CIS Center for Internet Security®

CIS Controls

CIS Community Defense Model

Version 2.0

Acknowledgments

The Center for Internet Security® (CIS) would like to thank the many security experts who volunteer their time and talent to support the CIS Controls® and other CIS work, especially the Community Defense Model (CDM). CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

We also acknowledge and greatly appreciate the work of the Verizon Data Breach team, CrowdStrike®, and the many contributors to the MITRE ATT&CK® framework. They are representative of the large community of technical excellence, good will, and open sharing that allows all of us to build greater confidence into the cyber world.

Editor

Valecia Stocchetti, CIS

Contributors

Ginger Anderson, CIS
Jennifer Jarose, CIS
Joshua M. Franklin, CIS
Joshua Palsgraf, CIS/MS-ISAC
Leanna Caton, CIS/MS-ISAC
Michael Woodward, CIS/MS-ISAC
Patrick Araya, CIS
Philippe Langlois, Verizon
Phyllis Lee, CIS
Randy Rose, CIS/MS-ISAC
Richard Nelson, CIS/MS-ISAC
Robin Regnier, CIS
Samuel P. Farnan, CIS/MS-ISAC
Stephen E. Jensen, CIS/MS-ISAC
Thomas Sager, CIS
Tiffany Bergeron, The MITRE Corp.
Tony Sager, CIS

Contents

Executive Summary

This guide is the second edition of the Center for Internet Security® (CIS) Community Defense Model (CDM). The same security experts who help create the CIS Critical Security Controls® (CIS Controls®) work with CIS to apply the CDM to current threat data.

Enterprises that adopt the CIS Controls have repeatedly asked us to identify "What should we do first?" In response, the Controls Community sorted the Safeguards in the CIS Controls into three Implementation Groups (IGs) based on their difficulty and cost to implement.

Implementation Group 1 (IG1), the group that is least costly and difficult to implement, is what we call essential cyber hygiene (formerly basic cyber hygiene) and are the Safeguards we assert that every enterprise should deploy. For enterprises that face more sophisticated attacks or that must protect more critical data or systems, these Safeguards also provide the foundation for the other two Implementation Groups (IG2 and IG3).

Enterprises naturally want to know "How effective are the CIS Controls against the most prevalent types of attacks?" The CDM was created to help answer that and other questions about the value of the Controls based on currently available threat data from industry reports.

Our methodology is straightforward.

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework allows us to express any attack type as a set of attack techniques, which we refer to as *attack patterns*. For each of the five most prevalent attack types, such as ransomware, we collect the corresponding attack patterns through analysis of industry threat data. We then track which Safeguards defend against each of the techniques found in those attack patterns. This methodology allows us to measure which Safeguards are most effective overall for defense across *attack types*.

Our results this year increased our confidence that our conclusions from the first CDM were correct. Based on additional industry threat data sources, the use of the updated version 8 of the CIS Controls and version 8.2 of the MITRE ATT&CK framework, we verified that the CIS Controls are effective at defending against 86% of the ATT&CK (sub-)techniques found in the ATT&CK framework. More importantly, the Controls are highly effective against the top five attack types found in industry threat data. The bottom line is that the CIS Controls, and specifically IG1, are a robust foundation for your cybersecurity program.

Our results also confirm that establishing and maintaining a secure configuration process (CIS Safeguard 4.1) is a linchpin Safeguard for all five attack types, which reinforces the importance of configurations, such as those found in the CIS Benchmarks™.

Results Summary

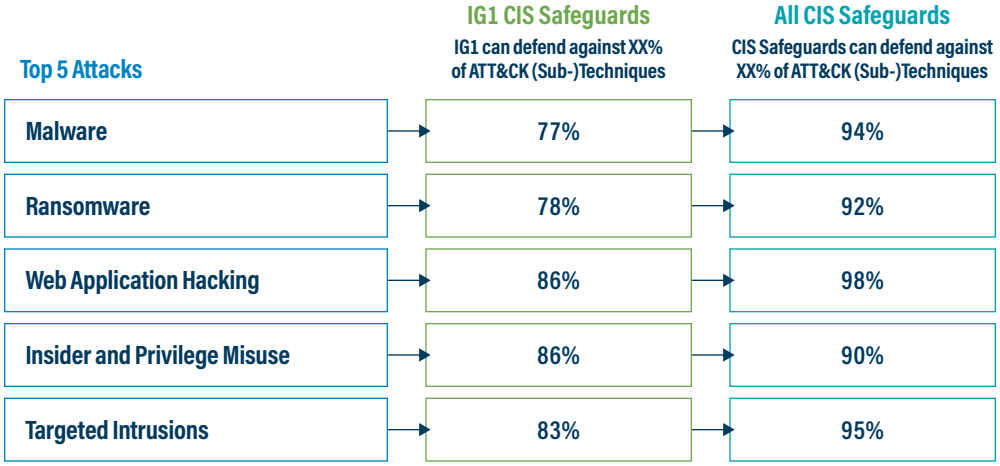
Overall, the findings from this year's CDM both reaffirmed and strengthened, with objective data, what we already thought to be true—IG1 provides a viable defense against the top five attacks.

For CDM v2.0, the top five attack types are: Malware, Ransomware, Web Application Hacking, Insider and Privilege Misuse, and Targeted Intrusions. Our analysis found that, overall, implementing IG1 Safeguards defends against 77% of ATT&CK (sub-)techniques used across the top five attack types. That percentage goes up to 91% if all CIS Safeguards are implemented. These results strongly reinforce the value of a relatively small number of well-chosen and basic defensive steps (IG1) and also support IG1 as the preferred on-ramp to implementing the CIS Controls. We also found that CIS Safeguard 4.1 "Establish and Maintain a Secure Configuration Process" is most effective in defending against the top five attacks, reinforcing the importance of secure configurations, such as those contained within the CIS Benchmarks.

Additionally, independent of any specific attack type, implementing IG1 Safeguards defends against 74%[1] of ATT&CK (sub-)techniques in the MITRE ATT&CK framework, and implementation of all CIS Safeguards defends against 86% of ATT&CK (sub-)techniques in the framework. Since many ATT&CK (sub-)techniques are used across multiple attack types, we can extrapolate that the CIS Controls defend against more than the top five attacks mentioned in this guide.

We also analyzed each attack type individually. As an example, our analysis determined that implementing IG1 Safeguards defends against 78% of Ransomware ATT&CK (sub-) techniques, and implementing all CIS Safeguards defends against 92% of those techniques. This, and other attack pattern findings, can be seen in Figure 1 below. It is worth noting that 100% coverage of all attacker techniques for any attack type is difficult, as some techniques are not able to be defended against. Additionally, some IG1 Safeguards are foundational and process-oriented, such as enterprise and software asset management. While these foundational Safeguards may not be included in the ATT&CK model as defensive measures, they are necessary in order to successfully implement other Safeguards that map to ATT&CK.

Figure 1. CDM v2.0 attack pattern analysis



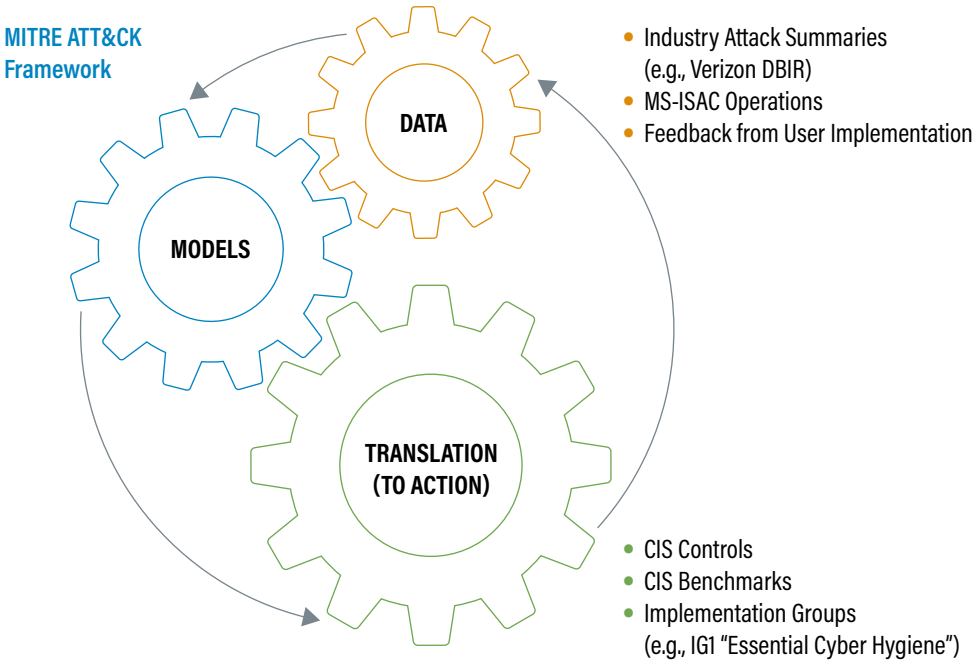
All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

1 All percentages based on ATT&CK (sub-)techniques that are assigned to an ATT&CK mitigation, and can therefore be defended.

Overview

In this guide, we present the CDM v2.0. Our goal is to bring another level of rigor and detail to support the development and prioritization of the CIS Controls. The CDM process takes data sources (such as the Verizon Data Breach Investigations Report (DBIR)), drives them into models (such as the MITRE ATT&CK framework), and then translates them into action—creating our best practices (e.g., CIS Controls and CIS Benchmarks). The CDM is continuous, with each cycle starting the process again.

Figure 2. CDM Process



As a part of the CDM process, we use the MITRE Enterprise ATT&CK framework v8.2, the industry-accepted way to describe the individual technical details of a cyber-attack, which provides answers to questions, such as: "Which ATT&CK tactics (the objectives of an attacker) does an attacker use?"; "What are the ATT&CK (sub-)techniques (specific technical actions) used within those tactics?"; and "What are the general ATT&CK mitigations that could help defend against them?" Equally important in the CDM process is using industry threat data (i.e., data sources) of the most prevalent and relevant attacks plaguing enterprises. As part of the CDM process, we research authoritative, industry-recognized data sources, both national and international, which allow us to determine the top five attack types and create comprehensive attack patterns. Our work with the CIS Controls and ATT&CK framework, combined with using authoritative data sources to back our analysis, is the backbone of the CDM.

The CDM was constructed using the following process:

- We mapped CIS Safeguards to the ATT&CK framework.
- We identified the *security function*—independent of any specific attack, the ability of a CIS Safeguard to defend against one or more attacker techniques (e.g., ATT&CK (sub-) techniques).
- Using authoritative data sources, we identified the top five *attack types* that enterprises should defend against. For CDM v2.0, the top five attack types are: *Malware*, *Ransomware*, *Web Application Hacking*, *Insider and Privilege Misuse*, and *Targeted Intrusions*.

- For each attack type, we used authoritative data sources to determine the *attack pattern*—the set of attacker techniques (e.g., ATT&CK (sub-)techniques) used in each attack type.
- We then identified the *security value*—the benefit of implementing a CIS Safeguard to defend against an individual attack or a group of attacks.

There are several ways that CDM analysis can be used to design, prioritize, implement, and improve an enterprise's security program. Our analysis affirms that enterprises should begin with implementing IG1 first (followed by IG2 and IG3, as appropriate) in order to, at a minimum, defend against the top five attacks. Our CDM v2.0 mappings also provide enterprises with more granularity, if needed. For example, if an enterprise implements CIS Safeguard "4.1–Establish and Maintain a Secure Configuration Process," our mappings can provide a list of ATT&CK (sub-)techniques that the Safeguard defends against. Attack Cards for each individual attack type, and all attack types combined, are also available on CIS WorkBench, to provide a listing of Safeguards that are the most effective in defending against specific ATT&CK (sub-)techniques.

CIS is dedicated to taking a "community-first" approach. Please join our CDM Community on CIS WorkBench to take advantage of these and other great resources, as well as to participate in next year's CDM (v3.0).

What's New in CDM v2.0

First, let's recap what we did in v1.0. Released in 2020, v1.0 made use of two publicly-available, authoritative industry resources: the MITRE ATT&CK framework and the Verizon DBIR. To establish the baseline model, a master mapping was created, starting with the 171 CIS Safeguards in CIS Controls v7.1. Following this, CIS Safeguards were mapped to the 41 ATT&CK mitigations in Enterprise ATT&CK v6.3, which MITRE already had mapped to the 266 ATT&CK techniques. This gave us the security function relationship between CIS Safeguards and ATT&CK techniques, identifying the ATT&CK techniques that could be defended against by implementing the CIS Safeguards.

We then selected the five most prevalent attack types (Malware, Ransomware, etc.) from the Verizon DBIR, and the ATT&CK techniques used within those attack types, forming what we call an attack pattern. Using the master mapping of the CIS Safeguards to ATT&CK, we then mapped each ATT&CK technique in the attack pattern back to the relevant CIS Safeguards. This allowed us to analyze the security value of the CIS Safeguards against these five attack types.

To build off of the foundational principles in v1.0, we made a few updates to v2.0, including the following:

- **Updated Version of the CIS Controls.** We used CIS Controls v8 as the basis for our mappings and analysis.
- **Updated Version of the ATT&CK Framework.** We used Enterprise ATT&CK v8.2, which is made up of 178 ATT&CK techniques, 352 ATT&CK sub-techniques (530 combined "ATT&CK (sub-)techniques"), and 42 ATT&CK mitigations. Note that the term "ATT&CK (sub-)techniques" is used throughout this guide to refer to ATT&CK techniques and ATT&CK sub-techniques as a whole, unless otherwise indicated.
- **Additional Data Sources Added.** We used several additional national and international data sources, such as the *2020 Verizon DBIR, ENISA Threat Landscape–The Year in Review,* and more, to determine the top five attacks. Additional data sources were used in CDM v2.0 to create more comprehensive attack patterns. A full listing of data sources used to identify attack types and create attack patterns can be found here.[2]
- **Updated Master Mapping.** We mapped at the ATT&CK (sub-)technique level, in order to provide more granularity and clarity for our analysis. ATT&CK mitigations were used as a guide to map to the ATT&CK (sub-)techniques, which allowed us to select the specific ATT&CK (sub-)techniques that can be defended against through the implementation of one or more CIS Safeguards.

2 Attack Types and Attack Patterns Attack Types and Attack Patterns

Glossary

The following are terms used throughout this guide and their specific meanings:

ATT&CK (sub-)technique	The combination of ATT&CK techniques and ATT&CK sub-techniques. Collectively referred to as ATT&CK (sub-) techniques, there are 530 in total for Enterprise ATT&CK v8.2.
ATT&CK mitigation	A list of defensive actions that can be taken to defend against an ATT&CK (sub-)technique.
ATT&CK sub-technique	The specific actions that an attacker takes to achieve an ATT&CK tactic, nested within ATT&CK techniques.
ATT&CK tactic	The objectives of an attacker such as reconnaissance, credential access, and exfiltration. A specific set of ATT&CK (sub-) techniques can be found within any given ATT&CK tactic.
ATT&CK technique	The specific actions that an attacker takes to achieve an ATT&CK tactic, listed under each ATT&CK tactic.
Attack pattern	The set of attacker techniques (e.g., ATT&CK (sub-)techniques) required to execute an attack. Attack patterns can change from year to year.
Attack type	The high-level grouping of attacks. For CDM v2.0, they are: Malware, Ransomware, Web Application Hacking, Insider and Privilege Misuse, and Targeted Intrusions.
Attacker techniques	A general term referring to actions that an attacker takes to compromise a system or network that's not assigned to a specific security framework.
CIS Critical Security Controls (CIS Controls)	A set of 18 best practice recommendations that help enterprises focus their resources on the most critical actions to defend against the most prevalent real-life attacks. Each CIS Control consists of a subset of Safeguards.
CIS Safeguards	A set of 153 specific recommendations that make up the CIS Controls. Organized into Implementation Groups, grouped as IG1, IG2, and IG3 Safeguards.
Data source	A threat report, or other dataset, that provides an analysis of attacks, attacker tactics, techniques, and procedures (TTPs), or other specific information related to cybersecurity. Also referred to as industry threat data sources. Used to determine attack types and attack patterns.
Data type	Can be one of multiple categorizations of data that are incorporated into a data source (e.g., self-reported data, sensor data, incident response data, product usage data, and open-source intelligence).
Implementation Group 1 (IG1)	Implementation Group 1, also known as essential cyber hygiene (formerly basic cyber hygiene). IG1 includes defensive actions that are applicable to even the smallest and least-funded enterprises.
Implementation Groups	A simple and accessible way to help enterprises prioritize the implementation of the CIS Controls.
Security function	Independent of a specific attack type, the ability of a CIS Safeguard to defend against one or more attacker techniques (e.g., ATT&CK (sub-)techniques).
Security value	The benefit a CIS Safeguard provides in defending against an individual attack type or a group of attack types.

Methodology

Implementation Groups and the CDM

In CIS Controls v7.1, we introduced a new prioritization scheme referred to as Implementation Groups (IGs). There are three IGs: IG1, IG2, and IG3. To develop the IGs, CIS identified a core set of CIS Safeguards that enterprises with limited resources, expertise, and risk exposure should focus on. This is IG1, or essential cyber hygiene. IG1 includes defensive actions that are applicable to even the smallest and least-funded enterprises. Each IG builds upon the previous one. IG2 identifies additional CIS Safeguards for enterprises with more resources and expertise than those in IG1, and also greater risk exposure. IG3, for enterprises that have the highest level of risk exposure, includes all 153 CIS Safeguards.

The CDM tells us that IG1 defends against the top five attacks. Specifically, the CDM can also help an enterprise focus on which technical IG1 Safeguards are most effective in defending against specific attacks. We at CIS feel that this is a powerful approach to an enterprise's risk management strategy. Additionally, some IG1 Safeguards are foundational and process-oriented, such as enterprise and software asset management. These foundational Safeguards may not be included in the ATT&CK model as defensive measures; however, they must be implemented before the more technical Safeguards that do map to ATT&CK can be properly implemented.

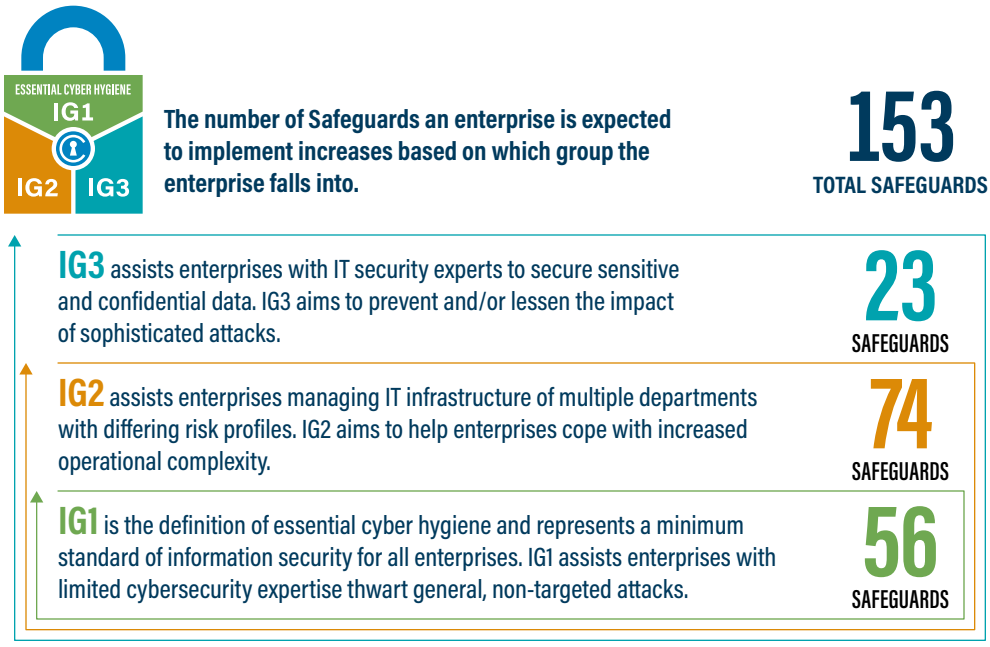


Figure 3. CIS Controls Implementation Group overview

Security Function vs. Security Value

Throughout the CDM v2.0, we focus on two main concepts: the *security function* and the *security value* of the CIS Safeguards. The security function can best be defined as the ability of a CIS Safeguard to defend against one or more ATT&CK (sub-)techniques, independent of any specific attack type. The security function does not necessarily answer the question of why we should implement a particular CIS Safeguard, or the benefit in doing so. Rather, the security function provides the foundation that allows us to analyze the security value, defined as the benefit a CIS Safeguard provides in defending against one or more attack types.

