MITRE ENGENUITY | Center for Threat Informed Defense

Design Principles and Methodology for the Insider Threat TTP Knowledge Base

Author(s):
Shelley Folk
Adam Hlavek
Suneel Sundar

January 2022

MITRE ENGENUITY | Center for Threat Informed Defense

Table of Contents

1 Purpose 1
2 Introduction 1
3 Scope 2
4 Relationship to Enterprise ATT&CK 2
5 The "Did" Criterion for Insider Threat Cases 3
6 Coding Insider Threat Cases to the Knowledge Base 4
7 Data Collected 6
8 Analysis of Data 6
9 Limiting Factors 7
10 Knowledge Base Inclusion Criteria 7
11 Findings 8
11.1 Evidence-based Inferences 10
11.2 Defense Against Insider Threat 11
11.3 Frequency of Use by Insiders 11
12 Next Steps: Expanding the Knowledge Base 14
13 Summary 14

MITRE ENGENUITY | Center for Threat Informed Defense

1 Purpose

The Center for Threat-Informed Defense's Insider Threat Tactics, Techniques, and Procedures (TTP) Knowledge Base is an emergent resource that aims to advance our collective understanding of the technical mechanisms that insider threats have used. With this knowledge, Insider Threat Programs and Security Operations Centers will detect, mitigate, and emulate insider actions on IT systems to stop insider threats. Utilizing the Knowledge Base, cyber defenders across organizations will identify insider threat activity on IT systems and limit the damage. Capturing and sharing the Design Principles and Methodology for developing the Knowledge Base is a foundational step to establishing this community resource and enabling its broad adoption and ongoing development.

2 Introduction

Malicious insiders represent a unique threat to organizations. Modern enterprise networks are frequently designed to defend against external threats while implicitly trusting their internal user base. In order to increase efficiency and productivity, employees are afforded a great deal of access to information. While that implicit trust is essential for allowing individuals to do their work, connect to the resources they need, and communicate across the organization, it also affords opportunities for those within the organization to abuse that trust. Employees can potentially do grave financial, operational, and reputational damage through malicious actions such as stealing sensitive data or deliberately sabotaging key systems. Thus, the detection and mitigation of the "insider threat" has become one of the standing challenges within the realm of cybersecurity.

Detecting such insider threats is inherently challenging for network defenders. Insider threat actors move on the network very much like trusted employees—because they are. This presents a unique challenge when differentiating the behavior of a normal user from a malicious one. Insiders typically leverage their existing accesses and privileges to obtain the information they are seeking or manipulate the systems they are targeting for sabotage. While external actors often deploy malicious software and actively scan network infrastructure to facilitate an intrusion, insiders typically need no such tools, as they have the privileges and knowledge required to execute their objectives. Furthermore, Security Operations Center (SOC) staff already find themselves prioritizing and triaging staggering amounts of alerts. The ongoing flood of noisy external threats can easily drown out the subtle insider.

Studying the problem of insider threats is difficult for several reasons. SOCs and insider threat analysts need to know which technical mechanisms are used by insiders and which security controls mitigate insider threats on information technology (IT) systems. This manifests as a local problem for each organization, but the challenge compounds when developing insider countermeasures across multiple organizations. Tackling the challenge of insider threats necessitates the sharing and analyzing of industry-wide data, yet there is an understandable hesitancy on the part of many organizations when it comes to sharing information about insider events. These incidents often lead to tangible reputational, financial, or operational damage to an organization, as well as highlight gaps in that organization's cybersecurity posture. This contributes to an unwillingness to publicize insider incidents when they do occur, lest they

expose these weaknesses to other would-be threat actors. This hesitancy, while understandable, leads to a lack of a robust, easily utilized body of knowledge.

