Powered by 911 CYBER.app

SOC ANALYST

STUDY NOTES

PART II: Insider Threats

Prepared By

CYBERMATERIAL

2025

INTRODUCTION

PART II : Insider Threats

This document is a direct continuation of Part 1 of the SOC Analyst Study Notes, which covered the foundational elements of Security Operations Center (SOC) operations, including SIEM architecture, endpoint detection and response (EDR), incident response frameworks, and analyst workflows.

Part 2 shifts focus to one of the most critical and complex areas in cybersecurity operations: insider threats. Unlike external attacks, insider threats stem from within the organization, often involving trusted users who may act maliciously, negligently, or unknowingly under the influence of external actors. These threats require a unique blend of behavioral analysis, technical monitoring, and cross-departmental collaboration.

In the following chapters, we explore the various types of insider threats, detection strategies, SOC workflows, real-world case studies, and best practices drawn from industry frameworks such as CERT and NIST. This section is designed to help analysts and security professionals recognize, respond to, and reduce insider risk across the organization.

CHAPTER 1

Insider Threat Overview

An insider threat arises when a trusted individual, such as an employee, contractor, or vendor uses their legitimate access to harm the organization.

Unlike external attackers, insiders already have a foothold within the system, making detection challenging.

According to CISA, insider threats may be intentional (malicious) or unintentional (negligent), and may result in data theft, sabotage, fraud, or regulatory violations.

Insider Threat Overview

Types of Insider Threats

1. Malicious Insiders (Intentional):
Actors who deliberately exploit their access for personal or financial gain, revenge, or ideological motives. Examples include data theft, sabotage, or espionage.

2. Compromised Insiders:
Employees whose accounts are hijacked by external attackers, often through phishing or malware, and used to perform unauthorized actions.

3. Negligent Insiders:
Well-meaning but careless users who accidentally cause harm by ignoring security policies for e.g., sending sensitive files to the wrong recipient or using weak passwords.

4. Collusive Insiders and Third Parties:
Cases where internal users cooperate with external actors or where trusted contractors misuse their access.

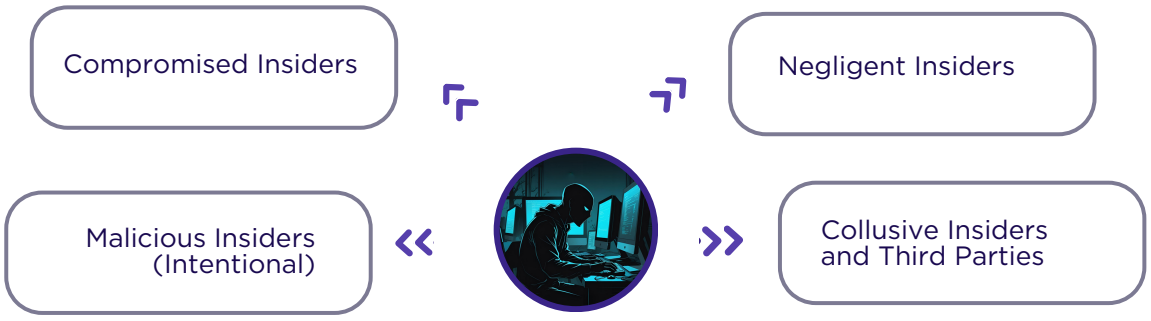
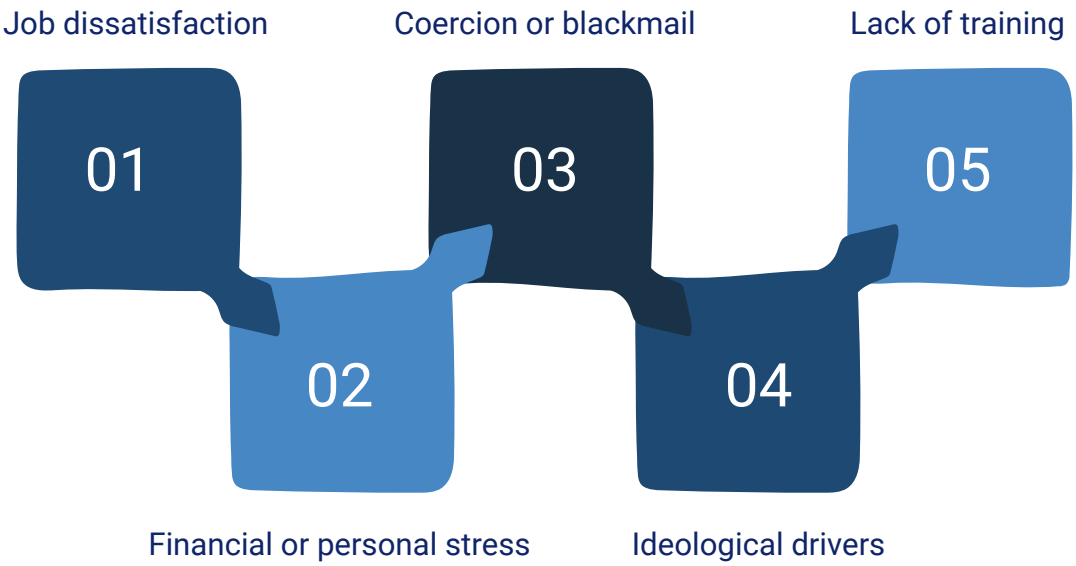


