Final Report

1. INTRODUCTION

1.1 Project Name

Leveraging Real-Time Security Intelligence for Enhanced Defense

1.2 Purpose

This project aims to enhance cybersecurity by leveraging real-time security intelligence for proactive threat detection and defense. It focuses on identifying vulnerabilities, analyzing risks, and implementing mitigation strategies to prevent potential cyber threats. The scope of the project includes threat intelligence gathering, vulnerability assessment, and the development of a secure framework.

---

2. IDEATION PHASE

2.1 Thought Behind the Project

With the rise in cyber threats, organizations need real-time intelligence to protect their systems. Our team brainstormed various ideas, including:

- Developing a security framework that detects vulnerabilities in real-time
- Implementing AI-driven threat detection mechanisms
- Utilizing open-source intelligence tools for cybersecurity monitoring

2.2 Features

This project involves:

- Collecting data on cybersecurity threats from various sources
- Implementing real-time monitoring and alerting systems
- Enhancing security policies based on threat intelligence reports

2.3 Empathy Map

Empathy mapping helped us understand the challenges faced by security teams:

- **What users say**: "We need faster threat detection and mitigation."
- **What users think**: "Current security tools are not sufficient for real-time defense."
- **What users feel**: "Concerned about data breaches and cyber attacks."
- **What users do**: "Continuously monitor security logs and reports."

---

3. REQUIREMENT ANALYSIS

3.1 List of Vulnerabilities

Common cybersecurity vulnerabilities include:

- SQL Injection
- Cross-Site Scripting (XSS)
- Phishing attacks
- Malware and ransomware threats
- Insider threats

3.2 Solution Requirement

To mitigate these vulnerabilities, the system must include:

- Real-time threat intelligence feeds
- Automated vulnerability scanning
- Incident response mechanisms
- Secure authentication and access control

3.3 Technology Stack

The project will use:

- **Security Tools**: Nessus, Snort, Metasploit
- **Programming Languages**: Python, Bash scripting
- **Cloud Platforms**: AWS Security Hub, Microsoft Defender
- **Databases**: PostgreSQL, Elasticsearch

---

4. PROJECT DESIGN

4.1 Overview of Nessus

Nessus is a vulnerability scanner that helps identify security flaws in IT systems. It performs comprehensive vulnerability assessments, providing detailed reports on system weaknesses and recommended fixes.

4.2 Proposed Solution

The proposed solution integrates:

- **Real-time security intelligence feeds** for proactive defense
- **Automated vulnerability scanning** using Nessus

- **AI-based threat detection models** for enhanced monitoring
- **Incident response framework** to mitigate attacks quickly