Threat Detection Dashboard Project

Project Title

Threat Detection Dashboard Using API Integration and Power BI

Project Overview

This project was about building a real-time Power BI dashboard to help visualize cybersecurity threats. Using APIs from tools like Splunk, CrowdStrike, and Microsoft Defender, I automated data collection and analysis. The dashboard brought together fragmented data and turned it into actionable insights. It provided a clear view of threats, their severity, and resolution statuses, helping teams stay ahead of potential risks and make better security decisions.

Project Challenge

The biggest hurdle was the scattered nature of cybersecurity data. With information coming from multiple tools, it was hard for stakeholders to see the bigger picture. I needed to automate data gathering, ensure it was accurate, and create a dashboard that anyone—technical or not—could easily use.

My Objectives

- Automate pulling threat data from Splunk, CrowdStrike, and Microsoft Defender APIs.
- Organize the data into a well-structured database.
- Design a Power BI dashboard that visualizes key metrics like threat trends and resolution times.
- Make the dashboard user-friendly and accessible for decision-makers.

What I Did

1. **API Integration**
    - Developed Python scripts to connect to APIs from Splunk, CrowdStrike, and Microsoft Defender.
    - Pulled real-time data and cleaned it for accuracy and consistency.
2. **Data Processing**
    - Preprocessed the data and stored it in a SQL database.
    - Organized fields like threat type, severity, timestamps, and resolution status.
3. **Dashboard Development**
    - Connected the SQL database to Power BI using direct query for real-time updates.

    - Created visuals, such as line charts for trends, pie charts for resolutions, and tables for detailed threat analysis.
    - Added interactive filters to let users explore specific date ranges, threat types, or severity levels.
4. **Deployment and Testing**
    - Published the dashboard on Power BI Service for easy access.
    - Tested its functionality and incorporated feedback from stakeholders to ensure it met their needs.

Results

- Delivered a fully functional, interactive Power BI dashboard that simplified threat monitoring.
- Helped the team improve resolution times for critical threats.
- Made it easier for stakeholders to understand cybersecurity risks through clear and actionable visuals.
- Boosted engagement with an easy-to-use, real-time dashboard.

What I Learned

- Enhanced my skills in integrating APIs using Python and working with real-time data.
- Learned how to preprocess and structure data to make it usable and reliable.
- Gained experience designing interactive, user-friendly dashboards in Power BI.
- Developed my ability to communicate complex cybersecurity information to non-technical audiences.

Challenges

- Handling inconsistent data formats from APIs required additional preprocessing steps.
- Ensuring real-time updates in Power BI without compromising performance.
- Balancing detailed insights with simplicity to make the dashboard useful for all users.

Competencies Gained

- **Technical Skills:**
    - Python for API integration.
    - SQL for database management.
    - Advanced Power BI for dashboard design.
- **Problem-Solving:**
    - Managed data inconsistencies and optimized performance for real-time updates.
- **Communication:**
    - Transformed complex data into clear visuals that made sense to everyone.