DFIR Investigation Playbook

Marwan – DFIR Lead / Project Manager

September 2025

Purpose

This document defines the investigation workflow for handling alerts generated by the Insider Threat Detection System. It ensures a consistent DFIR process to validate alerts, correlate evidence, and respond to insider threat activity.

1 Workflow Steps

1.1 Step 1: Alert Reception

- Receive alert from ELK Stack / Dashboard when a decoy is accessed.
- Log the alert details (time, user, host, type of decoy triggered).

1.2 Step 2: Verification

- Confirm that the alert corresponds to a decoy asset (avoid false triggers).
- Check if the user action is legitimate (testing, admin activity, or real insider action).

1.3 Step 3: Evidence Collection

- Gather logs related to the user session (authentication logs, access logs, file events).
- Collect metadata from the decoy interaction (filename, credential used, database query).
- Preserve evidence for potential escalation.

1.4 Step 4: Correlation & Analysis

- Correlate alerts with other user activities (e.g., multiple decoy touches, unusual login times).
- Assign or update the user's risk score.
- Determine if the behavior is anomalous compared to baseline activity.

1.5 Step 5: Decision

- **False Positive:** Dismiss the alert, document the reason.
- **Suspicious Activity:** Escalate to SOC for monitoring.
- **Confirmed Incident:** Trigger full Incident Response (account suspension, containment, forensic imaging).

1.6 Step 6: Response & Documentation

- Document investigation steps, findings, and decisions taken.
- If escalated, hand over to SOC/IR team with all collected evidence.
- Update case records for metrics and future tuning.

2 Incident Severity Levels

Severity Level	**Description**	**Response Actions**
Low	Single decoy interaction with no other anomalies detected.	• Verify if legitimate activity (e.g., testing/admin). • Log event and monitor user closely.
Medium	Multiple decoy interactions or unusual activity pattern.	• Escalate to SOC for enhanced monitoring. • Correlate with authentication logs and user behavior. • Increase risk score.
High	Confirmed malicious insider behavior (credential misuse, repeated decoy triggers, data exfiltration attempts).	• Initiate full Incident Response (suspend account, isolate system). • Collect and preserve forensic evidence. • Notify management and document detailed incident report.

3 Outputs

- Incident Case Report (per alert).
- Risk Score Updates.
- Metrics: detection time, investigation time, false positive rate.