Multi-Source Analysis of Top MITRE ATT&CK® TECHNIQUES

TIDAL CYBER & Cyentia INSTITUTE

THREAT-INFORMED DEFENSE

PUBLISHED DATE **2023**

"HOW WILL ADVERSARIES ATTACK US AND WHAT DEFENSES SHOULD WE PRIORITIZE?"

If you work in cybersecurity, chances are good you've asked—or been asked—a question like this one. The good news is that there's more information available than ever before to help answer that question. But that doesn't mean answering it is easy.

MITRE ATT&CK® is a knowledge base of adversary tactics and techniques based on real-world observations. Its purpose is to serve as a foundation for threat models and methodologies leading to more effective cybersecurity.

More and more cybersecurity industry reports include statistics on observed ATT&CK techniques. That's great in terms of having more data available for defenders and decision-makers, but a challenge arises to establish consensus among them regarding the most common techniques. Sources differ greatly in their visibility of ATT&CK, what they measure, how they report information, etc.

This study analyzes 22 public sources of ATT&CK statistics to find common trends among them. Our goal is to aid organizations in building a more threat-informed defense.

Contents of This Study

Key Findings

A third of ATT&CK techniques were not reported by our sources in the timeframe of study. 23% of them were reported by at least five sources.

Valid Accounts (T1078) and Exploit Public-Facing Application (T1190) are the most reported and most frequently observed techniques used by adversaries for Initial Access.

85% of ATT&CK sub-techniques were never reported by any source. 1% of them were reported by at least five sources.

Overall, the most frequently used techniques are Account Discovery (T1087), Command and Scripting Interpreter (T1059), and System Owner/ User Discovery (T1033). But there's a different top 10 for each source type.

Managed service or incident response providers report two to three times as many techniques as other types of sources.

Based on the overall most frequently observed techniques, the most relevant mitigations are M1040, M1038, and M1028.

Source coverage is best for tactics spanning Initial Access to Defense Evasion; it's worst for those that take place outside organizational sensors (Reconnaissance & Resource Development).

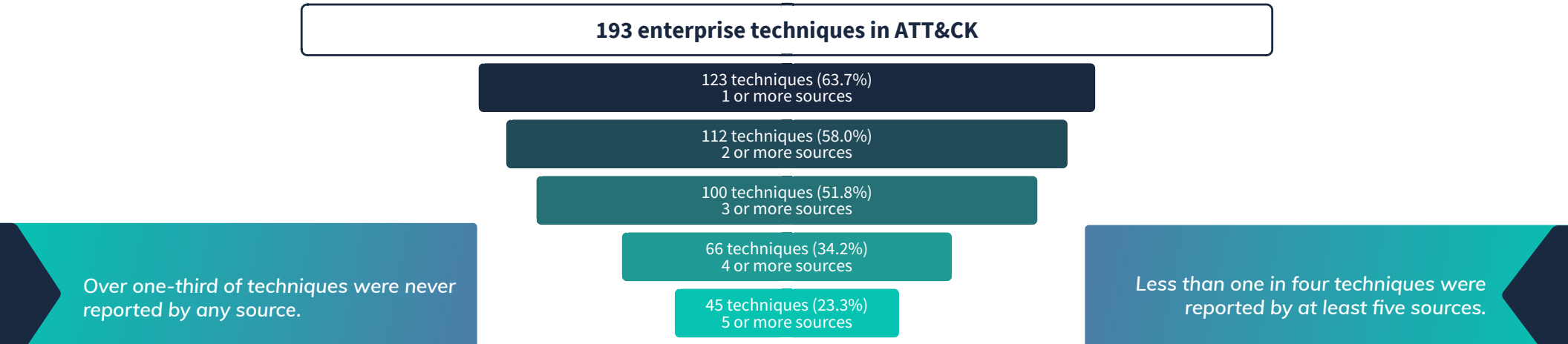
Primary challenges to security professionals and analysts seeking to leverage ATT&CK include the pace of updates, tactic-technique ambiguity, under-reporting of sub-techniques, and a dearth of reporting by segment (i.e., industry or specific to ICS environments).

Source Visibility & Reporting across ATT&CK

We'll kick things off by examining the breadth of visibility and reporting across the ATT&CK matrix. Are our sources collectively observing most of the techniques defined by MITRE or just a small slice of them? Are some techniques sighted by many sources, while others by just a few or not at all? This is important for assessing (and compensating for) any blind spots and reporting gaps that may exist.

Reporting of Techniques

According to MITRE, ATT&CK techniques represent how an adversary achieves a tactical goal by performing an action. Version 12.1[1] defines a total of 193 techniques, and the sources we analyzed reported sightings of 124 (64%) of those. We'll get into which ones were observed most often later, but for now, let's absorb the fact that over one-third (36%) of all techniques were not reported by any of the 22 sources we reviewed. Just over half (52%) of ATT&CK techniques were seen by three or more sources, and less than a quarter (23%) of them were reported by at least five sources. This demonstrates that ATT&CK visibility varies widely across different sources; we'll talk about why in a moment.



TAKEAW&Y: You need multiple reporting sources to build broad visibility of technique utilization.

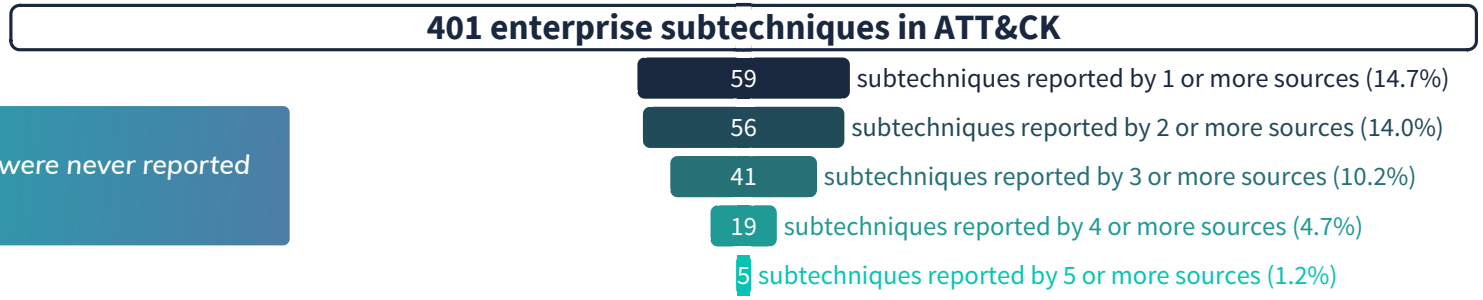
1 ATT&CK v13 was released in April 2023 as this study was in production. We're basing our analysis on v12 because v13 was not available during the timeframe our sources collected and reported their findings.

