**Detailed Project Plan**

**PROJECT TITLE**AI-Driven Cybersecurity Framework for Intelligent Threat Detection and Analysis

**1. PROJECT SUMMARY**

The project aims to develop a web-based platform that enables SOC analysts (cybersecurity analysts) to perform attack surface analysis, vulnerability tracking, IP blacklist management, email leakage and phishing analysis, traffic monitoring with IDS, and limited attack simulation on domains they own. The system will be a monolithic structure using backend and frontend framework with a relational database and a web dashboard. Target users are IT proficient security analysts who own at least one domain.

**2. OBJECTIVES**

Implementing secure user identity management (hashed passwords, 2FA), blacklist IP management, automated CVE/CVSS fetch and display, attack surface scanning (ports, SSL), email leak checking, controlled attack simulation, IDS integration for anomaly detection, phishing mail, cryptography utilities, and PDF export of reports.

Providing secure session management (TTL), background task processing, logging and basic security hardening.

**3. DEFINITIONS & ACRONYMS**

Domain: Internet domain owned by the user (e.g., example.com).

Subdomain: A domain-subdivision (e.g., app.example.com).

CVE: Common Vulnerabilities and Exposures.

CVSS: Common Vulnerability Scoring System.

IDS: Intrusion Detection System.

2FA: Two-Factor Authentication

TTL: Time-to-live

Email harvester: Tool that searches public sources for email addresses.

Phishing detection pipeline: ML based analysis chain for email phishing/malware scoring.

**4. SCOPE**

- User management, domain registration and domain ownership verification.

- Blacklisted IP CRUD(Create, Read, Update, Delete) and visualization.

- CVE parsing from NVD or equivalent sources.

- Subdomain attack-surface scans: port scanning, basic service identification, SSL certificate checks

- Email leak checks via public leak APIs or custom harvesters.

- Controlled attack simulation module (DoS/Port Scan/Brute Force) limited to user verified domains, sandboxed and rate-limited.

- IDS log ingestion and anomaly detection using ML algorithms.

- Mail connector and automatic phishing/malware analysis pipeline.

- Cryptography utilities (AES/RSA/hash) accessible via UI.

- PDF export of security reports.

**5. FUNCTIONAL REQUIREMENTS**

IEEE-SRS document includes all the requirements that have been identified.

**6. PROPOSED TECHNICAL ARCHITECTURE, DATA MODELS**

Will be discussed in the next sprint.

**7. LEGAL, ETHICAL & OPERATIONAL CONSTRAINTS**

All scan or simulation actions must be explicitly permitted by domain ownership verification prior to execution.

The platform must enforce Terms of Service and an Acceptable Use Policy and also users must accept before running scans/simulations.

Logging and data retention must follow privacy best practices; sensitive email content should be handled cautiously.

**8. ACCEPTANCE CRITERIA**

Each main feature is accepted when testable and verifiable:

- Auth & Security:

- Register/login flow works; passwords hashed; 2FA email OTP works.

- Session TTL enforces logout after the configured inactivity period.

- Blacklist:

- Users can add/remove IPs; dashboard widget reflects list.

- CVE Feed:

- CVE entries are fetched and stored; CVSS scores and references visible; filters work.

- Attack Surface Scans:

- Subdomain port scan returns open ports and services, SSL expiry and basic certificate checks reported.

- Email Pipeline:

- Mailbox connection works, sample mails produce analysis outputs.

- IDS:

- Received logs produce at least one detectable anomaly scenario in the dashboard.

- Cryptography:

- AES encrypt/decrypt and RSA encrypt/decrypt function correctly for sample inputs.

- Reporting:

- PDF export generates a readable report with findings.

**9. TEST PLAN**

- Unit tests: models, utilities, business logic.

- Integration tests: authentication flows, CVE ingestion, scan job execution.

- Security tests: Automated vulnerability scanners, input validation tests.

- Manual acceptance tests run acceptance criteria scenarios.

- Limited penetration testing within approved scope.

**10. DATA SECURITY & PRIVACY**

- Passwords hashed with argon2/bcrypt.

- Role-based access control (user and admin).

- Regular backups and at least weekly snapshots suggested for DB.