Cybersecurity Attacks Visualization: Unveiling Patterns and Insights

Timothy Harmon

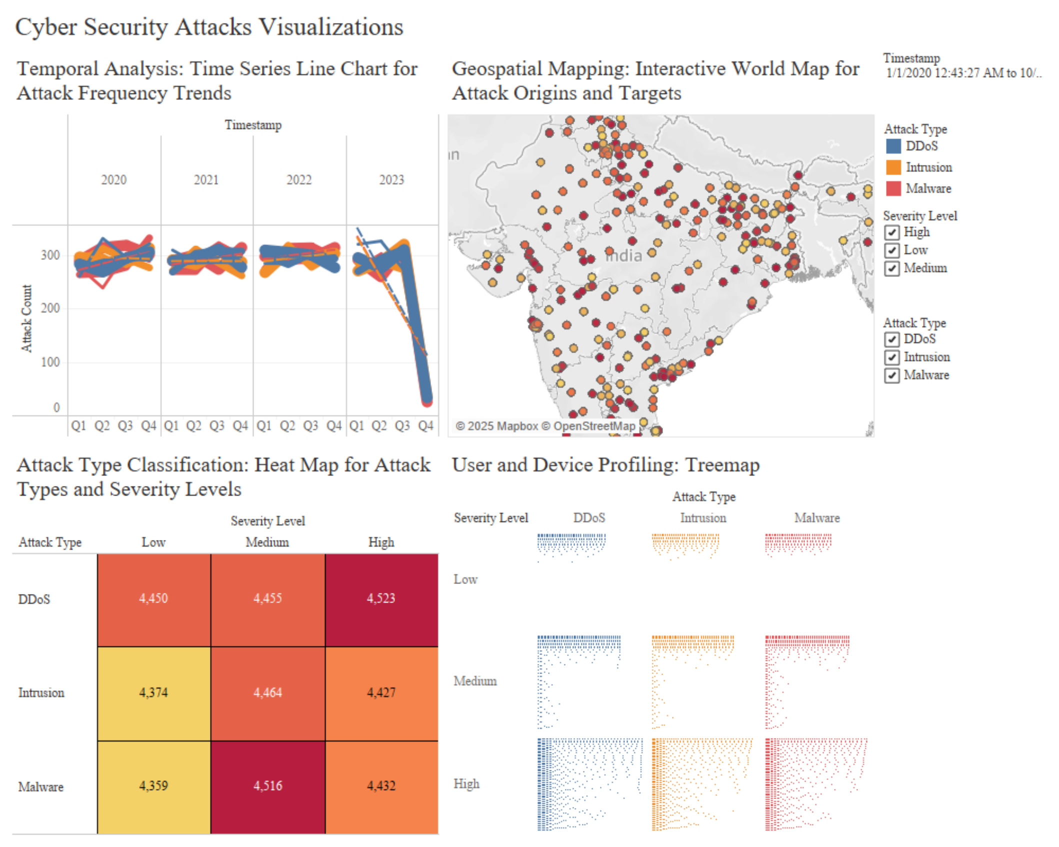
March 14, 2025

DSE 241: Data Visualization

UC San Diego
JACOBS SCHOOL OF ENGINEERING
Computer Science and Engineering

Motivation & Overview

- **Background**: Rising number of cybersecurity attacks poses critical risks to organizations worldwide.
- **Importance of Visualization**: Essential for uncovering hidden patterns and trends in complex cybersecurity data.



Cyber Security Attacks Visualizations

Temporal Analysis: Time Series Line Chart for Attack Frequency Trends

Timestamp
2020
2021
2022
2023
Attack Count
300
200
100
0
Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4

Geospatial Mapping: Interactive World Map for Attack Origins and Targets

India
© 2025 Mapbox © OpenStreetMap

Timestamp
1/1/2020 12:43:27 AM to 10/..

