CYBERSECURITY ATTACKS

-RASIKA JADHAV

OBJECTIVES:

The primary objective is to present a clear and concise overview of cybersecurity attack data, likely for analysis and decision-making purposes. By visualizing key metrics, the dashboard aims to provide actionable insights for security teams to mitigate and prevent future attacks.

DASHBOARD OVERVIEW:

The dashboard presents a comprehensive view of cybersecurity attacks, categorized by attack type, severity, location, and time. It utilizes a variety of visualizations, including:

- **Geographic Map of India:** Shows the distribution of attacks across different states in India.
- **Pie Chart:** Displays the proportion of different attack types (DDoS, Intrusion, Malware).
- **Stacked Bar Chart:** Illustrates the severity levels of attacks in different cities.
- **Line Chart:** Shows the trend of attacks over the years (2020-2023).
- **Bar Chart:** Presents the count of alerts by browser type (Mozilla, Opera).
- **Tables:** Provide detailed information on malware indicators and actions taken.

Key Components:

- **Interactive Map:** Allows users to explore attack data by location.
- **Filters**: Enable users to drill down into specific data subsets (e.g., state, city, traffic type, year).
- **Charts and Graphs:** Visually represent key metrics and trends.
- **Tables:** Provide detailed data for analysis.
- **Key Performance Indicators (KPIs):** Though not explicitly labelled, the counts and percentages act as KPIs, highlighting the volume and distribution of attacks.

Insights:

- **Dominant Attack Types:** The pie chart reveals that DDoS and Intrusion attacks each make up 35% of the total, followed by Malware at 30%. This suggests a need for strong defence against these prevalent attack vectors.
- **Geographic Distribution:** The map highlights that attacks are dispersed across India, with some states experiencing higher activity. This indicates a need for geographically targeted security measures.
- **Severity Levels:** The stacked bar chart shows the severity of attacks in different cities. Analyzing this can help prioritize resources to the most affected areas.
- **Temporal Trends:** The line chart indicates the trend of attacks over time. Analyzing the patterns and fluctuations can help anticipate future threats.

- **Browser-Specific Alerts:** The bar chart shows the number of alerts associated with different browsers, suggesting potential vulnerabilities or usage patterns.
- **Malware Indicators:** The table provides detailed information on specific malware indicators, enabling proactive threat detection and response.
- **Actions Taken:** The table detailing actions taken (Logged, Ignored, Blocked) provides insights into the effectiveness of incident response procedures.

CONCLUSION:

The dashboard provides a valuable tool for monitoring and analyzing cybersecurity attacks. By visualizing key data points and trends, it enables security teams to:

- Gain a comprehensive understanding of the attack landscape.
- Identify vulnerabilities and prioritize resources.
- Develop effective mitigation and prevention strategies.
- Improve incident response procedures.