Reporting of Sub-Techniques

MITRE introduced sub-techniques for ATT&CK in early 2020. Think of them as more specific instantiations of techniques. For instance, phishing is subdivided to differentiate the vector of delivery—attachment, link, or service. There are 401 sub-techniques defined in ATT&CK version 12.1.

Let's see how visibility and reporting fares at this level of the matrix. Something to keep in mind here is that not all sources report sub-techniques (13 of 22). So, it's difficult to distinguish true visibility from simply choosing to report at the technique level. Be that as it may, 59 of the 401 (15%) ATT&CK sub-techniques were reported by at least one source. About 10% were reported by three or more sources, while a scant 1% crossed the five-source mark. Clearly, the visibility (or at least reporting) of sub-techniques falls well below that of techniques.

85% of ATT&CK sub-techniques were never reported by any source.



As analysts, we prefer reporting sub-techniques for max specificity and utility. But we begrudgingly understand the desire/need to roll up to techniques when the data doesn't consistently enable the distinction of sub-techniques. For those looking to make sense of the inconsistent reporting that currently exists around techniques and sub-techniques, we suggest harvesting the lowest level provided. That way, you can drop down to sub-techniques or roll up to techniques based on your use case and data availability.

TAKEAW&Y: Most sub-techniques are not observed or not reported (or both), which limits actionability.

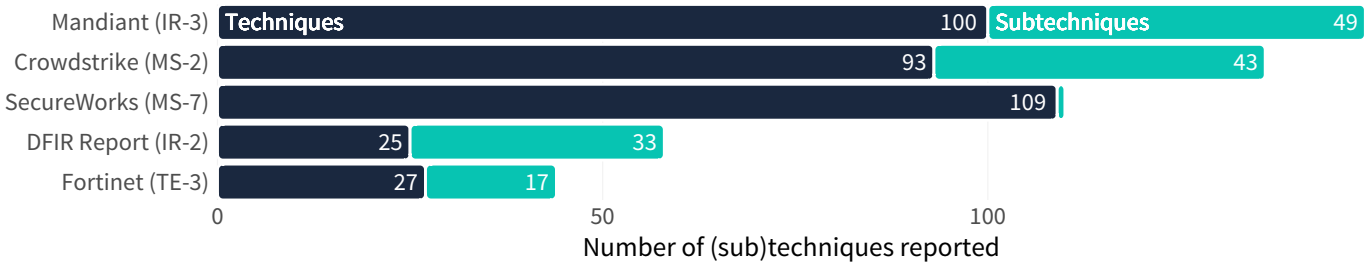
What about tactics?

Those familiar with the structure of ATT&CK may be asking this question. Tactics are the highest level expression of adversary activity, and there are 14 of them in the Enterprise Matrix. We don't focus much on tactics in this report because a) not many sources report at this level, and b) techniques (especially sub-techniques) are far more actionable.

Reporting by Source

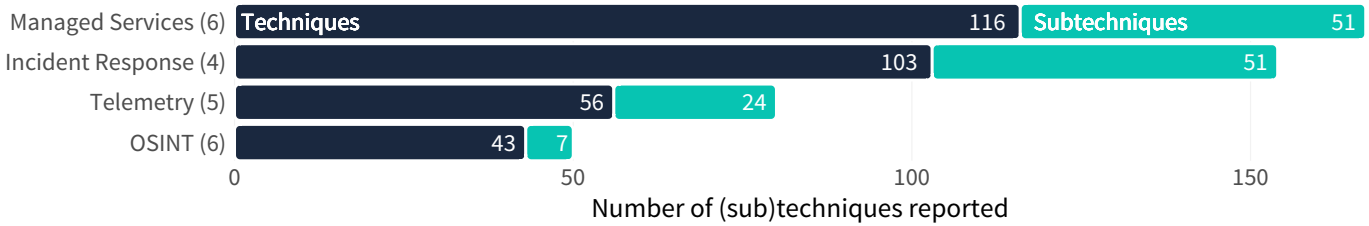
The previous two sections should drive home the point that you won't achieve comprehensive visibility across the ATT&CK matrix from any single source. But where's a good place to start? Do some sources—or types of sources—provide more comprehensive reporting of techniques or sub-techniques than others? We'll tackle those questions in this section.

Mandiant's M-Trends wins the prize for reporting the highest combined number of techniques and sub-techniques. Crowdstrike's Falcon OverWatch Threat Hunting Report runs a close second on both counts, while State of the Threat from SecureWorks stands atop the list for the most techniques reported. The DFIR Report punches well above its weight class by reporting a very respectable number of techniques and sub-techniques from a comparatively small number of incidents. Fortinet's Threat Landscape Report rounds out the top five and also earns a hat tip from us for making it easy to glean relative frequencies.



The number of techniques reported by these sources should NOT be viewed as a measure of capabilities. It's drawn from what's included in published reports.

It's tempting to conclude from this that one source is better than another based solely on the number of techniques reported. But more doesn't necessarily mean higher quality, superior usefulness, or greater relevance for your needs. Certain types of sources will inherently have broader visibility than others. To illustrate this, we grouped sources into the four types shown in the figure below.



Incident detection and response gives the broadest visibility across ATT&CK.

Managed service providers and incident responders are often tasked with recreating the entire attack chain through investigations. That will inevitably identify more techniques than focused telemetry (i.e., EDR or IDS). For this reason, we think it is more helpful to evaluate and compare source types than individual sources when it comes to the reporting of techniques and sub-techniques.

TAKEAW&Y: Leverage managed service or incident response providers to quickly broaden visibility.

Most Reported ATT&CK TTPs

We now shift focus from assessing the overall visibility across ATT&CK as a whole to the specific tactics, techniques, and sub-techniques that are most often reported among the sources in our study. In so doing, we want to identify which TTPs are covered by numerous sources and which ones are more limited in scope. The practical value of this for defenders is a sense of which parts of the ATT&CK matrix may be more challenging than others with respect to intel collection.

