Project Title:
Unified Cyberattack Simulation and Threat Intelligence Platform

TEAM NO.: 38
NAMES OF THE STUDENTS PARTICIPATED IN THE TEAM:
Archana S R, Ashwini B

COLLEGE: SAMBHRAM INSTITUTE OF TECHNOLOGY
SEMESTER: 8
DEPARTMENT: CSE (CYBER SECURITY)
CITY: BENGALURU
STATE: KARNATAKA
PROJECT MENTOR NAME: NARENDRA ELURI

Vodafone Idea Foundation

VOIS

Connecting Dreams Foundation

Project Details:

An interactive platform that simulates real-world cyberattacks to analyze user behavior, improve cybersecurity awareness, and reduce human-related risks through phishing simulations, threat intelligence, and suspicious website analysis.

Problem Statement:

Government employees are frequent targets of phishing, ransomware, and other cyberattacks due to their access to sensitive systems and data. Insufficient cybersecurity awareness and lack of practical training significantly increase the risk of data breaches, operational disruption, and compromise of sensitive national information.

Need of Project:

With the rapid growth of digital services, organizations—especially government and enterprise environments—are increasingly exposed to cyber threats such as phishing, ransomware, social engineering, and malicious websites. Despite deploying advanced technical security solutions, a large number of cyber incidents continue to occur due to **human error**, such as clicking on phishing links, sharing credentials, or failing to identify suspicious online activity.

Traditional cybersecurity awareness programs rely on static methods like presentations, videos, and one-time training sessions, which do not effectively prepare users to face real-world cyberattacks. These methods fail to measure actual user behavior, provide personalized feedback, or assess cybersecurity readiness in a continuous manner. As a result, organizations lack visibility into user-related risks and are unable to identify vulnerable users or areas requiring focused training.

There is also a growing need to integrate **real-time threat intelligence** and **practical investigation tools** into awareness platforms so that users remain informed about current attack trends and learn how attackers operate in real scenarios. Additionally, organizations require a unified mechanism to evaluate cybersecurity awareness through measurable metrics and analytical insights.

Therefore, this project is needed to provide an **interactive, behavior-driven cybersecurity simulation and threat intelligence platform** that enables realistic attack simulations, monitors user actions, delivers personalized awareness feedback, and generates actionable insights. The platform helps organizations reduce human-centric cyber risks, strengthen security culture, and improve overall cybersecurity preparedness.

Proposed Solution:

The proposed solution is a unified cybersecurity simulation and threat intelligence platform that delivers realistic phishing attack simulations to assess user behavior and cybersecurity awareness. The system integrates real-time threat intelligence and suspicious website analysis to provide personalized feedback, actionable insights, and a measurable Cyber Health Score, thereby reducing human-related cyber risks and improving overall security preparedness.

Technology Used:

- **Python:** Core programming language for system logic and analysis
- **Flask:** Backend framework for handling APIs, simulations, and processing
- **React.js:** Frontend framework for interactive and responsive user interface
- **SQLite:** Lightweight database for storing user data, logs, and scores
- **Machine Learning:** Used for behavior-based risk scoring and prediction
- **Email Analysis Engine:** Supports **user email-checking feature** to detect phishing indicators
- **Decision Logic Module:** Implements a **single intelligent decision button** for safe/unsafe guidance
- **DNS & SSL Analysis:** Used for suspicious website and domain investigation (SWHI)
- **REST APIs:** Integration of real-time threat intelligence from external sources

Project Outcomes:

The system effectively simulates real-world cyberattacks using guided phishing simulations and a user email-checking feature to analyze real emails. It monitors user behavior, identifies cybersecurity awareness gaps, and provides AI-driven actionable feedback along with real-time threat visibility. The platform also generates a measurable Cyber Health Score, helping organizations reduce human-related cyber risks and improve overall security readiness.

Modelling: The project consists of the following main steps:

1) Threat Scenario Creation and Data Collection

Realistic phishing email scenarios are created along with a **guided phishing decision mechanism** using a single intelligent decision button. In addition, a **user email-checking feature** allows users to submit real emails for phishing analysis. User interaction events such as clicking links, safe/unsafe decisions, reporting emails, quiz responses, and suspicious website inputs are collected. All user actions are securely logged by the system for further analysis.

