

The DTEX Insider Threat Kill Chain

Anatomy of Intent: How to Identify and Stop Real-World Insider Threats

GUIDE



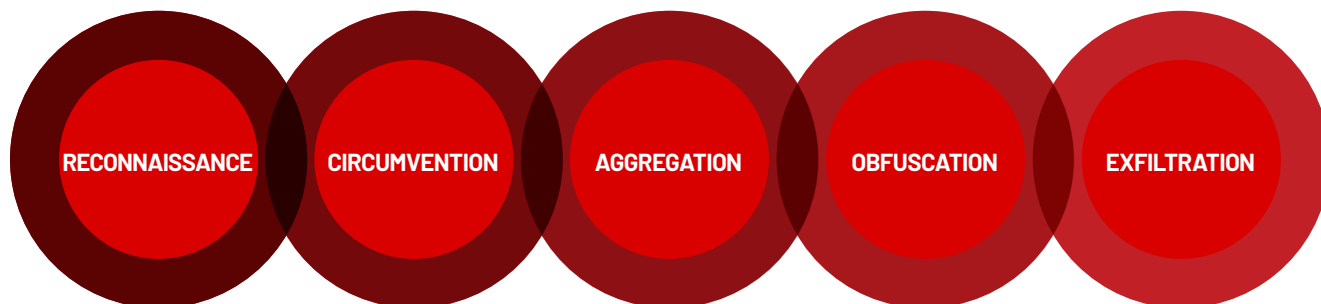
The vast majority of security threats follow a pattern of activity during an attack, and insider threats are no exception. But the truth is, insider threats are not the same as a typical malware attack. Insider threat investigations require a more nuanced approach and security analysts must have both the technical aptitude and human investigative domain knowledge to be effective.

Understanding the detailed steps taken during an insider attack plays a big part in preventing a data loss incident, enabling organizations to identify issues before an insider risk turns into an insider threat.

The DTEX Insider Threat Kill Chain

Over the course of thousands of insider threat investigations and incidents, DTEX analysts have developed the Insider Threat Kill Chain to increase awareness around the pattern of activity during a sometimes-slow moving attack. It's based on five steps present in nearly all insider attacks.

Insider Threat Kill Chain



Visibility into the entire kill chain — not just one or two steps — is imperative. This is because the earlier phases of the kill chain hold the answers to some of the most important questions, both for incidents that have yet to fully unfold and for those that have already occurred.

Questions that must be answered include:

- What is the intent of this user?
- Is this an accidental breach or a calculated attack?
- Is this truly an insider, or was this user's credentials compromised by an infiltrator?
- Did a security misconfiguration allow this to happen?
- What files were affected?
- Was generative AI involved?

DTEX offers comprehensive activity data and intelligence that spans every stage of the kill chain. With this data, analysts can answer these critical questions, and more, without resorting to hiring outside experts to investigate incidents. What's more, based on machine learning and behavioral risk modeling, DTEX has full visibility into the kill chain to elevate early warning signs that a breach may be imminent.

Security Solution Gaps

Too often, today's approach to security suggests developing complex, layered security architectures. But evolving attacks take advantage of this complexity to slip through siloed defenses. And while a wide range of security solutions suggest they protect against insider threats, they aren't collecting quality data to send to a comprehensive behavioral analytics platform.

Endpoint Detection and Response (EDR)

EDR solutions analyze activity data on endpoint devices.

They produce a large volume of data creating the potential for false positives, where benign activities are flagged as malicious, and actual threats go undetected. And the complexity of these solutions can lead to misconfigurations, and ultimately security gaps.

Identity Detection and Response (IDR)

Add-on IDR (or ITDR) capabilities are designed to provide oversight of identity access management (IAM) solutions.

These products are focused on compromised account detection, attacks specifically targeting user identities and access management infrastructure. They support only basic anomaly detection and are not a replacement for effective insider risk management. Stitching together more point products drives complexity and cost and creates a false sense of security.

Network Detection and Response (NDR)

NDR platforms analyze network traffic gathered from network devices like firewalls. Analyzing network data provides insight into only one aspect of the network and misses the behavioral context needed to stop insider attacks. Sending NDR log data to a SIEM only adds to the waterfall of overwhelming alerts to sort through.

