TERAMIND

Mitigating Insider Risk: How to Identify, Prevent, & Address Red Flags

An **Insider** is "any person who has, or previously had, authorized access to or knowledge of your organizations assets, including people, processes, technology, and facilities."

Insider Risk is defined as "the likelihood of harm or loss to an organization, and its subsequent impact, due to the action or inaction of an insider."

Insider Threats are any insiders who "intend to or are likely to cause harm or loss to your organization."

(**Source**, npsa.gov)

Insider Threat Drivers

- ✓ **Ignorance:** "Employees whose lack of awareness of organizations security policy, procedures, and protocols exposes the organization to external risks."
- ✓ **Complacency:** "Employees whose lax approach to policies, procedures, and information security exposes the organization to external risks."
- ✓ **Malicious Intent:** "Employees who intentionally abuse their privileged access to inflict damage on their organization or co-workers." This would include people who may feel disgruntled over recent actions like having been placed on a Performance Improvement Plan (PIP), reprimand, or conflict with a coworker or manager.
- ✓ **Self-Serving Career or Financial Gain:** Employees who are intent on exiting their roles or the organization. They may intend malice, but may also be focused solely on benefiting themselves or their new employers, often competitors – despite any resulting damage to their current employer.

Types of Insider Incidents

Information Theft

“Use of insider access to steal or exploit information.”

Physical Property Theft

“Use of insider access to steal material items (e.g., goods, equipment, badges).”

Security Compromise

“Use of access to facilitate and override security countermeasures (e.g., drug and contraband smuggling).”

Espionage

“Use of access to obtain sensitive info for exploitation that impacts national or corporate security and public safety.”

Terrorism

“Use of access to commit or facilitate an act of violence as a means of disruption or coercion for political purposes.”

Workplace Violence

“Use of violence or threats of violence, to influence others and impact the health and safety of an organization’s workforce.”

Sabotage

“Intentional destruction of equipment or IT to direct specific harm (e.g., inserting malicious code).”

Other

“Captures the evolving threat landscape including emerging threats not covered in the previous examples.”

(**Source**, Gelles, M. (2016). Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Elsevier.)

Types of Insider Incidents

We encourage you to follow best practices, aligning your mitigation strategy and security controls to the Insider Risk Persona and nature of each incident type.

Security Compromise

Insider Persona: Ignorant, Complacent, Malicious

Mitigation Strategy

- ✓ Create scriptable rules to alert on monitored users' access, misuse, or sharing of sensitive digital assets or environments.
- ✓ Use time-stamped screen recordings for rapid investigations and to provide context for what happened in the time leading up to and immediately after an attempt.

Information Theft

Insider Persona: Ignorant, Complacent, Malicious

Mitigation Strategy

- ✓ Detect and/or block information sharing actions such as USB use, emailing data outside the organization, uploads, downloads, printing, in-meeting screenshare, or emailing oneself.
- ✓ Detect and log attempted (or successful) access to file storage/upload, aligning rules to corporate policy and/or notable exceptions using scriptable rule logic.
- ✓ Use time-stamped screen recordings for rapid investigations and to provide context for what happened in the time leading up to and immediately after an attempt.

Sabotage

Insider Persona: Malicious

Mitigation Strategy

- ✓ Detect and alert on anomalous access of sensitive environments (spending more time in/on an application, file, or website longer than usual, more frequent than usual, at odd times of day, from different location, etc.).
- ✓ Detect and/or block exfiltration of data in motion, including USB use, download, upload, email, printing, or screenshare.
- ✓ Use time-stamped screen recordings for rapid investigations and to provide context for what happened in the time leading up to and immediately after an attempt.

Data Exfiltration – the Malicious Insider

Teramind detects actions including data access, use, and related behaviors often associated with malicious data theft. When an employee has experienced reprimand or is seeking to leave the company for another job, it is a good idea to increase their level of security monitoring, as they are at higher risk of becoming a threat.

1. Signs of Attempting to Cover One's Tracks

- Accessing Any use of The Onion Router (Tor)
- Knowledge of Tor use
- Presence of external encryption software on the endpoint
- Unusual use Anomalous use of encryption software (may be used to prevent detection)to avoid content inspection
- Presence of external encryption software on the endpoint
- Renaming of sensitive files
- Movement of virtual machines in the network
- Anomalous Unusual installation / use of virtual machines
- Unusual admin tool use (e.g., fsutil, alternate data streams)
- Unusual use of Incognito / Private Browsing mode
- Researching encoding or steganography tools
- Installing and using encoding or steganography tools
- Unusual disconnects from corporate network

2. Signs of Information Theft Using Approved Actions

Anomalous copying/moving files to one's endpoint

- Anomalous copying/moving files between servers
- Anomalous copying/moving files to off-network servers
- Anomalous copying/moving files to external drives, including USB
- Printing sensitive information to a networked, external, or local printer

3. Internet-Based File Theft

- Uploading corporate networked assets to cloud storage services
- Uploading corporate assets to external locations
- Sending corporate information to oneself via personal email accounts
- Uploading corporate data to "drafts" in corporate or personal email account
- Executing copy-paste of sensitive data into any application or website, including video conferencing applications, messaging applications, social media sites, or even design platforms.