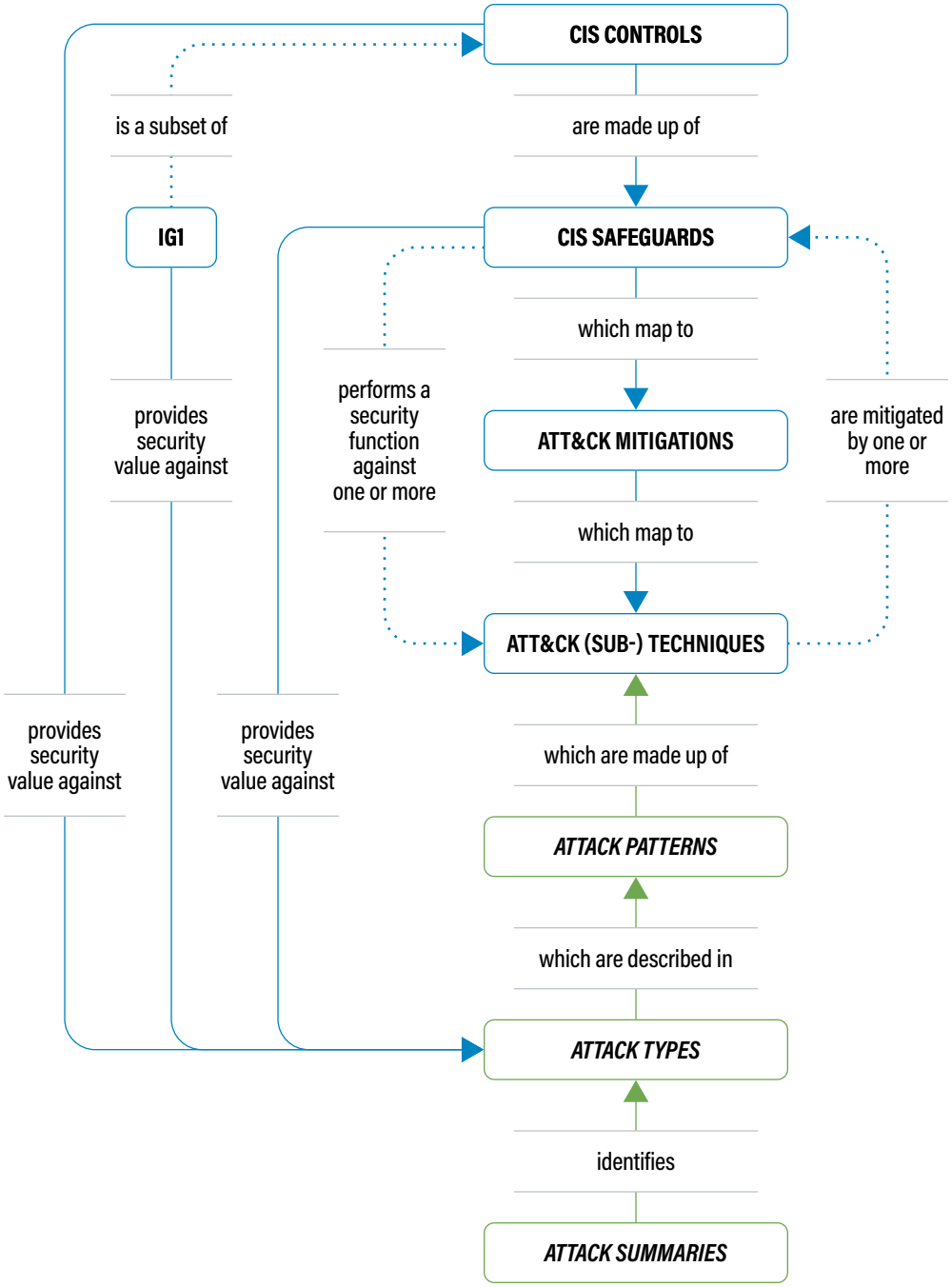
Overall Process

The CDM is comprised of a series of seven steps to get us to the end result. They are:

1. **Create master mapping.** We created a master mapping from CIS Controls v8 to Enterprise ATT&CK v8.2, mapping the CIS Safeguards to the ATT&CK (sub-)techniques. ATT&CK mitigations were used as a guide to map at the ATT&CK (sub-)technique level.
2. **Analyze security function.** We analyzed the security function of the CIS Safeguards against ATT&CK (sub-)techniques using the master mapping in Step 1.
3. **Identify top five attack types.** Using multiple data sources, we identified the five most prevalent attack types experienced by enterprises in 2020-2021: Malware, Ransomware, Web Application Hacking, Insider and Privilege Misuse, and Targeted Intrusions.
4. **Construct attack patterns.** For each attack type, we used multiple data sources to create comprehensive attack patterns—the set of attacker techniques (e.g., ATT&CK (sub-) techniques) used in an attack type.
5. **Perform reverse mapping.** We used the master mapping of the CIS Controls to ATT&CK (in Step 1) to map each ATT&CK (sub-)technique associated with an attack type back to the CIS Safeguards.
6. **Analyze security value.** The reverse mapping allowed us to analyze the security value of implementing the CIS Safeguards against one or more attack types, meaning, how well do the CIS Controls defend against the top five attacks.
7. **Create visualizations.** The MITRE ATT&CK Navigator allows users to create interactive "layers" of ATT&CK. This tooling allowed us to visualize each attack pattern individually and combined across all attack types. These layers can be found on CIS WorkBench here.

The detailed CDM process can be seen in Figure 4.

Figure 4. Detailed CDM Process



ATT&CK Structure

In order to fully understand the CDM methodology, it is fundamental to understand how the ATT&CK framework is organized and interconnects. The highest level within ATT&CK is called a tactic. These are, as previously mentioned, the objectives of an attacker, such as reconnaissance, credential access, and exfiltration. There are 14 tactics in ATT&CK v8.2, represented with a "TA" before their unique identifier. Each ATT&CK tactic contains multiple ATT&CK *techniques*, which contain ATT&CK *sub-techniques*, where applicable. ATT&CK (sub-)techniques are the specific actions that an attacker takes to achieve an ATT&CK tactic. They are represented with a "T" before their unique identifier, with ATT&CK sub-techniques having ".0XX" after the main unique identifier. There are 530 ATT&CK (sub-)techniques in total for v8.2.

ATT&CK also has *mitigations*, each including several ATT&CK (sub-)techniques. ATT&CK mitigations provide a list of actions that can be taken to defend against a specific ATT&CK (sub-)technique. The ATT&CK mitigations begin with the letter "M" followed by a unique identifier (e.g., M1047). There are 42 ATT&CK mitigations in v8.2. It is worth noting that ATT&CK techniques and their child sub-technique(s) do not always map back to the same ATT&CK mitigation. For example, "M1036–Account Use Policies" mitigates against "T1110–Brute Force," which has four ATT&CK sub-techniques. However, the mitigation M1036 is effective against only three of the four (sub-)techniques (T1110.001, T1110.003, and T1110.004), as indicated on the ATT&CK website. This warranted us to map at the ATT&CK (sub-) technique level for the CDM master mapping for accuracy.

It is important to note that out of the 530 ATT&CK (sub-)techniques in v8.2, 84 have no assignment to an ATT&CK mitigation, meaning that no matter what security framework is being implemented, these 84 ATT&CK (sub-)techniques cannot be easily mitigated, based on information provided on the ATT&CK website. An example of one of these ATT&CK (sub-)techniques is "T1546–Event Triggered Execution," which "cannot be easily mitigated with preventive controls since it is based on the abuse of system features," according to the ATT&CK website. Our assessment of these ATT&CK (sub-)techniques found that the majority are used in what is often referred to as "Living off the Land (LotL)" attacks, where attackers use existing tools and tactics on the targeted system or network to carry out an attack, rather than exploit a specific system or control weakness; these attacks are therefore difficult to defend against. Unless otherwise noted, all calculations in this guide do not take into account these ATT&CK (sub-)techniques. Additional information on ATT&CK v8.2 can be found on the ATT&CK website.

Mapping Relationships

As part of Step 1 of the CDM process, the CIS Safeguards are mapped to ATT&CK mitigations and then to ATT&CK (sub-)techniques. Ultimately, this high-level mapping (from CIS Safeguards to ATT&CK mitigations) serves as the guide for connecting CIS Safeguards to ATT&CK (sub-)techniques, and therefore it is worthwhile to analyze both: how well the CIS Safeguards map to ATT&CK mitigations and then to ATT&CK (sub-)techniques. The CIS Safeguard mapping to ATT&CK is available separately from this guide on CIS WorkBench and via the CIS website. Figure 5 below demonstrates the mapping relationship. It should be noted that the mapping creates a many-to-many relationship between CIS Safeguards and ATT&CK (sub-)techniques, meaning that implementing a single CIS Safeguard defends against multiple ATT&CK (sub-)techniques, and a single ATT&CK (sub-)technique can be defended through implementation of one or more CIS Safeguards.

It is worth noting that the ATT&CK mitigations represent defensive cybersecurity actions at a different level of abstraction than the CIS Safeguards. The CIS Safeguards cover a larger number of defensive cybersecurity concepts than the ATT&CK mitigations. This difference in granularity is perhaps best demonstrated through the number of defensive actions within each collection: CIS Controls v8 contains 153 CIS Safeguards, whereas ATT&CK v8.2 contains 42 ATT&CK mitigations.

How to Use This Document

For those looking to understand more about the CDM process, this guide is a perfect start to give readers:

- An overview of how the CDM works
- An explanation for why the CDM is helpful to build an enterprise's cybersecurity program
- A high-level overview of results from this year's CDM
- An in-depth analysis of ATT&CK (sub-)techniques that can be defended against through implementation of the CIS Safeguards, overall and for each attack type
- Additional links and resources

For those who wish to dive deeper into the CDM, we also provide the following:

- **CDM Master Mapping:** A Microsoft® Excel® spreadsheet containing[3]:
  - CIS Controls v8 to ATT&CK mapping: High-Level (to ATT&CK mitigations)
  - CIS Controls v8 to ATT&CK mapping: Low-Level (to ATT&CK (sub-)techniques)
- **ATT&CK Visualizations:** JavaScript Object Notation (JSON) files for each attack type, as well as one for all attack types combined[4]
  - A guide on how to visualize these JSON files
- **CDM Attack Cards:** IG1 Safeguards to implement for each attack type and all attack types combined (in terms of effectiveness)[5]
- **CDM Reverse Mapping:** A reverse mapping that provides which ATT&CK (sub-)techniques can be defended by implementing one or more CIS Safeguards, as well as which attack type(s) they defend against[6].

Please join our CDM Community on CIS WorkBench to take advantage of these and other great resources.

3 Found here: Note that a CIS WorkBench account is needed to obtain these files (free). Microsoft® Excel® workbooks are in database-friendly formats.

4 Found here: Note that a CIS WorkBench account is needed to obtain these files (free). JSON files can be imported into MITRE's ATT&CK Navigator tool here

5 Found here: Note that a CIS WorkBench account is needed to obtain this file (free).

6 Found here: Note that a CIS WorkBench account is needed to obtain this file (free).

Security Function Analysis

ATT&CK Mitigations

The first step in determining the security function of the CIS Safeguards is to map the CIS Safeguards to the ATT&CK mitigations. Note that a single Safeguard can map to multiple ATT&CK mitigations and vice versa.

All CIS Safeguards

Overall, the CIS Safeguards mapped to 93% of ATT&CK mitigations, or 39 out of 42. Table 1 below shows the top 10 ATT&CK mitigations that mapped to CIS Safeguards. For example, "M1047–Audit" is mapped to 23 CIS Safeguards, indicating that those 23 Safeguards perform some form of auditing activity, and therefore have the ability to defend against one or more ATT&CK (sub-)techniques that are contained within the Audit mitigation. Analysis found that "M1047–Audit" ranked #1 again this year with the most mappings, emphasizing the importance of implementing best practices, such as secure configurations (e.g., CIS Benchmarks), and auditing those configurations.

Table 1. Number of CIS Safeguards mapped to the top 10 ATT&CK mitigations

RANK	ATT&CK MITIGATION ID	ATT&CK MITIGATION NAME	NUMBER OF ATT&CK MITIGATIONS MAPPED TO CIS SAFEGUARDS
1	M1047	Audit	23
2	M1051	Update Software	19
3	M1016	Vulnerability Scanning	17
4	M1018	User Account Management	16
5	M1026	Privileged Account Management	15
6	M1042	Disable or Remove Feature or Program	14
7	M1029	Remote Data Storage	14
8	M1035	Limit Access to Resource Over Network	13
9	M1037	Filter Network Traffic	12
10	M1030	Network Segmentation	10

IG1 CIS Safeguards

In analyzing IG1 Safeguards, it was found that they mapped to 83% of ATT&CK mitigations. Additionally, eight of the ATT&CK mitigations shown in Table 1 above remained in the top 10 for IG1. However, others, such as "M1053–Data Backup," M1017–User Training," and "M1022–Restrict File and Directory Permissions," moved up in rank (since IG1 only focuses on a subset of the CIS Safeguards), as shown below in Table 2.

Table 2. Number of IG1 CIS Safeguards mapped to the top 10 ATT&CK mitigations

RANK	ATT&CK MITIGATION ID	ATT&CK MITIGATION NAME	NUMBER OF ATT&CK MITIGATIONS MAPPED TO CIS SAFEGUARDS
1	M1047	Audit	12
2	M1018	User Account Management	11
3	M1029	Remote Data Storage	9
4	M1026	Privileged Account Management	9
5	M1017	User Training	6
6	M1051	Update Software	6
7	M1035	Limit Access to Resource Over Network	6
8	M1030	Network Segmentation	5
9	M1022	Restrict File and Directory Permissions	5
10	M1053	Data Backup	4

Unmapped

Although the majority of ATT&CK mitigations had at least one mapping to a CIS Safeguard, a few mitigations were left unmapped, as shown below in Table 3. For v2.0, we are excited to include an ATT&CK mitigation that was not mapped in v1.0, "M1040–Behavior Prevention on Endpoint." Prior to CIS Controls v8, Safeguards relating to Endpoint Detection and Response (EDR) had not been included. However, we recognized the importance of including Safeguards surrounding EDR in an effort to keep up with the ever-changing threat landscape.

With the addition of CIS Safeguards such as, "13.2–Deploy a Host-Based Intrusion Detection Solution" and "13.7–Deploy a Host-Based Intrusion Prevention Solution," we were able to successfully map to the ATT&CK mitigation, "M1040–Behavior Prevention on Endpoint." We also recognized the addition of an ATT&CK mitigation that was not on this list in v1.0, "M1020–SSL/TLS Inspection." This was due to the retirement of CIS Safeguard (v7.1) 12.10, "Decrypt Network Traffic at Proxy" in v8 of the CIS Controls. While important, we felt that decryption of network traffic may not be appropriate, feasible, or attainable for some enterprises. Additionally, in some cases, privacy requirements/regulations may contradict or interfere with guidance to decrypt all network traffic.

Table 3. ATT&CK mitigations with no mapping to CIS Safeguards

ATT&CK MITIGATION ID	ATT&CK MITIGATION NAME	ATT&CK MITIGATION DESCRIPTION
M1019	Threat Intelligence Program	A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.
M1020	SSL/TLS Inspection	Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity.
M1055	Do Not Mitigate	This category is to associate techniques that mitigation might increase risk of compromise and therefore mitigation is not recommended.

ATT&CK (Sub-)Techniques

All CIS Safeguards

In addition to analyzing at the ATT&CK mitigation level, we also analyzed the mappings at an ATT&CK (sub-)technique level, providing us with a more granular and clarified dataset for analysis. Shown below in Table 4 is a listing of ATT&CK (sub-)techniques that had the highest number of CIS Safeguard mappings. At first glance, it may appear that in order to defend against a specific ATT&CK (sub-)technique, it would require the implementation of a significant number of CIS Safeguards. However, this is not the case. Since multiple CIS Safeguards can defend against the same ATT&CK (sub-)technique, this provides enterprises with multiple options to select the Safeguards that are most appropriate to implement for their environment. Multiple Safeguards mapping to an ATT&CK (sub-)technique also helps to illustrate defense-in-depth.

"T1021.001–Remote Desktop Protocol (RDP)" had the highest number of CIS Safeguards mapped to it, emphasizing the potential that the CIS Safeguards can provide in protecting RDP. Get the CIS RDP guide here.

Overall, out of 446 ATT&CK (sub-)techniques assigned to an ATT&CK mitigation, 383, or 86%, can be defended against through implementation of all CIS Safeguards. Additional analysis found that almost half of the ATT&CK (sub-)techniques, shown in Table 4 below, related to the exploitation of an external application, protocol, etc., emphasizing the importance of securing externally-facing systems. It also is worth noting that ATT&CK sub-technique "T1021.001–Remote Desktop Protocol (RDP)" had the highest number of CIS Safeguards mapped to it, demonstrating the potential that the CIS Safeguards can provide in protecting RDP. Recently, CIS released a guide about RDP, a protocol attackers often exploit, and which direct mitigations can be implemented to defend against an RDP-based attack.

Table 4. ATT&CK (sub-)techniques that had the highest number of CIS Safeguard mappings

RANK	ATT&CK (SUB-) TECHNIQUE ID	ATT&CK (SUB-)TECHNIQUE NAME	NUMBER OF CIS SAFEGUARDS MAPPED TO AN ATT&CK (SUB-)TECHNIQUE
1	T1021.001	Remote Desktop Protocol	42
2	T1563.002	RDP Hijacking	41
3	T1552	Unsecured Credentials	39
4	T1072	Software Deployment Tools	38
5	T1210	Exploitation of Remote Services	35
6	T1190	Exploit Public-Facing Application	33
7	T1059	Command and Scripting Interpreter	30
8	T1557	Man-in-the-Middle	29
9	T1530	Data from Cloud Storage Object	28
10	T1574	Hijack Execution Flow	27
11	T1003	OS Credential Dumping	25
12	T1133	External Remote Services	24
13	T1543.002	Systemd Service	24
14	T1563	Remote Service Session Hijacking	24
15	T1059.001	PowerShell	24
16	T1021.005	VNC	23
17	T1542.005	TFTP Boot	23
18	T1548	Abuse Elevation Control Mechanism	22
19	T1602.001	SNMP (MIB Dump)	22
20	T1543	Create or Modify System Process	22

IG1 CIS Safeguards

Overall, out of the ATT&CK (sub-)techniques assigned to an ATT&CK mitigation (446), IG1 Safeguards defend against 74% (332). This shows that by implementing IG1 alone, enterprises can defend against the majority of ATT&CK (sub-)techniques. Additionally, it is worth noting that some IG1 Safeguards are foundational and process-oriented, such as enterprise and software asset management. These foundational Safeguards may not be included in the

ATT&CK model as defensive measures, due to the technical nature of the ATT&CK framework; however, many are pre-requisites to successfully implement the more technical Safeguards that do map to ATT&CK.