Attack Type
🟦 DDoS
🟧 Intrusion
🟥 Malware

Severity Level
☑ High
☑ Low
☑ Medium

Attack Type
☑ DDoS
☑ Intrusion
☑ Malware

Attack Type Classification: Heat Map for Attack Types and Severity Levels

	Severity Level		
Attack Type	Low	Medium	High
DDoS	4,450	4,455	4,523
Intrusion	4,374	4,464	4,427
Malware	4,359	4,516	4,432

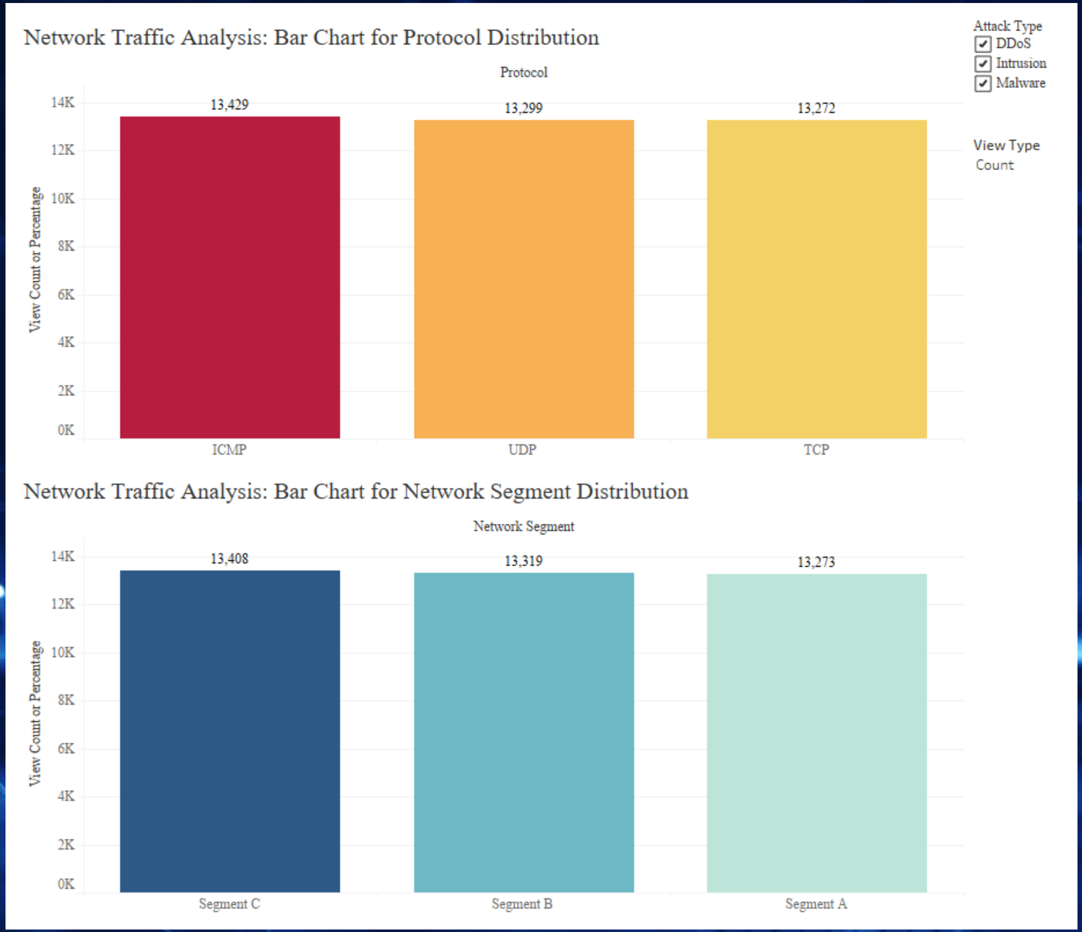
User and Device Profiling: Treemap

Project Goals:

1. Detect and visualize attack trends over time
2. Identify high-risk regions and network segments
3. Highlight severe attacks and common malware patterns