These challenges inspired the Center to develop an open knowledge base of the TTPs used by insider threats in IT environments. To facilitate this, the Center research team collaboratively engaged with Center Participants, outlining the intended methodology for establishing the knowledge base, providing examples of the type of insider threat activity that should be included, and describing the evidentiary standards required to support that inclusion. Using the TTPs contained within MITRE ATT&CK® (content version 10.1) for Enterprise as the baseline for describing adversarial cyber activity, Center participants verified insider TTPs observed in their real-world investigations, anonymizing any identifying information while preserving the requisite technical detail and context. The Center team then reviewed and analyzed the shared data, the results of which represent the foundation of the knowledge base. This paper describes the collection and analysis methodology used to create the knowledge base, details the techniques contained within it, and discusses the Center's proposed next steps to grow and evolve the project in the future.

3 Scope

The Insider Threat TTP Knowledge Base project addresses the unique challenges that insider threats pose by starting with a modest scope in pursuit of an evidence-based result. We constrained this research effort to the technical mechanisms that insiders use on information technology (IT) systems. This means that we deliberately excluded physical insider threats, such as workplace violence or smuggling documents on one's person; those are non-technical and independent of IT systems. For the scope of this project, we likewise rejected discussions of the insider's motive or what the insider did and could do once off the IT systems.

This distinction is important. Within a single organization, different departments that have purview over insider threat may and do define the insider differently. This project compounds that complexity by seeking to rigorously define insider TTPs that can be used across all organizations. We were able to meet this goal by defining insider TTPs for security operations centers and cyber defenders, and by following the model of the Enterprise ATT&CK framework, which is well-established for SOCs and cyber defense professionals.

4 Relationship to Enterprise ATT&CK

The Insider Threat TTP Knowledge Base is not part of Enterprise ATT&CK but represents a collection of insider threat actions that have been observed in enterprise networks and aligns this evidence to existing Enterprise ATT&CK TTPs.

The Enterprise ATT&CK matrix provided the baseline for the techniques identified by project participants. The participating organizations were asked to identify insider techniques within actual case files corresponding to existing Enterprise ATT&CK techniques, or to propose new techniques deemed novel or unique to insider threats. Based on the evidence submitted, the project did not identify any techniques that were unique enough to merit consideration as new techniques.

The addition of techniques to the Enterprise ATT&CK matrix requires publicly available, open sources as reference material. If a novel insider technique is identified, but is not referenced

through publicly available sources, it makes adding such a technique to Enterprise ATT&CK infeasible.

As the Knowledge Base evolves, we anticipate discovering and documenting new insider techniques that may not fit within Enterprise ATT&CK. These novel insider techniques will be added to our Knowledge Base. Eventually, the Knowledge Base will consist of a mix of techniques referenced in Enterprise ATT&CK and techniques that are unique to insider threats that are not included in Enterprise ATT&CK.

5 The "Did" Criterion for Insider Threat Cases

Many times, network defenders will focus on the TTPs of the last major insider threat case to hit the news, anticipating that every insider threat will act like a Manning, Snowden, or Hanssen. When so much attention is paid to the one-in-a-million indicators associated with these notorious cases, more mundane but equally damaging actions might be overlooked. Hunting the one-in-a-million cases often puts defenders into the mindset of thinking about what is possible, instead of what is *probable*. It causes defenders to "be creative" when designing sensors or searching for indicators because defenders must speculate on techniques that an insider could hypothetically execute. This creativity causes Insider Threat Programs and SOCs to lose focus. The researchers have deemed these TTPs as "could"—as in an insider threat *could* use these TTPs to harm an organization. *Could* comprise a superset of actual, hypothetical, and fantastical insider actions. Frederick the Great is quoted as saying "he who defends everything defends nothing." As a result of this Insider Threat TTP Knowledge Base, organizations can shift their mitigations from living up to Frederick the Great's warning to actionable detections and response.