Fig. 01 Types of Insider Threats

Insider Threat Overview

Common Triggers and Motivations include the following

- Job dissatisfaction or termination. The most common trigger.
- Financial or personal stress which makes individuals vulnerable to bribery or fraud.
- Coercion or blackmail where threat actors extort insiders.
- Ideological drivers such as Whistleblowers, hacktivism etc.
- Ignorance or lack of training. Especially in negligent insider cases



Tip: Organizations should pay special attention during resignations, layoffs, and known employee conflicts.

Indicators of Insider Threat Behavior

Technical Indicators:

- Unusual volumes of data access or download spikes.
- Unauthorized system access attempts.
- Disabling security software or clearing audit logs.
- Using unauthorized USB drives or cloud storage.
- Renaming or encrypting sensitive files.
- Anomalous IP addresses or off-hours access.

Behavioral Indicators:

- Working late without need, erratic logins.
- Hostility toward the organization or coworkers.
- Ignoring security policies repeatedly.
- Sudden lifestyle upgrades or financial changes.
- Asking questions outside their job scope.

Behavioral indicators often come before technical signs, training staff to spot these is critical.

Detection Techniques for Insider Threats

Detection Techniques

- **UEBA** (User & Entity Behavior Analytics): Learns normal patterns and alerts on anomalies.
- **SIEM** (Security Information & Event Management): Centralizes logs, triggers policy-violation alerts.
- **DLP** (Data Loss Prevention): Flags risky data movement.
- **EDR** (Endpoint Detection & Response): Watches USB usage, file access, remote control attempts.
- **Human Reporting**: Encouraging team members to report suspicious behavior confidentially.
- **Threat Hunting**: Proactive search for misuse or compromise based on risk patterns.

Detection requires a mix of automation, human vigilance, and contextual analysis.

