Enterprise Cybersecurity SOC Intelligence Dashboard - Power BI Project

Project Overview

This project focuses on building an enterprise-level Cybersecurity Security Operations Center (SOC) Intelligence Dashboard using Power BI. The dashboard helps organizations monitor cyber attacks, analyze threat patterns, measure security risks, and improve incident response performance.

Project Objectives

1. Monitor global cyber attack trends and threat patterns
2. Analyze attack types such as DDoS, brute force, and botnet attacks
3. Measure incident response time and security performance
4. Identify high-risk systems and vulnerabilities
5. Provide executive-level cybersecurity decision intelligence

Datasets Used

1. CICIDS 2017 Intrusion Detection Dataset

Source: Canadian Institute for Cybersecurity
Link: https://www.unb.ca/cic/datasets/ids-2017.html

Description:
This dataset contains real-world cyber attack traffic data used for intrusion detection research and SOC analytics.
Includes Attack Types:

1. Distributed Denial of Service (DDoS)
2. Brute Force Attacks
3. Botnet Attacks
4. Port Scanning
5. Web Attacks

2. MaxMind GeoLite2 IP Geolocation Dataset

Source: MaxMind
Link: https://dev.maxmind.com/geoip/geolite2-free-geolocation-data/

Purpose:
Used to map attack source locations and create geographic threat visualizations.

3. MITRE ATT&CK; Threat Intelligence Framework

Source: MITRE Organization
Link: https://attack.mitre.org/

Purpose:
Used to categorize cyber attacks into tactics, techniques, and procedures for advanced threat

analytics.

Recommended Data Model

Fact Tables:
1 Security Events
2 Network Traffic Logs
3 Incident Response Records
Dimension Tables:
1 Date and Time
2 Attack Type
3 IP Address
4 Country
5 Severity Level
6 Affected System

Dashboard Pages

1 Executive Cyber Risk Overview Dashboard
2 Live Attack Intelligence Map
3 Threat Pattern Analysis Dashboard
4 Incident Response Performance Dashboard
5 System and Asset Risk Dashboard

Tools and Technologies

1 Power BI Desktop
2 Power Query for Data Transformation
3 Advanced DAX Calculations
4 CSV and Large Log Dataset Handling
5 Python (Optional for anomaly detection)

Key Performance Indicators (KPIs)

1 Total Cyber Attacks
2 High Severity Attack Count
3 Mean Time to Detect (MTTD)
4 Mean Time to Respond (MTTR)
5 Risk Severity Score
6 Attack Growth Trend