With limited resources, an organization is better equipped to defend their networks if they can focus their efforts where they are most beneficial. This project informs defenders where their resources are best spent. To get there, the researchers reduced the set of TTPs in the "could" section down to a much more reasonable "would" set. These are TTPs that have a reasonable chance of being used by an insider threat. We assessed each TTP for the skill level needed for successful execution and the potential benefit each TTP would give to an insider threat. Inclusion in the "would" set was validated by the Center researchers and Center participants, as individuals with extensive experience across public and private sector cyber defense, with further specialized experience in detection and response to insider threat events. This experience and expertise drew out the "would" set of TTPs as a transition between the ephemerous "could" and the data-driven "did" TTPs, which comprise the Insider Threat TTP Knowledge Base. The TTPs were only counted as "did" if they were seen in the documented case files.

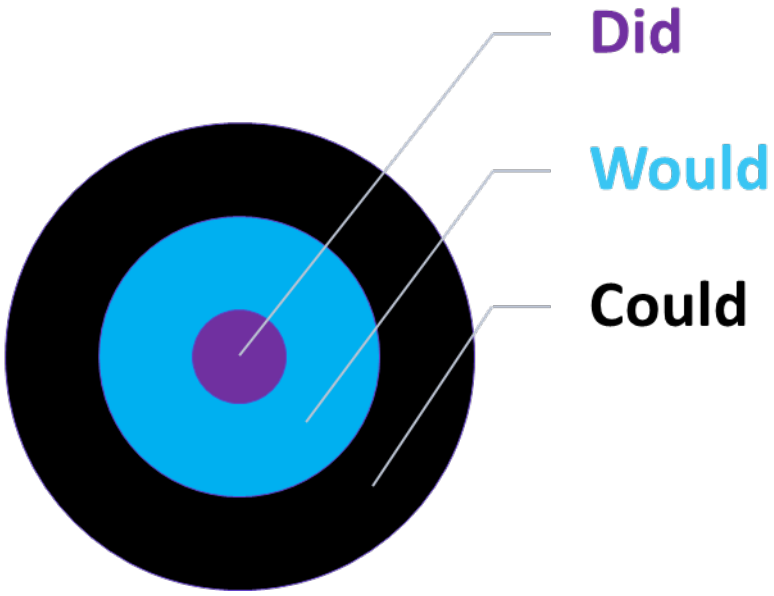

Figure 1 Focusing our defenses on real-world adversary behaviors-the "did"

6 Coding Insider Threat Cases to the Knowledge Base

Having established inclusion criteria for the knowledge base, the next step was to develop a system to code from an organization's case data to the format of the Insider Threat TTP Knowledge Base. Here too, the project inherited the structure developed by Enterprise ATT&CK. We began with a notional "would" set and worked with the contributing participants to define which techniques and sub-techniques were observed within each submitted case.

We addressed the sensitivities surrounding the exchange of insider incident data by letting the participant organizations share coded versions of their cases. Each organization anonymized and abstracted their insider case data and identified which Enterprise ATT&CK techniques and sub-techniques were expressed in that case. To facilitate this coding process, the Center research team provided the following to participants:

- A candidate matrix of tactics and techniques (the set of "woulds")
- A methodology for identifying specific TTPs within real insider threat case files

This exercise reduced the burden on the individuals coding their cases, since the full Enterprise ATT&CK matrix contains hundreds of individual techniques and sub-techniques. The researchers made the task of reviewing and coding cases less daunting by reducing the volume of candidate TTPs.

ID	Tactic	Technique	Description
ATT&CK T1548	Privilege Escalation	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions.
ATT&CK T1222	Defense Evasion	File and Directory Permissions Modification	Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files. File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions.
ITXXXX Ref ATT&CK T1039	Collection	Data from Network Shared Drive	Adversaries may search network shares on computers **to which they have been given access** to find files of interest.*
ITXXXX	Exfiltration	Send to personal email	Insider threats may send confidential or proprietary information to their own personal email account

Examples of TTPs taken directly from the ATT&CK Matrix

Example of ATT&CK TTPs modified for insider threat

Example of new TTPs specifically for insider threat

*Modified TTPs change some of the language in the description to more accurately reflect insider threats as opposed to APT/external threats. The original description of T1039 reads: "Adversaries may search network shares on computers **they have compromised** to find files of interest."

