Week 1 Tasks Breakdown

Insider Threat Detection Using Deception Technology

September 2025

Overview

Week 1 focuses on **Project Kick-off & Initial Setup**. Each team member has specific tasks to establish the foundation for the project.

1 Marwan (DFIR Lead / Project Manager)

Task: Project kick-off, define workflow.

- Organize a project kick-off meeting to align objectives and expectations.
- Define the high-level detection and response workflow (from decoy interaction to DFIR response).
- Map each workflow stage to team roles.
- Document incident investigation procedures for insider threat detection.

Expected Output:

- Kick-off meeting notes.
- Workflow document and diagram.

2 Sherfa (SOC / Monitoring Lead)

Task: ELK Stack initial setup.

- Install and configure Elasticsearch, Logstash, and Kibana.
- Verify that log ingestion works with sample test data.
- Prepare initial configuration for centralized log storage.

Expected Output:

- Running ELK Stack instance.
- Documentation of setup steps and configuration files.

3 Shweal (SOC / Alerting & Analysis)

Task: ELK Stack initial setup (support).

- Assist Sherfa in setting up ELK Stack.
- Focus on Kibana dashboards and ensuring logs are visible.
- Begin exploring alerting features in Kibana.

Expected Output:

- Verified log visibility in Kibana.
- Notes on possible alerting rules for decoy interactions.

4 Ahmed (Security / Honeytoken Lead)

Task: Research decoy ideas.

- Research types of honeytokens (files, credentials, fake DB entries).
- Identify suitable decoys for insider threat detection in enterprise settings.
- Draft templates for decoy files and credentials.

Expected Output:

- List of potential decoy assets.
- Draft decoy templates for review.

5 Karim (Pentest / Threat Simulation Lead)

Task: Plan attack simulations.

- Design scenarios of insider threats (credential misuse, unauthorized file access).
- Map scenarios to decoy interactions (e.g., accessing fake credentials).
- Define small-scale test cases for Week 4 validation.

Expected Output:

- Documented attack simulation plan.
- List of test cases for initial evaluation.

6 Joseph (Full-Stack / Dashboard Developer)

Task: Set up dashboard skeleton.

- Create a basic frontend skeleton using React.
- Define layout for alerts, logs, and risk scoring.
- Ensure backend integration points are prepared for ELK data.

Expected Output:

- Running dashboard skeleton with placeholder components.
- Wireframes and design documentation.