Dataset & Preprocessing

- **Dataset source**: Kaggle's "Cyber Security Attacks" dataset - https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks?select=cybersecurity_attacks.csv



- **Dataset**: 40,000 records with 25 varied metrics (timestamps, IP addresses, protocols, attack types, severity levels, geo-locations).
- **Preprocessing Steps**:
  1. **Cleaning**: Removed duplicates, handled missing values
  2. **Transformation**: Normalized categorical variables
  3. **Feature Engineering**: Created 'Attack Frequency Index' and 'Severity Trends'
  4. **Validation**: Ensured data integrity post-processing

Research Questions & Key Tasks

- **Research Questions:**
  - What are the predominant attack types?
  - How do attack trends evolve over time?
  - Which regions are most vulnerable?
  - Which protocols are most exploited?
  - What user and device patterns emerge from attacks?
- **Key Tasks:**
  - Attack Type Analysis
  - Temporal Trends
  - Geospatial Mapping
  - Network Traffic Analysis (Protocol & Network Segment)
  - User and Device Profiling

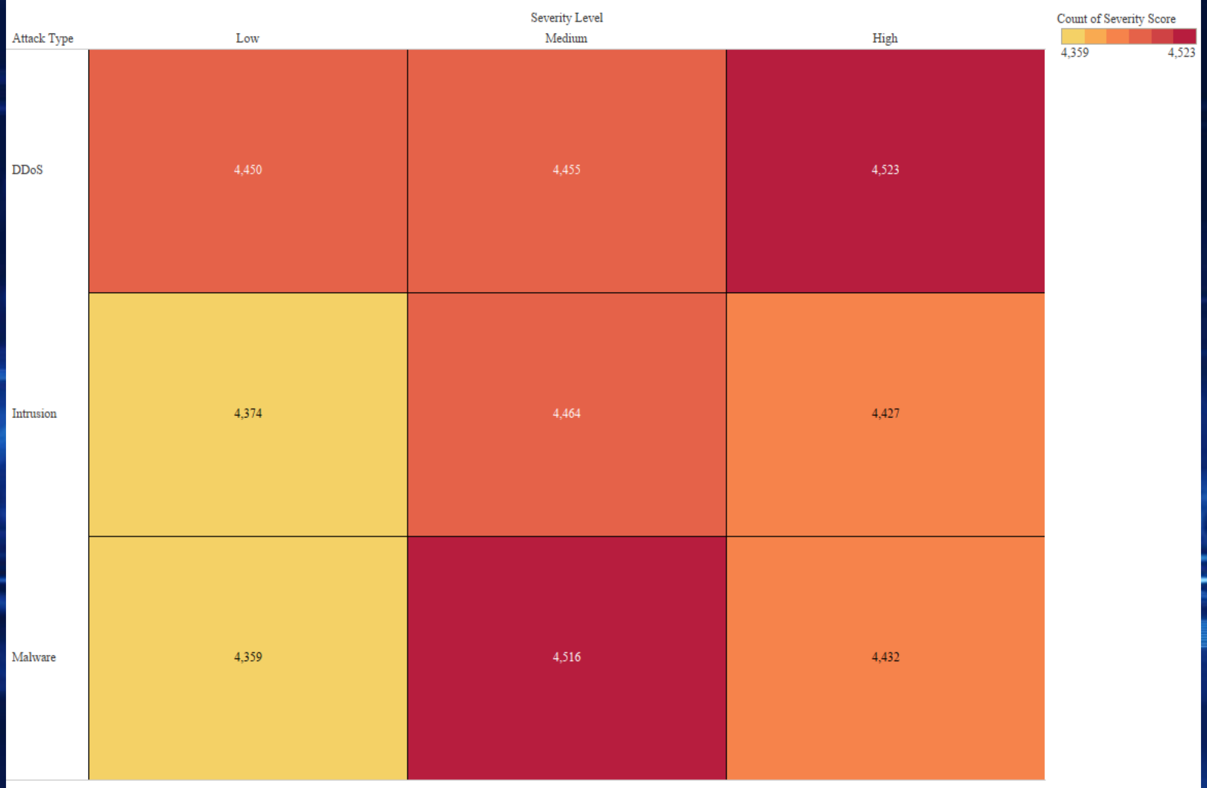
Attack Type Analysis

- **Methodology**: Categorized attacks by type and severity
- **Top Attack Types Distribution**:
  1. **DDOS**: 13,428 occurrences (33.57%)
  2. **Malware**: 13,307 occurrences (33.27%)
  3. **Intrusion**: 13,265 occurrences (33.16%)

- **Key Insight**: Nearly equal distribution of attack types suggests a diverse threat landscape

- **Visualization**: Heatmap showing distribution of attack types and severity levels

Attack Type Classification: Heat Map for Attack Types and Severity Levels

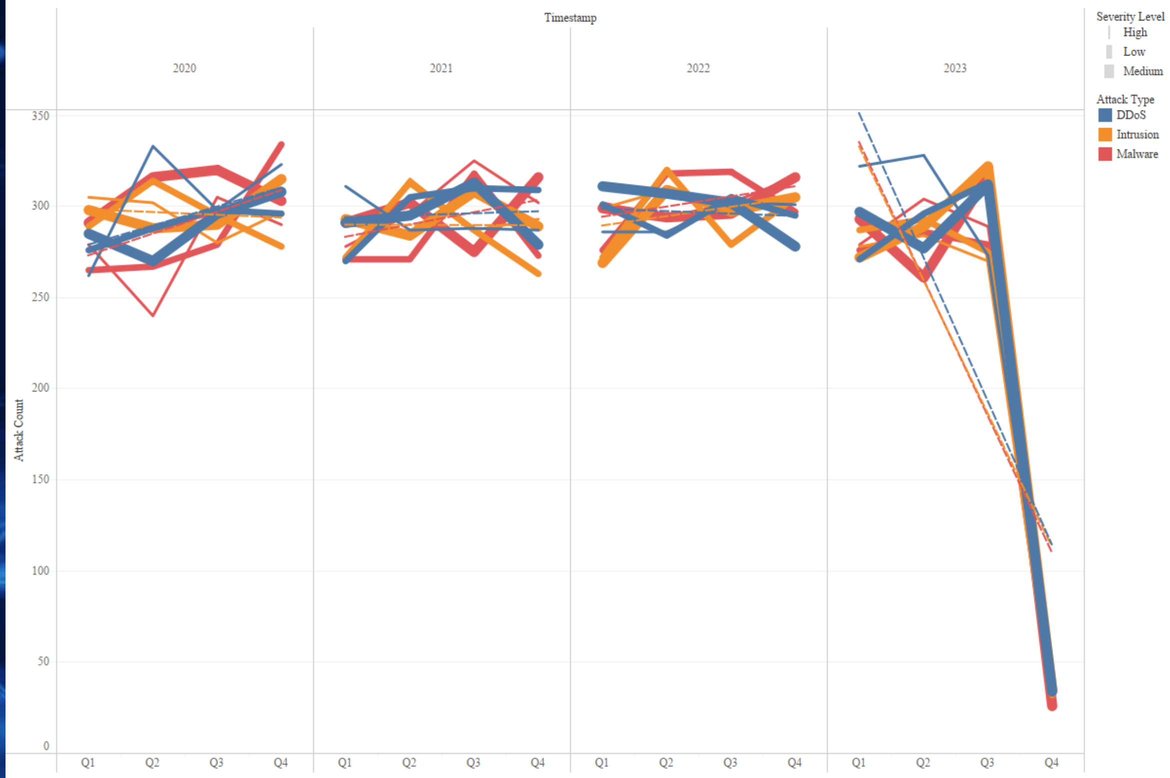


Count of cybersecurity_attacks_updated.csv broken down by Severity Level vs. Attack Type. Color shows count of Severity Score. The marks are labeled by count of cybersecurity_attacks_updated.csv. The data is filtered on Timestamp, which ranges from 1/1/2020 12:43:27 AM to 10/11/2023 7:34:23 PM. The view is filtered on Severity Level and Attack Type. The Severity Level filter keeps High, Low and Medium. The Attack Type filter keeps DDoS, Intrusion and Malware.