Figure 2 Referencing and expanding upon Enterprise ATT&CK

We established an iterative process of validating TTPs insider threats would use by connecting them to examples where insider threats did use those TTPs (i.e., taking them from "would" to "did" so they can be included in the Knowledge Base.)

1. We proposed TTPs that an insider would (reasonably) use.
2. Participants validated the proposed TTPs against reporting of what insiders did in cases.
3. Participants proposed additional TTPs – allowing for the possibility that an organization may have identified an insider action that was not part of Enterprise ATT&CK.
4. We reviewed proposals to ensure consistency and clarity in all proposed TTPs for the Knowledge Base, and deduplicate all TTP nominations. Any newly proposed TTPs then became candidates that were validated by other participants.

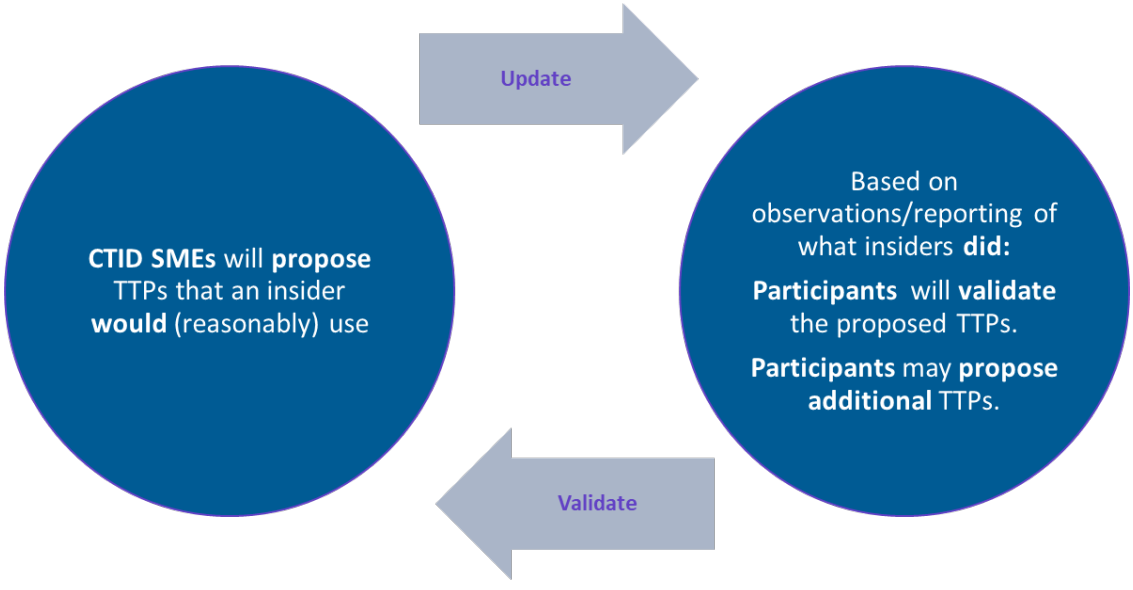

Figure 3 Iterative validation and expansion of the knowledge base

7 Data Collected

Project participants provided a sequential list of TTPs per case, with information on the data sources used to detect those TTPs. Our findings are therefore validated by both what TTPs were used by the insiders and how these TTPs were detected. Validating data appeared in the following forms:

- Types of logs, analytics, or other methods will help future SOCs and insider threat analysts.
  - Data source(s) used to identify/validate each TTP within each case
  - Format of each data source (if applicable)
  - Existing analytics used to detect TTP (if applicable)
  - Timestamps of each TTP to better understand the overall timeline
- The tactic each technique should fall under. Just like the Enterprise ATT&CK matrix, a technique can fall under multiple tactics depending on how the insider used the technique in each case.

Along the way, there may be insider actions that do not neatly fit into Enterprise ATT&CK tactics or techniques. Contributors can propose new or modified tactics and techniques.