Log File-Based Behavior Analytics

Log file-based behavior analytics products analyze aggregated log data (e.g. Windows event logs, OSQuery etc.), typically from a SIEM or XDR platform. Integrating log aggregation solutions with User and Entity Behavior Analytics (UEBA) does not address the fundamental challenge of data quality. And continuing to collect more data under the guise of better visibility only makes the problem worse. False positives are rampant because simply detecting "abnormal", also known as behavior that is different than normal, does not make behavior malicious.

Data Loss Prevention (DLP)

Legacy DLP vendors analyze the sharing, transferring, and use of sensitive data on network endpoints. Detection techniques are based on keywords, keyword patterns, regular expressions and hashing. These products rely on complex content rule configuration that require frequent maintenance and lack the context and behavioral analysis to understand threats. They are heavy on the endpoint, riddled with false positives, and primarily detect negligent behavior, not malicious data loss so many organizations ultimately find these solutions hard to use. Opening every file, email, IM, and web request creates many issues with privacy and compliance.

While each of these approaches may address one step or small part of the insider threat kill chain, none of them have been designed specifically as a holistic insider threat platform and so do not address the subtle and insidious ways insiders operate.

The Insider Threat Kill Chain Checklist

Below is a checklist that organizations can use to prepare for and identify real-world indicators of intent. The attack vectors included are taken from actual insider threat attacks that DTEX customers discovered using the DTEX Insider Threat Kill Chain.

Reconnaissance

When preparing for data theft, insiders typically begin with research. This is where they locate the data that they would like to steal, or, in the case of compromised credentials, where the insider will test the bounds of the stolen credentials' privileges.

	DTEX	IDR	NDR/EDR	Log File Analytics
Researching security bypass methods / tools	X			
Use of Network Scanning Tools	X	Partial	X	Partial
Anomalous Use of Network Scanning Tools in comparison to peer group	X	Partial		
Installation and Usage of Portable Applications	X	Partial		X
Unusual Usage of sysinternals Tools and Utilities	X	X		X
Network share enumeration	X	X	X	
File and Folder Access Denied Events	X	X	Partial	X
Unusual access to remote support tools	X	X		
Unusual rates of opening files	X			Partial
Unusual access to new file locations	X	Partial	Partial	X
Successful and failed attempts to mount USB drives or access cloud storage	X	X	X	
Commands issued through tools like cmd.exe, PowerShell, Terminal, etc.	X	X		
Suspicious internet search activities (e.g. google searches)	X			
Unusual login behaviors (e.g. outside of normal working hours)	X	X		Partial
AI Assistant searching and presenting results	X		Partial	

Circumvention

This is the stage where the insider attempts to get around existing security measures, such as web blocking and DLP tools. It is particularly important to have visibility into this activity because it can shed light on intent: if a user is going through great lengths to get around company security, they are acting very deliberately.

This is also where organizations can see where security tools are failing. By capturing circumvention activity, DTEX shows analysts where and how users are able to bypass existing measures.

	DTEX	IDR	NDR/EDR	Log File Analytics
Usage of anonymous web browsers (e.g. Tor), including the actual sites visited during these anonymous sessions	X			
Disabling of corporate VPN	X	X	X	Partial
Research into tampering of corporate security tools	X			
Tampering of corporate security tools	X		Partial	
Suspicious off network activities (including detection of corporate and non-corporate networks, Wi-Fi SSID etc)	X	X		
Unusual usage of privileged admin accounts	X	X		Partial
Usage of vulnerability exploit tools	X	X	X	X
Unusual usage or creation of local accounts	X	X		Partial
Anomalous modification of configuration files	X	X	Partial	
Modification of file and directory permissions	X	X	X	Partial
Unusual privilege escalation activities	X	X	Partial	Partial
Usage of non-approved AI tools to circumvent monitoring	X		Partial	

IMPORTANT NOTE:

Monitoring of privileged account activity including IT admins requires special consideration. DTEX IRM provides visibility into privileged users without slowing them down.

Aggregation

This is when the insider assembles all of the data to steal, often moving it into one file directory or compressing it in a single location.