Table 5. ATT&CK (sub-)techniques that had the highest number of IG1 Safeguard mappings

RANK	ATT&CK (SUB-) TECHNIQUE ID	ATT&CK (SUB-)TECHNIQUE NAME	NUMBER OF CIS SAFEGUARDS MAPPED TO AN ATT&CK (SUB-)TECHNIQUE
1	T1552	Unsecured Credentials	22
2	T1021.001	Remote Desktop Protocol	21
3	T1543.002	Systemd Service	20
4	T1563.002	RDP Hijacking	20
5	T1072	Software Deployment Tools	20
6	T1530	Data from Cloud Storage Object	19
7	T1530.006	Systemd Timers	18
8	T1574	Hijack Execution Flow	16
9	T1078.004	Cloud Accounts	16
10	T1543	Create or Modify System Process	16
11	T1601.002	Patch System Image	15
12	T1548	Forge Web Credentials	15
13	T1601	Downgrade System Image	15
14	T1569	Abuse Elevation Control Mechanism	15
15	T1098	Modify System Image	15
16	T1003	System Services	15
17	T1053.002	Account Manipulation	14
18	T1599	OS Credential Dumping	14
19	T1021.002	At (Windows)	14
20	T1599.001	Domain Policy Modification	14

Unmapped

While the majority of the ATT&CK (sub-)techniques can be defended against by one or more CIS Safeguards, 63 ATT&CK (sub-)techniques did not map back to a CIS Safeguard. Many of these ATT&CK (sub-)techniques are listed under ATT&CK mitigations that did not map to a CIS Safeguard, such as "M1055–Do Not Mitigate," "M1020–SSL/TLS Inspection," and "M1019–Threat Intelligence Program." Several ATT&CK (sub-)techniques from "M1056–Pre-compromise" were also among those that were unmapped. A listing of these ATT&CK (sub-) techniques can be found in Appendix D of this guide.

Additionally, the 84 ATT&CK (sub-)techniques with no assignment to an ATT&CK mitigation can be found in Appendix E of this guide. Our assessment of these ATT&CK (sub-)techniques found that the majority are used in LotL attacks, where an attacker uses existing tools and tactics on the targeted system or network to carry out an attack, rather than exploit a specific system or control weakness; these attacks are therefore difficult to defend against.

CIS Safeguards

All CIS Safeguards

In addition to the analysis above, we also analyzed the reverse—which CIS Safeguards defend against one or more ATT&CK (sub-)techniques. Our mapping revealed that out of 153 CIS Safeguards, 68% defend against one or more ATT&CK (sub-)techniques, with 19 CIS Safeguards defending against 50 or more ATT&CK (sub-)techniques, as shown below in Table 6.

We can see that CIS Safeguard "4.1–Establish and Maintain a Secure Configuration Process" defends against the highest number of ATT&CK (sub-)techniques, once again reinforcing the importance of secure configurations, such as those contained within the CIS Benchmarks.

Table 6. CIS Safeguards that had the highest number of mapped ATT&CK (sub-)techniques

RANK	CIS SAFEGUARD	CIS SAFEGUARD TITLE	NUMBER OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY A CIS SAFEGUARD	IG1	IG2	IG3
1	4.1	Establish and Maintain a Secure Configuration Process	342	✓	✓	✓
2	6.1	Establish an Access Granting Process	217	✓	✓	✓
3	6.2	Establish an Access Revoking Process	217	✓	✓	✓
4	18.3	Remediate Penetration Test Findings	214		✓	✓
5	6.8	Define and Maintain Role-Based Access Control	206			✓
6	4.7	Manage Default Accounts on Enterprise Assets and Software	188	✓	✓	✓
7	18.5	Perform Periodic Internal Penetration Tests	187			✓
8	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	164	✓	✓	✓
9	5.3	Disable Dormant Accounts	155	✓	✓	✓
10	2.5	Allowlist Authorized Software	101		✓	✓
11	2.7	Allowlist Authorized Scripts	81			✓
12	3.3	Configure Data Access Control Lists	75	✓	✓	✓
13	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	73	✓	✓	✓
14	2.3	Address Unauthorized Software	67	✓	✓	✓
15	4.4	Implement and Manage a Firewall on Servers	60	✓	✓	✓
16	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	54		✓	✓
17	13.8	Deploy a Network Intrusion Prevention Solution	53			✓
18	13.3	Deploy a Network Intrusion Detection Solution	53		✓	✓
19	12.2	Establish and Maintain a Secure Network Architecture	51		✓	✓
20	5.2	Use Unique Passwords	47	✓	✓	✓

IG1 CIS Safeguards

Overall, it was found that 86% of IG1 Safeguards defend against one or more ATT&CK (sub-)techniques, with many defending against 60 or more, as shown below in Table 7. This reinforces that implementing a relatively small set of defensive actions (IG1) provides an enterprise with the ability to defend against a wide array of potential attacks.

As previously mentioned, some of the IG1 Safeguards do not directly map to the ATT&CK framework. These are considered foundational Safeguards, such as keeping inventory of enterprise assets and software (CIS Controls 1 and 2) and implementing logging (CIS Control 8). These foundational Safeguards are important, since without them, there is no way of knowing which devices are, or could be, compromised. These foundational Safeguards may not be included in the ATT&CK model as defensive measures; however, they must be implemented before more technical Safeguards that do map to ATT&CK can be properly implemented.

Table 7. IG1 Safeguards that had the highest number of mapped ATT&CK (sub-)techniques

RANK	CIS SAFEGUARD	TITLE	NUMBER OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY A CIS SAFEGUARD
1	4.1	Establish and Maintain a Secure Configuration Process	342
2	6.1	Establish an Access Granting Process	217
3	6.2	Establish an Access Revoking Process	217
4	4.7	Manage Default Accounts on Enterprise Assets and Software	188
5	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	164
6	5.3	Disable Dormant Accounts	155
7	3.3	Configure Data Access Control Lists	75
8	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	73

9	2.3	Address Unauthorized Software	67
10	4.4	Implement and Manage a Firewall on Servers	60
11	5.2	Use Unique Passwords	47
12	6.5	Require MFA for Administrative Access	33
13	6.4	Require MFA for Remote Network Access	31
14	7.1	Establish and Maintain a Vulnerability Management Process	27
15	7.2	Establish and Maintain a Remediation Process	27
16	11.3	Protect Recovery Data	27
17	14.1	Establish and Maintain a Security Awareness Program	25
18	7.3	Perform Automated Operating System Patch Management	24
19	11.4	Establish and Maintain an Isolated Instance of Recovery Data	20
20	6.3	Require MFA for Externally-Exposed Applications	17

Unmapped

In total, 49 CIS Safeguards were not mapped to ATT&CK, only eight of which were IG1 Safeguards. As previously mentioned, some of these unmapped Safeguards are foundational Safeguards, such as "CIS Control 8: Audit Log Management" and "CIS Control 3: Data Protection." Other Safeguards, such as those in "CIS Control 15: Service Provider Management" and "CIS Control 17: Incident Response Management," as examples, are also not specifically addressed by any of the ATT&CK mitigations in the ATT&CK framework, and therefore are unable to be mapped.

A list of unmapped CIS Safeguards can be found in Appendix F of this guide.

Data Source Analysis

After determining the security function of the CIS Safeguards, based on their mapping to ATT&CK, we then determined the top five attack types and attack patterns. First, we selected the most common attack types that enterprises should defend against, through reviewing various data sources. Attack types are the high-level grouping of attacks. For v2.0, they are: Malware, Ransomware, Web Application Hacking, Insider and Privilege Misuse, and Targeted Intrusions.

Following this, we used additional data sources to determine the attack pattern—the set of ATT&CK (sub-)techniques required to execute the attack. Attack patterns are constructed with the most recent attacker techniques and can change from year to year. Lastly, we leveraged the master mapping to ATT&CK, to perform a reverse mapping back to the CIS Safeguards, which allowed us to analyze the security value of the Safeguards.

Data Types

Each year, multiple data sources (i.e., industry threat data sources) are published that contain various metrics, such as top malware, top ransomware, top attack types, etc. The data behind these reports contains valuable information and can be categorized into one of the following data types, all of which the CDM leverages:

- **Self-Reported Data:** Analysts and researchers are employed to contact companies and obtain first-hand information about how breaches occurred.
- **Sensor Data:** Vendors offering network and other types of cybersecurity monitoring or prevention services have access to raw network and other types of data.
- **Incident Response Data:** Created from incident response activities, the data obtained here is often rich and extremely granular; however, it may be unstructured and is provided in narrative form.
- **Product Usage Data:** Vendors offering software-as-a-service and cloud-based products may gather security-relevant data for customers using their products.
- **Open-Source Intelligence:** Information available from sources such as intelligence reports, publicly-available incident response reports, and other security-related publications.

If you're a vendor with data that fits into one or more categories, please contact us at controlsinfo@cisecurity.org.

In addition to data type, the longevity of the report and access to underlying datasets are also taken into consideration.

Attack Type Data Sources

We evaluated multiple data sources to determine the top five attack types, as shown below in Table 8.

Table 8. Attack type data sources

DATA SOURCE	PUBLISH DATE	TYPE	LONGEVITY	CIS ACCESS TO UNDERLYING DATA
Verizon DBIR	May 19, 2020	Self-reported data, Sensor data, Incident response data	2008	No[7]
IBM X-Force Threat Intelligence Index	February 24, 2021	Sensor data, Incident response data	2017	No
ENISA Threat Landscape – The Year in Review	October 20, 2020	Open-source intelligence	2012	No
CrowdStrike Services Cyber Front Lines Report	2020	Sensor data, Incident response data, Product usage data	2020	No
Akamai The State of the Internet: A Year in Review	2020	Sensor data, Product usage data	2008	No

Several sources were reviewed and some carried a heavier weight, such as the 2020 Verizon DBIR, since their dataset encompasses several different data sources, both public and private, and is based on multiple data types. As data sources may change from time to time, we are confident that our analysis and the data that backs it provides enterprises with the knowledge they need to put forth a robust security program and protect against the most pervasive cyber threats.

Top Attack Types

The top attack types for v2.0 are shown below in Table 9, in order of prevalence. The attack types remain unchanged from v1.0; however, the rank has changed, based on the cumulative analysis of the various data sources listed above in Table 8.

With these attack types, there is likely to be some overlap (e.g., a nation-state attacker that is working as an insider, a targeted intrusion attack that uses malware). However, every effort is made to group these top attack types into categories that have valuable data sources to determine their respective attack patterns. Therefore, some top attack types, such as general, non-specific categories (e.g., everything else, other, etc.) or a category that cannot be easily mitigated (e.g., Denial of Service (DoS), stolen assets, etc.), were not considered.

Table 9. Top 5 attack types for CDM v2.0

RANK	ATTACK TYPE	CHANGE FROM CDM V1.0
1	Malware	Moved up in rank
2	Ransomware	Moved up in rank
3	Web Application Hacking	Moved down in rank
4	Insider and Privilege Misuse	Moved down in rank
5	Targeted Intrusions	Rank remained the same

The following sections briefly describe each attack type and the justification for inclusion.

7 However, the Vocabulary for Event Recording and Incident Sharing (VERIS) Community Database (VCDB) is a random sample of only public breaches and is available at: https://github.com/vz-risk/VCDB. This data is a part of the larger DBIR dataset.

Malware

Malware continues to plague enterprises year after year. The Verizon DBIR describes malware as *"...the common type of commodity malware that everyone has probably seen on some email claiming to be a fax or a missed delivery package. These incidents and breaches tend to be opportunistic and financially motivated."* (Verizon DBIR, 2020).[8] The DBIR refers to this attack type as "crimeware," which includes malware that did not fall into another attack type. According to the 2020 DBIR, malware ranked #4 in breaches and #2 in incidents (Verizon DBIR, 2020). Malware continues to affect enterprises globally, as malware ranked #1 in ENISA's The Year in Review 2020 report (ENISA, 2020)[9]. Each month, the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) publishes the Top 10 Malware impacting SLTTs, a data source also used in the CDM.

Malware ranked #1 in ENISA's The Year in Review 2020 report.

Ransomware

Ransomware involves the encryption of files on a system or network, rendering them useless until a decryption key is used or backups are restored. Ransomware has taken its toll across all sectors over the years, and the threat continues to grow into 2021. According to the 2020 DBIR, 27% of malware incidents were categorized as ransomware (Verizon DBIR, 2020). Due to the differences in attacker tactics, techniques, and procedures (TTPs) and motives, we separated Ransomware from the Malware attack type. According to IBM®'s 2021 X-Force Threat Intelligence Index report, ransomware ranked as their number one threat type, totaling 23% of their X-Force® caseload (IBM X-Force, 2021)[10]. Additionally, X-Force estimated a staggering profit of $123 million from just one of the ransomware groups, Sodinokibi (aka REvil) (IBM X-Force, 2021). According to Bitdefender®'s 2020 Mid-Year Threat Landscape Report, there was a 715.08% increase of ransomware reports across the globe (Bitdefender, 2020)[11]. These findings stress the importance of protecting against ransomware attacks, as no one sector is immune.

According to Bitdefender's 2020 Mid-Year Threat Landscape Report, there was a 715.08% increase in ransomware reports across the globe.

Web Application Hacking

The DBIR defines this as "anything that has a web application as the target." Over 80% of breaches involved some type of web application hacking, according to the 2020 Verizon DBIR. Additionally, web applications were ranked #1 for breaches and #4 for incidents (Verizon DBIR, 2020). When it comes to the cloud, the report also states that 73% of the time, cloud-based breaches attacked an email or web application server, stressing the importance of protecting both on-premises and cloud assets (Verizon DBIR, 2020). It should come as no surprise that externally-facing applications are much more vulnerable to an attack, especially for those with misconfigurations and protocols that are left open and unprotected. At the top of the list for web application attacks are "Injections" (e.g., SQL, NoSQL, etc.) and "Cross-site Scripting (XSS)," according to the OWASP® Top 10[12] and 2020 CWE Top 25[13], respectively.

Insider and Privilege Misuse

Insider and Privilege Misuse can be defined as incidents that are intentionally carried out by an insider, according to the 2020 Verizon DBIR. These are incidents where the insider has malicious intent to cause harm. According to the 2021 IBM X-Force Threat Intelligence Report, *"25% of attacks against transportation in 2020 involved a malicious insider or misconfiguration."* Additionally, out of the 13% of insider threat incidents in the industrial control systems (ICS) and operational technology (OT) fields, 60% involved insiders with malicious intent (IBM X-Force, 2021).

8 2020 Verizon Data Breach Investigations Report (DBIR) https://enterprise.verizon.com/resources/reports/dbir/2020/introduction/

9 ENISA Threat Landscape–The Year in Review (Published October 20, 2020) https://www.enisa.europa.eu/publications/year-in-review

10 IBM X-Force Threat Intelligence Index 2021 https://www.ibm.com/security/data-breach/threat-intelligence

11 Bitdefender Mid-Year Threat Landscape Report 2020 https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

12 OWASP Top 10 https://owasp.org/www-project-top-ten/

13 2020 CWE Top 25 https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Targeted Intrusions

This attack type includes nation-state activity or state-affiliated actors that are looking for the crown jewels, such as an enterprise's data (Verizon DBIR, 2020). Additionally, the intent of Targeted Intrusions differs from other patterns, focusing on social, economic, and political gain. The 2020 DBIR states that these types of attacks typically focus on the social and malware vectors of the VERIS framework, with 81% using phishing and 92% using malware (Verizon DBIR, 2020).

Attack Pattern Data Sources

Once the top attack types were determined, data sources were selected in a similar fashion to create comprehensive attack patterns. Attack patterns are the selection of ATT&CK (sub-) techniques that are used in a given attack type. We focus on the most common and recently used techniques to form the attack patterns, as patterns can and will change from year to year. Several data sources were used to create the attack patterns, which can be seen in Table 10 below.

Table 10. Data sources used to create attack patterns (for each attack type)

ATTACK TYPE	ATTACK PATTERN DATA SOURCE
Malware	• Multi-State Information Sharing and Analysis Center® (MS-ISAC®) Top 10 Malware • CrowdStrike 2021 Global Threat Report[14] • IBM X-Force Threat Intelligence Index 2021 • ESET Threat Report Q4 2020[15] • Check Point 2021 Cyber Security Report[16]
Ransomware (as a subset of Malware)	• Multi-State Information Sharing and Analysis Center (MS-ISAC) Data • CrowdStrike 2021 Global Threat Report • IBM X-Force Threat Intelligence Index 2021 • Group-IB Ransomware Uncovered 2020–2021[17] • ESET Threat Report Q4 2020
Web Application Hacking	• OWASP Top 10 • 2020 CWE Top 25
Insider and Privilege Misuse	• Verizon Insider Threat Report 2019[18] • Securonix 2020 Insider Threat Report[19] • G-Research Introducing the Insider Attack Matrix[20]
Targeted Intrusions	• CrowdStrike 2021 Global Threat Report • CISA SolarWinds and Active Directory/M365 Compromise Threat Report[21]

14 CrowdStrike 2021 Global Threat Report https://www.crowdstrike.com/resources/reports/global-threat-report/

15 ESET Threat Report Q4 2020 https://www.welivesecurity.com/wp-content/uploads/2021/02/ESET_Threat_Report_Q42020.pdf

16 Check Point 2021 Cyber Security Report https://www.checkpoint.com/pages/cyber-security-report-2021/

17 Group-IB Ransomware Uncovered 2020–2021 https://www.group-ib.com/resources/threat-research/ransomware-2021.html

18 Verizon Insider Threat Report 2019 https://enterprise.verizon.com/resources/reports/insider-threat-report/

19 Securonix 2020 Insider Threat Report https://www.securonix.com/resources/2020-insider-threat-report/

20 G-Research Introducing the Insider Attack Matrix https://www.gresearch.co.uk/article/introducing-the-insider-attack-matrix/

21 CISA SolarWinds and Active Directory/M365 Compromise Threat Report: https://us-cert.cisa.gov/sites/default/files/publications/Supply_Chain_Compromise_Detecting_APT_Activity_from_known_TTPs.pdf

Security Value Analysis

There are several different ways to analyze the security value of the CIS Safeguards against the top five attack types. The next few sections provide an analysis of how well each attack pattern[22] is covered by the CIS Safeguards, against ATT&CK tactics and ATT&CK (sub-) techniques. Note that for the ATT&CK tactic analysis, multiple ATT&CK (sub-)techniques can appear across multiple ATT&CK tactics.

Malware

Shown below in Figure 6 is the Malware attack pattern analysis, by IG, across all ATT&CK tactics. Overall, nine of the 14 ATT&CK tactics had 75% or more coverage. Table 11 shows the percentage of Malware ATT&CK (sub-)techniques, within each ATT&CK tactic, that CIS Safeguards defend against.

Figure 6. Malware attack pattern coverage against CIS Safeguards (by IG) across ATT&CK tactics

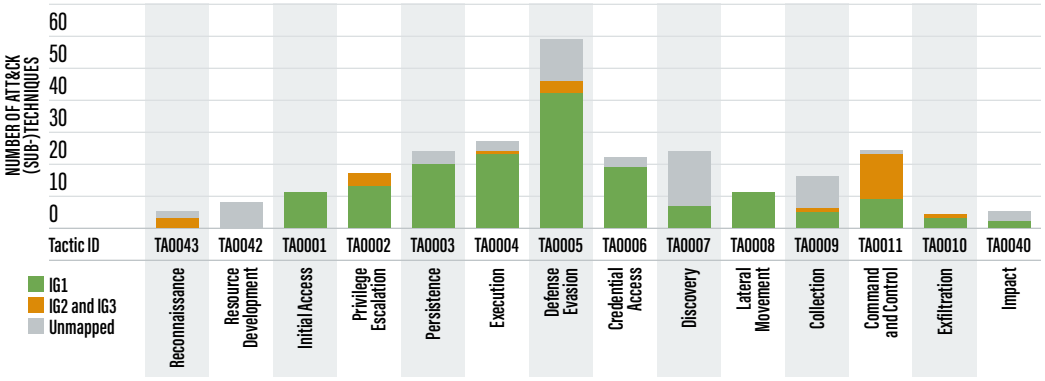


Table 11. Percentage of ATT&CK (sub-)techniques that can be defended against for the Malware attack pattern

TACTIC ID	TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040
	60%	0%	100%	100%	83%	89%	78%	86%	29%	100%	38%	96%	100%	40%

94% of ATT&CK (sub-) techniques in the Malware attack pattern can be defended against through implementation of CIS Safeguards.