Most Reported Tactics

As mentioned in an earlier callout, tactics are the highest-level expression of adversary activity in ATT&CK, and not many sources report on them directly. Even so, we wanted to begin this section with tactics to examine how visibility varies across them. To address the absence of tactic-level info from most sources, we created simple logic to mark a tactic as observed if any of its techniques or sub-techniques were reported.[2]

The figure to the right records the number of sources reporting techniques for each tactic for each of the four source types presented in the previous section. This makes it easy to see that reporting is sparse for pre-intrusion tactics, solid as adversaries gain access, persistence, and privileges, and then erodes a tad as adversaries broaden their presence, control, and impact across the environment.

TAKEAW&Y: Source coverage is sparse for some tactics; visibility will be harder to gain for those.

It's also apparent that different source types are more (or less) likely to report techniques in some tactics than others.

2 *ATT&CK aficionados will undoubtedly have objections here because some techniques fall under more than one tactic. If the source didn't distinguish which tactic was in scope (which is almost always the case, unfortunately), we just marked all relevant tactics. This inevitably results in some amount of over-reporting for certain tactics, but we do not assess that this invalidates the main findings we share here.*

Most Reported Techniques

Here we want to compare technique-level coverage by tallying the number of sources reporting each of them. The challenge is that 123 techniques were observed by at least one source, which is a lot to squeeze into a chart. Thankfully, the enterprise ATT&CK matrix offers a form well-suited to this purpose.

Fewer sources — More sources

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
T1595	T1586	T1078	T1059	T1078	T1055	T1055	T1003	T1082	T1021	T1056	T1071	T1041	T1486
T1590		T1190	T1047	T1053	T1078	T1036	T1110	T1018	T1091	T1005	T1090	T1567	T1485
		T1566	T1053	T1133	T1053	T1078	T1056	T1057	T1210	T1560	T1105	T1020	T1490
		T1189	T1203	T1547	T1547	T1027	T1555	T1083	T1550	T1114	T1219	T1048	T1489
		T1133	T1204	T1098	T1543	T1112	T1552	T1012	T1570	T1119	T1572	T1030	T1496
		T1195	T1129	T1136	T1574	T1562	T1558	T1040	T1534	T1039	T1573	T1011	T1491
		T1091	T1569	T1543	T1068	T1218	T1040	T1497	T1080	T1074	T1001	T1537	T1495
		T1199	T1106	T1574	T1134	T1070	T1539	T1518		T1113	T1095		T1498
		T1200		T1197	T1037	T1140	T1212	T1007		T1115	T1102		
				T1037	T1546	T1574	T1522	T1010		T1530	T1132		
				T1176	T1548	T1127		T1016		T1123	T1571		
				T1505		T1134		T1033		T1185			
				T1546		T1197		T1049					
				T1525		T1202		T1069					
						T1497		T1087					
						T1222		T1120					
						T1548		T1135					
						T1550		T1201					
						T1564		T1482					
						T1211		T1614					
						T1216		T1217					
						T1220							
						T1207							

TAKEAW&Y: Source-level coverage is noticeably higher for a dozen or so techniques. That doesn't mean they're the most critical—but it's a good reason to keep them on your radar.

All techniques in this chart are sorted under each tactic according to the number of sources reporting them.

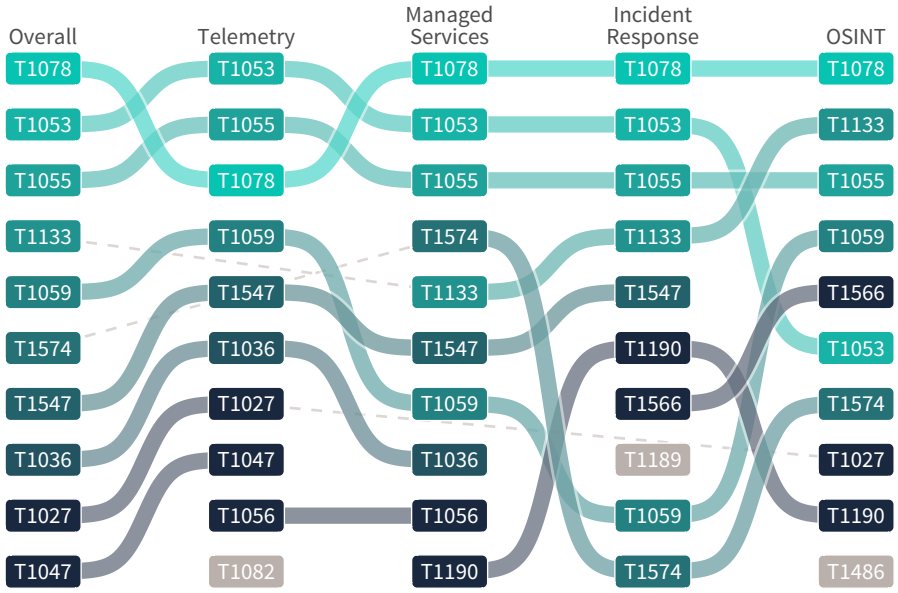
Ten Most Reported Techniques

1. Execution: Command & Scripting Interpreter (T1059)
2. Privilege Escalation: Process Injection (T1055)
3. Defense Evasion: Process Injection (T1055)
4. Initial Access: Valid Accounts (T1078)
5. Persistence: Valid Accounts (T1078)
6. Privilege Escalation: Valid Accounts (T1078)
7. Defense Evasion: Masquerading (T1036)
8. Defense Evasion: Valid Accounts (T1078)
9. Initial Access: Exploit Public-Facing Application (T1190)
10. Execution: Windows Management Instrumentation (T1047)

The "heat" shading is also based on the number of sources but adjusted relative to the overall matrix rather than each tactic. This enables you to discern that the #6 technique under Defense Evasion (Modify Registry) was reported by more sources than the #1 technique under Exfiltration (C2 channel).

Most Reported Techniques by Source Type

Aggregate views of technique reporting are certainly helpful, but it is also important to acknowledge that things may look a bit different on a source-by-source basis. The chart below should help visualize that. The ordering of each column is based on the number of sources of each type reporting that technique. The lines connecting the techniques help your eyes follow the change in rank across the different types of sources. The fill color represents the total number of sources reporting each technique (not type-specific). We often call this kind of visualization a "subway" or "worm" chart.



