**Cybersecurity Attacks - Q4**

A Descriptive Analysis of Cyberattacks During Q4

# 1. Project Overview

This project explores cyberattack patterns during the fourth quarter (Q4) using sample data containing timestamps, countries, IP addresses, attack types, severity levels, and outcomes (success/failure). The main goal is to identify the most targeted time zones and analyze trends based on time, severity, and success rate.

# 2. Dataset Description

The dataset used in this analysis was generated using ChatGPT. It contains six columns: Timestamp, Country, IP Address, Attack Type, Severity, and Success.

# 3. Analytical Question and Type

**Analytical Question:**  
What are the most targeted time zones for cyberattacks during Q4, and what time-based patterns can be observed?

**Type of Analysis:**  
Descriptive Analysis  
Time-based (Temporal) Analysis

# 4. Excel Analysis

The Excel file contains two sheets:

• Sheet 1: Raw data with additional columns derived from Timestamp (Date, Month, Hour), along with several COUNTIF-based metrics:

* - Total and average number of attacks  
  - Frequency of attacks by selected countries (South Korea, USA, Germany, Brazil, Egypt)  
  - Frequency by Severity level (Low, Medium, High, Critical)  
  - Count of successful vs. failed attacks  
  - Count of attack types and their frequency by month  
  - Attack success/failure per country

• Sheet 2: Pivot Tables highlighting:

* - Attacks by Month and Severity  
  - Attacks by Type and Severity  
  - Country vs. Type  
  - Attack success/failure by Type  
  - Top 10 Peak Hours for Cyberattacks

# 5. Power BI Dashboard

The Power BI report consists of five pages:

• Home: Contains project title, author name, bootcamp name (Hash Plus), and a project description.

• Overview:

* - 2 Cards: Total Attack Count, Most Common Attack Type  
  - Stacked Bar Chart: Attack Types  
  - Line Chart: Attack Types by Month  
  - Clustered Column Chart: Attack Type by Hour and Success

• Attack Details:

* - Line Chart: Attack Count by Month  
  - Clustered Column Chart: Type by Month  
  - Donut Chart: Attack Types  
  - Funnel: Hour by Attack Type

• Severity and Risk:

* - Pie Chart: Attack Type by Severity  
  - Donut Chart: Severity by Month  
  - Clustered Column Chart: Attack Type by Severity  
  - Stacked Bar: Day by Severity

• Dashboard (Interactive):

* - Clustered Column Chart: Attack Type by Month  
  - Clustered Bar Chart: Attack Type by Severity  
  - Map: Attack Distribution by Country  
  - Slicers: Month, Attack Type

# 6. Key Findings

* Specific time zones experience higher attack rates, especially during peak evening hours.
* Certain attack types appear more frequently in specific months.
* The majority of high-severity attacks were concentrated in a few countries.
* A significant number of attacks were unsuccessful, with notable variation across countries.
* Based on the analysis, the most targeted hours for cyberattacks were between 6 PM and 10 PM, with a noticeable peak around 8 PM.
* The month of October recorded the highest number of attacks during Q4, followed by November and December.
* Most of the attacks during peak hours were of high severity, and phishing was the most common attack type observed.

# 7. Recommendations

- Monitor high-risk time zones more closely, especially during peak hours.  
- Improve defense mechanisms against frequently used attack types.  
- Investigate regions with high critical severity attacks for root causes.  
- Enhance success detection and logging mechanisms to reduce gaps in visibility.