The Malware attack pattern mapped to 209 unique ATT&CK (sub-)techniques[23], with CIS Safeguards defending against 152 of them. This number may seem low; however, out of the 209 ATT&CK (sub-)techniques, only 162 were assigned to an ATT&CK mitigation, which indicates the highest possible number of techniques that can be defended against across any security framework. Taking this into consideration, it was found that 94% of ATT&CK (sub-)techniques in the Malware attack pattern can be defended against through implementation of the CIS Safeguards, as shown below in Table 12.

Furthermore, out of the 162, 125 ATT&CK (sub-)techniques, or 77%, can be defended through implementation of IG1. This reinforces the security value that IG1 Safeguards can bring to an enterprise to defend against malware.

Table 12. Malware attack pattern data table

# OF MAPPED ATT&CK (SUB-)TECHNIQUES	# OF ATT&CK (SUB-) TECHNIQUES ASSIGNED TO AN ATT&CK MITIGATION	# OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY THE CIS SAFEGUARDS	% OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY THE CIS SAFEGUARDS	# OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY IG1 CIS SAFEGUARDS	% OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY IG1 CIS SAFEGUARDS
209	162	152	94%	125	77%

22 The set of ATT&CK (sub-)techniques required to execute an attack.

23 Out of 530 total ATT&CK (sub-)techniques

Ransomware

Analysis found that 75% or more of the ATT&CK (sub-)techniques in 10 of the 14 ATT&CK tactics for the Ransomware attack pattern can be defended against through implementation of the CIS Safeguards, as shown below in Figure 7 and Table 13.

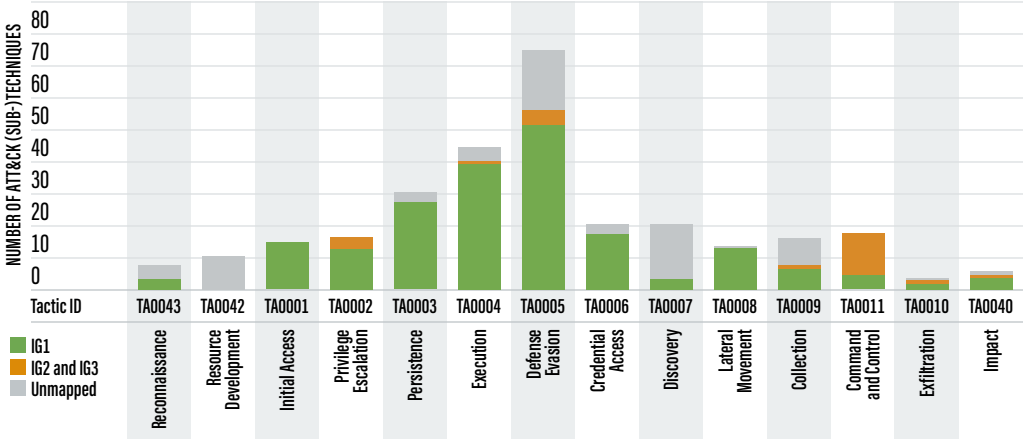


Figure 7. Ransomware attack pattern coverage against CIS Safeguards (by IG) across ATT&CK tactics

Table 13. Percentage of ATT&CK (sub-)techniques that can be defended against for the Ransomware attack pattern

TACTIC ID	TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040
	50%	0%	100%	100%	90%	91%	75%	86%	19%	93%	50%	100%	75%	83%

The Ransomware attack pattern mapped to a total of 229 unique ATT&CK (sub-)techniques (Table 14). Out of the 229, 182 ATT&CK (sub-)techniques were assigned an ATT&CK mitigation, indicating the highest possible number of techniques that can be defended against. Factoring this into the analysis, it was found that CIS Safeguards defend against 92% of the ATT&CK (sub-)techniques. Additionally, IG1 alone defend against 78% of Ransomware ATT&CK (sub-)techniques.

Table 14. Ransomware attack pattern data table

# OF MAPPED ATT&CK (SUB-)TECHNIQUES	# OF ATT&CK (SUB-)TECHNIQUES ASSIGNED TO AN ATT&CK MITIGATION	# OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY THE CIS SAFEGUARDS	% OF ATT&CK (SUB-)TECHNIQUES DEFENDED BY THE CIS SAFEGUARDS	# OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY IG1 CIS SAFEGUARDS	% OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY IG1 CIS SAFEGUARDS
229	182	167	92%	142	78%

Web Application Hacking

Analysis of the Web Application Hacking attack pattern found that the CIS Safeguards defend against 75% or more ATT&CK (sub-)techniques in 11 of the 14 ATT&CK tactics, with six of those ATT&CK tactics having 100% coverage, as shown below in Figure 8 and Table 15.

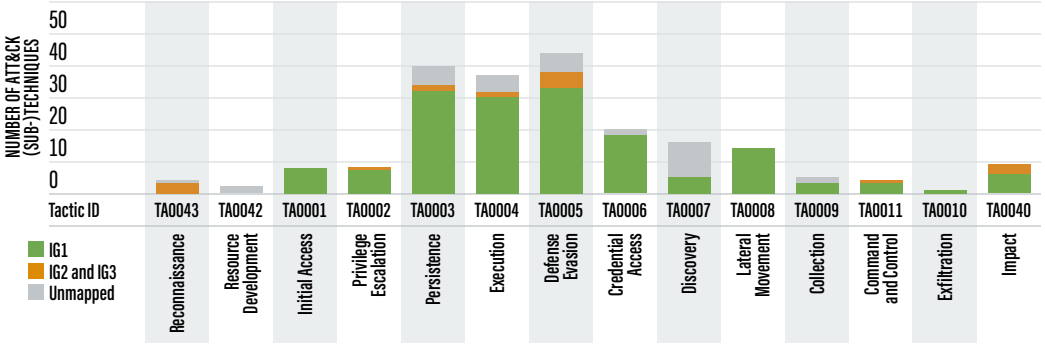


Figure 8. Web Application Hacking attack pattern coverage against CIS Safeguards (by IG) across ATT&CK tactics

TACTIC ID	TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0010	TA0011	TA0040
	75%	0%	100%	100%	85%	86%	86%	90%	31%	100%	60%	100%	100%	100%

Table 15. Percentage of ATT&CK (sub-)techniques that can be defended against for the Web Application Hacking attack pattern

In total, 143 unique ATT&CK (sub-)techniques were mapped to the Web Application Hacking attack pattern (Table 16). Of the 143, 120 ATT&CK (sub-)techniques were assigned to an ATT&CK mitigation and 117, or 98%, are defended through implementation of the CIS Safeguards. Of the 120, IG1 defends against 86% of the ATT&CK (sub-)techniques in this pattern.

# OF MAPPED ATT&CK (SUB-)TECHNIQUES	# OF ATT&CK (SUB-)TECHNIQUES ASSIGNED TO AN ATT&CK MITIGATION	# OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY THE CIS SAFEGUARDS	% OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY THE CIS SAFEGUARDS	# OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY IG1 CIS SAFEGUARDS	% OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY IG1 CIS SAFEGUARDS
143	120	117	98%	103	86%

Table 16. Web Application Hacking attack pattern data table

Insider and Privilege Misuse

Analysis of the Insider and Privilege Misuse attack pattern found that the CIS Safeguards defend against 85% or more of the ATT&CK (sub-)techniques in 10 of the 14 ATT&CK tactics, seven of which have 100% coverage (shown in Figure 9 and Table 17 below).

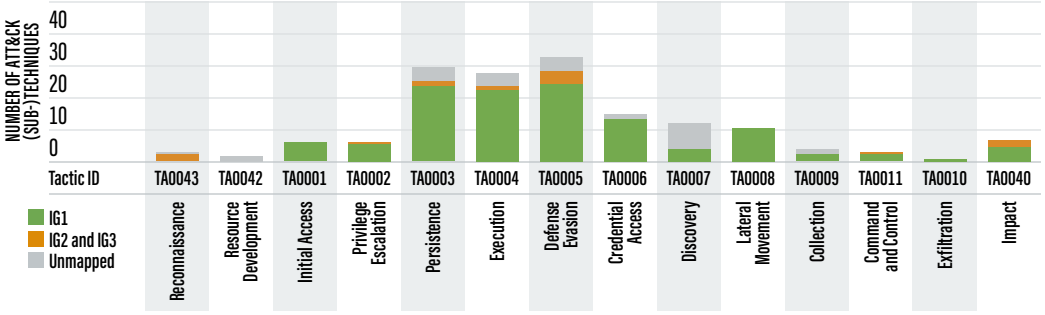


Figure 9. Insider and Privilege Misuse attack pattern coverage against CIS Safeguards (by IG) across ATT&CK tactics

TACTIC ID	TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0010	TA0011	TA0040
	0%	0%	100%	100%	100%	100%	85%	87%	30%	100%	40%	90%	100%	100%

Table 17. Percentage of ATT&CK (sub-)techniques that can be defended against for the Insider and Privilege Misuse attack pattern

Overall, 149 unique ATT&CK (sub-)techniques mapped to the Insider and Privilege Misuse attack pattern, with 112 having an assignment to an ATT&CK mitigation (Table 18). Analysis found that the CIS Safeguards defend against 90% of Insider and Privilege Misuse ATT&CK (sub-)techniques assigned to an ATT&CK mitigation, with IG1 defending against 86% of ATT&CK (sub-)techniques.

# OF MAPPED ATT&CK (SUB-)TECHNIQUES	# OF ATT&CK (SUB-)TECHNIQUES ASSIGNED TO AN ATT&CK MITIGATION	# OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY THE CIS SAFEGUARDS	% OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY THE CIS SAFEGUARDS	# OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY IG1 CIS SAFEGUARDS	% OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY IG1 CIS SAFEGUARDS
149	112	101	90%	96	86%

Table 18. Insider and Privilege Misuse attack pattern data table

Targeted Intrusions

In 10 of the 14 ATT&CK tactics, the CIS Safeguards defend against 75% or more ATT&CK (sub-)techniques associated with the Targeted Intrusions attack pattern, with five of those ATT&CK tactics having 100% coverage (shown in Figure 10 and Table 19 below).

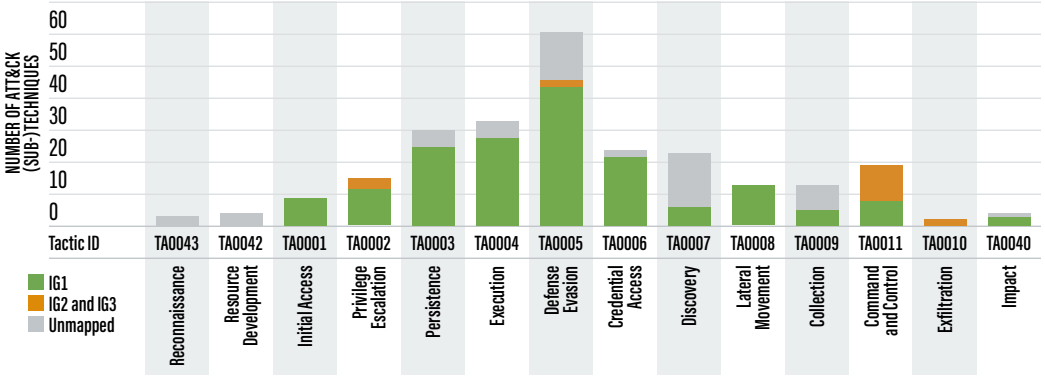


Figure 10. Targeted Intrusions attack pattern coverage against CIS Safeguards (by IG) across ATT&CK tactics

TACTIC ID	TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0010	TA0011	TA0040
	0%	0%	100%	100%	83%	85%	75%	92%	26%	100%	38%	100%	100%	75%

Table 19. Percentage of ATT&CK (sub-)techniques that can be defended against for the Targeted Intrusions attack pattern

Overall, 197 unique ATT&CK (sub-)techniques were mapped to the Targeted Intrusions attack pattern (Table 20). Of the 197, 154 were assigned to an ATT&CK mitigation. As a result, CIS Safeguards defend against 95% of the Targeted Intrusions ATT&CK (sub-)techniques, with IG1 defending against 83%.

# OF MAPPED ATT&CK (SUB-)TECHNIQUES	# OF ATT&CK (SUB-)TECHNIQUES ASSIGNED TO AN ATT&CK MITIGATION	# OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY THE CIS SAFEGUARDS	% OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY THE CIS SAFEGUARDS	# OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY IG1 CIS SAFEGUARDS	% OF ATT&CK (SUB-) TECHNIQUES DEFENDED BY IG1 CIS SAFEGUARDS
197	154	146	95%	128	83%

Table 20. Targeted Intrusions attack pattern data table

Summary

One of the goals of the CDM is to determine the security value of IG1. We determined that an enterprise implementing IG1 can defend itself against the top five attack types. Overall, IG1 defends against 77% or more of ATT&CK (sub-)techniques[24]. Implementing all of the CIS Safeguards defends against 90% or more of the ATT&CK (sub-)techniques. Shown in Table 21 below are the individual percentages for each attack type, broken down by IG1 Safeguards and all CIS Safeguards.

Table 21. Overall security value analysis

ATTACK TYPE	% OF ATT&CK (SUB-)TECHNIQUES DEFENDED AGAINST BY IG1 CIS SAFEGUARDS	% OF ATT&CK (SUB-)TECHNIQUES DEFENDED AGAINST BY CIS SAFEGUARDS
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider and Privilege Misuse	86%	90%
Targeted Intrusions	83%	95%

We also looked at CIS Safeguard coverage for the superset of ATT&CK (sub-)techniques used across all five attack types. Shown below in Figure 11 is the number of ATT&CK (sub-) techniques, by ATT&CK tactic and IG, that the CIS Safeguards defend against. When analyzed, it was found that the CIS Safeguards defend against 77% or more of the ATT&CK (sub-)techniques in 10 of the 14 ATT&CK tactics, as shown in Table 22 below. Also of note, was a particularly low percentage in ATT&CK tactics: TA0007, TA0009, TA0042, and TA0043. This is due to the majority of these ATT&CK (sub-)techniques having no assignment to an ATT&CK mitigation, or assigned, but difficult to defend against (e.g., LotL techniques).

Figure 11. CIS Safeguard coverage (by IG) across all five attack types combined

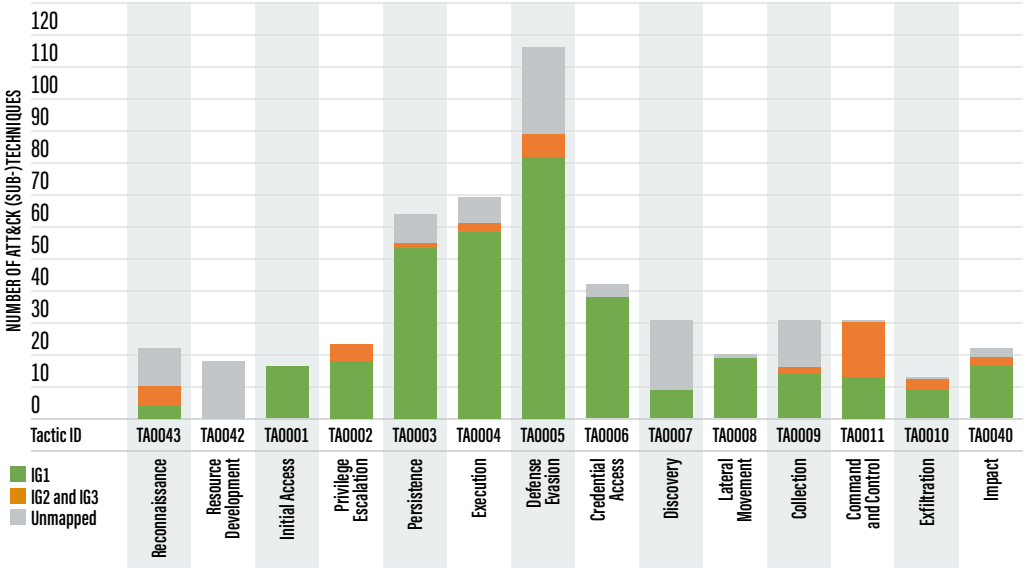


Table 22. Data table showing number of ATT&CK (sub-) techniques mapped across all five attack types combined

TACTIC ID	TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0010	TA0011	TA0040
	45%	0%	100%	100%	86%	88%	77%	90%	29%	95%	52%	92%	97%	86%

24 Assigned to an ATT&CK mitigation

CDM data also allowed us to look at a smaller subset of ATT&CK (sub-)techniques that apply to all five attack types, and the specific CIS Safeguards that can defend against those techniques. Shown below in Figures 12 and 13 are two heat maps, one for IG1 and one for all CIS Safeguards. The checkmarks symbolize that a specific CIS Safeguard can defend against a particular ATT&CK (sub-)technique. The varying "temperatures" of the charts tell us that the higher the total, the higher the effectiveness. This is yet another way that our analysis can be used to determine the effectiveness of implementing the CIS Safeguards in terms of defending against attacks.

Figure 12. IG1 CIS Safeguard heatmap against the top ATT&CK (sub-)techniques across all attack types

ATT&CK (SUB-)TECHNIQUES USED ACROSS ALL ATTACK PATTERNS		IG1 CIS SAFEGUARDS (IN ORDER OF EFFECTIVENESS)																										
(SUB-)TECHNIQUE ID	(SUB-)TECHNIQUE NAME	4.1	4.7	5.3	6.1	6.2	5.4	6.4	6.5	5.2	2.3	4.2	4.4	6.3	11.3	3.3	5.1	10.1	10.2	11.4	3.1	3.4	8.1	8.2	8.3	14.1	14.3	TOTAL
T1098	Account Manipulation	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓				✓								14
T1136	Create Account	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓					✓								13
T1003	OS Credential Dumping	✓	✓	✓	✓	✓	✓			✓					✓											✓	✓	10
T1021.001	Remote Desktop Protocol	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓															10
T1070	Indicator Removal on Host	✓			✓	✓	✓									✓					✓	✓	✓	✓	✓			10
T1078.002	Domain Accounts		✓	✓	✓	✓	✓	✓	✓	✓							✓											9
T1059	Command and Scripting Interpreter	✓	✓	✓	✓	✓	✓				✓							✓	✓									9
T1110	Brute Force	✓	✓	✓				✓	✓	✓				✓														7
T1078	Valid Accounts		✓	✓	✓	✓	✓			✓							✓											7
T1543.003	Windows Service	✓	✓	✓	✓	✓	✓																					6
T1027	Obfuscated Files or Information																	✓	✓									2
T1127	Trusted Developer Utilities Proxy Execution	✓									✓																	2
T1078.001	Default Accounts		✓							✓																		2
T1087	Account Discovery	✓																										1
	TOTAL	10	10	9	9	9	8	5	5	5	3	3	3	3	3	2	2	2	2	2	1	1	1	1	1	1	1	

Figure 13. CIS Safeguard heatmap against the top ATT&CK (sub-)techniques across all attack types

ATT&CK (SUB-)TECHNIQUES USED ACROSS ALL ATTACK PATTERNS		CIS SAFEGUARDS (IN ORDER OF EFFECTIVENESS) IG1 IG2 IG3																																																							
(SUB-)TECHNIQUE ID	(SUB-)TECHNIQUE NAME	4.1	4.7	5.3	6.1	6.2	5.4	18.3	18.5	6.8	4.8	3.12	5.2	6.4	6.5	12.8	2.3	2.5	4.2	4.4	6.3	11.3	12.2	16.10	2.7	3.11	3.3	5.1	5.5	10.1	10.2	10.7	11.4	13.2	13.7	16.1	16.9	2.6	3.1	3.10	3.4	4.10	7.6	7.7	8.1	8.2	8.3	8.9	8.10	9.3	9.6	9.7	12.7	13.5	13.10	14.1	14.3	16.8	TOTAL
T1021.001	Remote Desktop Protocol	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓			✓	✓																			✓	✓									✓	✓	✓				24
T1059	Command and Scripting Interpreter	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓						✓	✓						✓	✓					✓	✓	✓		✓	✓															✓	✓	✓							22
T1098	Account Manipulation	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓			✓	✓	✓	✓	✓				✓						✓																									✓	21
T1003	OS Credential Dumping	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓									✓				✓										✓	✓	✓																		✓	✓		19
T1136	Create Account	✓	✓	✓	✓	✓	✓	✓	✓			✓		✓	✓	✓			✓	✓	✓	✓	✓										✓																										18
T1070	Indicator Removal on Host	✓			✓	✓	✓			✓		✓				✓										✓	✓												✓	✓	✓				✓	✓	✓	✓	✓										17
T1078	Valid Accounts		✓	✓	✓	✓	✓			✓			✓															✓	✓							✓	✓																						11
T1078.002	Domain Accounts		✓	✓	✓	✓	✓			✓			✓	✓	✓													✓	✓																														11
T1543.003	Windows Service	✓	✓	✓	✓	✓	✓	✓	✓	✓																																																	9
T1110	Brute Force	✓	✓	✓									✓	✓	✓						✓																					✓																	8
T1127	Trusted Developer Utilities Proxy Execution	✓						✓	✓		✓						✓	✓						✓	✓																																		8
T1027	Obfuscated Files or Information																													✓	✓	✓		✓	✓																								5
T1087	Account Discovery	✓						✓	✓		✓																																																4
T1078.001	Default Accounts		✓										✓																																														2
	TOTAL	10	10	9	9	9	8	8	8	7	6	5	5	5	5	4	3	3	3	3	3	3	3	3	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

Additionally, we created "attack cards" for each attack type, which provide a list of IG1 CIS Safeguards, in order of effectiveness, along with the corresponding ATT&CK (sub-)techniques that an enterprise will defend against through implementation. These, and other resources, can be found onCIS WorkBench.