- Techniques can be modified from an existing Enterprise ATT&CK technique with new language to make it applicable to insider threats.
- Brand new techniques can also be created when an existing technique is not sufficient.

8 Analysis of Data

We are confident in the following conclusions from the data received and analyzed to date.

- **The insider goal of data exfiltration is prevalent.** The motivation can range from malicious to benign. For this project, motivation is not germane. This project is scoped to the technical mechanisms used by insiders,
- **These TTPs are easy to execute**. Most insider threat actors that are detected lack the technical expertise or access necessary to execute many potential insider threat TTPs.
- **SOCs and Insider Threat Programs catch what they look for**. One purpose of this project is to identify TTPs used by insider threats so organizations can better protect themselves. Defenders often focus on threats from outside the organization because it is easier for them to understand how those actors operate.

These observations confirm the intuition of our researchers and contributors regarding insider threats. The project adds unique value in confirming our insider “hunches” with empirical data across multiple organizations and verticals.

9 Limiting Factors

This project was privy to an incomplete set of insider case data. Our contributing organizations possessed more insider cases than our participants submitted to create this stage of the Insider Threat TTP Knowledge Base.

- **Cases may have been pre-screened.** Despite the anonymized nature of our methodology, some organizations might not have been comfortable sharing data on some of their more sensitive cases, especially if some of these cases are still ongoing.
- **Individuals coding the cases might not have had access to the breadth of cases within their organization.** Large organizations tend to have multiple departments with overlapping missions that all create insider threat type cases on employees. Insider threat programs, SOCs, personnel security, and human resources organizations may have different sets of cases on employees depending on their own insider threat criteria, the activity that opened the case, or how the activity was detected or reported. Different organizations also have different levels of sharing among their departments. The organizations coding these cases likely did not have access to every case within their organization. This filter may contribute to the tendency for cases to share attributes.

In acknowledging these, we in turn foresee immense opportunity to expand the Knowledge Base with additional insider threat case data.

10 Knowledge Base Inclusion Criteria

The data shared by contributors to this project was required to meet certain criteria for inclusion in the analysis. The TTPs included were either found in Enterprise ATT&CK or were of a similar technical nature. Actions taken by insider threats have a very wide range. Some of these actions can be detected through log files and structured data (e.g., an employee emailing proprietary information to themselves), while others can only be detected through analysis of written words (e.g., an employee threatening a coworker in person or over email) or purely physical actions (e.g., violence against a coworker or committing arson). To scope to the Knowledge Base to technical TTPs and keep it in line with the rigorous evidentiary standards inspired by the Enterprise ATT&CK framework, we have only included actions that can be detected through structured data logs. Although analysis of human-language collections has improved in recent years, sentiment analysis falls outside the bounds of this research project. We have intentionally kept the focus of this project on technical mechanisms used by insiders on IT systems in order to best serve the intended audience of Security Operations Centers, insider threat analysts, and cyber defense practitioners. Many other research programs focus on sentiment analysis, psychological predecessors, and other aspects of insider threat detection outside of this project's intended scope.

We also only included TTPs that were validated by documentation, requiring that participants draw from existing casefiles. This gives us the specificity necessary to identify all the individual techniques and sub-techniques an insider threat used and the timeline in which they were used. This also prevented the project from drifting away from the "did" category of TTPs into "would." Techniques included as unvalidated "woulds" do not meet evidence-based standards.

They are still useful as a guide for defenders and will be marked as unconfirmed insider techniques (i.e., “woulds”) until they meet the evidence criteria.

11 Findings

The following graphic illustrates, based on participant-validated evidence, the prevalence of Enterprise ATT&CK techniques used by insider threats within the full Enterprise matrix.

Figure 4 ATT&CK Navigator view of validated insider TTPs.