4. Bypassing Security Measures

- ✓ Requesting IT override of security tools for seemingly legitimate business reasons, but leveraging the bypass for other means
- ✓ Researching, installing and using proxy bypass / VPN / tunneling
- ✓ Researching, installing and using peer-to-peer applications or DarkNet channels
- ✓ Use of password cracking applications to get to sensitive data
- ✓ Accessing someone else's account / Unauthorized access
- ✓ Using any security bypass applications
- ✓ Copy-paste of sensitive data to any website
- ✓ Copy-paste of sensitive data to any application or seemingly harmless file
- ✓ Presence of hacking tools on the endpoint (may be used for reconnaissance)
- ✓ Attempting to disable or adjust any existing security controls
- ✓ Unusual installation of new software, especially remote desktop protocol (RDP) applications, even if whitelisted
- ✓ Any unusual activity that takes place when endpoint is not connected to corporate network (can be detected by a locally installed monitoring agent that collects data even when machines are offline)

5. Privileged User Actions

- ✓ Anomalous disconnects from corporate network
- ✓ Shared / admin / service account identification
- ✓ Anomalous connections using shared / admin accounts
- ✓ Anomalous use of shared / admin accounts on network
- ✓ Anomalous use of shared / admin accounts on local machine
- ✓ Unusual applications being run under shared / admin accounts
- ✓ Anomalous local admin/root account use
- ✓ Anomalous local admin activity (e.g., scripts, file activity)
- ✓ Anomalous local or network movement of virtual machines
- ✓ Using shared/generic accounts to copy shared data

Important Note:

Monitoring of super users and IT admins requires special consideration in the development of Insider Risk programs. It's important not to impose too many controls on these staff members as they're typically already overburdened. Teramind customers use Teramind to gain visibility into super user activity without slowing their admins down, opting for a "trust but verify" approach instead of "locking and blocking".

Account Compromise – **the External Insider**

With the rise of zero-day vulnerabilities, phishing attacks, and watering hole attacks, compromised credentials and remotely controlled machines are external attacks that masquerade as insiders. Compromised credentials and machines can be detected by analyzing user activity for anomalies and behavioral changes.

- ✓ Machine accessing unusual IP addresses
- ✓ Machine accessing unusual network ports
- ✓ Machine accessing unusual or known bad website address
- ✓ Web browser used to access IP address directly (without DNS)
- ✓ Multiple machines attempting to connect to the same location
- ✓ Use of port scanning tools for reconnaissance
- ✓ Use of port scanning tools from external machines or IP addresses
- ✓ Anomalous failed access to servers or domain names
- ✓ Anomalous rate of VPN connections by user
- ✓ "Fast travel" detection of any user

Note: VPNs can be used to obfuscate location and make users appear to be in the proper geography. Teramind's geo-location feature pulls from additional data points to validate actual location.

- ✓ Lateral movement via network devices or servers
- ✓ Unusual access to devices outside firewall
- ✓ Downloading unusual/suspicious file (e.g., .JAR, .PDF)
- ✓ Activity during unusual hours, even when not connected to corporate networks (can be detected using a local monitoring agent that functions even when machines are offline)
- ✓ Machine installing or running a new and unnecessary application, even if whitelisted for other users (e.g. RDP for a non-IT user)
- ✓ Machine running application from an unusual location (see above note for geo-location feature)
- ✓ Application saving data to any unusual location
- ✓ Machine executing unusual script
- ✓ Evidence of privilege escalation
- ✓ Unusual use of packet capture/proxy/network analysis tools
- ✓ Presence of a corporate machine at IP where known malware was installed
- ✓ Presence of a corporate machine where known malware was run
- ✓ Presence of unknown keylogger application

The Endpoint Advantage

A proper defense-in-depth strategy around insider risk includes a layered approach across endpoint telemetry, log analysis, and network monitoring.

Less mature Insider Risk detection solutions often have a limited capability to detect the real-world attack vectors that large enterprises face. **As you're building your Insider Threat program, make sure that you have the granular visibility you need to mitigate insider risk and, in worst-case scenarios, detect and stop insider threats.**

Request Your
Custom Demo Now

Get Demo