Temporal Trends & Severity Analysis

- **Visualization**: Time series chart showing attack frequency and severity over time

Temporal Analysis: Time Series Line Chart for Attack Frequency Trends



The trend of Attack Count for Timestamp Quarter broken down by Timestamp Year. Color shows details about Attack Type. Size shows details about Severity Level. The data is filtered on Timestamp, which ranges from 1/1/2020 12:43:27 AM to 10/11/2023 7:34:23 PM. The view is filtered on Severity Level and Attack Type. The Severity Level filter keeps High, Low and Medium. The Attack Type filter keeps DDoS, Intrusion and Malware.

- **Methodology**: Analyzed attack frequencies over time
- **Severity Level Distribution**:
  1. **Medium**: 13,435 occurrences (33.59%)
  2. **High**: 13,382 occurrences (33.46%)
  3. **Low**: 13,183 occurrences (32.96%)

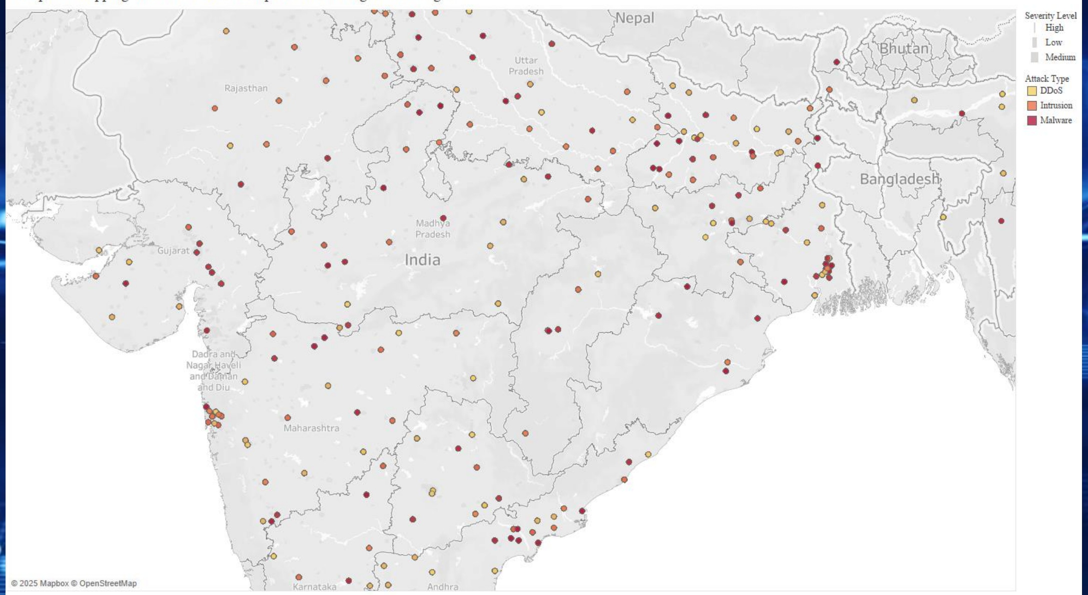
- **Key Insight**: Majority of attacks (67.05%) are medium to high severity, indicating significant potential impact