It is worth noting that some ATT&CK (sub-)techniques were mapped to an attack pattern and were assigned an ATT&CK mitigation, but had no mapping to a CIS Safeguard. This list can be found in Appendix H of this guide.

Lastly, some ATT&CK (sub-)techniques were mapped to an attack pattern, but were not assigned to an ATT&CK mitigation (and therefore, had no mapping to a CIS Safeguard). This list can be found in Appendix I of this guide.

Conclusion

CDM v2.0 affirms the prioritization of the CIS Critical Security Controls and Implementation Groups. In particular, CDM data backs the premise that all enterprises should start with essential cyber hygiene, or IG1, as a way to defend against the top five attacks.

In summary, our analysis provides us with three key findings:

- **IG1 provides a viable defense against the top five attack types.** Enterprises achieve a high level of protection and are well-positioned to defend against the top five attack types through implementation of essential cyber hygiene, or IG1. These results strongly reinforce the value of a relatively small number of well-chosen and basic defensive steps (IG1). As such, enterprises should aim to start with IG1 to obtain the highest value and work up to IG2 and IG3, as appropriate.
- **Independent of any specific attack type, the CIS Controls are effective at defending against a wide array of attacks.** Specifically, the CIS Controls are effective at defending against 86% of the ATT&CK (sub-)techniques found in the ATT&CK framework. More importantly, the Controls are highly effective against the five attack types found in industry threat data. The bottom line is that the CIS Controls, and specifically IG1, are a robust foundation for your cybersecurity program.
- **Establishing and maintaining a secure configuration process (CIS Safeguard 4.1) is a linchpin Safeguard for all five attack types.** CIS Safeguard 4.1 is most effective in defending against the top five attack types, reinforcing the importance of secure configurations, such as those contained within the CIS Benchmarks.

Join our CDM Community on CIS WorkBench to take advantage of these and other great resources.

CIS is dedicated to taking a "community-first" approach. Further resources can be found on our WorkBench site here. Please join our CDM Community on CIS WorkBench to take advantage of these and other great resources, as well as to participate in next year's CDM (v3.0).

Closing Notes

As a nonprofit organization driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at: controlsinfo@cisecurity.org.

All references to tools or other products in this guide are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information

Center for Internet Security
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org

Future Work

The CDM is very much a continuous process, and will change as new threats emerge, new technologies are released, and new data is published. Our work is dynamic, and for all the right reasons. Results of this work feed into the evolution of the CIS Controls, as well as other CIS products and services.

For CDM v3.0, we hope to address the following:

- **Additional data sources.** Find additional data sources for the top attack types and patterns. This will help to further strengthen our analysis and provide additional insight to other sectors that may not be represented in the current data sources.
- **Re-categorization of top attack types.** During the writing of v2.0, and after analysis was completed, the 2021 Verizon DBIR was published along with their new categorization for attack patterns (what we call attack types). These attack patterns take a whole new approach to the way that attacks are viewed. We hope to further review the DBIR categorization schemas, as well as other data sources, to continually improve our categorization of attack types.
- **More specific analyses.** As we evolve with future versions of the CDM, our analysis will seek to perform even more in-depth analyses, to answer questions such as: "What is the specific 'point' in an attack where it can be thwarted completely?" and "What are the minimal set of Safeguards within IG1 that I need to implement to stop that attack?"
- **More collaboration and correlation.** As CIS Security Best Practices continues to mature our mappings to ATT&CK, we hope to incorporate CIS Benchmark mappings in next year's CDM.
- **More external stakeholder engagement.** As we all know, CIS is appreciative of our many volunteers within the CIS Community. None of this is possible without all of you. Next year, we will look to collaborate with even more enterprises to enhance and evolve future versions of the CDM.

We believe that future versions of the CDM can also provide a foundation for more detailed and specific analyses. For example, combined with other information (e.g., cost estimates for CIS Safeguards or through using different data sets), we could answer questions, such as:

- What is the most cost-effective way to obtain the security value of IG1?
- How can I make best security use of what I already own before I add technology, expense, and processes?
- If I use attack data that is unique to my industry sector, or threat intelligence that is unique to my company, which Safeguards should I implement to achieve an appropriate defensive strategy?
- Will my defenses be effective at multiple steps or tactics of the attack lifecycle?
- If I know the effectiveness of a specific CIS Safeguard (or its absence), can I intelligently 'tailor' my defenses to accommodate specific operational constraints (like the need to run legacy applications)?

We encourage readers to join our communities on CIS WorkBench to get updates, as well as contribute to future versions of the CDM. Email controlsinfo@cisecurity.org to get information on how to become a community member and more.

APPENDIX A

Acronyms and Abbreviations

ATT&CK (sub-)techniques	ATT&CK techniques + ATT&CK sub-techniques
CDM	Community Defense Model
CISA®	Cybersecurity and Infrastructure Security Agency
CWE	Common Weakness Enumeration
DMARC	Domain-based Message Authentication, Reporting & Conformance
DNS	Domain Name System
DoS	Denial of Service
EDR	Endpoint Detection and Response
ENISA	European Network and Information Security Agency
ESET	Executive Security & Engineering Technologies, Inc.
IBM	International Business Machines Corporation
ICS	Industrial Control Systems
IG	Implementation Group
IG1	Implementation Group 1
JSON	JavaScript Object Notation
LotL	Living off the Land
MBR	Master Boot Record
MFA	Multi-Factor Authentication
MIB	Management Information Base
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST® CSF	National Institute of Standards and Technology Cybersecurity Framework
OS	Operating System
OT	Occupational Technology
OWASP®	Open Web Application Security Project®
RDP	Remote Desktop Protocol
SLTT	State, Local, Tribal, and Territorial
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TTP	Tactics, Techniques, and Procedures
URL	Uniform Resource Locator
VERIS Community Database	Vocabulary for Event Recording and Incident Sharing Community Database
Verizon DBIR	Verizon Data Breach Investigations Report
VNC	Virtual Network Computing
XSS	Cross-Site Scripting

APPENDIX B

Links and Resources

- CIS Controls: https://www.cisecurity.org/controls/
- MITRE ATT&CK: https://attack.mitre.org/
- CIS Critical Security Controls v8: https://www.cisecurity.org/controls/v8/
- CDM v1.0: https://www.cisecurity.org/white-papers/cis-community-defense-model/
- CIS WorkBench: https://workbench.cisecurity.org/
- CIS Controls Navigator: https://www.cisecurity.org/controls/cis-controls-navigator/
- CIS Controls Guide: Exploited Protocols: Remote Desktop Protocol: https://www.cisecurity.org/white-papers/exploited-protocols-remote-desktop-protocol-rdp/
- 2020 Verizon[1] Data Breach Investigations Report (DBIR): https://enterprise.verizon.com/resources/reports/dbir/2020/introduction/
- IBM X-Force[2] Threat Intelligence Index 2021: https://www.ibm.com/security/data-breach/threat-intelligence
- ENISA Threat Landscape – The Year in Review (Published October 20, 2020): https://www.enisa.europa.eu/publications/year-in-review
- CrowdStrike Services Cyber Front Lines Report 2020: https://www.crowdstrike.com/services/cyber-front-lines/
- Akamai The State of the Internet: A Year in Review 2020: https://www.akamai.com/our-thinking/the-state-of-the-internet
- Bitdefender[3] Mid-Year Threat Landscape Report 2020: https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf
- Multi-State Information Sharing and Analysis Center (MS-ISAC) Top 10 Malware: https://www.cisecurity.org/ms-isac/
- CrowdStrike 2021 Global Threat Report: https://www.crowdstrike.com/resources/reports/global-threat-report/
- ESET Threat Report Q4 2020: https://www.welivesecurity.com/wp-content/uploads/2021/02/ESET_Threat_Report_Q42020.pdf
- Check Point 2021 Cyber Security Report: https://www.checkpoint.com/pages/cyber-security-report-2021/
- Group-IB Ransomware Uncovered 2020–2021: https://www.group-ib.com/resources/threat-research/ransomware-2021.html
- OWASP Top 10[4]: https://owasp.org/www-project-top-ten/
- 2020 CWE Top 25: https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html
- Verizon Insider Threat Report 2019: https://enterprise.verizon.com/resources/reports/insider-threat-report/
- Securonix 2020 Insider Threat Report: https://www.securonix.com/resources/2020-insider-threat-report/
- G-Research Introducing the Insider Attack Matrix: https://www.gresearch.co.uk/article/introducing-the-insider-attack-matrix/
- CISA SolarWinds and Active Directory/M365 Compromise Threat Report: https://us-cert.cisa.gov/sites/default/files/publications/Supply_Chain_Compromise_Detecting_APT_Activity_from_known_TTPs.pdf

1 Verizon is a registered trademark of Verizon Trademark Services, LLC.
2 IBM and X-Force are registered trademarks of International Business Machines Corporation.
3 Bitdefender is a registered trademark of Bitdefender IPR Management Ltd.
4 OWASP is a registered trademark of OWASP Foundation, Inc.

APPENDIX C

Background

The CIS Critical Security Controls (CIS Controls) are a prioritized set of CIS Safeguards to mitigate the most common cyber-attacks against systems and networks. The volunteer experts who develop the CIS Controls come from a wide range of sectors including defense, education, government, healthcare, manufacturing, retail, transportation, and others.

The earliest versions of the CIS Controls were based on the consensus judgment of a relatively small number of experienced people and validated with public feedback from across the industry. The analysis was supported by a simple list of important attacks against which to examine possible CIS Controls. Over more recent versions, CIS has started to develop more data and rigor to underpin the process.

CIS started by working with the emerging marketplace of authoritative summaries of "real world" data about attacks—beginning with the Verizon Data Breach Investigations Report (DBIR) in 2013. After the Verizon® team completed their initial attack analysis, a CIS volunteer team worked with Verizon to map the most important categories or types of attacks seen in the prior year's data to the CIS Controls, and this map became part of the Verizon DBIR Recommendations. Over the next couple of years, we repeated this process with several other security vendors.

While this approach is useful and based on summaries of data derived by each vendor from their own business model, there were several areas that had to be resolved:

- The vendor reports typically came from marketing departments, so the use of language was inconsistent across vendors and tended to be buzzword heavy
- There was no rigorous way to normalize the data and conclusions across different vendors
- The mapping from summaries and patterns of attack to the CIS Controls was still informal and based on the judgment of relatively few people

In our next step (in 2016), we developed the CIS Community Attack Model as a way to structure the discussion and the mapping from classes of attacks to the CIS Controls. Our goal was to create an open, high-level model in which classes of countermeasures (CIS Safeguards) were organized in two dimensions:

1. Steps of the attacker's lifecycle (similar to the well-known Lockheed Martin Cyber Kill Chain)
2. Categories of defensive effect, for which we used the Core Functions of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

This approach helped CIS focus on questions like, "What types of countermeasures could help prevent the delivery phase of an attacker's lifecycle?"

You could also take a strategic view of defense by asking: "Am I over-invested in tools for detecting and preventing the early stages of attack, and under-invested if the initial steps of an attack succeed?"

While it was never fully operationalized, the Community Attack Model was a useful way to structure and capture the discussion about the value of Control selection. Ultimately, the Community Attack Model laid the groundwork for what we now know to be the Community Defense Model.

APPENDIX D

ATT&CK (Sub-)Techniques with No Mapping to CIS Safeguards

The following ATT&CK (sub-)techniques were assigned to an ATT&CK mitigation; however, they had no mapping back to a CIS Safeguard.

ATT&CK (SUB-) TECHNIQUE ID	ATT&CK (SUB-)TECHNIQUE NAME
T1090.004	Domain Fronting
T1480	Execution Guardrails
T1480.001	Environmental Keying
T1583	Acquire Infrastructure
T1583.001	Domains
T1583.002	DNS Server
T1583.003	Virtual Private Server
T1583.004	Server
T1583.005	Botnet
T1583.006	Web Services
T1584	Compromise Infrastructure
T1584.001	Domains
T1584.002	DNS Server
T1584.003	Virtual Private Server
T1584.004	Server
T1584.005	Botnet
T1584.006	Web Services
T1585	Establish Accounts
T1585.001	Social Media Accounts
T1585.002	Email Accounts
T1586	Compromise Accounts
T1586.001	Social Media Accounts
T1586.002	Email Accounts
T1587	Develop Capabilities
T1587.001	Malware
T1587.002	Code Signing Certificates
T1587.003	Digital Certificates
T1587.004	Exploits
T1588	Obtain Capabilities
T1588.001	Malware
T1588.002	Tool
T1588.003	Code Signing Certificates
T1588.004	Digital Certificates
T1588.005	Exploits
T1588.006	Vulnerabilities
T1589	Gather Victim Identity Information
T1589.001	Credentials
T1589.002	Email Addresses
T1589.003	Employee Names
T1590.003	Network Trust Dependencies
T1591	Gather Victim Org Information
T1591.001	Determine Physical Locations
T1591.002	Business Relationships
T1591.003	Identify Business Tempo
T1591.004	Identify Roles
T1592	Gather Victim Host Information
T1592.001	Hardware
T1592.002	Software
T1592.003	Firmware
T1592.004	Client Configurations
T1593	Search Open Websites/Domains
T1593.001	Social Media
T1593.002	Search Engines
T1594	Search Victim-Owned Websites
T1596	Search Open Technical Databases
T1596.001	DNS/Passive DNS
T1596.002	WHOIS
T1596.003	Digital Certificates
T1596.004	CDNs
T1596.005	Scan Databases
T1597	Search Closed Sources
T1597.001	Threat Intel Vendors
T1597.002	Purchase Technical Data

APPENDIX E

ATT&CK (Sub-)Techniques with No Mapping to ATT&CK Mitigations

The following are the 84 MITRE ATT&CK (sub-)techniques that had no assignment to an ATT&CK mitigation. As per MITRE, these ATT&CK (sub-)techniques "cannot be easily mitigated with preventative controls since it is based on the abuse of system features," and therefore had no mapping to a CIS Safeguard (MITRE, 2021)[1].

ATT&CK (SUB-) TECHNIQUE ID	ATT&CK (SUB-)TECHNIQUE NAME
T1005	Data from Local System
T1006	Direct Volume Access
T1007	System Service Discovery
T1010	Application Window Discovery
T1012	Query Registry
T1014	Rootkit
T1016	System Network Config. Discovery
T1018	Remote System Discovery
T1020	Automated Exfiltration
T1025	Data from Removable Media
T1027.001	Binary Padding
T1027.003	Steganography
T1027.004	Compile After Delivery
T1027.005	Indicator Removal from Tools
T1033	System Owner/User Discovery
T1036.002	Right-to-Left Override
T1036.004	Masquerade Task or Service
T1036.006	Space after Filename
T1039	Data from Network Shared Drive
T1049	System Network Conn. Discovery
T1056	Input Capture
T1586.001	Social Media Accounts
T1586.002	Email Accounts
T1056.001	Keylogging
T1056.004	Credential API Hooking
T1057	Process Discovery
T1069	Permission Groups Discovery
T1069.001	Local Groups
T1069.002	Domain Groups
T1069.003	Cloud Groups
T1070.004	File Deletion
T1070.005	Network Share Conn. Removal
T1070.006	Timestomp
T1074	Data Staged
T1074.001	Local Data Staging
T1074.002	Remote Data Staging
T1082	System Information Discovery
T1083	File and Directory Discovery
T1087.003	Email Account
T1113	Screen Capture
T1115	Clipboard Data
T1120	Peripheral Device Discovery
T1123	Audio Capture
T1124	System Time Discovery
T1125	Video Capture
T1134.004	Parent PID Spoofing
T1137.006	Add-ins
T1140	Deobfuscate/Decode Files or Info.
T1202	Indirect Command Execution
T1207	Rogue Domain Controller
T1217	Browser Bookmark Discovery
T1496	Resource Hijacking
T1497	Virtualization/Sandbox Evasion
T1497.001	System Checks
T1497.002	User Activity Based Checks
T1497.003	Time Based Evasion
T1505.003	Web Shell
T1518	Software Discovery
T1518.001	Security Software Discovery
T1526	Cloud Service Discovery
T1529	System Shutdown/Reboot
T1531	Account Access Removal
T1534	Internal Spearphishing
T1542.002	Component Firmware
T1546	Event Triggered Execution
T1546.001	Change Default File Association
T1546.005	Trap
T1546.007	Netsh Helper DLL
T1546.012	Image File Exec. Options Injection
T1546.015	Component Obj. Model Hijacking
T1547	Boot or Logon Autostart Execution
T1547.001	Registry Run Keys / Startup Folder
T1547.010	Port Monitors
T1553.002	Code Signing
T1555.002	Securityd Memory
T1560.002	Archive via Library
T1560.003	Archive via Custom Method
T1564	Hide Artifacts
T1564.001	Hidden Files and Directories
T1564.005	Hidden File System
T1568.001	Fast Flux DNS
T1568.003	DNS Calculation
T1578.004	Revert Cloud Instance
T1600	Weaken Encryption
T1600.001	Reduce Key Space
T1600.002	Disable Crypto Hardware

1 MITRE ATT&CK https://attack.mitre.org/

APPENDIX F

Unmapped CIS Safeguards to ATT&CK Framework

The following CIS Safeguards had no mapping to an ATT&CK mitigation or (sub-)technique.

