CASE STUDY

Enhanced Security Insights through Custom Threat Modeling and PowerBI Integration.

A global organisation with a global user base

A leading multinational software corporation with a significant online presence was facing escalating cybersecurity threats due to its vast digital infrastructure. The company specializes in providing digital services to a global user base, necessitating a robust network of applications and data flows that require constant monitoring and protection.

CHALLENGE

Inconsistent data

The security team was using multiple tools to assess and mitigate threats, leading to fragmented and sometimes inconsistent data analysis. They needed a unified Threat Modeling Software-as-a-Service (TMSaaS) solution that could:

- Seamlessly integrate with their existing cybersecurity framework.
- Allow for the generation of custom reports to visualize and track potential threats effectively.
- Provide actionable insights to refine their security measures continuously.

Threat Modeling as a Service

The company selected a TMSaaS solution known for its comprehensive analysis features and robust API support. This solution enabled them to model threats across various assets and provided a framework for ongoing security assessments.

Extensible and Flexible API

- API Capabilities: The TMSaaS's APIs allowed for detailed data extraction on assets, threats, vulnerabilities, and countermeasures, which could be tailored to their specific needs.
- Custom Integration: Developers used these APIs to create custom connectors that pushed threat modeling data into PowerBI, ensuring that the data flow was both secure and consistent.
- Automation: Scripts were set up to periodically update the threat data, ensuring that the PowerBI dashboards always reflected the most current information.

Configuring PowerBI for Custom Reporting

To maximize the utility of the Threat Modeling SaaS, the company took several steps to configure PowerBI to ingest this data and display insightful reports:

Data Ingestion and Transformation

1. API Data Fetching:
    - Developers wrote Python scripts that called the Threat Modeling SaaS’s API endpoints to fetch the latest threat data.
    - These scripts ran on a scheduled basis, ensuring that data was regularly updated.
2. Data Processing:
    - The raw data from APIs was processed using Power Query in PowerBI. This included filtering, sorting, and transforming data to fit the company’s reporting needs.
    - Relationships were established between different data tables (e.g., linking assets to identified threats) to enable comprehensive analysis.

Dashboard and Report Design

3. Visualizations:
    - Custom visualizations were created in PowerBI to represent the threat data effectively. This included:
        - Heat Maps: To show the distribution of threats across different assets.
        - Bar Charts: To display the number of threats by severity and category.
        - Line Graphs: To track threat evolution over time.
        - Pie Charts: To illustrate the breakdown of vulnerabilities by type.
4. Interactive Features:
    - Slicers and filters were added to allow users to drill down into specific time frames or threat categories:
    - Tooltips and drill-through capabilities were configured so that users could get more detailed information on specific threats or assets by clicking on visual elements.

Alerts and Notifications

5. PowerBI Alerts:
    - The company set up PowerBI to send alerts when certain thresholds were met, such as a high number of threats detected within a short period.
    - These alerts were configured to trigger emails to the security team, ensuring prompt attention to potential issues.

Training and Support

- Training: Comprehensive documentation and internal training sessions were provided to ensure the security team could fully leverage the new PowerBI dashboards.
- Support: Continuous technical support ensured smooth functioning of the APIs and helped resolve any issues with data integration or visualization.

Success Criteria

The implementation was evaluated against key performance indicators:

1. Efficiency: The time required to identify and respond to threats decreased by 40% due to real-time data updates and enhanced visual analytics.
2. Accuracy: The precision in pinpointing vulnerabilities improved by 30%, facilitated by tailored reports and comprehensive dashboards.
3. User Adoption: More than 95% of the security team utilized the new dashboards within the first month, indicating strong adoption and approval.
4. Scalability: The solution proved highly scalable, easily accommodating additional assets and threat models without major overhauls.

Conclusion

The integration of an extensible Threat Modeling SaaS with a flexible API into PowerBI transformed the company's approach to cybersecurity. Custom reports and dashboards provide deep insights into the security landscape, enabling the team to act swiftly and accurately against threats. This strategic implementation not only enhanced their security posture but also underscored the importance of a proactive, data-driven approach in cybersecurity management.