T1078 (Valid Accounts) is reported most often overall and by IR, Managed Services, & OSINT sources. But it drops to #3 among telemetry-based sources.

Some techniques bob up and down in rank across the different source types (e.g., T1053) or even drop out of a source type's top 10 altogether (e.g., T1574).

And then there are some (e.g., T1189, T1486, T1082) that only make the top 10 for a single source.

The moral of the story is that different sources can only report what they're able to see, and they don't all see the same techniques equally well. Diversify your sources to help ensure you see the complete picture across all ATT&CK techniques.

The obvious question from this is why these source-level differences exist. It's not easy to answer, but let's look at a couple of examples. T1189 (drive-by compromise) is only reported by IR sources, probably because it requires some amount of investigation to determine that an external site was the vector of an internal malware infection. Similarly, OSINT is often biased toward higher profile, publicly-disclosed events, so it makes sense to see T1486 (data encrypted for impact) given the glut of ransomware events in recent years.

TAKEAW&Y: Diversify your sources to ensure you see the complete picture of ATT&CK.

Most Reported Sub-techniques

We'll conclude this section by diving down to the lowest layer of ATT&CK to examine reporting of sub-techniques. Like the earlier technique-based version, sub-techniques are sorted under each tactic based on the number of sources reporting them. The shading is normalized across the whole matrix to enable comparisons of sub-techniques under different tactics..

Fewer sources — More sources

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration
T1566.002	T1059.001	T1547.001	T1547.001	T1218.011	T1003.001	T1518.001	T1021.001	T1056.001	T1071.001	T1567.002
T1566.001	T1053.005	T1053.005	T1053.005	T1562.001	T1003.002		T1021.002	T1560.001	T1090.002	
T1078.002	T1204.002	T1505.003	T1055.001	T1055.001	T1056.001		T1021.003	T1056.004		
T1078.003	T1569.002	T1574.001	T1055.012	T1055.012	T1110.004		T1021.006	T1114.003		
T1078.001	T1059.003	T1078.002	T1134.001	T1070.004	T1555.003		T1550.002			
T1078.004	T1059.005	T1078.003	T1574.001	T1134.001	T1555.004					
T1566.003	T1059.006	T1136.001	T1078.002	T1218.010	T1558.003					
	T1204.001	T1543.003	T1078.003	T1574.001	T1056.004					
	T1559.001	T1546.003	T1543.003	T1070.006						
		T1546.012	T1546.003	T1078.002						
		T1078.001	T1546.012	T1078.003						
		T1078.004	T1055.002	T1218.005						
		T1542.003	T1055.003	T1550.002						
		T1547.009	T1078.001	T1564.003						
		T1546.011	T1078.004	T1055.002						
			T1547.009	T1055.003						
			T1546.011	T1078.001						
				T1078.004						
				T1542.003						
				T1564.001						
				T1553.005						

Ten Most Reported Sub-techniques

1. Execution: PowerShell (T1059.001)
2. Defense Evasion: Rundll32 (T1218.011)
3. Initial Access: Spearphishing Link (T1566.002)
4. Persistence: Registry Run Keys / Startup Folder (T1547.001)
5. Privilege Escalation: Registry Run Keys / Startup Folder (T1547.001)
6. Defense Evasion: Disable / Modify Tools (T1562.001)
7. Credential Access: LSASS Memory (T1003.001)
8. Command & Control: Web Protocols (T1071.001)
9. Exfiltration: Exfiltration to Cloud Storage (T1567.002)
10. Initial Access: Spearphishing Attachment (T1566.001)

We already know that sub-techniques are grossly underreported overall. But there are some bright spots. In general, tactics with high numbers of reported techniques also show higher counts for sub-techniques.

The major exception to that generalization is Discovery. It racked up the second-highest tally for techniques, but only one of its 13 defined sub-techniques was reported. We suspect this stems from a combination of sources thinking the techniques are "good enough" and lacking the optics to distinguish between sub-techniques.

TAKEAW&Y: Sub-techniques are widely underreported—some particularly so.

Most Frequent ATT&CK Techniques

The previous section compared the visibility of TTPs based on the number of sources reporting them. This section seeks to analyze how often adversaries actually use these techniques. In an ideal world, every source would report the frequency of observed AT-T&CK techniques using the same measure and in the same format so that we could derive one synthesized frequency to rule them all. We don't live in that world, unfortunately.

Instead, we live in this world: Three of our sources reported counts, 11 gave percentages, two used color to distinguish relative frequency, four provided rankings, and two simply indicated whether they observed it or not. What's more, even among the 11 that reported percentages, the values don't all measure the same thing. Some reported a percentage of cases, others the percentage of detections, and still others a percentage of all techniques observed. This all makes "apples to apples" comparisons of frequencies nigh impossible and of dubious insight.

The chart to the right demonstrates this dilemma. On the surface, it indicates big and important differences in reported frequency among sources. But closer inspection reveals that many of the values aren't really comparable. For example, IR-1 shows 100% for T1486 (data encryption) because that study focused exclusively on ransomware cases, while IR-3 did not. Thus, it doesn't make sense to simply average across sources to derive a consensus frequency.

	TE-2	TE-3	TE-4	MS-4	MS-5	MS-6	IR-1	IR-3	IR-4	OS-3	OS-4
T1486			23.0%				100.0%	22.6%		44.0%	
T1059	12.9%	5.0%	31.0%		38.1%	53.4%	78.6%	44.9%		12.0%	15.8%
T1056	0.4%	99.0%						7.5%		0.1%	
T1027		7.0%	13.0%			19.4%	58.5%	51.4%			1.4%
T1055	2.6%	24.0%	22.0%		25.1%	21.7%	73.3%	28.5%			1.8%
T1082		0.1%	20.0%				42.5%	31.8%			
T1190				26.0%	15.4%		15.4%	25.8%	33.0%	17.0%	
T1189		95.0%					1.1%	4.3%	6.0%	0.3%	
T1003	7.9%		25.0%		34.5%	18.3%		9.8%			
T1133				12.0%			61.1%	8.8%	12.0%	1.0%	
T1036	14.9%	7.0%	9.0%		22.9%	22.1%	59.6%	3.2%			4.0%
T1112	0.0%	20.0%			13.2%		47.1%	22.3%			1.3%
T1053	1.0%	38.0%	12.0%		12.2%	14.7%		15.8%			24.1%
T1562	0.2%				9.2%		55.3%	13.4%			1.7%
T1566	0.3%						9.3%	8.6%	43.0%	8.0%	
T1218	10.1%					34.8%		5.4%			4.0%
T1047	8.7%	0.5%	15.0%			15.4%	45.4%	4.0%			1.4%
T1547	7.5%	0.2%					34.0%	6.9%			
T1204	0.1%	29.0%						5.8%		0.9%	
T1078					18.9%		8.9%	6.3%	3.0%	3.2%	

This makes reported frequencies of the same practical value as a ranking, which is why we've chosen to use ranks as our standard for comparing the relative frequency of techniques.

