DTEX AND THE MITRE ATT&CK MATRIX

The MITRE ATT&CK framework – which stands for Adversarial Tactics, Techniques, and Common Knowledge – outlines common adversary tactics and techniques based on real-world observations. This matrix provides both public and private sector organizations a roadmap of attack vectors that their security postures should address in order to achieve the most complete protection possible.

Dtex provides unparalleled user behavior visibility directly from the endpoint. This uninterrupted audit trail provides visibility into nearly every item in the MITRE matrix, resulting in stronger detection for each of these categories. Dtex also offers dashboards and alerts mapped to the ATT&CK Framework for organizations that wish to approach security efforts from the perspective of the matrix.

While Dtex's visibility extends to most items of the matrix, we most frequently receive inquiries about the ten use cases below from organizations that aim to achieve the greatest possible coverage:

SCREEN CAPTURE

As referenced in Framework entry T1113

Attackers often want to understand the underlying architecture of their target, including the system, network, etc. In order to collect this information, they may attempt to take screen captures or video captures of a user's desktop.

Dtex captures the usage of any tools that are being utilized for screen, audio, or video capture of the endpoint. This includes information like when the capture application was executed, when the recordings took place, and where the subsequent video/audio/image files were saved. In addition, Dtex's audit trail will depict how those recording files were subsequently moved or handled, including how they may be exfiltrated.

HARDWARE ADDITIONS/REMOVABLE MEDIA

Referenced in multiple framework entries, including T1091, T1025, T1092, & T1052

There are a plethora of ways that adversaries can use removable media, such as USB drives, to harm an organization – whether it be by collecting data from removable media, using external media as a method of lateral movement, or simply exfiltrating data via a physical medium.

Dtex detects all user activity around removable media, including insertions, removal, deletion, file activity, etc. With this visibility, organizations can understand exactly when removable devices are used, which files are moved to and from those devices, or whether portable applications or other suspicious activity occurred from the device in question.

NETWORK SNIFFING

As referenced in framework entry T1040

Adversaries may use hacking tools or network sniffing tools, such as WireShark, to passively monitor network traffic, or collect sensitive information such as credentials and other data passed over the network.

While Dtex is focused on endpoint and user behavior and therefore does not collect packet data, it does detect the use of hacking tools, network tools, and other applications that an attacker would use to conduct this kind of monitoring.

KEYLOGGING

As referenced in framework entry T1056

The MITRE ATT&CK matrix identifies keylogging as the most common type of input capture used by adversaries. Attackers will use this method to capture user input, most often with the goal of gaining credentials – which can lead to even more catastrophic results, if it is not quickly detected.

Dtex detects if a keylogging application is installed or active on the endpoint. It also provides visibility into how such applications are used, such as when they were installed, what type of application is being used, how often and how long it has been active, and other important data that allows organizations to quickly be alerted to and fully understand the threat.

PROCESS SPAWNING

As referenced in framework entry T1179

Attackers commonly attempt to infiltrate organizations with unsuspecting documents and applications that are seemingly normal from an organizational or user view. However, these documents or applications may contain malicious code or software that will spawn other processes, communicate over the network, or otherwise.

Dtex's provides visibility into application parent and child relationships that can indicate malicious behavior. And after pinpointing atypical process activity that could indicate malicious behavior, Dtex's audit trail then allows investigators to use contextual information to understand the background of the potential attack as well as immediately identify affected users within the corporate infrastructure.

RECONNAISSANCE

Referenced in multiple items, including the whole "Discovery" column of the Matrix.

Adversaries will almost always try to understand the target system and network before they launch their attack. They will do this through a variety of methods (including the network sniffing tactic mentioned previously), but most commonly, reconnaissance will take place through specific commands on tools like cmd.exe, PowerShell, Terminal, etc.

Dtex captures commands executed, providing a record of suspicious commands or activity. What's more, Dtex also baselines each user's historical behavior and detects anomalies, allowing for early detection of potential reconnaissance activity. For example, if a user who typically never accesses PowerShell suddenly begins running file discovery commands, Dtex will immediately alert on this suspicious activity.

PRIVILEGE ESCALATION AND MANIPULATION

Referenced in many framework items, including the entire "Privilege Escalation" column of the Matrix.

Once an attacker has entered the network, they will often try to escalate the privileges of their user in order to achieve greater access. Dtex detects and alerts on many common privilege escalation methods. This includes use cases like the creation or modification of security groups, escalating privileges utilizing 'runas' commands, manipulating accessibility features, and manipulation of the application launching, among others.

DATA EXFILTRATION

Referenced in the entire "Exfiltration" column of the Matrix.

The ultimate goal of a data thief is to exfiltrate data from the organization. Though there are many ways an adversary can attempt to do this, Dtex was built to detect all methods of data exfiltration.

Dtex has visibility into files that leave the organization through traditional methods like e-mail clients or removable media. It also provides visibility into the use of file sharing services (such as DropBox, Google Drive, etc.), personal webmail, or other browser-based exfiltration methods. In addition, it detects the use of other applications associated with file movement – such as FTP clients – and can identify file uploads. This data includes which attachments were included in the transfers, their size, names, etc., as well as when the upload occurred and how the files were handled and manipulated before that point.

Most importantly, Dtex was created to recognize signs of exfiltration before it happens. Unusual download, renaming, or compression of files, for example, would trigger an alert – and Dtex sees a full audit trail of this activity, providing a timeline of suspicious data aggregation.

STEGANOGRAPHY

As referenced in framework item T1001

Steganography is a common form of data obfuscation that involves hiding data within another file in order to avoid detection. Because Dtex captures such a complete trail of user and endpoint behavior, it detects virtually all methods of steganography creation. If an attacker uses a steganography application, Dtex will recognize the tool being used based

on its name, the product, or even the vendor ID associated with it. It will also capture every instance of interaction with this tool, even if the activity takes place through the browser.

Dtex also captures steganography carried out through command line interfaces, including file creations, command executions, etc.

COPY AND PASTE

As referenced in many framework entries

Copy and paste activity is relevant to many entries in the MITRE matrix, as it can be key to many forms of lateral movement, privilege escalation, and forms of data exfiltration. Without a clear understanding of copy/paste activity, investigators cannot truly understand how an attacker has moved data or files through the organization.

Dtex captures all clipboard activities between files, directories, browsers, etc. It also detects copy and paste activities executed over Remote Desktop Protocol sessions. This fills in a critical gap in the audit trail, providing a clear view of how data moves throughout an attack.

ENTERPRISE USER INTELLIGENCE:
VISIBILITY TO ENHANCE MITRE ATT&CK MATRIX PROTECTION

As has been illustrated, Dtex provides visibility that is key to understanding what happens in the organization and protecting against both internal and external threats. While the above ten use cases demonstrate some particularly useful ways that Dtex's visibility helps cover the ATT&CK framework entries, they far from the only ways that Dtex is helping organizations achieve full coverage.

Contact us or reach out to your sales representative to learn more details about Dtex's MITRE ATT&CK Framework coverage, purpose-built dashboards, and additional capabilities:

info@dtexsystems.com | www.dtexsystems.com