CONTROL	SAFEGUARD	TITLE	IG1	IG2	IG3
1	1.3	Utilize an Active Discovery Tool		✓	✓
1	1.5	Use a Passive Asset Discovery Tool			✓
3	3.5	Securely Dispose of Data	✓	✓	✓
3	3.7	Establish and Maintain a Data Classification Scheme		✓	✓
3	3.8	Document Data Flows		✓	✓
3	3.9	Encrypt Data on Removable Media		✓	✓
3	3.13	Deploy a Data Loss Prevention Solution			✓
3	3.14	Log Sensitive Data Access			✓
4	4.3	Configure Automatic Session Locking on Enterprise Assets	✓	✓	✓
4	4.11	Enforce Remote Wipe Capability on Portable End-User Devices		✓	✓
4	4.12	Separate Enterprise Workspaces on Mobile End-User Devices			✓
5	5.6	Centralize Account Management		✓	✓
6	6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems		✓	✓
6	6.7	Centralize Access Control		✓	✓
8	8.4	Standardize Time Synchronization		✓	✓
8	8.6	Collect DNS Query Audit Logs		✓	✓
8	8.7	Collect URL Request Audit Logs		✓	✓
8	8.8	Collect Command-Line Audit Logs		✓	✓
8	8.12	Collect Service Provider Logs			✓
9	9.5	Implement DMARC		✓	✓
10	10.4	Configure Automatic Anti-Malware Scanning of Removable Media		✓	✓
10	10.6	Centrally Manage Anti-Malware Software		✓	✓
12	12.3	Securely Manage Network Infrastructure		✓	✓
12	12.4	Establish and Maintain Architecture Diagram(s)		✓	✓
13	13.1	Centralize Security Event Alerting		✓	✓
13	13.6	Collect Network Traffic Flow Logs		✓	✓
13	13.11	Tune Security Event Alerting Thresholds			✓
14	14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	✓	✓	✓
14	14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	✓	✓	✓
15	15.1	Establish and Maintain an Inventory of Service Providers	✓	✓	✓
15	15.2	Establish and Maintain a Service Provider Management Policy		✓	✓
15	15.3	Classify Service Providers		✓	✓
15	15.4	Ensure Service Provider Contracts Include Security Requirements		✓	✓
15	15.5	Assess Service Providers			✓
15	15.6	Monitor Service Providers			✓
16	16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		✓	✓
16	16.7	Use Standard Hardening Configuration Templates for Application Infrastructure		✓	✓
16	16.10	Apply Secure Design Principles in Application Architectures		✓	✓
16	16.14	Conduct Threat Modeling			✓
17	17.1	Designate Personnel to Manage Incident Handling	✓	✓	✓
17	17.2	Establish and Maintain Contact Information for Reporting Security Incidents	✓	✓	✓
17	17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	✓	✓	✓
17	17.4	Establish and Maintain an Incident Response Process		✓	✓
17	17.5	Assign Key Roles and Responsibilities		✓	✓
17	17.6	Define Mechanisms for Communicating During Incident Response		✓	✓
17	17.7	Conduct Routine Incident Response Exercises		✓	✓
17	17.8	Conduct Post-Incident Reviews		✓	✓
17	17.9	Establish and Maintain Security Incident Thresholds			✓
18	18.4	Validate Security Measures			✓

APPENDIX G

ATT&CK Navigator[1] Visualizations for Attack Patterns

A full listing of JavaScript Object Notation (JSON) files can be found on CIS WorkBench here.

Malware

Domain: Enterprise ATT&CK v8

Platforms: Linux®, macOS®, Windows®, Office 365®, Azure® AD, IaaS, SaaS, PRE, Network

TA0043: Reconnaissance
- T1595: Active Scanning
- T1592: Gather Victim Host Information
  - T1592.004: Client Configurations
  - T1592.003: Firmware
  - T1592.001: Hardware
  - T1592.002: Software
- T1589: Gather Victim Identity Information
- T1590: Gather Victim Network Information
  - T1590.002: DNS
  - T1590.001: Domain Properties
  - T1590.005: IP Addresses
  - T1590.006: Network Security Appliances
  - T1590.004: Network Topology
  - T1590.003: Network Trust Dependencies
- T1591: Gather Victim Org Information
- T1598: Phishing for Information
- T1597: Search Closed Sources
- T1596: Search Open Technical Databases
- T1593: Search Open Websites/Domains
- T1594: Search Victim-Owned Websites

TA0042: Resource Development
- T1583: Acquire Infrastructure
  - T1583.005: Botnet
  - T1583.002: DNS Server
  - T1583.001: Domains
  - T1583.004: Server
  - T1583.003: Virtual Private Server
  - T1583.006: Web Services
- T1586: Compromise Accounts
  - T1586.002: Email Accounts
  - T1586.001: Social Media Accounts
- T1584: Compromise Infrastructure
  - T1584.005: Botnet
  - T1584.002: DNS Server
  - T1584.001: Domains
  - T1584.004: Server
  - T1584.003: Virtual Private Server
  - T1584.006: Web Services
- T1587: Develop Capabilities
  - T1587.002: Code Signing Certificates
  - T1587.003: Digital Certificates
  - T1587.004: Exploits
  - T1587.001: Malware
- T1585: Establish Accounts
- T1588: Obtain Capabilities
  - T1588.003: Code Signing Certificates
  - T1588.004: Digital Certificates
  - T1588.005: Exploits
  - T1588.001: Malware
  - T1588.002: Tool
  - T1588.006: Vulnerabilities

TA0001: Initial Access
- T1189: Drive-by Compromise
- T1190: Exploit Public-Facing Application
- T1133: External Remote Services
- T1200: Hardware Additions
- T1566: Phishing
  - T1566.001: Spearphishing Attachment
  - T1566.002: Spearphishing Link
  - T1566.003: Spearphishing via Service
- T1091: Replication Through Removable Media
- T1195: Supply Chain Compromise
- T1199: Trusted Relationship
- T1078: Valid Accounts

TA0002: Execution
- T1059: Command and Scripting Interpreter
  - T1059.002: AppleScript
  - T1059.007: JavaScript/JScript
  - T1059.008: Network Device CLI
  - T1059.001: PowerShell
  - T1059.006: Python
  - T1059.004: Unix Shell
  - T1059.005: Visual Basic
  - T1059.003: Windows Command Shell
- T1203: Exploitation for Client Execution
- T1559: Inter-Process Communication
  - T1559.001: Component Object Model
  - T1559.002: Dynamic Data Exchange
- T1106: Native API
- T1053: Scheduled Task/Job
  - T1053.001: At (Linux)
  - T1053.002: At (Windows)
  - T1053.003: Cron
  - T1053.004: Launchd
  - T1053.005: Scheduled Task
  - T1053.006: Systemd Timers
- T1129: Shared Modules
- T1072: Software Deployment Tools
- T1569: System Services
  - T1569.001: Launchctl
  - T1569.002: Service Execution
- T1204: User Execution
  - T1204.002: Malicious File
  - T1204.001: Malicious Link
- T1047: Windows Management Instrumentation

TA0003: Persistence
- T1098: Account Manipulation
- T1197: BITS Jobs
- T1547: Boot or Logon Autostart Execution
- T1037: Boot or Logon Initialization Scripts
- T1176: Browser Extensions
- T1554: Compromise Client Software Binary
- T1136: Create Account
  - T1136.003: Cloud Account
  - T1136.002: Domain Account
  - T1136.001: Local Account
- T1543: Create or Modify System Process
- T1546: Event Triggered Execution
  - T1546.004: .bash_profile and .bashrc
  - T1546.008: Accessibility Features
  - T1546.009: AppCert DLLs
  - T1546.010: AppInit DLLs
  - T1546.011: Application Shimming
  - T1546.001: Change Default File Association
  - T1546.015: Component Object Model Hijacking
  - T1546.014: Emond
  - T1546.012: Image File Execution Options Injection
  - T1546.006: LC_LOAD_DYLIB Addition
  - T1546.007: Netsh Helper DLL
  - T1546.013: PowerShell Profile
  - T1546.002: Screensaver
  - T1546.005: Trap
  - T1546.003: Windows Management Instrumentation Event Subscription
- T1133: External Remote Services
- T1574: Hijack Execution Flow
- T1137: Office Application Startup
  - T1137.006: Add-ins
  - T1137.001: Office Template Macros
  - T1137.002: Office Test
  - T1137.003: Outlook Forms
  - T1137.004: Outlook Home Page
  - T1137.005: Outlook Rules
- T1542: Pre-OS Boot
- T1053: Scheduled Task/Job
- T1505: Server Software Component
  - T1505.001: SQL Stored Procedures
  - T1505.002: Transport Agent
  - T1505.003: Web Shell
- T1205: Traffic Signaling
- T1078: Valid Accounts

TA0004: Privilege Escalation
- T1548: Abuse Elevation Control Mechanism
  - T1548.002: Bypass User Account Control
  - T1548.004: Elevated Execution with Prompt
  - T1548.001: Setuid and Setgid
  - T1548.003: Sudo and Sudo Caching
- T1134: Access Token Manipulation
- T1547: Boot or Logon Autostart Execution
  - T1547.002: Authentication Package
  - T1547.006: Kernel Modules and Extensions
  - T1547.008: LSASS Driver
  - T1547.011: Plist Modification
  - T1547.010: Port Monitors
  - T1547.012: Print Processors
  - T1547.007: Re-opened Applications
  - T1547.001: Registry Run Keys / Startup Folder
  - T1547.005: Security Support Provider
  - T1547.009: Shortcut Modification
  - T1547.003: Time Providers
  - T1547.004: Winlogon Helper DLL
- T1037: Boot or Logon Initialization Scripts
- T1543: Create or Modify System Process
  - T1543.001: Launch Agent
  - T1543.004: Launch Daemon
  - T1543.002: Systemd Service
  - T1543.003: Windows Service
- T1484: Domain Policy Modification
  - T1484.002: Domain Trust Modification
  - T1484.001: Group Policy Modification
- T1546: Event Triggered Execution
- T1068: Exploitation for Privilege Escalation
- T1574: Hijack Execution Flow
- T1055: Process Injection
  - T1055.004: Asynchronous Procedure Call
  - T1055.001: Dynamic-link Library Injection
  - T1055.011: Extra Window Memory Injection
  - T1055.002: Portable Executable Injection
  - T1055.009: Proc Memory
  - T1055.013: Process Doppelgänging
  - T1055.012: Process Hollowing
  - T1055.008: Ptrace System Calls
  - T1055.003: Thread Execution Hijacking
  - T1055.005: Thread Local Storage
  - T1055.014: VDSO Hijacking
- T1053: Scheduled Task/Job
- T1078: Valid Accounts
  - T1078.004: Cloud Accounts
  - T1078.001: Default Accounts
  - T1078.002: Domain Accounts
  - T1078.003: Local Accounts

TA0005: Defense Evasion
- T1548: Abuse Elevation Control Mechanism
- T1134: Access Token Manipulation
- T1197: BITS Jobs
- T1140: Deobfuscate/Decode Files or Information
- T1006: Direct Volume Access
- T1484: Domain Policy Modification
- T1480: Execution Guardrails
- T1211: Exploitation for Defense Evasion
- T1222: File and Directory Permissions Modification
  - T1222.002: Linux and Mac File and Dir. Permissions Modification
  - T1222.001: Windows File and Directory Permissions Modification
- T1564: Hide Artifacts
  - T1564.005: Hidden File System
  - T1564.001: Hidden Files and Directories
  - T1564.002: Hidden Users
  - T1564.003: Hidden Window
  - T1564.004: NTFS File Attributes
  - T1564.006: Run Virtual Instance
  - T1564.007: VBA Stomping
- T1574: Hijack Execution Flow
  - T1574.012: COR_PROFILER
  - T1574.001: DLL Search Order Hijacking
  - T1574.002: DLL Side-Loading
  - T1574.004: Dylib Hijacking
  - T1574.005: Executable Installer File Permissions Weakness
  - T1574.006: LD_PRELOAD
  - T1574.007: Path Interception by PATH Environment Variable
  - T1574.008: Path Interception by Search Order Hijacking
  - T1574.009: Path Interception by Unquoted Path
  - T1574.010: Services File Permissions Weakness
  - T1574.011: Services Registry Permissions Weakness
- T1562: Impair Defenses
  - T1562.004: Disable or Modify System Firewall
  - T1562.001: Disable or Modify Tools
  - T1562.002: Disable Windows Event Logging
  - T1562.003: Impair Command History Logging
  - T1562.006: Indicator Blocking
- T1070: Indicator Removal on Host
  - T1070.003: Clear Command History
  - T1070.002: Clear Linux or Mac System Logs
  - T1070.001: Clear Windows Event Logs
  - T1070.004: File Deletion
  - T1070.005: Network Share Connection Removal
  - T1070.006: Timestomp
- T1202: Indirect Command Execution
- T1036: Masquerading
  - T1036.001: Invalid Code Signature
  - T1036.004: Masquerade Task or Service
  - T1036.005: Match Legitimate Name or Location
  - T1036.003: Rename System Utilities
  - T1036.002: Right-to-Left Override
  - T1036.006: Space after Filename
- T1556: Modify Authentication Process
- T1112: Modify Registry
- T1601: Modify System Image
- T1599: Network Boundary Bridging
- T1027: Obfuscated Files or Information
  - T1027.001: Binary Padding
  - T1027.004: Compile After Delivery
  - T1027.005: Indicator Removal from Tools
  - T1027.002: Software Packing
  - T1027.003: Steganography
- T1542: Pre-OS Boot
- T1055: Process Injection
- T1207: Rogue Domain Controller
- T1014: Rootkit
- T1218: Signed Binary Proxy Execution
  - T1218.003: CMSTP
  - T1218.001: Compiled HTML File
  - T1218.002: Control Panel
  - T1218.004: InstallUtil
  - T1218.005: Mshta
  - T1218.007: Msiexec
  - T1218.008: Odbcconf
  - T1218.009: Regsvcs/Regasm
  - T1218.010: Regsvr32
  - T1218.011: Rundll32
  - T1218.012: Verclsid
- T1216: Signed Script Proxy Execution
- T1553: Subvert Trust Controls
  - T1553.002: Code Signing
  - T1553.001: Gatekeeper Bypass
  - T1553.004: Install Root Certificate
  - T1553.003: SIP and Trust Provider Hijacking
- T1205: Traffic Signaling
- T1127: Trusted Developer Utilities Proxy Execution
  - T1127.001: MSBuild
- T1550: Use Alternate Authentication Material
- T1078: Valid Accounts
- T1497: Virtualization/Sandbox Evasion
- T1600: Weaken Encryption
- T1220: XSL Script Processing

TA0006: Credential Access
- T1110: Brute Force
  - T1110.004: Credential Stuffing
  - T1110.002: Password Cracking
  - T1110.001: Password Guessing
  - T1110.003: Password Spraying
- T1555: Credentials from Password Stores
  - T1555.003: Credentials from Web Browsers
  - T1555.001: Keychain
  - T1555.002: Securityd Memory
- T1212: Exploitation for Credential Access
- T1187: Forced Authentication
- T1606: Forge Web Credentials
- T1056: Input Capture
  - T1056.004: Credential API Hooking
  - T1056.002: GUI Input Capture
  - T1056.001: Keylogging
  - T1056.003: Web Portal Capture
- T1557: Man-in-the-Middle
- T1556: Modify Authentication Process
- T1040: Network Sniffing
- T1003: OS Credential Dumping
  - T1003.008: /etc/passwd and /etc/shadow
  - T1003.005: Cached Domain Credentials
  - T1003.006: DCSync
  - T1003.004: LSA Secrets
  - T1003.001: LSASS Memory
  - T1003.003: NTDS
  - T1003.007: Proc Filesystem
  - T1003.002: Security Account Manager
- T1528: Steal Application Access Token
- T1558: Steal or Forge Kerberos Tickets
- T1539: Steal Web Session Cookie
- T1111: Two-Factor Authentication Interception
- T1552: Unsecured Credentials
  - T1552.003: Bash History
  - T1552.001: Credentials In Files
  - T1552.002: Credentials in Registry
  - T1552.006: Group Policy Preferences
  - T1552.004: Private Keys

TA0007: Discovery
- T1087: Account Discovery
  - T1087.002: Domain Account
  - T1087.003: Email Account
  - T1087.001: Local Account
- T1010: Application Window Discovery
- T1217: Browser Bookmark Discovery
- T1538: Cloud Service Dashboard
- T1526: Cloud Service Discovery
- T1482: Domain Trust Discovery
- T1083: File and Directory Discovery
- T1046: Network Service Scanning
- T1135: Network Share Discovery
- T1040: Network Sniffing
- T1201: Password Policy Discovery
- T1120: Peripheral Device Discovery
- T1069: Permission Groups Discovery
  - T1069.003: Cloud Groups
  - T1069.002: Domain Groups
  - T1069.001: Local Groups
- T1057: Process Discovery
- T1012: Query Registry
- T1018: Remote System Discovery
- T1518: Software Discovery
  - T1518.001: Security Software Discovery
- T1082: System Information Discovery
- T1016: System Network Configuration Discovery
- T1049: System Network Connections Discovery
- T1033: System Owner/User Discovery
- T1007: System Service Discovery
- T1124: System Time Discovery
- T1497: Virtualization/Sandbox Evasion

TA0008: Lateral Movement
- T1210: Exploitation of Remote Services
- T1534: Internal Spearphishing
- T1570: Lateral Tool Transfer
- T1563: Remote Service Session Hijacking
- T1021: Remote Services
  - T1021.003: Distributed Component Object Model
  - T1021.001: Remote Desktop Protocol
  - T1021.002: SMB/Windows Admin Shares
  - T1021.004: SSH
  - T1021.005: VNC
  - T1021.006: Windows Remote Management
- T1091: Replication Through Removable Media
- T1072: Software Deployment Tools
- T1080: Taint Shared Content
- T1550: Use Alternate Authentication Material
  - T1550.001: Application Access Token
  - T1550.002: Pass the Hash
  - T1550.003: Pass the Ticket
  - T1550.004: Web Session Cookie

TA0009: Collection
- T1560: Archive Collected Data
  - T1560.003: Archive via Custom Method
  - T1560.002: Archive via Library
  - T1560.001: Archive via Utility
- T1123: Audio Capture
- T1119: Automated Collection
- T1115: Clipboard Data
- T1602: Data from Configuration Repository
- T1213: Data from Information Repositories
- T1005: Data from Local System
- T1039: Data from Network Shared Drive
- T1025: Data from Removable Media
- T1074: Data Staged
  - T1074.001: Local Data Staging
  - T1074.002: Remote Data Staging
- T1114: Email Collection
  - T1114.003: Email Forwarding Rule
  - T1114.001: Local Email Collection
  - T1114.002: Remote Email Collection
- T1056: Input Capture
- T1185: Man in the Browser
- T1557: Man-in-the-Middle
- T1113: Screen Capture
- T1125: Video Capture

TA0011: Command and Control
- T1071: Application Layer Protocol
  - T1071.004: DNS
  - T1071.002: File Transfer Protocols
  - T1071.003: Mail Protocols
  - T1071.001: Web Protocols
- T1092: Communication Through Removable Media
- T1132: Data Encoding
  - T1132.002: Non-Standard Encoding
  - T1132.001: Standard Encoding
- T1001: Data Obfuscation
- T1568: Dynamic Resolution
  - T1568.003: DNS Calculation
  - T1568.002: Domain Generation Algorithms
  - T1568.001: Fast Flux DNS
- T1573: Encrypted Channel
  - T1573.002: Asymmetric Cryptography
  - T1573.001: Symmetric Cryptography
- T1008: Fallback Channels
- T1105: Ingress Tool Transfer
- T1104: Multi-Stage Channels
- T1095: Non-Application Layer Protocol
- T1571: Non-Standard Port
- T1572: Protocol Tunneling
- T1090: Proxy
  - T1090.004: Domain Fronting
  - T1090.002: External Proxy
  - T1090.001: Internal Proxy
  - T1090.003: Multi-hop Proxy
- T1219: Remote Access Software
- T1205: Traffic Signaling
- T1102: Web Service
  - T1102.002: Bidirectional Communication
  - T1102.001: Dead Drop Resolver
  - T1102.003: One-Way Communication