TAKEAW&Y: Be cautious comparing percentages; sources often don't measure the same thing.

Techniques Ranked by Overall Frequency

If you're reading this report hoping for a comprehensive view of ATT&CK techniques generally accepted as the most common based on real-world observations, here it is. Techniques are sorted for tactics based on the consensus ranking across all sources and colored according to overall prevalence.

Less frequent ← → More frequent

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
T1595	T1078	T1059	T1078	T1078	T1078	T1003	T1087	T1021	T1056	T1071	T1020	T1490
	T1190	T1106	T1133	T1055	T1564	T1110	T1033	T1210	T1005	T1105	T1048	T1486
	T1133	T1047	T1053	T1053	T1036	T1056	T1016	T1091	T1560	T1090	T1567	T1496
	T1566	T1053	T1505	T1134	T1140	T1555	T1057	T1570	T1119	T1219	T1041	T1489
	T1091	T1569	T1136	T1547	T1055	T1552	T1069	T1534	T1115	T1102	T1030	T1485
	T1189	T1204	T1197	T1574	T1070	T1558	T1083	T1550	T1039	T1132	T1011	T1491
	T1199	T1203	T1547	T1543	T1218	T1040	T1082		T1074	T1001		
	T1195	T1129	T1574	T1037	T1027	T1539	T1018		T1530	T1095		
	T1200		T1543	T1546	T1562	T1212	T1049		T1113	T1573		
			T1098	T1548	T1112		T1518		T1114	T1572		
			T1037	T1068	T1202		T1497			T1571		
			T1176		T1197		T1135					
			T1546		T1134		T1482					
					T1222		T1010					
					T1497		T1012					
					T1574		T1614					
					T1550		T1040					
					T1220		T1007					
					T1211		T1120					
					T1127		T1201					
					T1548							
					T1216							

Ten Most Frequent Techniques

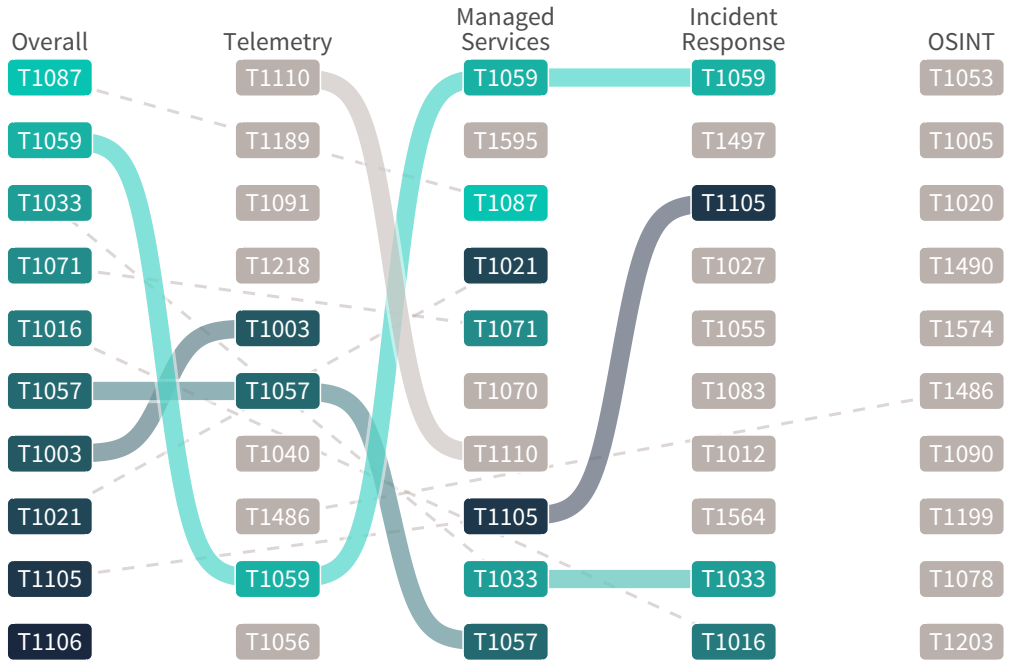
1. Discovery: Account Discovery (T1087)
2. Execution: Command and Scripting Interpreter (T1059)
3. Discovery: System Owner/User Discovery (T1033)
4. Command & Control: Application Layer Protocol (T1071)
5. Discovery: System Network Configuration Discovery (T1016)
6. Discovery: Process Discovery (T1057)
7. Credential Access: OS Credential Dumping (T1003)
8. Lateral Movement: Remote Services (T1021)
9. Command & Control: Ingress Tool Transfer (T1105)
10. Execution: Native API (T1106)

We used this process to derive the overall rankings shown here:

1. *Converted non-rank frequency data to rankings.*
2. *Rescaled the ranks for each source to account for varied numbers of reported techniques.*
3. *Took the arithmetic mean of rankings across sources.*
4. *Removed techniques reported by only one source and re-ranked.*
5. *The result is the ranked list of 113 techniques shown here.*

Most Frequent Techniques by Source Type

The single consensus view of top techniques in the prior section was the magnum opus we were aiming to create with this analysis. But since we've made a point to convey that any list of top techniques is heavily dependent upon the vantage point collecting those observations, we feel compelled to share a comparison of the most frequent techniques among the four source types. We use the same method of consensus ranking described in the previous section.[3]



This frequency-based version of the chart is decidedly less busy than its source-based cousin shared in an earlier section. Fewer connecting lines and more one-off techniques indicate less agreement among source types regarding what belongs in the top 10.

Nine of the ten most frequent techniques observed by OSINT, for example, didn't make it to the top of the charts for any other source type. Speaking for ourselves as one of those sources (IRIS 2020), we wonder if it's because of limitations of teasing TTPs from publicly-reported data, which tends to be shallower than, for example, forensic-level details.