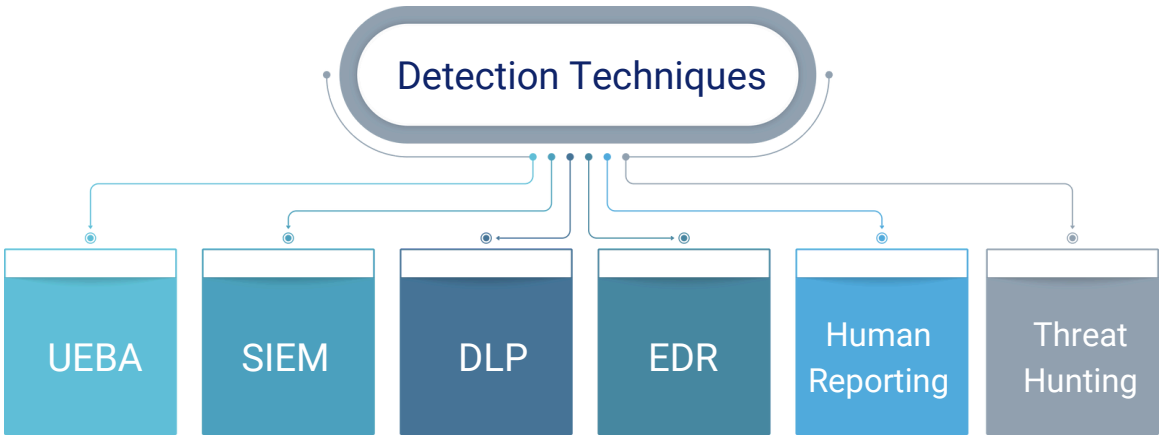


Fig. 02 Detection Techniques

Layered Defense Model Against Insider Threats

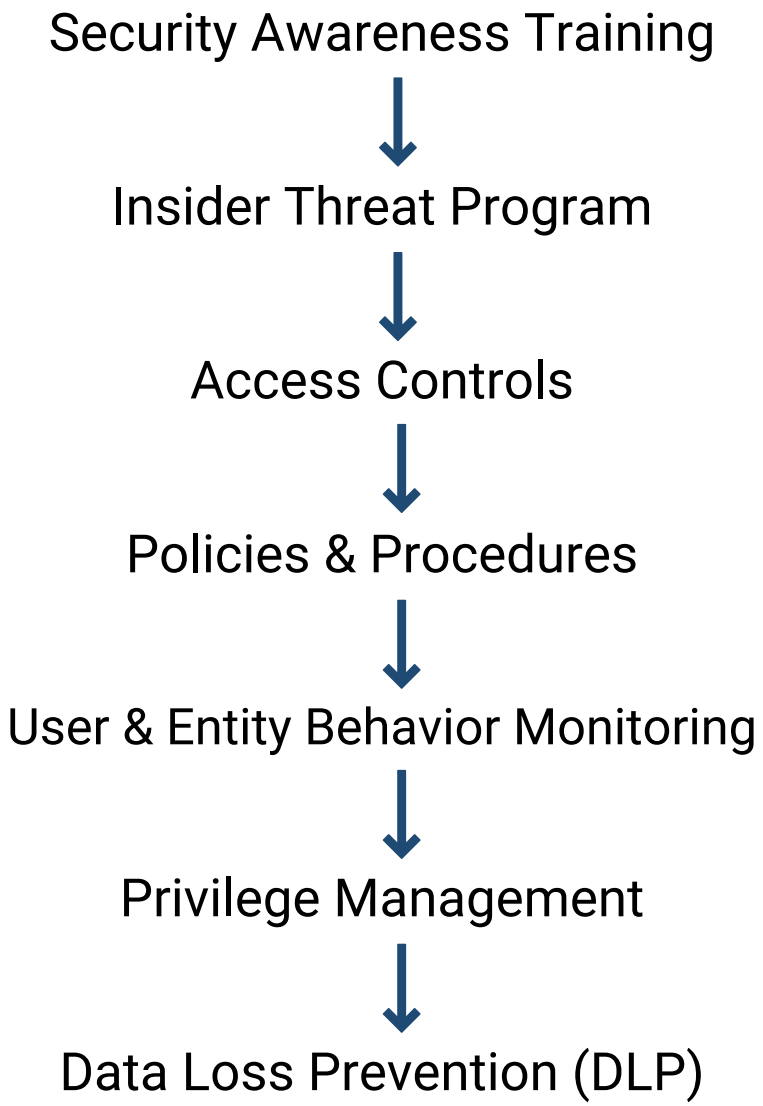


Fig. 03 Layered Defense

Insider Threat Tools and Technologies

- SIEM + UEBA: Identify patterns across time, detect subtle misuse.
- DLP: Detects emails, uploads, or file transfers containing sensitive content.
- EDR: Tracks what processes are run on endpoints, isolates rogue devices.
- IAM/PAM: Enforces least privilege, tracks account escalations and privilege misuse.
- Network IDS/NTA: Detects anomalies in network communication, lateral movement.
- Insider Threat Platforms: Aggregate behavioral, HR, and IT signals for case management.

