DTEX

DTEX AND THE

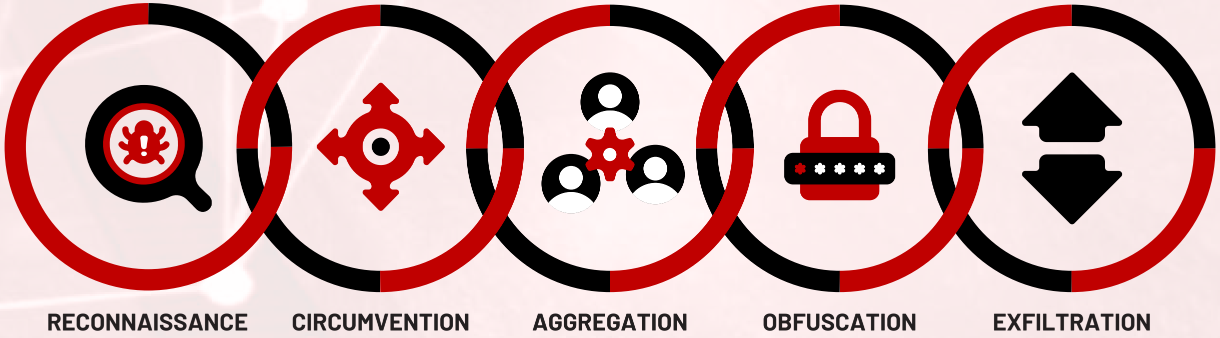
Insider Threat Kill Chain

eBook

Introduction

The vast majority of security threats follow a pattern of activity during an attack, and insider threats are no exception. Many security professionals will already be familiar with Lockheed Martin's Cyber Kill Chain, which outlines the steps that APT attacks tend to follow from beginning to end. Since human behavior is more nuanced than machine behavior, however, insider attacks follow a slightly different path. Over the course of thousands of insider threat investigations and incidents, DTEX analysts have identified the insider equivalent: the Insider Threat Kill Chain, which encompasses the five steps present in nearly all insider attacks.

THE INSIDER THREAT KILL CHAIN



In order to fully understand any insider incident, 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. These include:

- What was the intent of this user? Was this an accidental breach or a calculated attack?
- Was this truly an insider, or were this user's credential compromised by an infiltrator?
- If this was a case of stolen credentials, how did the credential thief get into the account?
- Did a security misconfiguration allow this to happen?
- What other files were affected?
- ...and many more.

DTEX offers comprehensive user visibility data and intelligence that spans every stage of the kill chain. With this data, analysts can answer all of these questions, and more, at a glance — without resorting to hiring outside contractors to investigate incidents. What's more, DTEX's full visibility of the kill chain, combined with machine learning and behavioral models that highlight anomalous behavior, allows it to elevate early warning signs before a breach occurs.

Insider Threat Kill Chain – Reconnaissance

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

- Use of hacking tools
- Use of network sniffing tools
- Unusual rates of opening files
- Unusual access to new file locations
- Successful and failed attempts to mount USB drives or access cloud storage
- Commands issued through tools like cmd.exe, PowerShell, Terminal, etc.

RECONNAISSANCE

Insider Threat Kill Chain – Circumvention

This is the stage where the attacker attempts to get around existing security measures, such as web blocking, DLP tools, etc. 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 often where organizations can see where their security tools are failing. By capturing circumvention activity, DTEX shows analysts where and how users are able to bypass existing measures. DTEX sees circumvention activity like:

- Researching how to get around security measures (search terms like, "How to disable DTEX" or "How to turn off web blocking")
- Use of VPN tools
- Use of "Incognito Mode" or other private browsing
- Use of true private browsers like TOR
- Unusual access to new file locations
- Use of different messaging tools than those typically used in the organization
- Activity that takes place off of the corporate network, or on a mobile hotspot

CIRCUMVENTION

Insider Threat Kill Chain – Aggregation

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

DTEX sees this step by capturing activity like:

- File activity, such as files being moved, renamed, or compressed.
- Where files are being saved - including to unusual locations on a user’s endpoint
- Use of “Incognito Mode” or other private browsing
- Saving unusual file types
- Unusual rates of compression

AGGREGATION

Insider Threat Kill Chain – Obfuscation

In the Obfuscation step, the attacker 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 captures all evidence of obfuscation activity, including:

- Clearing cookies and event viewer logs, or unusual use of browser “stealth” settings like Incognito mode
- Off-network activity
- Hiding sensitive information in image, video, and other misleading file types
- Unusual rates of file renaming, especially to different file types
- Use of steganography applications, based on name, product, or vendor ID — even through the browser — as well as steganography carried out through command line interfaces

OBFUSCATION

Insider Threat Kill Chain – 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.

A few examples include:

- Copy and Paste activity
- Screen capture activity
- Use of removable media
- Use of file sharing and cloud services
- Use of AirDrop
- Use of personal email

EXFILTRATION

CONCLUSION

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.

Detecting and investigating human-based risks requires dedicated user activity intelligence delivered from the endpoint. To learn more about DTEX's approach, visit dtexsystems.com.

CONTACT US

🌐 www.dtexsystems.com

✉ info@dtexsystems.com

☎ +1 (408) 418-3786

🏠 3055 Olin Ave, Suite 2000
San Jose, CA 95128