	DTEX	IDR	NDR/EDR	Log File Analytics
Download of sensitive files from corporate web portal	X			
Archive creation including correlation of files within the archive	X			
Unusual network file transfers (both from the file server and the endpoint)	X	Partial	X	Partial
Anomalous data aggregation behaviors based on file type, file size and other meta-data	X	X		
Unusual Clipboard Activity (e.g. excessive screenshots during a conference call or presentation)	X			
Anomalous mapped drive creation and data transfers	X	X		Partial
Automatic data collection (RPA)	X		Partial	
Anomalous email archive creation and transfers	X			
Administrative file copy utilities	X		X	
Unusual symbolic link creation	X			
Automated backup software (e.g. time machine)	X			
AI Assistant summarizes into consolidated document	X			

Obfuscation

In the Obfuscation step, insiders will cover their tracks in order to avoid detection, often by renaming files, changing file types, or by using more advanced tactics such as steganography. This is another important step to capture in order to prove malicious intent, as well as to understand where other security tools might be failing.

	DTEX	IDR	NDR/EDR	Log File Analytics
Use of private browsing modes (e.g. incognito)	X	X		
Data hidden within the Alternate Data Stream (ADS)	X			
Steganography use cases	X		Partial	
Unusual clearing of event viewer logos	X			X
Unusual clearing of browser history	X			
Suspicious file extension renaming	X			
Suspicious file renaming, especially sensitive files given innocuous file names	X			
Anomalous off-network activity (including device tethering)	X	X		
Unusual rates of file deletes	X			
Anomalous usage of disk erasing software	X			
Hidden Files and Attribute Changes	X		X	
Use of anomalous web browsers (e.g. Tor), including the actual sites visited during these anonymous sessions	X	X		
Monitoring browser-based Agentic AI performing work functions	X			

Exfiltration

This is the final step in the process of stealing data: the moment that the data is actually transferred out of the organization. Many security tools focus only on this specific step, and often by way of blocking tools. Rigid rules, however, can't catch the hundreds of methods that can be used to get data out of the organization. Since DTEX sees all activity from the point closest to the user, it has visibility into less common exfiltration methods that other tools often miss.

	DTEX	IDR	NDR/EDR	Log File Analytics
Airdrop Exfiltration	X			
Bluetooth	X			
Encrypted USB	X	X	Partial	
Unencrypted USB	X	X	Partial	
FTP / sFTP Transfers	X			Partial
Online File Sharing	X			
Personal Webmail Uploads	X		Partial	
Printing	X			X
Anomalous Uploads	X	X	X	X
Network to Removable Device	X			Partial
Remote Support Tool Upload	X			
Messaging Tool Upload	X			
Automated Exfiltration / Scheduled Transfers	X		Partial	
Exfiltration over Alternative Protocol	X		X	Partial
Exfiltration over Command & Control	X		X	Partial
Exfiltration over Physical Medium	X	X	Partial	Partial
Data Transfer Size Limits	X	X		X
Exfiltration of High Sensitivity Score Documents	X			
Agentic AI using cloud-based storage or mail servers to exfiltrate data	X			

IMPORTANT NOTE:
Employees leaving the company are significantly more likely to take sensitive data with them when they leave. DTEX looks for signs of pending departure or disengagement.

DTEX Insider Risk Management

DTEX IRM is a purpose-built insider risk management platform that consolidates the essential capabilities of user and entity behavior analytics (UEBA), user activity monitoring (UAM) and data loss prevention (DLP) in a single, light-weight platform to provide early detection and mitigation of insider risks.



To learn more about DTEX, please visit dtex.ai.

ABOUT DTEX

DTEX is the leader in risk-adaptive security, unifying human, data, and AI risk through a behavioral intelligence platform. Built for enterprise scale, it detects threats early and prevents breaches. Organizations and governments worldwide rely on DTEX to protect sensitive data, accelerate innovation, and safeguard trust with privacy-by-design telemetry and adaptive controls. The DTEX platform integrates Insider Risk Management, Data Loss Prevention, User and Entity Behavior Analytics, User Activity Monitoring, and AI security into one cohesive solution.