## **Draft Implementation Roadmap – SOC Analyst Platform**

### **Phase 1: Project Setup & Architecture Design (Weeks 1–3)**

**Objectives:**

* Complete all requirement specifications (SRS, STP, PMP, QMP).
* Establish a monolithic backend structure.
* Implement the frontend environment.
* Configure testing, staging, and production environments.

**Deliverables:**

* System architecture document.
* Initialized project repository with directory structure.
* CI/CD pipeline for automated build and deployment.

### **Phase 2: User Management & Security Layer (Weeks 3–5)**

**Features:**

* User registration and login.
* Email-based two-factor authentication (2FA).
* Session TTL (time-to-live) control.
* Password hashing and secure credential storage.
* Role-based access control for Admin, Analyst, and ReadOnly roles.

**Deliverables:**

* Authentication and authorization module.
* Security validation and session tests.
* Role management functionality.

### **Phase 3: Domain Management & Dashboard Core (Weeks 5–7)**

**Features:**

* Domain addition, modification, and removal.
* Domain verification and linking with scanning functions.
* Central dashboard for displaying domain status and system overview.
* Presentation of key indicators such as open ports, SSL validity, and DNS configuration.

**Deliverables:**

* Operational domain management component.
* Backend endpoints for domain operations.
* Integrated dashboard interface.

### **Phase 4: Core Functional Modules (Weeks 7–12)**

**Modules:**

1. **Blacklist & Threat Management**
   1. IP viewing, addition, and removal.
   2. External threat intelligence API integration.
2. **CVE & Vulnerability Management**
   1. Automatic fetching and parsing of CVE data.
   2. Display of vulnerability details and CVSS scores.
3. **IDS & Attack Detection**
   1. Continuous network monitoring and anomaly detection.
   2. Alert generation and notification.
4. **Phishing & Malware Analysis**
   1. Email and file input for automated analysis.
   2. Classification into clean, suspicious, or malicious categories.
5. **Cryptography Tools**
   1. Data encryption and decryption operations.
   2. Public/private key generation utilities.

**Deliverables:**

* Fully functional backend modules.
* Module integration with the dashboard.
* Unit and integration tests for each feature.

### **Phase 5: Reporting & Log Management (Weeks 12–14)**

**Features:**

* Centralized activity logging with timestamp, source, and destination.
* Log viewing and filtering for users and administrators.
* Export of analytical and security reports in PDF format.

**Deliverables:**

* Logging and reporting subsystem.
* PDF export functionality.
* Administrative log interface.

### **Phase 6: Integration & Finalization (Weeks 14–16)**

**Tasks:**

* Integration of all backend modules with frontend components.
* Real-time data update through WebSocket and asynchronous communication.
* Performance, load, and security testing.
* Final UI refinement and documentation.

**Deliverables:**

* Complete integrated system (Version 1.0).
* Final test results and evaluation report.
* Technical and user documentation.

### **Phase 7: Post-Release Enhancements (After Week 16)**

**Extensions:**

* SMS notification system for anomaly alerts.
* Automated isolation of systems during active intrusion.
* Multi-domain support and analysis.
* AI-based risk scoring mechanism.
* Multi-tenant customer management.