Geospatial Insights & Protocol Analysis

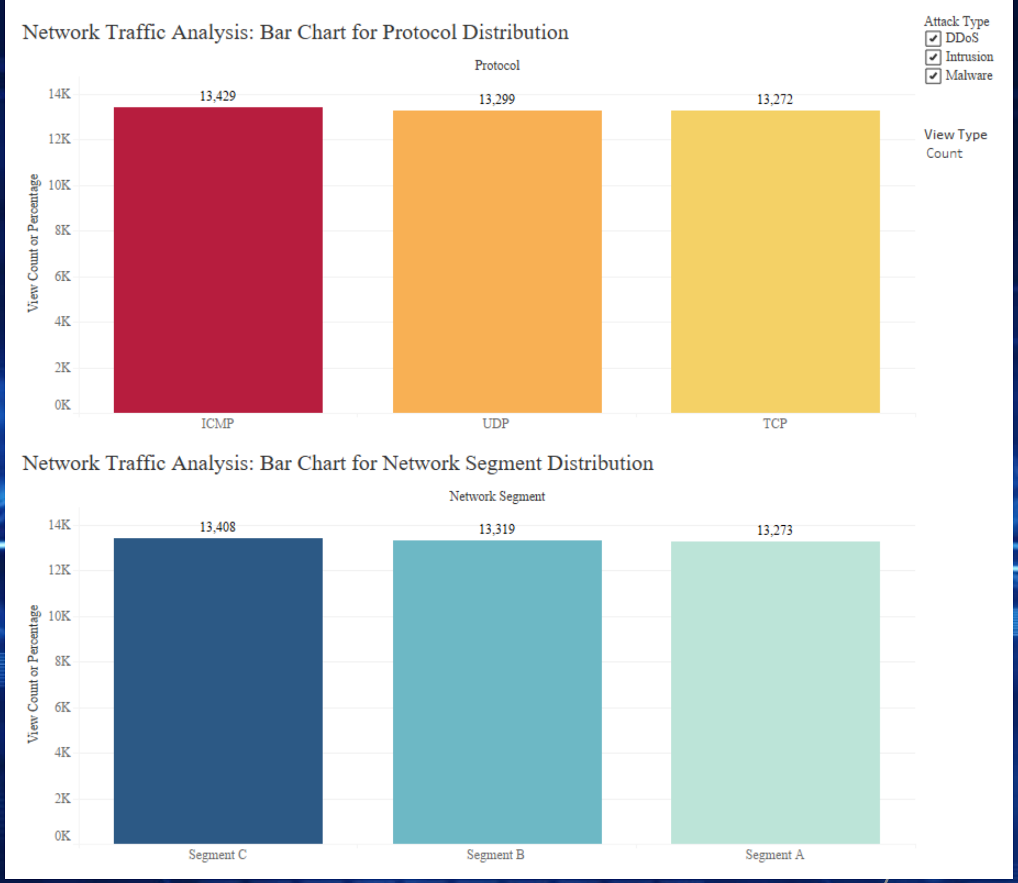
- **Top 5 Source Cities of Attacks**:
  - Ghaziabad, Aurangabad, Rourkela, Rohtak, Ramagundam
- **Protocol Distribution**:
  - **ICMP**: 13,429 occurrences (33.57%)
  - **UDP**: 13,299 occurrences (33.25%)
  - **TCP**: 13,272 occurrences (33.18%)
- **Key Insight**: Diverse origins and protocols necessitate global and multi-layer security measures

- **Visualization**: World map and Network Traffic Analysis bar chart highlighting attack origins, intensities, protocol and network segment distribution.