TA0010: Exfiltration
- T1020: Automated Exfiltration
- T1030: Data Transfer Size Limits
- T1048: Exfiltration Over Alternative Protocol
  - T1048.002: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
  - T1048.001: Exfiltration Over Symmetric Encrypted Non-C2 Protocol
  - T1048.003: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
- T1041: Exfiltration Over C2 Channel
- T1011: Exfiltration Over Other Network Medium
- T1052: Exfiltration Over Physical Medium
- T1567: Exfiltration Over Web Service
  - T1567.002: Exfiltration to Cloud Storage
  - T1567.001: Exfiltration to Code Repository
- T1029: Scheduled Transfer

TA0040: Impact
- T1531: Account Access Removal
- T1485: Data Destruction
- T1486: Data Encrypted for Impact
- T1565: Data Manipulation
- T1491: Defacement
- T1561: Disk Wipe
- T1499: Endpoint Denial of Service
- T1495: Firmware Corruption
- T1490: Inhibit System Recovery
- T1498: Network Denial of Service
- T1496: Resource Hijacking
- T1489: Service Stop
- T1529: System Shutdown/Reboot

1 Linux® is a registered trademark of Linus Torvalds; macOS® is a registered trademark of Apple, Inc.; Windows®, Office 365® and Azure® are registered trademarks of Microsoft Corporation

Ransomware

Domain: Enterprise ATT&CK v8

Platforms: Linux®, macOS®, Windows®, Office 365®, Azure® AD, IaaS, SaaS, PRE, Network

TA0043: Reconnaissance
- T1595: Active Scanning
- T1592: Gather Victim Host Information
  - T1592.004: Client Configurations
  - T1592.003: Firmware
  - T1592.001: Hardware
  - T1592.002: Software
- T1589: Gather Victim Identity Information
  - T1589.001: Credentials
  - T1589.002: Email Addresses
  - T1589.003: Employee Names
- T1590: Gather Victim Network Information
- T1591: Gather Victim Org Information
- T1598: Phishing for Information
  - T1598.002: Spearphishing Attachment
  - T1598.003: Spearphishing Link
  - T1598.001: Spearphishing Service
- T1597: Search Closed Sources
- T1596: Search Open Technical Databases
- T1593: Search Open Websites/Domains
- T1594: Search Victim-Owned Websites

TA0042: Resource Development
- T1583: Acquire Infrastructure
  - T1583.005: Botnet
  - T1583.002: DNS Server
  - T1583.001: Domains
  - T1583.004: Server
  - T1583.003: Virtual Private Server
  - T1583.006: Web Services
- T1586: Compromise Accounts
- T1584: Compromise Infrastructure
- T1587: Develop Capabilities
  - T1587.002: Code Signing Certificates
  - T1587.003: Digital Certificates
  - T1587.004: Exploits
  - T1587.001: Malware
- T1585: Establish Accounts
- T1588: Obtain Capabilities
  - T1588.003: Code Signing Certificates
  - T1588.004: Digital Certificates
  - T1588.005: Exploits
  - T1588.001: Malware
  - T1588.002: Tool
  - T1588.006: Vulnerabilities

TA0001: Initial Access
- T1189: Drive-by Compromise
- T1190: Exploit Public-Facing Application
- T1133: External Remote Services
- T1200: Hardware Additions
- T1566: Phishing
  - T1566.001: Spearphishing Attachment
  - T1566.002: Spearphishing Link
  - T1566.003: Spearphishing via Service
- T1091: Replication Through Removable Media
- T1195: Supply Chain Compromise
  - T1195.003: Compromise Hardware Supply Chain
  - T1195.001: Compromise Software Dependencies and Development Tools
  - T1195.002: Compromise Software Supply Chain
- T1199: Trusted Relationship
- T1078: Valid Accounts
  - T1078.004: Cloud Accounts
  - T1078.001: Default Accounts
  - T1078.002: Domain Accounts
  - T1078.003: Local Accounts

TA0002: Execution
- T1059: Command and Scripting Interpreter
  - T1059.002: AppleScript
  - T1059.007: JavaScript/JScript
  - T1059.008: Network Device CLI
  - T1059.001: PowerShell
  - T1059.006: Python
  - T1059.004: Unix Shell
  - T1059.005: Visual Basic
  - T1059.003: Windows Command Shell
- T1203: Exploitation for Client Execution
- T1559: Inter-Process Communication
- T1106: Native API
- T1053: Scheduled Task/Job
- T1129: Shared Modules
- T1072: Software Deployment Tools
- T1569: System Services
  - T1569.001: Launchctl
  - T1569.002: Service Execution
- T1204: User Execution
  - T1204.002: Malicious File
  - T1204.001: Malicious Link
- T1047: Windows Management Instrumentation

TA0003: Persistence
- T1098: Account Manipulation
- T1197: BITS Jobs
- T1547: Boot or Logon Autostart Execution
- T1037: Boot or Logon Initialization Scripts
  - T1037.002: Logon Script (Mac)
  - T1037.001: Logon Script (Windows)
  - T1037.003: Network Logon Script
  - T1037.004: Rc.common
  - T1037.005: Startup Items
- T1176: Browser Extensions
- T1554: Compromise Client Software Binary
- T1136: Create Account
- T1543: Create or Modify System Process
- T1546: Event Triggered Execution
- T1133: External Remote Services
- T1574: Hijack Execution Flow
- T1137: Office Application Startup
  - T1137.006: Add-ins
  - T1137.001: Office Template Macros
  - T1137.002: Office Test
  - T1137.003: Outlook Forms
  - T1137.004: Outlook Home Page
  - T1137.005: Outlook Rules
- T1542: Pre-OS Boot
- T1053: Scheduled Task/Job
- T1505: Server Software Component
  - T1505.001: SQL Stored Procedures
  - T1505.002: Transport Agent
  - T1505.003: Web Shell
- T1205: Traffic Signaling
- T1078: Valid Accounts

TA0004: Privilege Escalation
- T1548: Abuse Elevation Control Mechanism
  - T1548.002: Bypass User Account Control
  - T1548.004: Elevated Execution with Prompt
  - T1548.001: Setuid and Setgid
  - T1548.003: Sudo and Sudo Caching
- T1134: Access Token Manipulation
  - T1134.002: Create Process with Token
  - T1134.003: Make and Impersonate Token
  - T1134.004: Parent PID Spoofing
  - T1134.005: SID-History Injection
  - T1134.001: Token Impersonation/Theft
- T1547: Boot or Logon Autostart Execution
  - T1547.002: Authentication Package
  - T1547.006: Kernel Modules and Extensions
  - T1547.008: LSASS Driver
  - T1547.011: Plist Modification
  - T1547.010: Port Monitors
  - T1547.012: Print Processors
  - T1547.007: Re-opened Applications
  - T1547.001: Registry Run Keys / Startup Folder
  - T1547.005: Security Support Provider
  - T1547.009: Shortcut Modification
  - T1547.003: Time Providers
  - T1547.004: Winlogon Helper DLL
- T1037: Boot or Logon Initialization Scripts
- T1543: Create or Modify System Process
  - T1543.001: Launch Agent
  - T1543.004: Launch Daemon
  - T1543.002: Systemd Service
  - T1543.003: Windows Service
- T1484: Domain Policy Modification
- T1546: Event Triggered Execution
  - T1546.004: .bash_profile and .bashrc
  - T1546.008: Accessibility Features
  - T1546.009: AppCert DLLs
  - T1546.010: AppInit DLLs
  - T1546.011: Application Shimming
  - T1546.001: Change Default File Association
  - T1546.015: Component Object Model Hijacking
  - T1546.014: Emond
  - T1546.012: Image File Execution Options Injection
  - T1546.006: LC_LOAD_DYLIB Addition
  - T1546.007: Netsh Helper DLL
  - T1546.013: PowerShell Profile
  - T1546.002: Screensaver
  - T1546.005: Trap
  - T1546.003: Windows Management Instrumentation Event Subscription
- T1068: Exploitation for Privilege Escalation
- T1574: Hijack Execution Flow
- T1055: Process Injection
  - T1055.004: Asynchronous Procedure Call
  - T1055.001: Dynamic-link Library Injection
  - T1055.011: Extra Window Memory Injection
  - T1055.002: Portable Executable Injection
  - T1055.009: Proc Memory
  - T1055.013: Process Doppelgänging
  - T1055.012: Process Hollowing
  - T1055.008: Ptrace System Calls
  - T1055.003: Thread Execution Hijacking
  - T1055.005: Thread Local Storage
  - T1055.014: VDSO Hijacking
- T1053: Scheduled Task/Job
  - T1053.001: At (Linux)
  - T1053.002: At (Windows)
  - T1053.003: Cron
  - T1053.004: Launchd
  - T1053.005: Scheduled Task
  - T1053.006: Systemd Timers
- T1078: Valid Accounts

TA0005: Defense Evasion
- T1548: Abuse Elevation Control Mechanism
- T1134: Access Token Manipulation
  - T1134.002: Create Process with Token
  - T1134.003: Make and Impersonate Token
  - T1134.004: Parent PID Spoofing
  - T1134.005: SID-History Injection
  - T1134.001: Token Impersonation/Theft
- T1197: BITS Jobs
- T1140: Deobfuscate/Decode Files or Information
- T1006: Direct Volume Access
- T1484: Domain Policy Modification
  - T1484.002: Domain Trust Modification
  - T1484.001: Group Policy Modification
- T1480: Execution Guardrails
- T1211: Exploitation for Defense Evasion
- T1222: File and Directory Permissions Modification
- T1564: Hide Artifacts
  - T1564.005: Hidden File System
  - T1564.001: Hidden Files and Directories
  - T1564.002: Hidden Users
  - T1564.003: Hidden Window
  - T1564.004: NTFS File Attributes
  - T1564.006: Run Virtual Instance
  - T1564.007: VBA Stomping
- T1574: Hijack Execution Flow
  - T1574.012: COR_PROFILER
  - T1574.001: DLL Search Order Hijacking
  - T1574.002: DLL Side-Loading
  - T1574.004: Dylib Hijacking
  - T1574.005: Executable Installer File Permissions Weakness
  - T1574.006: LD_PRELOAD
  - T1574.007: Path Interception by PATH Environment Variable
  - T1574.008: Path Interception by Search Order Hijacking
  - T1574.009: Path Interception by Unquoted Path
  - T1574.010: Services File Permissions Weakness
  - T1574.011: Services Registry Permissions Weakness
- T1562: Impair Defenses
  - T1562.004: Disable or Modify System Firewall
  - T1562.001: Disable or Modify Tools
  - T1562.002: Disable Windows Event Logging
  - T1562.003: Impair Command History Logging
  - T1562.006: Indicator Blocking
- T1070: Indicator Removal on Host
  - T1070.003: Clear Command History
  - T1070.002: Clear Linux or Mac System Logs
  - T1070.001: Clear Windows Event Logs
  - T1070.004: File Deletion
  - T1070.005: Network Share Connection Removal
  - T1070.006: Timestomp
- T1202: Indirect Command Execution
- T1036: Masquerading
  - T1036.001: Invalid Code Signature
  - T1036.004: Masquerade Task or Service
  - T1036.005: Match Legitimate Name or Location
  - T1036.003: Rename System Utilities
  - T1036.002: Right-to-Left Override
  - T1036.006: Space after Filename
- T1556: Modify Authentication Process
  - T1556.001: Domain Controller Authentication
  - T1556.004: Network Device Authentication
  - T1556.002: Password Filter DLL
  - T1556.003: Pluggable Authentication Modules
- T1112: Modify Registry
- T1601: Modify System Image
- T1599: Network Boundary Bridging
- T1027: Obfuscated Files or Information
  - T1027.001: Binary Padding
  - T1027.004: Compile After Delivery
  - T1027.005: Indicator Removal from Tools
  - T1027.002: Software Packing
  - T1027.003: Steganography
- T1542: Pre-OS Boot
- T1055: Process Injection
- T1207: Rogue Domain Controller
- T1014: Rootkit
- T1218: Signed Binary Proxy Execution
  - T1218.003: CMSTP
  - T1218.001: Compiled HTML File
  - T1218.002: Control Panel
  - T1218.004: InstallUtil
  - T1218.005: Mshta
  - T1218.007: Msiexec
  - T1218.008: Odbcconf
  - T1218.009: Regsvcs/Regasm
  - T1218.010: Regsvr32
  - T1218.011: Rundll32
  - T1218.012: Verclsid
- T1216: Signed Script Proxy Execution
- T1553: Subvert Trust Controls
  - T1553.002: Code Signing
  - T1553.001: Gatekeeper Bypass
  - T1553.004: Install Root Certificate
  - T1553.003: SIP and Trust Provider Hijacking
- T1221: Template Injection
- T1205: Traffic Signaling
- T1127: Trusted Developer Utilities Proxy Execution
  - T1127.001: MSBuild
- T1550: Use Alternate Authentication Material
  - T1550.001: Application Access Token
  - T1550.002: Pass the Hash
  - T1550.003: Pass the Ticket
  - T1550.004: Web Session Cookie
- T1078: Valid Accounts
- T1497: Virtualization/Sandbox Evasion
  - T1497.001: System Checks
  - T1497.003: Time Based Evasion
  - T1497.002: User Activity Based Checks
- T1600: Weaken Encryption
  - T1600.002: Disable Crypto Hardware
  - T1600.001: Reduce Key Space
- T1220: XSL Script Processing

TA0006: Credential Access
- T1110: Brute Force
  - T1110.004: Credential Stuffing
  - T1110.002: Password Cracking
  - T1110.001: Password Guessing
  - T1110.003: Password Spraying
- T1555: Credentials from Password Stores
  - T1555.003: Credentials from Web Browsers
  - T1555.001: Keychain
  - T1555.002: Securityd Memory
- T1212: Exploitation for Credential Access
- T1187: Forced Authentication
- T1606: Forge Web Credentials
- T1056: Input Capture
  - T1056.004: Credential API Hooking
  - T1056.002: GUI Input Capture
  - T1056.001: Keylogging
  - T1056.003: Web Portal Capture
- T1557: Man-in-the-Middle
  - T1557.002: ARP Cache Poisoning
  - T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay
- T1556: Modify Authentication Process
- T1040: Network Sniffing
- T1003: OS Credential Dumping
  - T1003.008: /etc/passwd and /etc/shadow
  - T1003.005: Cached Domain Credentials
  - T1003.006: DCSync
  - T1003.004: LSA Secrets
  - T1003.001: LSASS Memory
  - T1003.003: NTDS
  - T1003.007: Proc Filesystem
  - T1003.002: Security Account Manager
- T1528: Steal Application Access Token
- T1558: Steal or Forge Kerberos Tickets
- T1539: Steal Web Session Cookie
- T1111: Two-Factor Authentication Interception
- T1552: Unsecured Credentials
  - T1552.003: Bash History
  - T1552.001: Credentials In Files
  - T1552.002: Credentials in Registry
  - T1552.006: Group Policy Preferences
  - T1552.004: Private Keys

TA0007: Discovery
- T1087: Account Discovery
- T1010: Application Window Discovery
- T1217: Browser Bookmark Discovery
- T1538: Cloud Service Dashboard
- T1526: Cloud Service Discovery
- T1482: Domain Trust Discovery
- T1083: File and Directory Discovery
- T1046: Network Service Scanning
- T1135: Network Share Discovery
- T1040: Network Sniffing
- T1201: Password Policy Discovery
- T1120: Peripheral Device Discovery
- T1069: Permission Groups Discovery
  - T1069.003: Cloud Groups
  - T1069.002: Domain Groups
  - T1069.001: Local Groups
- T1057: Process Discovery
- T1012: Query Registry
- T1018: Remote System Discovery
- T1518: Software Discovery
  - T1518.001: Security Software Discovery
- T1082: System Information Discovery
- T1016: System Network Configuration Discovery
- T1049: System Network Connections Discovery
- T1033: System Owner/User Discovery
- T1007: System Service Discovery
- T1124: System Time Discovery
- T1497: Virtualization/Sandbox Evasion

TA0008: Lateral Movement
- T1210: Exploitation of Remote Services
- T1534: Internal Spearphishing
- T1570: Lateral Tool Transfer
- T1563: Remote Service Session Hijacking
  - T1563.002: RDP Hijacking
  - T1563.001: SSH Hijacking
- T1021: Remote Services
  - T1021.003: Distributed Component Object Model
  - T1021.001: Remote Desktop Protocol
  - T1021.002: SMB/Windows Admin Shares
  - T1021.004: SSH
  - T1021.005: VNC
  - T1021.006: Windows Remote Management
- T1091: Replication Through Removable Media
- T1072: Software Deployment Tools
- T1080: Taint Shared Content
- T1550: Use Alternate Authentication Material

TA0009: Collection
- T1560: Archive Collected Data
  - T1560.003: Archive via Custom Method
  - T1560.002: Archive via Library
  - T1560.001: Archive via Utility
- T1123: Audio Capture
- T1119: Automated Collection
- T1115: Clipboard Data
- T1602: Data from Configuration Repository
- T1213: Data from Information Repositories
  - T1213.001: Confluence
  - T1213.002: Sharepoint
- T1005: Data from Local System
- T1039: Data from Network Shared Drive
- T1025: Data from Removable Media
- T1074: Data Staged
- T1114: Email Collection
  - T1114.003: Email Forwarding Rule
  - T1114.001: Local Email Collection
  - T1114.002: Remote Email Collection
- T1056: Input Capture
- T1185: Man in the Browser
- T1557: Man-in-the-Middle
- T1113: Screen Capture
- T1125: Video Capture

TA0011: Command and Control
- T1071: Application Layer Protocol
  - T1071.004: DNS
  - T1071.002: File Transfer Protocols
  - T1071.003: Mail Protocols
  - T1071.001: Web Protocols
- T1092: Communication Through Removable Media
- T1132: Data Encoding
  - T1132.002: Non-Standard Encoding
  - T1132.001: Standard Encoding
- T1001: Data Obfuscation
  - T1001.001: Junk Data
  - T1001.003: Protocol Impersonation
  - T1001.002: Steganography
- T1568: Dynamic Resolution
- T1573: Encrypted Channel
  - T1573.002: Asymmetric Cryptography
  - T1573.001: Symmetric Cryptography
- T1008: Fallback Channels
- T1105: Ingress Tool Transfer
- T1104: Multi-Stage Channels
- T1095: Non-Application Layer Protocol
- T1571: Non-Standard Port
- T1572: Protocol Tunneling
- T1090: Proxy
  - T1090.004: Domain Fronting
  - T1090.002: External Proxy
  - T1090.001: Internal Proxy
  - T1090.003: Multi-hop Proxy
- T1219: Remote Access Software
- T1205: Traffic Signaling
- T1102: Web Service

TA0010: Exfiltration
- T1020: Automated Exfiltration
- T1030: Data Transfer Size Limits
- T1048: Exfiltration Over Alternative Protocol
- T1041: Exfiltration Over C2 Channel
- T1011: Exfiltration Over Other Network Medium
- T1052: Exfiltration Over Physical Medium
- T1567: Exfiltration Over Web Service
  - T1567.002: Exfiltration to Cloud Storage
  - T1567.001: Exfiltration to Code Repository
- T1029: Scheduled Transfer

TA0040: Impact
- T1531: Account Access Removal
- T1485: Data Destruction
- T1486: Data Encrypted for Impact
- T1565: Data Manipulation
- T1491: Defacement
- T1561: Disk Wipe
- T1499: Endpoint Denial of Service
- T1495: Firmware Corruption
- T1490: Inhibit System Recovery
- T1498: Network Denial of Service
- T1496: Resource Hijacking
- T1489: Service Stop
- T1529: System Shutdown/Reboot

Web Application Hacking

Domain: Enterprise ATT&CK v8

Platforms: Linux®, macOS®, Windows®, Office 365®, Azure® AD, IaaS, SaaS, PRE, Network