11.1 Evidence-based Inferences

Based on the case data shared with the Center team, the following inferences were observed:

Insider threats routinely use unsophisticated TTPs to access and exfiltrate data. Perhaps unsurprisingly, malicious insiders were frequently observed using relatively "low tech" techniques that are readily available to most enterprise users. These methods are easy to understand and can reliably be taken advantage of by users lacking elevated privileges or advanced technical know-how. It is worth acknowledging, however, that these techniques may be observed more frequently because defenders are good at detecting these TTPs and the underlying data sources used to illuminate these techniques are readily available.

Insider threats routinely leverage existing privileged access to facilitate data theft or other malicious actions. The use of valid accounts (T1078) was widely observed, with evidence suggesting valid existing accounts were used at multiple stages of insider activity. Ample evidence of domain (T1078.002) and cloud (T1078.004) accounts was also observed. This activity is not especially surprising, as malicious insiders have the unique advantage of being provided legitimate access to an organization's systems and data. However, the prevalence of such techniques does underscore the importance of auditing legitimate user access to effectively detect insider threats.

Insiders routinely "stage" data they intend to steal prior to exfiltration. Collections of targeted files are frequently aggregated by insiders shortly before attempting to move the data outside of the network, typically being saved to a specific folder on the user's local system (T1074) or saved into an archive file (T1560).

External/removable media remains a common exfiltration channel. External media (T1052), particularly USB-connected external media (T1052.001), was often used as a means to move data outside the corporate perimeter. As such external media is inexpensive, widely available, familiar to users, and can be easily hidden due to its small physical size, it represents an appealing exfiltration vector to insiders. While technical controls restricting the use of external media have become increasingly popular in recent years, some organizations are undoubtedly hesitant to block access to USB drives wholesale, as this limits user flexibility. Those organizations that choose to allow the use of such external drives must be conscientious of this threat.

Email remains a common exfiltration channel. As cybersecurity practitioners have long observed, users frequently leverage email (T1114) as a means to get data in and out of an organization. While cloud services and other newer technologies have gained traction as exfiltration channels, evidence shows that many malicious insiders continue to use email as a simple and expedient way to pass files to personal accounts or others outside an organization. Incidents of users taking additional steps to obfuscate this activity by sending data in the form of attached ZIP files or other types of compressed archives were also observed.

Cloud storage represents both a collection target for insiders and a common exfiltration channel. The broad adoption of cloud storage solutions such as Microsoft OneDrive, Google Drive, and Dropbox, has positioned these platforms as key repositories of data. Users were

frequently observed harvesting large numbers of files from such cloud storage locations (T1213) during insider incidents. Conversely, insiders were observed using cloud storage services as an exfiltration channel (T1567.002), uploading data to personal cloud storage accounts following the collection and staging of targeted files.

Taken in totality, techniques used in instances of data theft by insiders often followed a pattern that could be roughly be described as "dump, stage, and steal." The combined sequence of downloading substantial amounts data, organizing or aggregating it, and exfiltrating it over email, cloud services, or USB devices was observed to be used by malicious insiders by nearly every participant. While this pattern is not applicable to other types of insider threats, such as those seeking to do harm via data destruction or sabotage, the evidence suggests that this is a common pathway for the theft of intellectual property or other sensitive or proprietary data. Further research into this type of "event chaining" would be valuable, particularly for differentiating malicious sequences of events from legitimate user activity.

11.2 Defense Against Insider Threat

Given the insider actions confirmed in the "did" list, we discussed some characteristics that separate actions an insider "would" engage from those confirmed insiders "did" execute. Consequently, we identified the following attributes of defenders:

- Given their sustained prevalence, defenders must continue to rigorously monitor common exfiltration sources such as removable media, email, and cloud storage platforms.
- Insider threat teams vary in the types of data sources and detection tools they have access to, which may influence how they focus their analysis and which data sources prove most lucrative to them.
- Data sources and tools that are valuable for detecting insider threats may be split across multiple teams within an organization (SOC, incident response, legal, etc.).
- Insider threats are often not fully identified as such until an investigation approaches its conclusion.
- Determining user intent is extremely challenging. Defenders often lack the context to distinguish user negligence or errors from deliberate, malicious actions. We repeat that intent and other behavioral indicators are outside the scope of this research, which addresses insider actions on IT systems, captured by logs, irrespective of intent.

