Insider Threat Response Playbook

The Challenge of Insider Threats

Insider threats represent one of the most complex and sensitive security challenges any organization faces. Unlike external attackers who must overcome firewalls and identity management systems, the insider already possesses legitimate access and often has deep knowledge of organizational data structures and security weaknesses. This legitimate access makes detection difficult and necessitates a playbook that balances robust security protection with essential employee **privacy** and strict **legal compliance**. Our response must always be measured, ethical, and fully authorized. A report by SYSTECA shows the impact of Insider Threat in great detail.

Establishing the Detection Framework

Effective detection relies on establishing a clear picture of **normal behavior** across the organization and setting up controls to flag deviations. A multi layered approach is essential to catch subtle, nonobvious indicators.

Behavior and Data Monitoring

1. **User Behavior Analytics Baseline:** We must first define the baseline for every role and team. What does normal look like? Once established, we can use user behavior analytics tools to detect anomalies. Examples include a finance employee suddenly accessing engineering schematics, or an employee who normally works nine to five starting to log in consistently at two oclock in the morning. These are changes that demand attention.
2. **Data Loss Prevention (DLP) Thresholds:** DLP is our last line of defense against data leaving the network. The playbook defines specific alert thresholds for

sensitive data types. For instance, attempting to transfer more than fifty customer records, or downloading proprietary source code, must trigger an immediate high severity alert that starts a formal verification procedure.

3. **Privileged Account Monitoring:** Accounts with elevated access are the highest risk. The playbook mandates detailed parameters for **privileged account monitoring**, logging every command and file accessed. Any deviation from established job duties or the introduction of new executable files should immediately trigger an escalation to security operations.
4. **Off Hours and Unusual Access:** Any system access outside of an employees standard working hours, especially from remote locations, must be monitored. The system needs to flag these events and require a clear, documented **justification workflow** from the users manager or department head to clear the flag.
5. **Database and File Access Patterns:** We monitor for unusual patterns like **mass file access** or **unauthorized database queries**. An employee should not suddenly read every document in a SharePoint folder they have never touched before. These are often the earliest indications of preparation for a data exfiltration event.

The Crucial Step: Authorization

Before any formal investigation begins, authorization is paramount. Security teams must never initiate covert surveillance or forensic investigation without unanimous approval. The playbook requires documented signoff from three key groups: **Legal counsel**, **Human Resources (HR)**, and **Executive Leadership**. This step ensures the investigation remains legally defensible, respects employee rights, and has the full backing of the organization.

Detailing the Investigation Process

Once authorization is secured, the investigative process shifts into a formal digital evidence collection phase, treating the entire process as if it were leading to litigation.

1. **Digital Evidence Collection Protocols:** All evidence must be collected using forensically sound methods. This maintains the **chain of custody**, proving the evidence has not been tampered with and is admissible in potential disciplinary or legal action. Evidence includes drive images, volatile memory captures, and configuration files.
2. **Network Traffic Analysis:** The investigation must specifically focus on identifying **data exfiltration channels**. This means analyzing network logs for

large encrypted transfers to unapproved cloud storage or suspicious connections to personal email accounts that bypass standard DLP controls.

3. **Access Log Correlation:** A dedicated team correlates access logs across disparate systems: physical access, network login times, file access timestamps, and email activity. This **timeline reconstruction** methodology is essential to establish a clear pattern of behavior and intent.
4. **Interview Procedures:** When the case warrants interviews, the playbook outlines strict procedures for manager and colleague interviews. These interviews are typically conducted by HR and Legal, with security personnel present only to provide technical context. The goal is to gather facts while maintaining discretion and avoiding premature accusations.
5. **Documentation Requirements:** Every step of the investigation, every log, and every piece of evidence must be documented rigorously. This comprehensive case file must be organized to support potential **disciplinary actions**, criminal charges, or civil litigation, providing a clear audit trail of the findings.

Containment and Mitigation Strategies

The response must be carefully calibrated to minimize organizational impact while neutralizing the threat. The core principle here is **proportional response**. Actions should match the severity and certainty of the threat.

1. **Covert Monitoring Escalation:** If malicious activity is confirmed but operational necessity dictates waiting for more evidence, the playbook allows for the escalation of **covert monitoring**. This is only permitted with explicit, renewed executive authorization.
2. **Account Privilege Adjustments:** Often, the initial containment step is a surgical reduction of access rights rather than a full lockout. Procedures are detailed to adjust account privileges based on the **least privilege principles**, minimizing disruption to legitimate business operations while cutting off access to sensitive data.
3. **System Access Revocation:** The playbook includes specific protocols for the immediate, clean **revocation of access** under various termination scenarios. These procedures ensure that all digital access, including VPN, cloud services, and email, is terminated precisely when required.
4. **Physical Access Control Modifications:** In cases involving physical risk or theft of property, the playbook outlines procedures for immediate modification of

physical access controls, including disabling key cards or restricting building access.

The Resolution and Improvement Framework

The final phase closes the incident, addresses its root causes, and strengthens the overall security posture.

1. **Interdepartmental Coordination:** Successful resolution requires close, detailed **coordination procedures** between the security operations team, Human Resources, and the Legal department. Every communication, decision, and public statement must be mutually agreed upon.
2. **Legal and HR Documentation:** The organization must finalize all documentation required for potential **legal proceedings**, including compiling affidavits and preparing for discovery. HR manages the personnel file and ensures disciplinary actions align with corporate policy and labor laws.
3. **Knowledge Transfer Protocols:** When a key employee is removed from their role, the playbook mandates careful **knowledge transfer protocols** to ensure business continuity. Critical data, passwords, and project files must be seamlessly transferred to designated personnel to prevent operational paralysis.
4. **Program Improvement Mechanisms:** The most crucial final step is to review the entire incident. The team must identify all **security control gaps** that enabled the threat. Was it a weakness in the DLP system? Were the UBA thresholds set too high? This postmortem review feeds directly into **program improvement mechanisms**, ensuring that lessons learned are translated into permanent, stronger security controls, closing the door on similar future incidents.