Geospatial Mapping: Interactive World Map for Attack Origins and Targets

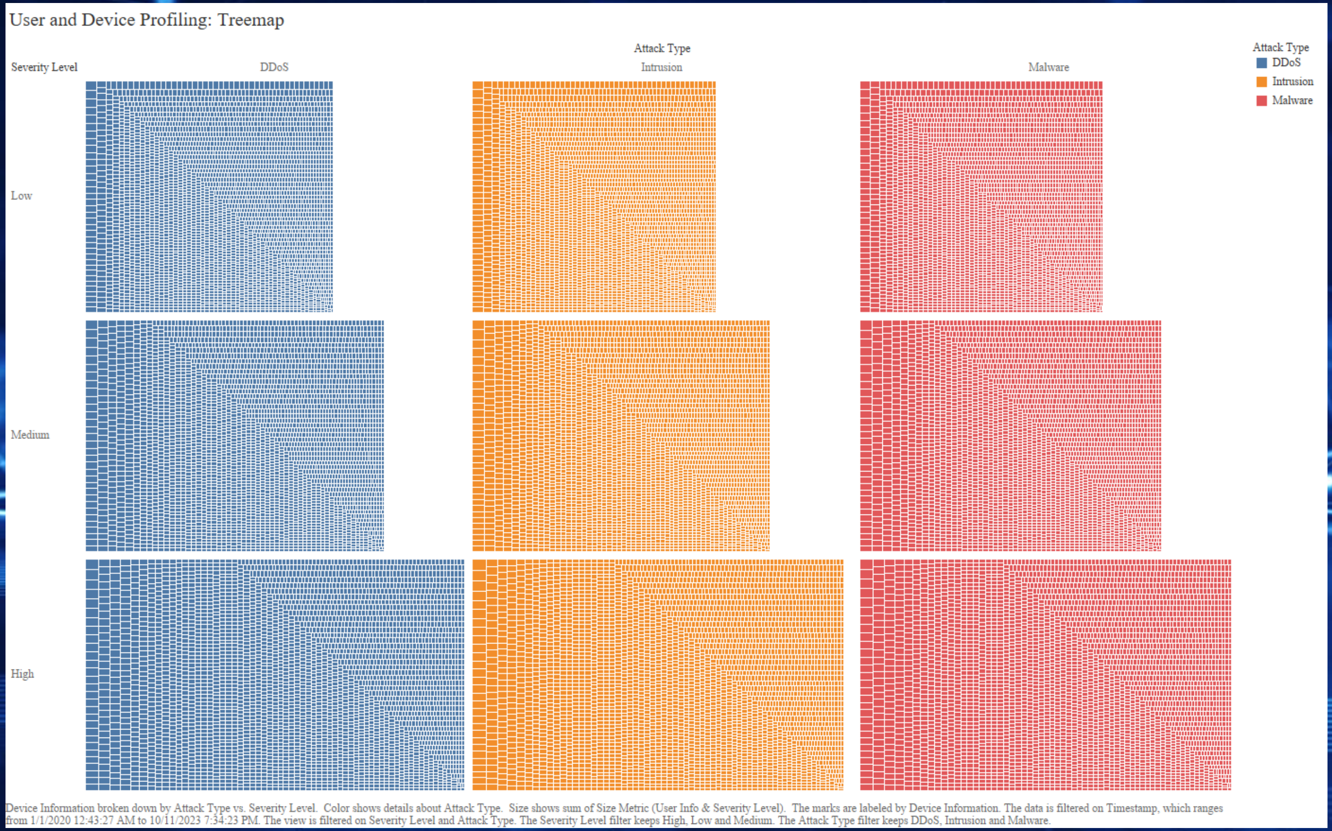


Map based on average of Longitude and average of Latitude. Color shows details about Attack Type as an attribute. Size shows details about Severity Level. Details are shown for Source IP Address. The data is filtered on Attack Type and Timestamp. The Attack Type filter keeps DDoS, Intrusion and Malware. The Timestamp filter ranges from 1/1/2020 12:43:27 AM to 10/11/2023 7:34:23 PM. The view is filtered on Severity Level, which keeps High, Low and Medium.