11.3 Frequency of Use by Insiders

The Center team reviewed the validated, participant provided TTP data and identified the Enterprise ATT&CK techniques which occurred most frequently. As described in Section 10.2, several patterns and trends of techniques emerged. The team then divided these techniques into the following categories:

Frequent Insider Use

- Many documented examples of the technique were provided, and examples were provided by multiple participants.

Moderate Insider Use

- Multiple documented examples of the technique were provided, but examples were only provided by a single participant, or examples were provided by multiple participants in small numbers.

Infrequent Insider Use

- Documented examples of a given technique was provided, however only one or two instances of the technique were observed across all participants.

The following graphic illustrates the prevalence of those Enterprise ATT&CK techniques used by insider threats based on participant validated evidence, organized by associated tactic.

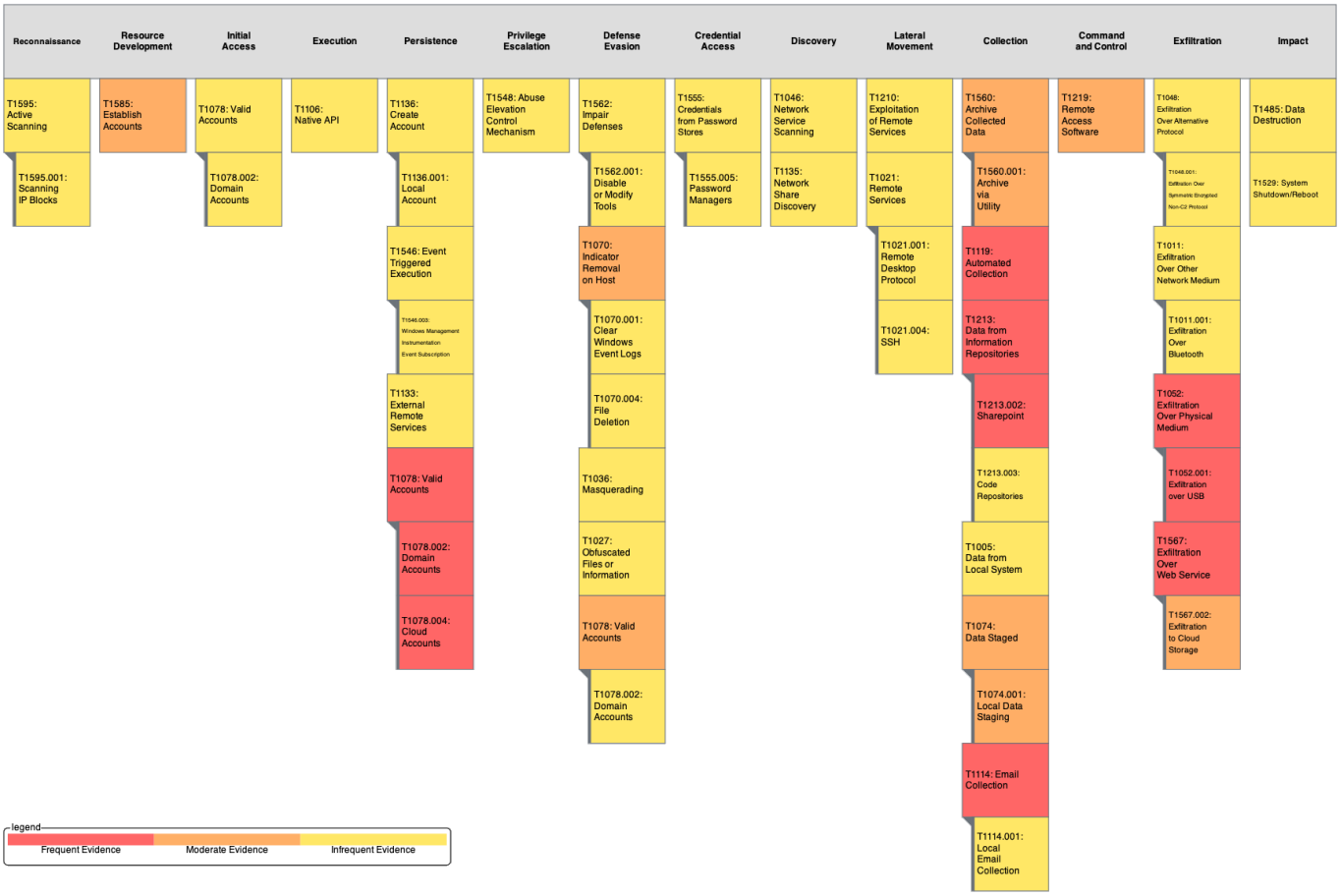

Figure 5 Prevalence of techniques in participant cases

The following table illustrates the prevalence of those Enterprise ATT&CK techniques used by insider threats based on participant validated evidence, organized by frequency.

Frequency of Use by Insiders

Frequent Evidence of Insider Use	Moderate Evidence of Insider Use	Infrequent Evidence of Insider Use
T1078: Valid Accounts	T1560: Archive Collected Data	T1021: Remote Services
T1213: Data from Information Repositories	T1070: Indicator Removal on Host	T1048: Exfiltration Over Alternative Protocol
T1052: Exfiltration Over Physical Medium	T1074: Local Data Staging	T1005: Data from Local System
T1114: Email Collection	T1106: Native API	T1529: System Shutdown/Reboot
T1119: Automated Collection	T1219: Remote Access Software	T1562: Impair Defenses
T1567: Exfiltration Over Web Service	T1585: Establish Accounts	T1548: Abuse Elevation Control Mechanism
		T1595: Active Scanning
		T1485: Data Destruction
		T1210: Exploitation of Remote Services
		T1546: Windows Management Instrumentation Event Subscription
		T1027: Obfuscated Files or Information
		T1555: Password Manager
		T1046: Network Service Scanning
		T1306: Masquerading
		T1572: Disable or Modify Tools
		T1135: Network Share Discovery
		T1011: Exfiltration over Bluetooth
		T1136: Create Account
		T1133: External Remote Services

12 Next Steps: Expanding the Knowledge Base

