Insider Threat Detection Using Deception Technology

Team: Marwan, Sherfa, Shweal, Ahmed, Karim, Joseph

September 19, 2025

Project Brief

Project Title: Insider Threat Detection Using Deception Technology

Objective: Develop a proactive system to detect and respond to insider threats by deploying decoy assets (documents, credentials, databases) that lure malicious insiders. The system monitors interactions, logs activity, profiles user behavior, and triggers alerts in real-time.

Key Features:

1. **Deception Deployment:** Decoy files, credentials, and databases embedded with honeytokens.
2. **Monitoring & Logging:** Centralized log collection using ELK Stack; real-time tracking of decoy interactions.
3. **Alerting System:** Trigger alerts when decoys are accessed and assign risk scores to users.
4. **User Profiling & Analysis:** Distinguish suspicious from normal activity and reduce false positives.
5. **Dashboard & Reporting:** Visualize alerts, interaction trends, and risk scores; evaluate time-to-detection and false positives.

Technologies: Python, ELK Stack (Elasticsearch, Logstash, Kibana), Honeytokens/Decoy files, Optional ML (anomaly detection), Full-stack dashboard (HTML/CSS/React).

Team Roles & Responsibilities

Member	Role	Responsibilities
Marwan	DFIR Lead / Project Manager	Design detection and response workflow; define incident investigation procedures; oversee module integration

Sherfa	SOC / Monitoring Lead	Configure ELK Stack, log collection, alerting, SOC dashboards
Shweal	SOC / Alerting & Analysis	Analyze incoming alerts, correlate events with user activity, define suspicious behavior patterns
Ahmed	Security / Honeytoken Lead	Create decoy documents, credentials, folders, and databases; implement honeytokens; ensure decoy security
Karim	Pentest / Threat Simulation Lead	Simulate insider attacks, evaluate decoy effectiveness, validate system reliability
Joseph	Full-Stack / Dashboard Developer	Enhance Kibana dashboards or web interfaces; visualize decoy interactions, risk scores, alerts; integrate backend logs with frontend UI

3-Month Balanced Roadmap

Month 1: Planning & Setup

Week	Marwan	Sherfa	Shweal	Ahmed	Karim	Joseph
1	Project kick-off, define workflow	ELK Stack initial setup	ELK Stack initial setup	Research decoy ideas	Plan attack simulations	Set up dashboard skeleton
2	Define investigation procedures	Configure log collection	Configure alert rules	Start creating decoy templates	Help Ahmed refine decoys	Dashboard design, wireframes
3	Review module integration plan	Test logging of decoy access	Develop alert triggers	Finalize decoy templates	Define pentest scenarios	Build basic dashboard backend
4	Oversee initial integration	Monitor initial decoy access logs	Analyze early interactions	Deploy initial decoys	Perform first small-scale test attacks	Connect dashboard to backend logs

Month 2: Core Development

Week	Marwan	Sherfa	Shweal	Ahmed	Karim	Joseph

5	Document detection workflow	Refine log collection and alerts	Start risk scoring logic	Deploy full decoy set	Execute controlled insider attacks	Implement dashboard data visualization
6	Analyze results from simulations	Tune alerts based on anomalies	Update behavior analysis algorithms	Add honeytokens to databases	Test attack variations	Enhance dashboard with risk scoring
7	Integrate DFIR procedures with alerts	Monitor real-time decoy interactions	Refine anomaly detection	Adjust decoys for better engagement	Simulate insider attacks on network services	Add alert notifications to dashboard
8	Review core module integration	Verify SOC monitoring effectiveness	Fine-tune behavior profiling	Deploy final decoy batch	Stress-test system with multiple simulated attacks	Add analytics charts and reporting features

Month 3: Testing, Optimization & Reporting

Week	**Marwan**	**Sherfa**	**Shweal**	**Ahmed**	**Karim**	**Joseph**
9	Lead full system test	Monitor alerts for false positives	Analyze risk scores	Adjust decoy placement	Perform advanced penetration tests	Ensure dashboard reflects real-time data
10	Review detection metrics	Validate ELK dashboards	Update anomaly detection logic	Security review of decoys/logs	Test multiple attack scenarios	Improve dashboard usability
11	Oversee final integration	Confirm SOC alert workflow	Finalize behavior profiling	Conduct system security audit	Run final pentest simulations	Finalize dashboard and reporting tools
12	Compile final report and presentation	Assist in dashboard demo	Prepare DFIR workflows for demo	Document honeytoken effectiveness	Document pentest results	Prepare interactive dashboard demo

Deliverables

- Functional insider threat detection system with decoys.
- Real-time alerting and monitoring dashboard.

- Evaluation metrics: detection time, number of alerts, false positives.
- Comprehensive project report and demo.