The number of unique entries in the top 10 for other sources isn't quite so dramatic: Telemetry = 5/10, Managed Services = 2/10, Incident Response = 6/10.

That's not to say there's an utter lack of accord. T1059 (Command and Scripting Interpreter) makes the top 10 list in three of four source types. Quite a few others can be found in two columns.

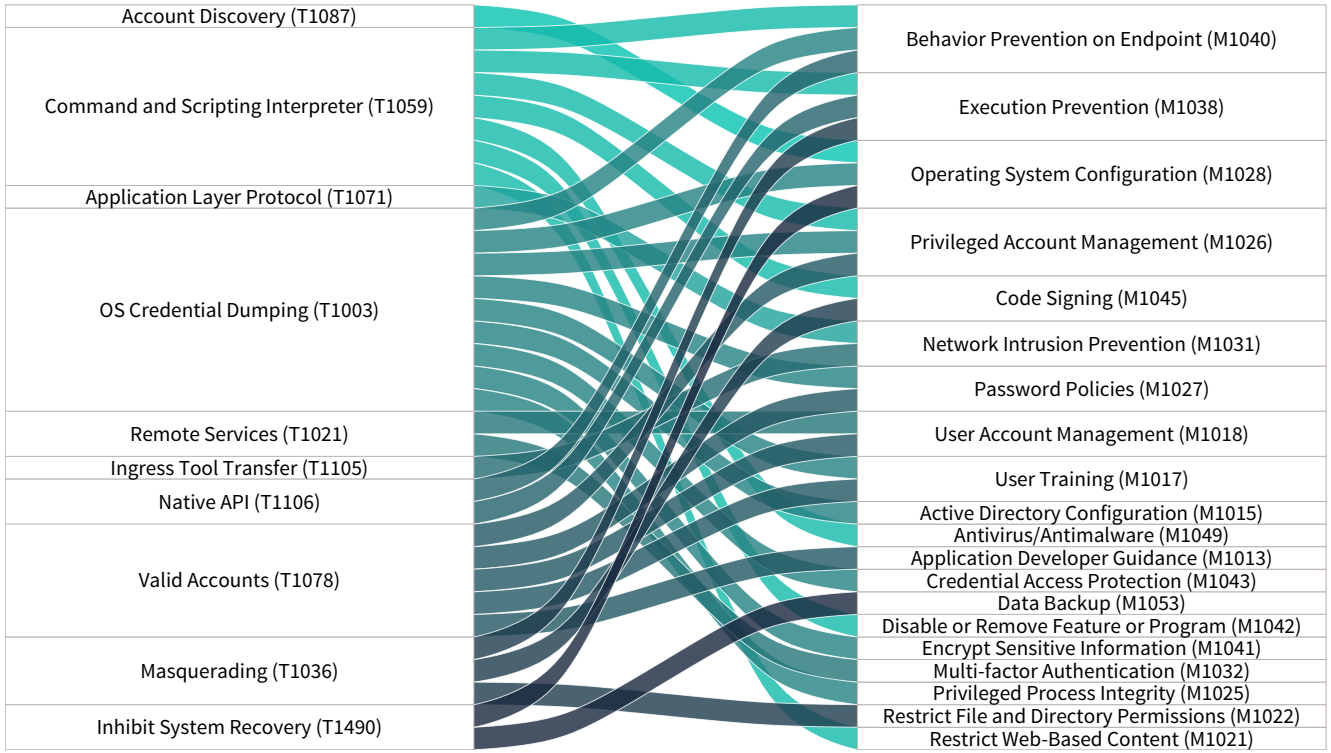
At the risk of sounding like a broken record, these source biases need to be acknowledged, better understood, and factored into analysis in order to make the most of multi-source data like this. Sure—it's a lot less messy to just go with a trusted single source for all your ATT&CK prioritization needs. But it's also a lot less likely that one source represents the totality of the environment you defend. It's a classic Elephant in the Dark problem. Thanks to the efforts of so many in our community to share this information, we're shedding more and more light on that problem to see the whole elephant.

TAKEAW&Y: The overall top 10 techniques expand to 36 if we create that list for each source type.

3 *Order = ranked frequency within source type; color = rank of technique across all source types*

Top Mitigations Based on Technique Frequency

ATT&CK is best known for cataloging and organizing adversary TTPs, but mitigations are also listed for many techniques. Of the 193 enterprise techniques in version 12.1 of ATT&CK, 151 link to at least one mitigation—nearly 80%! This can go a long way toward bridging the gap between red and blue teams by translating an organization's exposure into actionable steps toward reducing risk.



We think there is a good deal of untapped potential here for enterprise defenders. The two main applications would be 1) identifying mitigations that provide the most coverage for TTPs of concern and 2) determining what other TTPs are addressed by those mitigations as a byproduct. The latter is a welcome assist to those evaluating the costs and benefits of implementing new controls.

We mentioned that not all techniques are mapped to mitigations. Here we've taken the ten highest-ranked techniques that have such mappings (left) and connected them to their mitigations (right).

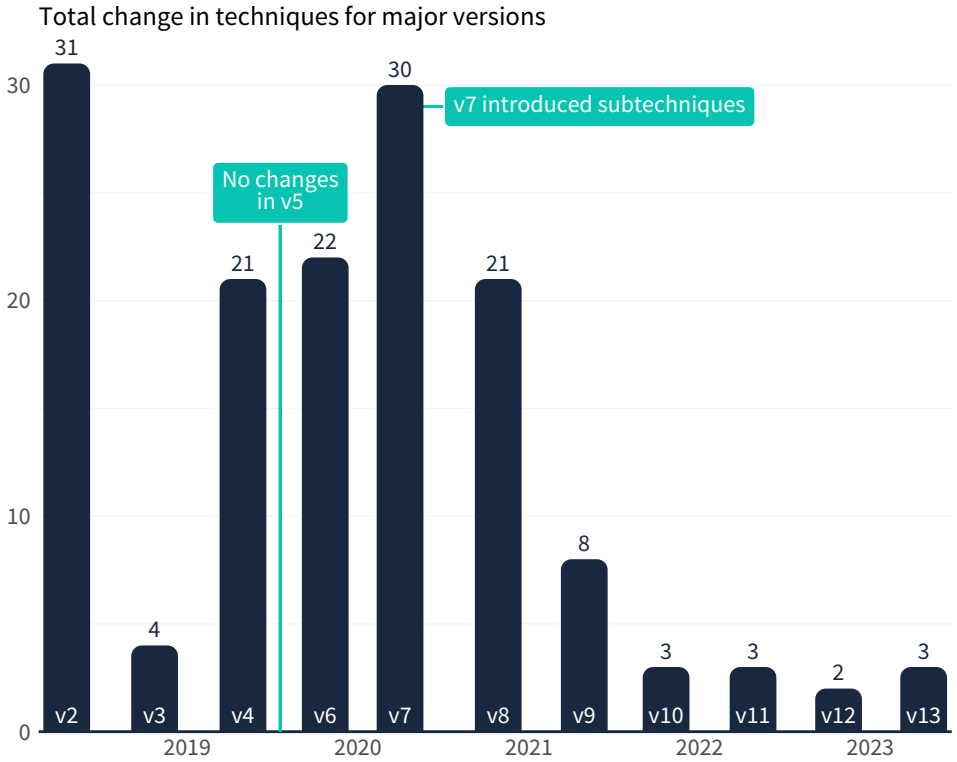
Such a view can help defenders quickly assess defensive gaps as well as identify new controls that have collateral benefits—e.g., the four mitigations that each map to three techniques.