User and Device Profiling

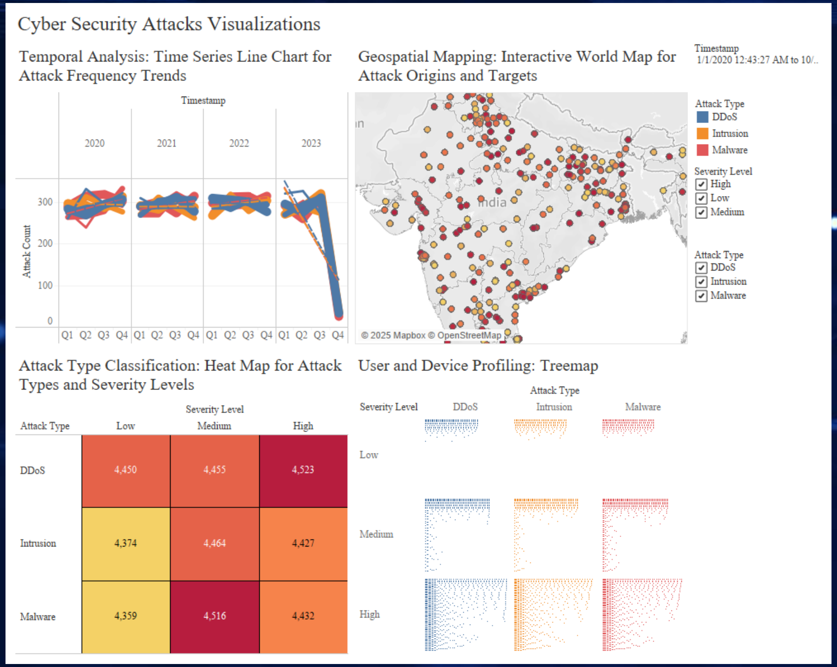
- **Methodology:**
  - Profiling based on severity levels and attack types.
- **Insight:**
  - Identified vulnerable devices and user patterns for targeted defense strategies.



User and Device Profiling: Treemap

Device Information broken down by Attack Type vs. Severity Level. Color shows details about Attack Type. Size shows sum of Size Metric (User Info & Severity Level). The marks are labeled by Device Information. The data is filtered on Timestamp, which ranges from 1/1/2020 12:43:27 AM to 10/11/2023 7:34:23 PM. The view is filtered on Severity Level and Attack Type. The Severity Level filter keeps High, Low and Medium. The Attack Type filter keeps DDoS, Intrusion and Malware.

Key Findings & Actionable Insights



Cyber Security Attacks Visualizations

Temporal Analysis: Time Series Line Chart for Attack Frequency Trends

Timestamp
2020
2021
2022
2023
Attack Count
300
200
100
0
Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4 Q1 Q2 Q3 Q4

Geospatial Mapping: Interactive World Map for Attack Origins and Targets

India
© 2025 Mapbox © OpenStreetMap

Timestamp
1/1/2020 12:43:27 AM to 10/..

Attack Type
🟦 DDoS
🟧 Intrusion
🟥 Malware

Severity Level
☑ High
☑ Low
☑ Medium

Attack Type
☑ DDoS
☑ Intrusion
☑ Malware

Attack Type Classification: Heat Map for Attack Types and Severity Levels

	Severity Level		
Attack Type	Low	Medium	High
DDoS	4,450	4,455	4,523
Intrusion	4,374	4,464	4,427
Malware	4,359	4,516	4,432

User and Device Profiling: Treemap

- **Findings:**
  - Equal distribution of attack types suggests need for comprehensive security
  - 67.05% of attacks are medium to high severity, necessitating prompt response
  - Diverse geographical origins highlight need for global threat intelligence
  - Balanced protocol usage calls for multi-layer security approach

- **Recommendations / Actionable Insights:**
  - Implement targeted security for DDOS, Malware, and Intrusion attacks
  - Prioritize response strategies based on severity
  - Strengthen defenses across all protocol types

Live Demonstration

Challenges & Future Work

- **Challenges:**
  1. Managing large, complex datasets with multiple metrics
  2. Creating intuitive and clear visualizations from complex data
- **Future Improvements:**
  1. Integrate real-time data feeds for live analysis
  2. Develop AI-driven predictive models based on identified patterns
  3. Expand dataset to include more diverse attack vectors

THANK YOU

QUESTIONS?

TIHARMON@USCD.EDU

YOUTUBE: @SECURITYCYBERGEEK