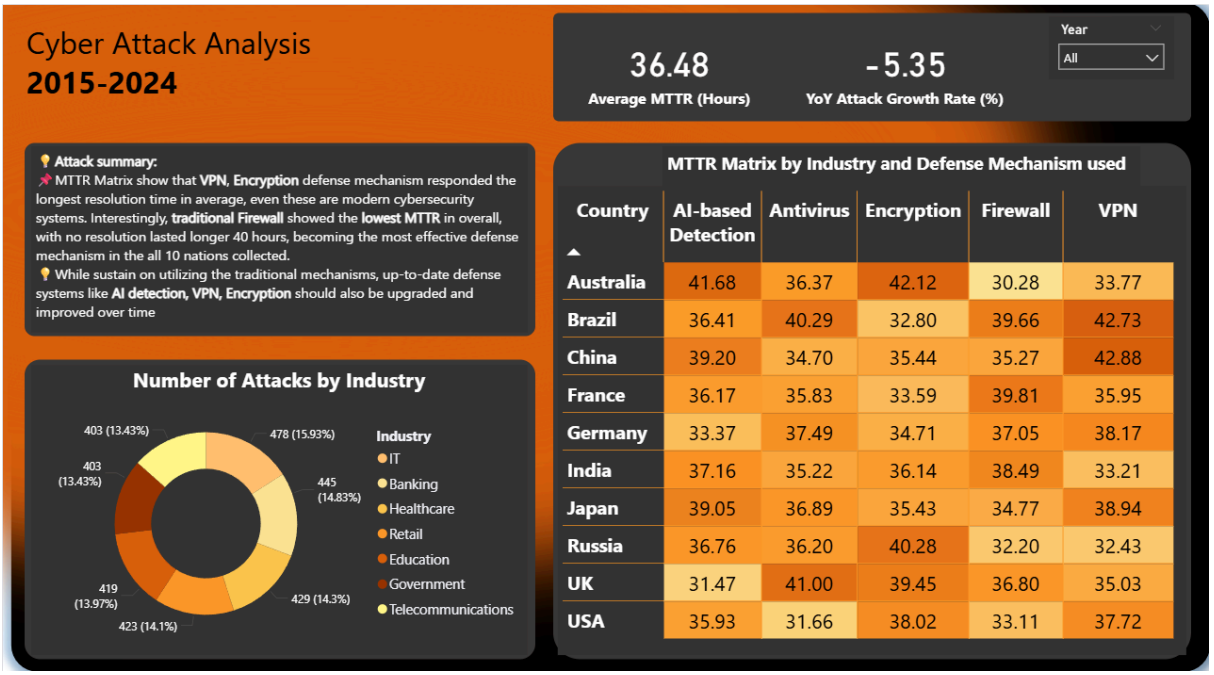
3.2.1 Financial Loss Report



Loss Summary:

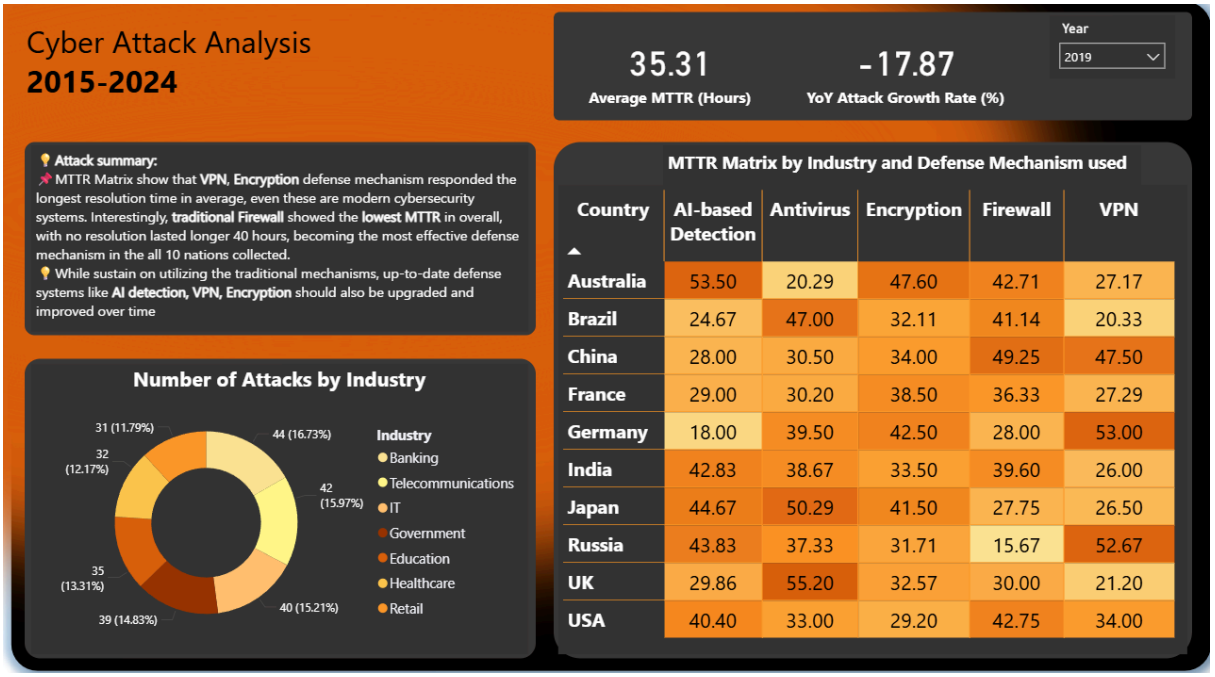
- Over a 10-year period, the total estimated **financial loss** caused by cyberattacks reached **$151.48 billion**, with over **3,000** recorded **incidents** across major industries worldwide.
- **Two billion of users** were affected by the cyber crime attacks in global reach.
- **Nation-State** and **Insider threats** generated the largest financial damage, particularly through **DDoS** and **Phishing attacks**
- The **Government** and **IT** sectors experienced the highest average losses per attack, reflecting the high value and sensitivity of their digital assets
- Financial losses are not only increasing in scale but also in **complexity**.
- The attacks are launched across **all regions** in the world, focusing on even the nation with the most protected security system

3.2.2 Cyber Attack Analysis



Attack summary:

- MTTR Matrix show that VPN, Encryption defense mechanism responded the longest resolution time in average, even these are modern cybersecurity systems. Interestingly, traditional Firewall showed the lowest MTTR in overall, with no resolution lasted longer 40 hours, becoming the most effective defense mechanism in the all 10 nations collected.
- While sustain on utilizing the traditional mechanisms, up-to-date defense systems like AI detection, VPN, Encryption should also be upgraded and improved over time



- Remarkably, there was a strong decline in the Attack Growth Rate in 2019, however the amount of attacks aim at **Banking**, **Telecommunications** and **IT** fields accounted more in the proportion of the overall stats, indicating that these three fields contains core digital value and more strict cyber protection system should be focused on these industries.

4. Recommendations

Which stakeholder is proposed to	Strategy	Justification	Recommendation
Security Operations Teams	Decrease **incident response** through automation and AI-driven analytics	The current **Mean Time to Resolution (MTTR)** averages **36.48 hours**, suggesting delays in incident resolution.	Implement **AI-assisted threat detection** tools that automatically correlate attack signatures across sources.
IT Infrastructure Managers	Strengthen network security with layered defense.	The implementation of modern defense mechanisms like **Encryption, AI-detection, VPN** has not yet shown effectiveness	Combine and attach many layers of defense mechanisms to strengthen the security network while still utilizing traditional solutions

			such as Antivirus or Firewall