Reporting and Analytical Challenges

As stated in the introduction, our goal in conducting this study was to pull together a consensus view of top ATT&CK techniques across numerous sources to support a more threat-informed defense. We were able to meet that goal but encountered several challenges along the way. We want to share those here in the hope that it will help further improve the quality and utility of reported information as well as guide others engaging in similar analysis.

Pace & Scope of ATT&CK Updates

The ATT&CK matrix is not a static construct. Each year brings a couple of major versions, and some of those involve a substantial number of changes. The figure below shows the typical version upgrade in 2019-2020 changed about 10% of the techniques on average, while that's down to ~1% for 2021 and 2022. We see this as an indication that ATT&CK has progressed from the rapid development phase to a steadier state—which is good for reporting and analysis.



A few years ago, harmonizing reported ATT&CK TTPs across different sources was a bigger issue due to the substantial changes from version to version. If you relied heavily on annual threat reports for TTP prioritization, there was a good chance any given source would be several versions behind by the time it was published.

It's better now, but we still encountered versioning challenges during this study. That's partly because sources don't typically distinguish which version of ATT&CK they're using, and error messages served as our impetus to manually translate to v12.1. As long as those checks are in place, this is a minor inconvenience. But do take the time to ensure the techniques and sub-techniques you leverage from public reports are still valid and update accordingly so those discrepancies aren't propagated forward.

Tactic-Technique Ambiguity

Many encountering ATT&CK for the first time assume all techniques fall under just one tactic. But closer inspection brings an understandable yet frustrating realization—it's not a 1:1 relationship. How common is that across the enterprise ATT&CK matrix? Of the 193 techniques in ATT&CK v12.1, 25 appear in more than one tactic (13%)[4]. So, not extreme—but enough to cause some analytical challenges that can be tricky to navigate.

If sources collect and report tactic-technique pairings, this wouldn't be much of a problem. But they rarely do. As best we can tell, most sources tally observations at the individual technique level. We base this on the fact that we routinely observed the same value recorded for the same technique under multiple tactics. In the case of Valid Accounts, which falls under four tactics, this potentially results in quadruple counting if you're not careful. And unfortunately, there's usually no way to know what proportion of those observations relate to Initial Access, Persistence, Privilege Escalation, and Defense Evasion.

Aside from getting the numbers right for ranking relevant techniques, perhaps the bigger issue at stake here is the prioritization of mitigating controls. The things we could do to counter stolen credentials as an intrusion vector are not the same things we'd need to consider if that technique is being used for lateral movement. We thus recommend that reporting organizations endeavor to make these tactic-technique associations clear to aid defenders in interpreting and applying this valuable information.

4 *One technique falls under four tactics, four under three tactics, and 20 under two tactics.*

The Dearth of Reporting by Segment

We undertook this study hoping to compare top ATT&CK TTPs among different firmographic, geographic, and technographic segments. Alas, it was not to be. But we do want to call this out as an opportunity for reporting sources to make the information more relevant to the community.

Here's a rundown of where things stand now:

- **Zero** sources reported techniques used against **mobile devices.**
- **Zero** sources compared techniques based on **organization size.**
- **One** source compared techniques among specific **global regions.**
- **One** source reported techniques used in **ICS environments.**
- **Two** sources reported techniques by **industry.**

The story was similar for threat actors and types. Three sources reported techniques specific to ransomware, but no other major categories of threats received individualized treatment. Two sources shared top techniques observed for particular threat groups.

It's not really a segment, but we'll go ahead and mention another area we'd like to see reported. All sources in our study reported frequency-based statistics. Not a single one (that we found) reported techniques by share of financial losses, system downtime, compromised data records, etc. That kind of information—in combination with the most frequently observed TTPs—would go a long way toward supporting cyber risk assessments and decisions.

Reflections from Tidal Cyber: Empowering Threat-Informed Defense

The MITRE ATT&CK® knowledge base has had a significant impact on cybersecurity, which only increases every year with additional adoption. Tidal estimates that the proportion of public threat reports that map to ATT&CK has grown six-fold over the past four years, creating a growing body of metrics to enable the insights produced in this study.

Protecting an enterprise from cyber threats can be a daunting task. It's easy for your security team to fall into an endless cycle of figuring out which among the myriad well-known and newly reported threats are relevant, without any clarity on whether you're already defended or if you need to take action. Fortunately, this report has given you a key jumpstart to understanding the most relevant techniques. This can offer a foundation as you implement a more tailored threat profile.

TIDAL'S ENTERPRISE EDITION helps you get started, offering several ways to immediately operationalize the insights developed in this study:

- Tidal maintains and continually refines default priority weightings for each of the 600+ Tactics, Techniques, & Sub-Techniques in the ATT&CK knowledge base. We have taken the output of this report and correlated it against other key inputs to give teams out-of-the-box technique priority weightings.
- Tidal regularly adds threat content extensions to the ATT&CK knowledge base, which derive from the range of source types covered in this report, including reports from incident response and managed service firms, telemetry providers, and OSINT research, adding depth of technique visibility. Tidal metadata enrichment enables sector-specific threat profiling and technique analysis.
- The Tidal platform allows users to add their own knowledge base extensions based on internal telemetry or CTI or commercial threat intelligence that the team leverages, enabling further technique visibility & source diversity.
- Tidal helps you operationalize threat-informed defense for your organization by making it easy to identify the threats that are most likely to target your organization or specific business units, track your defensive coverage with your existing security stack, and take advantage of opportunities to strengthen and streamline your defenses by filling gaps or removing redundancies.

