Cybersecurity Incident Reporting System

Project Overview

This project addresses the common organizational challenge of inconsistent and inefficient cybersecurity incident reporting. Employees often lack a clear method for reporting threats, resulting in delayed responses and limited visibility for security teams. The proposed solution introduces a centralized, automated reporting ecosystem built entirely within the Microsoft Power Platform.

Solution Summary

The system integrates three key components: a streamlined incident submission form, automated alert workflows, and an analytical dashboard. Together, they create a fast, reliable, and data-driven reporting loop that enhances security awareness and responsiveness across the organization.

Key Components

1. Incident Submission Interface

A clean and intuitive reporting form is developed using Microsoft Power Apps or SharePoint. The interface captures essential incident attributes such as category, severity, time, user details, and a concise description. The design emphasizes accessibility and ease of use to ensure consistent reporting across teams.

2. Automated Alert Workflow

Using Microsoft Power Automate, every submitted incident triggers an immediate notification to the security team. Alerts are delivered via Microsoft Teams or email and include all relevant details for rapid triage. This automation eliminates manual follow-up and ensures that no incident goes unnoticed.

3. Real-Time Incident Dashboard

A dynamic Power BI dashboard visualizes trends, severity levels, incident status, and recurring patterns. The dashboard enables security teams to make informed decisions, prioritize threats, and assess overall risk posture—all in real time.

Implementation Approach

The project follows a structured rollout:

• Design & Setup: Requirements gathering, data structure planning, and form prototyping.
• Automation & Integration: Building and testing workflows for timely notifications.
• Visualization & Validation: Developing the dashboard and conducting end-to-end testing.
• Deployment & Handover: Final rollout with documentation, training, and operational guidance.

Project Benefits

This solution transforms cybersecurity incident handling into a streamlined, proactive, and data-enriched process. It enhances user engagement, strengthens organizational readiness, and provides security teams with immediate visibility into emerging threats.

Conclusion

By integrating Microsoft 365 tools into one cohesive workflow, the organization gains a modern, scalable, and efficient incident reporting system. The solution not only accelerates response times but also supports a long-term security strategy through improved awareness, accountability, and analytics.