# Project Kick-off & Workflow Definition

Insider Threat Detection Using Deception Technology

September 2025

## 1 Objectives

- Build an **Insider Threat Detection System** using deception technology.
- Detect and respond to suspicious insider activities in **real-time**.
- Provide **visibility** via centralized logging and dashboards.

## 2 Team Roles & Responsibilities

- **Marwan (DFIR Lead / Project Manager)** – Design workflow, investigation & response, oversee integration.
- **Sherfa (SOC / Monitoring Lead)** – ELK Stack setup, log collection, dashboard configuration.
- **Shweal (SOC / Alerting & Analysis)** – Define alert rules, analyze logs, detect anomalies.
- **Ahmed (Security / Honeytoken Lead)** – Create & deploy decoys (files, credentials, databases).
- **Karim (Pentest / Threat Simulation Lead)** – Simulate insider threats, validate detection & response.
- **Joseph (Full-Stack / Dashboard Developer)** – Dashboard development, visualization, frontend integration.

## 3 High-Level Workflow

1. **Decoy Deployment** – Honeytokens (fake documents, credentials, databases) deployed in monitored locations.
2. **Monitoring & Logging** – All access attempts logged centrally in the ELK Stack.
3. **Alerting** – Rules trigger alerts when decoys are accessed.
4. **Risk Scoring & Profiling** – User activity analyzed, suspicious behavior flagged, and risk scores assigned.
5. **DFIR Investigation & Response** – Alerts verified and correlated with logs; escalation to Incident Response if malicious activity is confirmed.
6. **Visualization & Reporting** – Dashboard displays alerts, interaction trends, and risk scores. Metrics include detection time, number of alerts, and false positives.

## 4 Tools & Technologies

- Python – Automation and backend scripts.

- ELK Stack (Elasticsearch, Logstash, Kibana) – Logging, alerting, dashboards.
- Honeytokens/Decoys – Detection triggers.
- React / Web UI – Interactive dashboard.
- (Optional) Machine Learning – Anomaly detection and false positive reduction.

## 5 Expected Deliverables (Week 1)

- Workflow diagram.
- Documented workflow (this file).
- Team alignment on objectives, roles, and tools.

## Workflow Diagram