The research team continues to seek submissions to the Knowledge Base. Future contributions will require the standard of evidence as outlined above. As additional contributions are collected, validated, and assessed, this new evidence of insider activity will likely expand the number of techniques included within the Knowledge Base and better capture the frequency with which techniques are being actively used by insiders. Similar to the data collected to date, future contributions must fit the guidelines listed below:

- Only include actions that involve the use of IT systems and can be detected through structured data logs.
- Only include TTPs that are validated by documentation (e.g., exist within an organization's case files or tracking system).
    - Contributors are required to provide a minimum level of detail, to include:
        - A corresponding technique and tactic (either an existing ATT&CK technique or a new proposed technique).
        - A date or date/time offset.
        - A data source.
        - Contextual information describing the event.
    - Details that would clearly identify organizations or individuals involved must be anonymized.

13 Summary

This paper describes the challenges of detecting insider threats in enterprise networks and the challenges of sharing technical evidence of insider events. It lays out a framework for building an open Insider Threat Knowledge Base, applicable across organizations and across industries. This Knowledge Base conforms to the structure and philosophy of MITRE ATT&CK for Enterprise. The paper describes the methodology used by the Center research team to collect and organize validated, anonymized evidence of insider incidents, and highlights some of the initial findings and inferences gleaned from this data sample. These findings are evidence-supported and represent what insiders did on IT systems across industries. We are confident that the initial knowledge base and the insights into the process of designing and building it can be of benefit to the cybersecurity community.

We acknowledge that we analyzed a small set of data, especially relative to the collection of insider cases that readers of this paper could code and contribute. We intend to further grow and refine the knowledge base by including submissions of additional case data and sparking discussion of the challenges and opportunities within the insider threat detection space.