A layered defense-in-depth model is most effective.

Wazuh
For SIEM

OpenDLP
For DLP

Velociraptor
For EDR

OPA
For IAM

Zeek
For NTA/IDS

DTEX InTERCEPT
For Insider Threat

SOC Analyst Workflow in Insider Incidents

L1 SOC Analyst Tasks:

- Triage alerts for data access spikes, unauthorized activity.
- Correlate user actions with HR context (e.g., employee resignation).
- Escalate credible incidents to L2.
- If authorized, contain obvious threats (lock account, block USB).
- Document findings for investigation chain.

L2 SOC Analyst Tasks:

- Investigate user timeline across logs, emails, endpoints.
- Compare access with job role and HR status.
- Validate threat level: negligence vs. malice vs. compromise.
- Work with HR/legal for context.
- Advise on containment and coordinate evidence preservation.

L3 SOC Analyst Tasks:

- Manage multi-department response (security, HR, legal).
- Decide when/how to revoke access, confront the insider.
- Communicate with executives, legal counsel, and compliance.
- Oversee full forensics and review controls.
- Lead post-incident improvement and reporting.

Real-World Case Examples

🔥 The Case of Malicious Sabotage

Fired IT Admin Deletes 21.3 GB of Data

A former IT administrator at a New York credit union, angry over her termination, accessed the company's network remotely using still-active credentials. She launched a deliberate sabotage operation targeting core systems and backup infrastructure. The incident crippled IT operations and demonstrated how dangerous delayed deprovisioning can be.

Key events:

- Logged in remotely via VPN using an unrevoked domain account.
- Deleted backup files, operational data, and anti-ransomware utilities.
- Cleared system logs to cover her tracks.
- Took advantage of unrestricted admin privileges post-termination.

Real-World Case Examples

📤 The Case of Negligent Insider

Employee Emails PII of 3,700 Staff by Mistake

In Calgary, a city employee requested IT support by email and accidentally attached a file containing the personal data of over 3,700 staff members. The unintended recipient now had access to names, addresses, and other private identifiers, triggering a privacy breach and internal audit.

Key events:

- Attached sensitive employee data to a support request.
- No email DLP was in place to scan or block the outbound message.
- Failure to encrypt or verify recipient before sending.
- Prompted a review of internal security awareness and controls.

Real-World Case Examples

🎣 The Case of Compromised Insider

Uber Breached Through MFA Fatigue Attack

In 2022, an attacker repeatedly bombarded an Uber contractor with MFA push notifications until the exhausted user accepted one. This allowed the threat actor to impersonate the insider and move laterally within Uber's infrastructure, accessing multiple systems.

Key events:

- Repeated MFA requests sent via Duo (MFA fatigue tactic).
- Social engineered the contractor to approve a fraudulent request.
- Accessed Slack, Google Workspace, and internal admin tools.
- Used PowerShell and token manipulation for lateral movement.

Coordination with HR, Legal, and Compliance

HR:

- Tracks at-risk employees and transitions.
- Participates in investigations and terminations.
- Handles internal messaging and employee interviews.

Legal:

- Ensures lawful monitoring, evidence preservation.
- Oversees breach disclosures, subpoenas, or prosecution.
- Reviews investigation procedures and employee rights.

Compliance:

- Ensures adherence to HIPAA, GDPR, NIST, ISO.
- Maintains risk registers and audit trails.
- Interfaces with regulators and external auditors if needed.

Collaboration is essential as technical indicators alone are insufficient without organizational context.

Conclusion

Insider threats blend human behavior and cyber risk. With layered tools (SIEM, UEBA, DLP), strong processes, and cross-functional teamwork, organizations can detect and contain these threats effectively.

The SOC plays a critical role in orchestrating this defense, from triage to containment and recovery. Continuous vigilance, awareness, and well-defined protocols turn insider threat management from a reactive scramble into a proactive discipline.