"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 *****

Problem Statement

In many organizations, cybersecurity incident reporting is inconsistent, fragmented, or entirely manual. Employees often lack a clear, standardized process for reporting security-related issues such as phishing attempts, unauthorized access, or suspicious system behavior. As a result, valuable time is lost in identifying, escalating, and resolving potential threats.

This lack of an efficient incident reporting mechanism can lead to:

- **Delayed response times** increase the likelihood of damage or data loss.
- **Incomplete or inaccurate information** that hinders proper risk assessment.
- **Limited visibility** for the security team into recurring or high-risk patterns.

To address these challenges, there is a need for a **streamlined, centralized, and automated solution** that enables employees to easily report incidents and empowers the security team with real-time insights for rapid response and risk mitigation.

Objectives and Scope

Objectives

The primary objectives of this project are to:

1. **Develop a centralized incident reporting tool** that simplifies and standardizes how employees report cybersecurity issues.
2. **Automate notifications and escalation** to ensure the security team receives instant alerts for every submitted incident.
3. **Enable data-driven decision-making** by visualizing incident trends, severity, and resolution status through interactive dashboards.
4. **Promote cybersecurity awareness** by embedding easy-to-use reporting features and encouraging proactive user behavior.

Scope

The project's technical scope includes:

- **Incident Submission Form:** Built using Microsoft Power Apps or SharePoint, capturing key fields such as incident type, risk level, date, user, and description.

- **Automation Workflow:** Implemented in Microsoft Power Automate to trigger alerts to the security team's Microsoft Teams channel or email upon new incident submission.
- **Incident Dashboard:** Developed in Microsoft Power BI to track incident counts, categories, severity levels, and resolution status in real time.

Out of scope are external integrations beyond Microsoft 365, mobile app development, and large-scale enterprise deployment — these may be considered in future phases.

Proposed Solution and Implementation Plan

Proposed Solution

To address the identified challenges in cybersecurity incident reporting and awareness, the project proposes developing an **integrated, automated incident reporting and monitoring tool** using Microsoft's Power Platform suite.

The solution will consist of three interconnected components:

1. **Incident Reporting Interface (Power Apps or SharePoint):**

    - A user-friendly form that allows employees to log incidents quickly and accurately.
    - Fields will include *incident type*, *risk level*, *date/time*, *reporting user*, and *description*.
    - Designed with simplicity and accessibility in mind to encourage consistent reporting across departments.

2. **Automated Notification Workflow (Power Automate):**

    - Upon submission of a new incident, an automated process will instantly notify the cybersecurity team through Microsoft Teams and/or email.
    - Notifications will include key incident details for immediate triage.

- Automation ensures no report is missed and reduces manual communication overhead.

3. **Incident Monitoring Dashboard (Power BI):**

   - A dynamic dashboard visualizing incident data in real time.
   - Tracks metrics such as *total incidents*, *severity distribution*, *incident status (open/resolved)*, and *trend over time*.
   - Enables the security team to assess risk levels, identify recurring threats, and monitor response effectiveness.

This integrated ecosystem ensures a **closed-loop process** — from incident submission to notification, analysis, and resolution — thereby improving security visibility, accountability, and responsiveness.

Implementation Plan

The implementation will be executed in **three key phases**, ensuring quality, alignment, and timely delivery:

Phase	Description	Key Deliverables
Phase 1 – Design & Setup	Gather requirements, design form layout, define data fields, and configure SharePoint/Power Apps.	Incident submission form prototype
Phase 2 – Automation & Integration	Develop automated workflows for notifications and escalation using Power Automate; connect with Teams or email.	Functional automation workflow
Phase 3 – Visualization & Testing	Create Power BI dashboards, integrate data sources, and conduct testing for accuracy and user experience.	Fully functional incident tracking dashboard
Phase 4 – Deployment & Documentation	Deploy the solution in a controlled environment; create a user guide and technical documentation for handover.	Deployed solution and documentation

Each phase will include review checkpoints, testing, and user validation to ensure the tool aligns with organizational cybersecurity policies and operational needs.