Appendix A: Methods & Sources

We began by identifying industry reports published in 2022 or early 2023 that include statistics on ATT&CK techniques. Our focus is on the relative frequency of techniques, so we removed sources that did not report actual observations or sightings[5]. This resulted in 22 reports for inclusion in this study. We reviewed the methodology of each source and categorized them into four main categories: telemetry, incident response (IR), managed services, and open-source intelligence (OSINT).

Next, we harvested relevant ATT&CK statistics reported by each source. Where possible, we captured the data exactly as reported. Some sources required inference or intermediate processing to convert the reported information to a count, percentage, ranking, etc., that could be compared to other sources[6]. This produced the core dataset analyzed in the following sections.

It's also worth noting that we standardized on ATT&CK v12.1. Any sources reporting techniques from an earlier version were converted to 12.1 based on MITRE's log of updates to ATT&CK. Given the timeframe, none of our sources used the latest version (v13).

We will likely produce an updated version of this study in the future. If you'd like your organization's report included as a source or have recommendations on other public data sources to include, please contact us at info@cyentia.com.

SOURCE	ID	TITLE	SOURCE TYPE	NOTES
Arete	IR-1	*Arete Reining in Ransomware*	Incident Response	Percent of ransomware cases in which TTPs were observed.
BlackBerry	TE-1	*Global Threat Intelligence Report*	Telemetry	An unordered list of TTPs observed.
Connectwise	MS-1	*2023 MSP Threat Report*	Managed Services	Unlabeled pie charts converted to rankings.
Crowdstrike	MS-2	*2022 Falcon OverWatch Threat Hunting Report*	Managed Services	Color-shaded list of TTPs we converted to rankings.
Cyentia	OS-1	*Information Risk Insights Study 2022*	OSINT	Ranking of initial access techniques by sector.
Cymulate	AS-1	*2022 State of Cybersecurity Effectiveness*	Attack Simulation	Borderline for inclusion because observations are drawn from attack simulations rather than true attacks.
Deepwatch	MS-3	*Annual Threat Intel Report 2022*	Managed Services	Percent of alerts tied to each tactic (no techniques).

5 For example, a couple of sources listed "top" ATT&CK based on mappings to detection rules but did not report how often those rules (or mapped techniques) were triggered by malicious activity. We also removed reports that based "top" techniques on their association with threat groups as mapped by MITRE.

6 For example, we converted color scales corresponding to frequency to a relative ranking of techniques.

SOURCE	ID	TITLE	SOURCE TYPE	NOTES
DFIR Report	IR-2	*The 2022 Year in Review*	Incident Response	Percent of techniques observed for each tactic across ~14 cases.
Elastic	TE-2	*2022 Global Threat Report*	Telemetry	Percent of tactics/techniques across major cloud platforms.
ENISA	OS-2	*Threat Landscape Report for Ransomware Attacks*	OSINT	Count of Initial Access techniques observed in ransomware incidents.
F5 Labs	OS-3	*2022 Application Protection Report*	OSINT	Percent of tactics & techniques used in public data breaches.
Fortinet	TE-3	*Global Threat Landscape Report 2H-2022*	Telemetry	Percent of attacks relative to tactics overall and by region.
IBM X-Force	MS-4	*Threat Intelligence Index 2023*	Managed Services	Initial access techniques as a percentage of cases remediated. Gives region & sector stats.
Logpoint	MS-5	*Logpoint's Top Ten MITRE ATT&CK Techniques*	Managed Services	Percent of ransomware incidents triggered by each technique.
Mandiant	IR-3	*M-Trends 2022*	Incident Response	Percent of incident investigations in which techniques were observed.
MITRE	OS-4	*A Data-driven Analysis of ATT&CK in the Wild*	OSINT	Top 15 techniques based on observations from 2019 to mid-2021. These comprised 90% of sightings.
MITRE	OS-5	*Ransomware Top Ten List*	OSINT	Top 10 ransomware techniques based on this methodology and analysis of 22 threat groups.
NCC Group	IR-4	*Annual Threat Monitor 2022*	Incident Response	Percent of initial access techniques observed in IR cases
PICUS	TE-4	*The Red Report 2023*	Telemetry	Top 10 techniques by percent of detected malware samples.

SOURCE	ID	TITLE	SOURCE TYPE	NOTES
Recorded Future	OS-6	*2022 Annual Report*	OSINT	Top 10 techniques ranked by reference count in Insikt Analyst Notes
Red Canary	MS-6	*2022 Threat Detection Report*	Managed Services	Top 20 techniques based on the percent of affected customers.
SecureWorks	MS-7	*2022 State of the Threat*	Managed Services	Frequency-scaled heatmap of TTPs we converted to rankings.
Trellix	TE-5	*The Threat Report Feb 2023*	Telemetry	Percent of observations related to ransomware detections & nation-state activity.

TIDAL CYBER
THREAT-INFORMED DEFENSE

& 119 Cyentia INSTITUTE

This study was commissioned by Tidal Cyber.

Data collection and analysis for this study was conducted by the Cyentia Institute.

Cyentia is a research and data science firm working to advance cybersecurity knowledge and practice. We pursue that goal by collaborating with security companies and other organizations to publish data-driven reports like this one. Learn more at https://www.cyentia.com

Founded in January 2022 by a team of threat intelligence veterans with experience at MITRE, Department of Homeland Security, and a wide range of innovative security providers, Tidal Cyber enables businesses to implement a threat-informed defense more easily and efficiently. The Tidal Platform helps our customers map the security capabilities of their unique environment against the industry's most complete knowledgebase of adversary tactics and techniques including the MITRE ATT&CK® knowledge base, additional open-source threat intelligence sources, and a Tidal-curated registry of security product capabilities mapped to specific adversary techniques. The result is actionable insight to track and improve their defensive coverage, gaps, and overlaps. For more information, please visit: www.tidalcyber.com.


TIDAL CYBER
THREAT-INFORMED DEFENSE
&
119
Cyentia
INSTITUTE