2) Behavioral Analysis and Risk Evaluation

The collected interaction data is processed using predefined behavioral rules and scoring logic. User actions are analyzed to identify risky behavior, awareness gaps, and threat susceptibility. Based on this evaluation, cybersecurity risk levels and awareness scores are calculated, reflecting the user's security decision-making ability.

3) Real-Time Simulation, Analysis, and Feedback

During real-time usage, the system continuously monitors user behavior while interacting with phishing simulations, the email-checking feature, quizzes, and suspicious website analysis modules. The analyzed results are visualized through dashboards, **personalized AI-driven feedback** is generated, and a **dynamic Cyber Health Score** is updated to improve individual awareness and organizational security posture. The overall workflow of these steps is illustrated in the block diagram below.

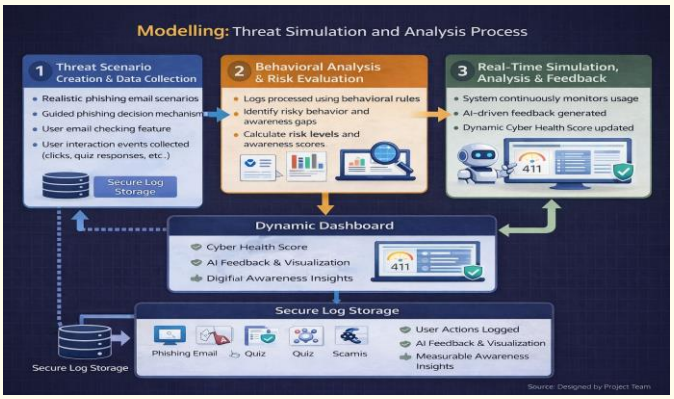
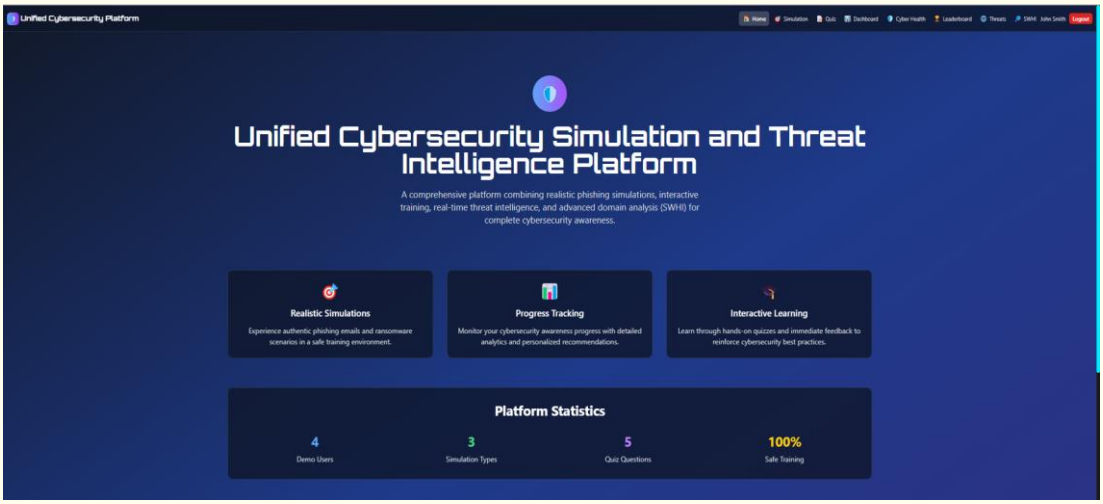


