"Guarding Your Feline's World with Excellence"

Protection - "Guarding" reinforces the defense aspect
Care - "Your Feline's World" shows personalized attention
Quality - "Excellence" reflects the premium nature of the brand

***** Internal Confidential *****

Technical Design Document

Project Title: Cybersecurity Awareness and Incident Reporting Tool
Version: 1.0
Date: November 2025
Author: Premium Cat Defense

1. Executive Summary

The *Cybersecurity Awareness and Incident Reporting Tool* is designed to streamline the reporting, triaging, and monitoring of cybersecurity incidents within the organization. By leveraging the Microsoft Power Platform, this solution empowers employees to report incidents efficiently while providing the security team with real-time insights and analytics.

The system integrates **Power Apps**, **Power Automate**, and **Power BI** to create a unified, low-code solution that enhances awareness, responsiveness, and accountability in incident management.

2. Objectives

- Simplify cybersecurity incident reporting for all employees.
- Enable automatic notification of the security response team through Microsoft Teams and email.
- Provide real-time analytics and visualization of incident data using Power BI.
- Improve visibility into incident trends and response effectiveness.

3. Scope

In-Scope

- Creation of an incident submission interface (Power Apps or SharePoint).
- Automation of alerts and notifications (Power Automate).
- Development of a Power BI dashboard for tracking and analytics.
- User access management aligned with Microsoft 365 roles.

Out-of-Scope

- Integration with external ticketing systems (e.g., ServiceNow).
- Automated remediation or threat intelligence correlation.
- Mobile app development beyond Power Apps' default compatibility.

4. System Architecture Overview

Architecture Layers

1. **Presentation Layer:**
    - Power Apps or a SharePoint form for incident submission.
2. **Logic & Automation Layer:**
    - Power Automate workflows for routing and notifications.
3. **Data Layer:**
    - SharePoint List (or Dataverse table) to store incident data.
4. **Analytics Layer:**
    - Power BI Dashboard connected to the incident data source.

Architecture Diagram (Conceptual)

[User]
  ↓
[Power Apps Form / SharePoint List]
  ↓
[Power Automate Flow]
  ↳ Notify [Microsoft Teams Channel]
  ↳ Send [Email Alert to Security Team]
  ↓
[SharePoint / Dataverse Database]
  ↓
[Power BI Dashboard]

5. Functional Design

5.1 Incident Submission

- Users access a Power Apps form or SharePoint list titled **"Cyber Incident Submission."**
- Required fields:
    - Reporter Name (auto-filled from Microsoft 365 profile)
    - Department
    - Incident Type (Phishing, Data Loss, Unauthorized Access, etc.)
    - Description
    - Severity (Low / Medium / High / Critical)
    - Attachments (optional)
    - Status (default: *Open*)

5.2 Workflow Automation

- Power Automate triggers when a new incident record is created.
- Actions:
    1. Parse form data.
    2. Send nota notification message to a predefined **Microsoft Teams Security Channel**.
    3. Send email to **Security Team Distribution List**.
    4. Update the SharePoint List with timestamp and unique Incident ID.

5.3 Incident Tracking & Analytics

- Power BI connects to the same data source.
- Dashboard visuals include:
    - **Incident Volume by Severity**
    - **Incident Status (Open, In-Progress, Resolved)**
    - **Incident Trends Over Time**
    - **Top Incident Types**
    - **Department-wise Breakdown**

5.4 User Roles

Role	Description	Access Level
Employee	Submits incidents	Power Apps form access only
Security Analyst	Reviews and updates the status	Edit rights on the SharePoint List
Administrator	Manages flows, dashboard, and permissions	Full access

6. Data Design

6.1 Data Model

Primary Table: Incident_Reports

Field Name	Data Type	Description
IncidentID	Auto-number	Unique incident identifier
ReporterName	Text	Auto-filled from user profile
Department	Choice	Department list
IncidentType	Choice	Type of cybersecurity incident
Description	Multi-line text	User-provided details
Severity	Choice	Low / Medium / High / Critical
Status	Choice	Open / In-Progress / Resolved
CreatedDate	DateTime	Auto-generated
ResolvedDate	DateTime	Optional

7. Security & Compliance

- **Authentication:** Microsoft 365 SSO via Power Platform.
- **Authorization:** Role-based permissions via SharePoint/Dataverse.
- **Data Protection:**
  - All data is stored in Microsoft 365 cloud (encrypted at rest and in transit).
  - Access restricted to authorized internal users.
- **Compliance:** Aligns with internal cybersecurity policy and GDPR principles.

8. Workflow Automation Logic

Step	Trigger	Action	Output
1	New incident submitted	Power Automate Flow starts	Capture incident details
2	Parse input data	Generate Incident ID	Unique key created
3	Notify Teams	Adaptive Card sent to Security Channel	Instant visibility
4	Send Email	Email sent to Security Distribution	Confirmation alert
5	Update Record	Timestamp stored	Log completed

9. Power BI Dashboard Specification

Data Source: SharePoint List / Dataverse
Refresh Frequency: Every 30 minutes
Visual Components:

- KPI Cards (Total Incidents, Open Incidents, Critical Severity)
- Donut Chart (Incident by Severity)
- Line Chart (Monthly Trend)
- Table View (Detailed listing)
- Filter Pane (Status, Department, Date Range)

10. Deployment and Maintenance

10.1 Environment Setup

Environment	Description
Development	For building and testing of Power Apps and flows
Production	Live environment for business users
Data Source	M365 SharePoint site collection

10.2 Maintenance Plan

- Weekly data validation by admin.
- Monthly dashboard performance review.
- Power Automate health check for failed runs.

11. Risk Assessment

Risk	Impact	Mitigation
Incorrect form submission	Medium	Validation rules in Power Apps
Notification delivery failure	High	Enable flow retry policy
Unauthorized data access	High	Enforce M365 conditional access
Data growth over time	Medium	Archive old incidents annually

12. Future Enhancements

- Integration with Microsoft Sentinel for SIEM correlation.
- AI-based incident classification using Power Automate AI Builder.
- End-user training modules within Power Apps (Cyber Awareness Tips).

13. Appendix

References:

- Microsoft Power Platform Documentation
- Microsoft 365 Security & Compliance Center
- Organization's Cybersecurity Policy (v3.2)