68 Insider Threat Red Flags

Are you prepared to stop the insider threat?

Enterprises of all shapes and sizes are taking a fresh look at their insider threat programs.

As a company that's been in the insider threat space for over 10 years, Dtex sees a number of trends converging that are making insider threat a top area of concern for CIOs and CISOs:

- Research indicates that 90% of all data breach incidents are caused by people,
- Highly publicized data theft continues unabated,
- CISOs are increasingly frustrated with DLP tools that fail to stop data exfiltration,
- Governments are mandating the implementation of new insider threat programs, and
- Perimeter security has become more effective, shifting attention to higher areas of risk.

In the past year, security vendors have flooded into the insider threat market, causing confusion amongst teams looking to build an insider threat program. These broadly fall into four categories:

- **Log Analytics** vendors who analyze aggregated log data (typically from a SIEM system). Examples include Bay Dynamics, Red Owl Analytics, Securonix, Gurucul, Exabeam, and Fortscale.
- **Network Monitoring** vendors who analyze activity data gathered directly from network devices. Examples include DarkTrace and Vectra Networks.
- **Heavyweight Endpoint Monitoring** vendors who gather large amounts of data from endpoints (including videos, keystroke logging, and screenshots). Examples include SpectorSoft, Raytheon, and ObserveIT. These vendors will not be covered in this paper as they are typically too heavyweight to deploy across a large enterprise.
- **Lightweight Endpoint Monitoring** vendors like Dtex, who focus on collecting and analyzing metadata from endpoints.

While each of these approaches promise to "solve" insider threat, it's important for organizations to take a risk-based approach when evaluating and selecting an Insider Threat platform.

This document is a checklist that organizations can use to measure how well your Insider Threat program is prepared to identify real-world attacks. All of the attack vectors described on the following pages are taken from actual Insider Threat attacks that have been discovered by Dtex.

Data Exfiltration – the Malicious Insider

Even in companies with “mature” data loss prevention programs, here are the tactics we’ve found users actually employing when trying to exfiltrate data:

1. FILE THEFT VIA ALLOWED MECHANISMS

❏ Unusual rate of copying/moving files to a local machine

❏ Unusual rate of copying/moving files between servers

❏ Unusual rate of copying/moving files to off-network servers

❏ Unusual rate of copying/moving files to USB drives

❏ Unusual rate of writing files to CD/DVD drives

❏ Printing sensitive data to a networked printers

❏ Printing sensitive data to a local printer

❏ Printing sensitive data to an off-site printer (e.g., home office)

IMPORTANT NOTE:
Employees leaving the company are significantly more likely to take sensitive data with them when they leave. Dtex customers use our endpoint visibility to look for signs of pending departure like job searches, resume updates, and LinkedIn edits.

2. FILE THEFT VIA INTERNET

❏ Uploading to cloud services FROM the corporate network

❏ Uploading to cloud services OFF the corporate network

❏ Uploading to personal webmail from the corporate network

❏ Uploading to personal webmail off the corporate network

❏ Copying and pasting sensitive data to a website

3. OBFUSCATION AND COVERING TRACKS

- ❑ Accessing The Onion Router (Tor)
- ❑ Knowing which sites where accessed via Tor
- ❑ Unusual use of encryption software to avoid content inspection
- ❑ Unusual rate of renaming a file to something innocuous
- ❑ Unusual movement of virtual machines in the network
- ❑ Unusual installation / use of virtual machines
- ❑ Unusual admin tool use (e.g., fsutil, alternate data streams)
- ❑ Unusual use of Incognito / Private Browsing mode
- ❑ Researching steganography tools
- ❑ Installing and using steganography tools
- ❑ Unusual disconnects from corporate network

4. BYPASSING SECURITY MEASURES

- ❑ Researching, installing and using proxy bypass / VPN / tunneling
- ❑ Researching, installing and using peer-to-peer applications
- ❑ Use of password cracking applications to get to sensitive data
- ❑ Use of portable applications to bypass security measures
- ❑ Copying and pasting sensitive data to a website
- ❑ Copying and pasting sensitive data to an innocuous file
- ❑ Installation of hacking tools to probe for control weaknesses
- ❑ Attempting to disable / tamper with existing controls (e.g., DLP)
- ❑ Unusual use of non-corporate wifi networks
- ❑ Installing and using steganography tools

5. PRIVILEGED USER SECURITY

❑ Unusual disconnects from corporate network

❑ Shared / admin / service account identification

❑ Unusual connections using shared / admin accounts

❑ Unauthorized use of shared / admin accounts on network

❑ Unauthorized use of shared / admin accounts on local machine

❑ Unusual applications being run under shared / admin accounts

❑ Unusual use of local admin/root accounts

❑ Unusual local admin activity (e.g., scripts, file activity)

❑ Unusual local or network movement of virtual machines

❑ Detect use of shared/generic accounts to copy shared data

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

Credential and Machine 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 machine 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 (no DNS) directly

❑ Multiple machines attempting to connect to same target

Credential and Machine Compromise – Continued

❑ Use of port scanning tools for reconnaissance

❑ Use of port scanning tools from external machines

❑ Unusual failed access to servers or domain names

❑ Unusual rate of VPN connections by user

❑ “Fast travel” detection of VPN users

❑ Lateral movement via network devices / Linux servers

❑ Unusual access to devices / Linux servers outside firewall

❑ Machine downloading unusual/suspicious file (e.g., .JAR, .PDF)

❑ Machine performing network activity during unusual hours

❑ Machine performing local activity during unusual hours

❑ Machine installing or running unusual application

❑ Machine running application from an unusual location

❑ Application saving data to an unusual location

❑ Machine executing unusual script or privilege escalation

❑ Unusual use of packet capture/ proxy/network analysis tools

❑ Find machine where known malware was installed

❑ Find machine where known malware was run

❑ Machine attacked with local keylogger / Rubber Ducky

The Endpoint Advantage

A proper defense-in-depth strategy around insider threat would include a layered defense that includes endpoint visibility, log analysis, and network monitoring.

As you can see, though, newcomers to the Insider Threat space only 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 full visibility that you need to detect insider threats.