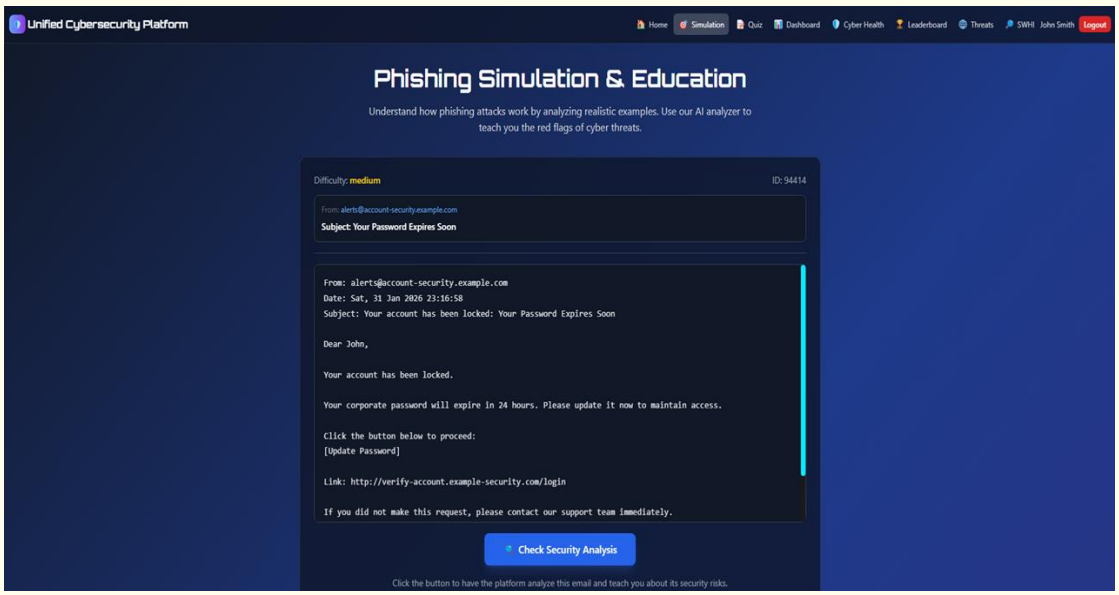
Fig: Modelling

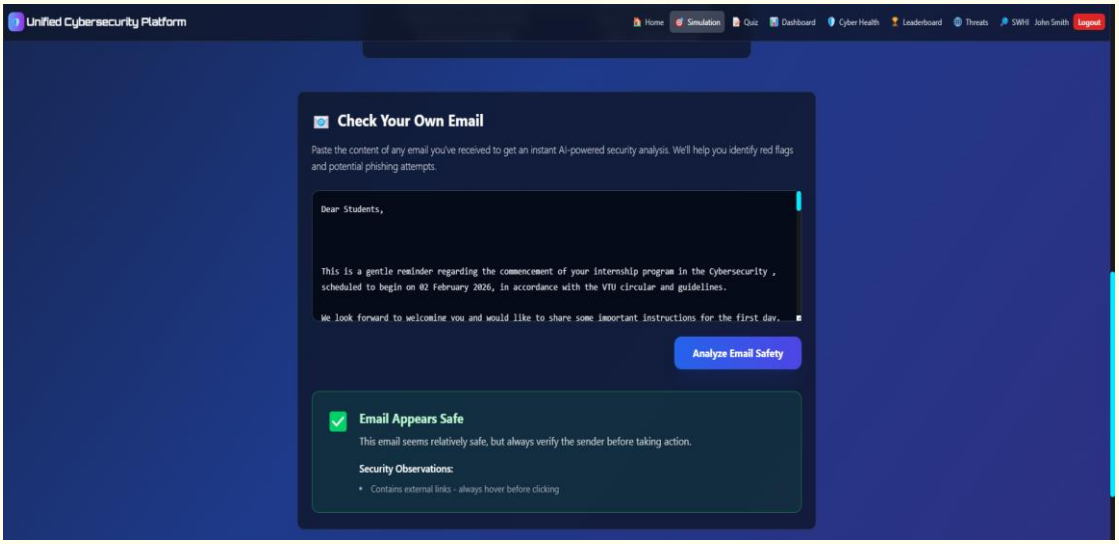
Results:

1. Home Page

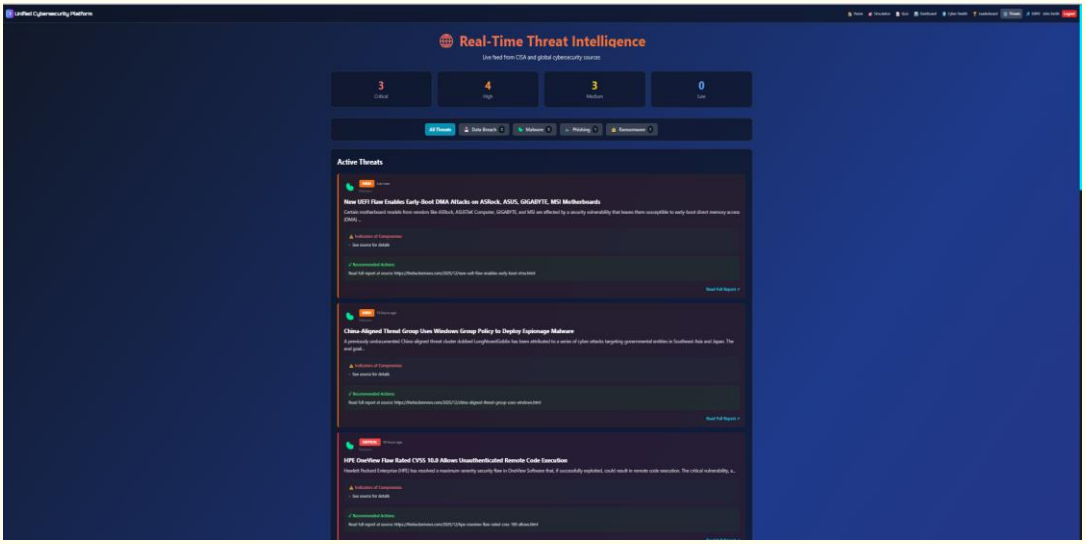


2. Phishing Simulation

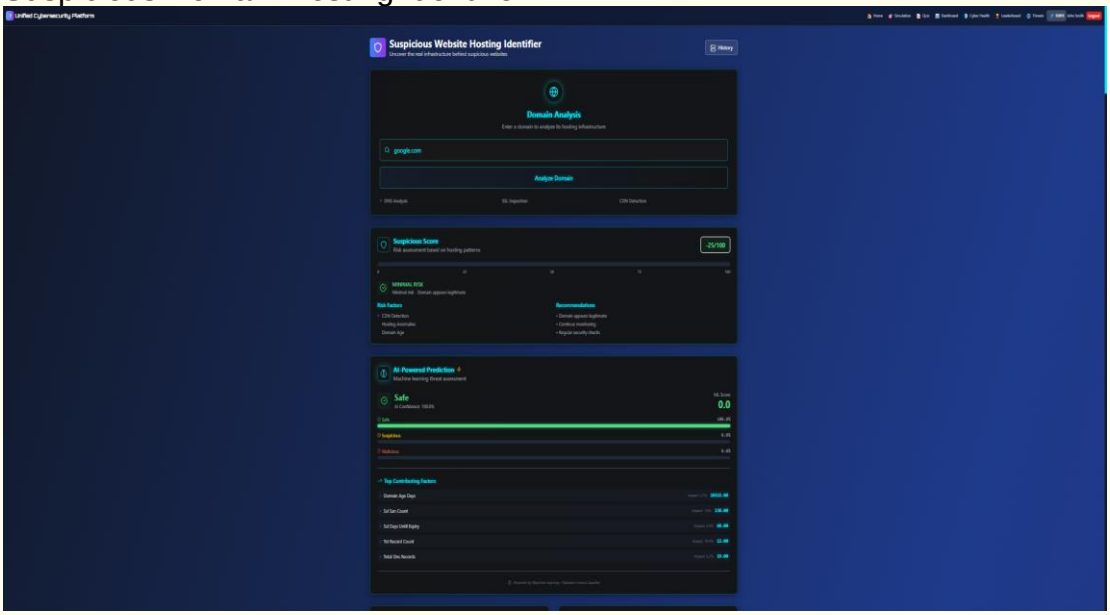




3. Real-time Threat Intelligence Feeds



4. Suspicious Domain Hosting Identifier



5. Results of SWHI

6. Dashboard

Future Scope for Project Enhancement:

The proposed system can be further enhanced by introducing more advanced phishing scenarios and attack variations to better simulate real-world cyber threats. The platform can be extended to support a larger number of users and organizations with improved scalability and cloud deployment. Integration of advanced AI models can enable more accurate behavior prediction and risk assessment. Additionally, expanding threat intelligence sources and automating report generation will further improve decision-making and strengthen overall cybersecurity awareness.