TA0043: Reconnaissance
- **T1595: Active Scanning**
  - T1595.001: Scanning IP Blocks
  - T1595.002: Vulnerability Scanning
- **T1592: Gather Victim Host Information**
- **T1589: Gather Victim Identity Information**
- **T1590: Gather Victim Network Information**
- **T1591: Gather Victim Org Information**
- **T1598: Phishing for Information**
- **T1597: Search Closed Sources**
- **T1596: Search Open Technical Databases**
  - T1596.004: CDNs
  - T1596.003: Digital Certificates
  - T1596.001: DNS/Passive DNS
  - T1596.005: Scan Databases
  - T1596.002: WHOIS
- **T1593: Search Open Websites/Domains**
- **T1594: Search Victim-Owned Websites**

TA0042: Resource Development
- **T1583: Acquire Infrastructure**
  - T1583.005: Botnet
  - T1583.002: DNS Server
  - T1583.001: Domains
  - T1583.004: Server
  - T1583.003: Virtual Private Server
  - T1583.006: Web Services
- **T1586: Compromise Accounts**
- **T1584: Compromise Infrastructure**
  - T1584.005: Botnet
  - T1584.002: DNS Server
  - T1584.001: Domains
  - T1584.004: Server
  - T1584.003: Virtual Private Server
  - T1584.006: Web Services
- **T1587: Develop Capabilities**
- **T1585: Establish Accounts**
- **T1588: Obtain Capabilities**

TA0001: Initial Access
- **T1189: Drive-by Compromise**
- **T1190: Exploit Public-Facing Application**
- **T1133: External Remote Services**
- **T1200: Hardware Additions**
- **T1566: Phishing**
- **T1091: Replication Through Removable Media**
- **T1195: Supply Chain Compromise**
- **T1199: Trusted Relationship**
- **T1078: Valid Accounts**
  - T1078.004: Cloud Accounts
  - T1078.001: Default Accounts
  - T1078.002: Domain Accounts
  - T1078.003: Local Accounts

TA0002: Execution
- **T1059: Command and Scripting Interpreter**
  - T1059.002: AppleScript
  - T1059.007: JavaScript/JScript
  - T1059.008: Network Device CLI
  - T1059.001: PowerShell
  - T1059.006: Python
  - T1059.004: Unix Shell
  - T1059.005: Visual Basic
  - T1059.003: Windows Command Shell
- **T1203: Exploitation for Client Execution**
- **T1559: Inter-Process Communication**
  - T1559.001: Component Object Model
  - T1559.002: Dynamic Data Exchange
- **T1106: Native API**
- **T1053: Scheduled Task/Job**
- **T1129: Shared Modules**
- **T1072: Software Deployment Tools**
- **T1569: System Services**
  - T1569.001: Launchctl
  - T1569.002: Service Execution
- **T1204: User Execution**
- **T1047: Windows Management Instrumentation**

TA0003: Persistence
- **T1098: Account Manipulation**
- **T1197: BITS Jobs**
- **T1547: Boot or Logon Autostart Execution**
- **T1037: Boot or Logon Initialization Scripts**
  - T1037.002: Logon Script (Mac)
  - T1037.001: Logon Script (Windows)
  - T1037.003: Network Logon Script
  - T1037.004: Rc.common
  - T1037.005: Startup Items
- **T1176: Browser Extensions**
- **T1554: Compromise Client Software Binary**
- **T1136: Create Account**
- **T1543: Create or Modify System Process**
- **T1546: Event Triggered Execution**
- **T1133: External Remote Services**
- **T1574: Hijack Execution Flow**
- **T1525: Implant Container Image**
- **T1137: Office Application Startup**
- **T1542: Pre-OS Boot**
- **T1053: Scheduled Task/Job**
- **T1505: Server Software Component**
  - T1505.001: SQL Stored Procedures
  - T1505.002: Transport Agent
  - T1505.003: Web Shell
- **T1205: Traffic Signaling**
  - T1205.001: Port Knocking
- **T1078: Valid Accounts**

TA0004: Privilege Escalation
- **T1548: Abuse Elevation Control Mechanism**
  - T1548.002: Bypass User Account Control
  - T1548.004: Elevated Execution with Prompt
  - T1548.001: Setuid and Setgid
  - T1548.003: Sudo and Sudo Caching
- **T1134: Access Token Manipulation**
  - T1134.002: Create Process with Token
  - T1134.003: Make and Impersonate Token
  - T1134.004: Parent PID Spoofing
  - T1134.005: SID-History Injection
  - T1134.001: Token Impersonation/Theft
- **T1547: Boot or Logon Autostart Execution**
  - T1547.002: Authentication Package
  - T1547.006: Kernel Modules and Extensions
  - T1547.008: LSASS Driver
  - T1547.011: Plist Modification
  - T1547.010: Port Monitors
  - T1547.012: Print Processors
  - T1547.007: Re-opened Applications
  - T1547.001: Registry Run Keys / Startup Folder
  - T1547.005: Security Support Provider
  - T1547.009: Shortcut Modification
  - T1547.003: Time Providers
  - T1547.004: Winlogon Helper DLL
- **T1037: Boot or Logon Initialization Scripts**
- **T1543: Create or Modify System Process**
  - T1543.001: Launch Agent
  - T1543.004: Launch Daemon
  - T1543.002: Systemd Service
  - T1543.003: Windows Service
- **T1484: Domain Policy Modification**
- **T1546: Event Triggered Execution**
  - T1546.004: .bash_profile and .bashrc
  - T1546.008: Accessibility Features
  - T1546.009: AppCert DLLs
  - T1546.010: AppInit DLLs
  - T1546.011: Application Shimming
  - T1546.001: Change Default File Association
  - T1546.015: Component Object Model Hijacking
  - T1546.014: Emond
  - T1546.012: Image File Execution Options Injection
  - T1546.006: LC_LOAD_DYLIB Addition
  - T1546.007: Netsh Helper DLL
  - T1546.013: PowerShell Profile
  - T1546.002: Screensaver
  - T1546.005: Trap
  - T1546.003: Windows Management Instrumentation Event Subscription
- **T1068: Exploitation for Privilege Escalation**
- **T1574: Hijack Execution Flow**
- **T1055: Process Injection**
  - T1055.004: Asynchronous Procedure Call
  - T1055.001: Dynamic-link Library Injection
  - T1055.011: Extra Window Memory Injection
  - T1055.002: Portable Executable Injection
  - T1055.009: Proc Memory
  - T1055.013: Process Doppelgänging
  - T1055.012: Process Hollowing
  - T1055.008: Ptrace System Calls
  - T1055.003: Thread Execution Hijacking
  - T1055.005: Thread Local Storage
  - T1055.014: VDSO Hijacking
- **T1053: Scheduled Task/Job**
  - T1053.001: At (Linux)
  - T1053.002: At (Windows)
  - T1053.003: Cron
  - T1053.004: Launchd
  - T1053.005: Scheduled Task
  - T1053.006: Systemd Timers
- **T1078: Valid Accounts**

TA0005: Defense Evasion
- **T1548: Abuse Elevation Control Mechanism**
  - T1134: Access Token Manipulation
  - T1197: BITS Jobs
- **T1140: Deobfuscate/Decode Files or Information**
- **T1006: Direct Volume Access**
- **T1484: Domain Policy Modification**
- **T1480: Execution Guardrails**
- **T1211: Exploitation for Defense Evasion**
- **T1222: File and Directory Permissions Modification**
- **T1564: Hide Artifacts**
- **T1574: Hijack Execution Flow**
  - T1574.012: COR_PROFILER
  - T1574.001: DLL Search Order Hijacking
  - T1574.002: DLL Side-Loading
  - T1574.004: Dylib Hijacking
  - T1574.005: Executable Installer File Permissions Weakness
  - T1574.006: LD_PRELOAD
  - T1574.007: Path Interception by PATH Environment Variable
  - T1574.008: Path Interception by Search Order Hijacking
  - T1574.009: Path Interception by Unquoted Path
  - T1574.010: Services File Permissions Weakness
  - T1574.011: Services Registry Permissions Weakness
- **T1562: Impair Defenses**
- **T1070: Indicator Removal on Host**
- **T1202: Indirect Command Execution**
- **T1036: Masquerading**
  - T1036.001: Invalid Code Signature
  - T1036.004: Masquerade Task or Service
  - T1036.005: Match Legitimate Name or Location
  - T1036.003: Rename System Utilities
  - T1036.002: Right-to-Left Override
  - T1036.006: Space after Filename
- **T1556: Modify Authentication Process**
- **T1578: Modify Cloud Compute Infrastructure**
- **T1112: Modify Registry**
- **T1601: Modify System Image**
- **T1599: Network Boundary Bridging**
- **T1027: Obfuscated Files or Information**
- **T1542: Pre-OS Boot**
  - T1542.003: Bootkit
  - T1542.002: Component Firmware
  - T1542.004: ROMMONkit
  - T1542.001: System Firmware
  - T1542.005: TFTP Boot
- **T1055: Process Injection**
- **T1207: Rogue Domain Controller**
- **T1014: Rootkit**
- **T1218: Signed Binary Proxy Execution**
  - T1218.003: CMSTP
  - T1218.001: Compiled HTML File
  - T1218.002: Control Panel
  - T1218.004: InstallUtil
  - T1218.005: Mshta
  - T1218.007: Msiexec
  - T1218.008: Odbcconf
  - T1218.009: Regsvcs/Regasm
  - T1218.010: Regsvr32
  - T1218.011: Rundll32
  - T1218.012: Verclsid
- **T1216: Signed Script Proxy Execution**
- **T1553: Subvert Trust Controls**
  - T1553.002: Code Signing
  - T1553.001: Gatekeeper Bypass
  - T1553.004: Install Root Certificate
  - T1553.003: SIP and Trust Provider Hijacking
- **T1221: Template Injection**
- **T1205: Traffic Signaling**
- **T1127: Trusted Developer Utilities Proxy Execution**
- **T1535: Unused/Unsupported Cloud Regions**
- **T1550: Use Alternate Authentication Material**
  - T1550.001: Application Access Token
  - T1550.002: Pass the Hash
  - T1550.003: Pass the Ticket
  - T1550.004: Web Session Cookie
- **T1078: Valid Accounts**
- **T1497: Virtualization/Sandbox Evasion**
- **T1600: Weaken Encryption**
- **T1220: XSL Script Processing**

TA0006: Credential Access
- **T1110: Brute Force**
  - T1110.004: Credential Stuffing
  - T1110.002: Password Cracking
  - T1110.001: Password Guessing
  - T1110.003: Password Spraying
- **T1555: Credentials from Password Stores**
  - T1555.003: Credentials from Web Browsers
  - T1555.001: Keychain
  - T1555.002: Securityd Memory
- **T1212: Exploitation for Credential Access**
- **T1187: Forced Authentication**
- **T1606: Forge Web Credentials**
  - T1606.002: SAML Tokens
  - T1606.001: Web Cookies
- **T1056: Input Capture**
  - T1056.004: Credential API Hooking
  - T1056.002: GUI Input Capture
  - T1056.001: Keylogging
  - T1056.003: Web Portal Capture
- **T1557: Man-in-the-Middle**
- **T1556: Modify Authentication Process**
- **T1040: Network Sniffing**
- **T1003: OS Credential Dumping**
- **T1528: Steal Application Access Token**
- **T1558: Steal or Forge Kerberos Tickets**
  - T1558.004: AS-REP Roasting
  - T1558.001: Golden Ticket
  - T1558.003: Kerberoasting
  - T1558.002: Silver Ticket
- **T1539: Steal Web Session Cookie**
- **T1111: Two-Factor Authentication Interception**
- **T1552: Unsecured Credentials**
  - T1552.003: Bash History
  - T1552.005: Cloud Instance Metadata API
  - T1552.001: Credentials In Files
  - T1552.002: Credentials in Registry
  - T1552.006: Group Policy Preferences
  - T1552.004: Private Keys

TA0006: Credential Access
- **T1110: Brute Force**
  - T1110.004: Credential Stuffing
  - T1110.002: Password Cracking
  - T1110.001: Password Guessing
  - T1110.003: Password Spraying
- **T1555: Credentials from Password Stores**
  - T1555.003: Credentials from Web Browsers
  - T1555.001: Keychain
  - T1555.002: Securityd Memory
- **T1212: Exploitation for Credential Access**
- **T1187: Forced Authentication**
- **T1606: Forge Web Credentials**
  - T1606.002: SAML Tokens
  - T1606.001: Web Cookies
- **T1056: Input Capture**
  - T1056.004: Credential API Hooking
  - T1056.002: GUI Input Capture
  - T1056.001: Keylogging
  - T1056.003: Web Portal Capture
- **T1557: Man-in-the-Middle**
- **T1556: Modify Authentication Process**
- **T1040: Network Sniffing**
- **T1003: OS Credential Dumping**
- **T1528: Steal Application Access Token**
- **T1558: Steal or Forge Kerberos Tickets**
  - T1558.004: AS-REP Roasting
  - T1558.001: Golden Ticket
  - T1558.003: Kerberoasting
  - T1558.002: Silver Ticket
- **T1539: Steal Web Session Cookie**
- **T1111: Two-Factor Authentication Interception**
- **T1552: Unsecured Credentials**
  - T1552.003: Bash History
  - T1552.005: Cloud Instance Metadata API
  - T1552.001: Credentials In Files
  - T1552.002: Credentials in Registry
  - T1552.006: Group Policy Preferences
  - T1552.004: Private Keys

TA0008: Lateral Movement
- **T1210: Exploitation of Remote Services**
- **T1534: Internal Spearphishing**
- **T1570: Lateral Tool Transfer**
- **T1563: Remote Service Session Hijacking**
- **T1021: Remote Services**
  - T1021.003: Distributed Component Object Model
  - T1021.001: Remote Desktop Protocol
  - T1021.002: SMB/Windows Admin Shares
  - T1021.004: SSH
  - T1021.005: VNC
  - T1021.006: Windows Remote Management
- **T1091: Replication Through Removable Media**
- **T1072: Software Deployment Tools**
- **T1080: Taint Shared Content**
- **T1550: Use Alternate Authentication Material**

TA0009: Collection
- **T1560: Archive Collected Data**
- **T1123: Audio Capture**
- **T1119: Automated Collection**
- **T1115: Clipboard Data**
- **T1530: Data from Cloud Storage Object**
- **T1602: Data from Configuration Repository**
- **T1213: Data from Information Repositories**
- **T1005: Data from Local System**
- **T1039: Data from Network Shared Drive**
- **T1025: Data from Removable Media**
- **T1074: Data Staged**
- **T1114: Email Collection**
- **T1056: Input Capture**
- **T1185: Man in the Browser**
- **T1557: Man-in-the-Middle**
- **T1113: Screen Capture**
- **T1125: Video Capture**

TA0011: Command and Control
- **T1071: Application Layer Protocol**
  - T1071.004: DNS
  - T1071.002: File Transfer Protocols
  - T1071.003: Mail Protocols
  - T1071.001: Web Protocols
- **T1092: Communication Through Removable Media**
- **T1132: Data Encoding**
- **T1001: Data Obfuscation**
- **T1568: Dynamic Resolution**
- **T1573: Encrypted Channel**
- **T1008: Fallback Channels**
- **T1105: Ingress Tool Transfer**
- **T1104: Multi-Stage Channels**
- **T1095: Non-Application Layer Protocol**
- **T1571: Non-Standard Port**
- **T1572: Protocol Tunneling**
- **T1090: Proxy**
- **T1219: Remote Access Software**
- **T1205: Traffic Signaling**
- **T1102: Web Service**

TA0010: Exfiltration
- **T1020: Automated Exfiltration**
- **T1030: Data Transfer Size Limits**
- **T1048: Exfiltration Over Alternative Protocol**
- **T1041: Exfiltration Over C2 Channel**
- **T1011: Exfiltration Over Other Network Medium**
- **T1052: Exfiltration Over Physical Medium**
- **T1567: Exfiltration Over Web Service**
- **T1029: Scheduled Transfer**
- **T1537: Transfer Data to Cloud Account**

TA0040: Impact
- **T1531: Account Access Removal**
- **T1485: Data Destruction**
- **T1486: Data Encrypted for Impact**
- **T1565: Data Manipulation**
- **T1491: Defacement**
- **T1561: Disk Wipe**
- **T1499: Endpoint Denial of Service**
  - T1499.003: Application Exhaustion Flood
  - T1499.004: Application or System Exploitation
  - T1499.001: OS Exhaustion Flood
  - T1499.002: Service Exhaustion Flood
- **T1495: Firmware Corruption**
- **T1490: Inhibit System Recovery**
- **T1498: Network Denial of Service**
  - T1498.001: Direct Network Flood
  - T1498.002: Reflection Amplification
- **T1496: Resource Hijacking**
- **T1489: Service Stop**
- **T1529: System Shutdown/Reboot**

Insider and Privilege Misuse

Domain: Enterprise ATT&CK v8

Platforms: Linux®, macOS®, Windows®, Office 365®, Azure® AD, AWS®, GCP®, Azure®, SaaS, PRE, Network

TA0043: Reconnaissance
T1595: Active Scanning
T1592: Gather Victim Host Information
T1592.004: Client Configurations
T1592.003: Firmware
T1592.001: Hardware
T1592.002: Software
T1589: Gather Victim Identity Information
T1589.001: Credentials
T1589.002: Email Addresses
T1589.003: Employee Names
T1590: Gather Victim Network Information
T1591: Gather Victim Org Information
T1591.002: Business Relationships
T1591.001: Determine Physical Locations
T1591.003: Identify Business Tempo
T1591.004: Identify Roles
T1598: Phishing for Information
T1597: Search Closed Sources
T1596: Search Open Technical Databases
T1593: Search Open Websites/ Domains
T1594: Search Victim-Owned Websites

TA0042: Resource Development
T1583: Acquire Infrastructure
T1586: Compromise Accounts
T1584: Compromise Infrastructure
T1587: Develop Capabilities
T1587.002: Code Signing Certificates
T1587.003: Digital Certificates
T1587.004: Exploits
T1587.001: Malware
T1585: Establish Accounts
T1588: Obtain Capabilities
T1588.003: Code Signing Certificates
T1588.004: Digital Certificates
T1588.005: Exploits
T1588.001: Malware
T1588.002: Tool
T1588.006: Vulnerabilities

TA0001: Initial Access
T1189: Drive-by Compromise
T1190: Exploit Public-Facing Application
T1133: External Remote Services
T1200: Hardware Additions
T1566: Phishing
T1091: Replication Through Removable Media
T1195: Supply Chain Compromise
T1195.003: Compromise Hardware Supply Chain
T1195.001: Compromise Software Dependencies and Development Tools
T1195.002: Compromise Software Supply Chain
T1199: Trusted Relationship
T1078: Valid Accounts
T1078.004: Cloud Accounts
T1078.001: Default Accounts
T1078.002: Domain Accounts
T1078.003: Local Accounts

TA0002: Execution
T1059: Command and Scripting Interpreter
T1059.002: AppleScript
T1059.007: JavaScript/JScript
T1059.008: Network Device CLI
T1059.001: PowerShell
T1059.006: Python
T1059.004: Unix Shell
T1059.005: Visual Basic
T1059.003: Windows Command Shell
T1203: Exploitation for Client Execution
T1559: Inter-Process Communication
T1106: Native API
T1053: Scheduled Task/Job
T1129: Shared Modules
T1072: Software Deployment Tools
T1569: System Services
T1204: User Execution
T1204.002: Malicious File
T1204.001: Malicious Link
T1047: Windows Management Instrumentation

TA0003: Persistence
T1098: Account Manipulation
T1197: BITS Jobs
T1547: Boot or Logon Autostart Execution
T1037: Boot or Logon Initialization Scripts
T1176: Browser Extensions
T1554: Compromise Client Software Binary
T1136: Create Account
T1543: Create or Modify System Process
T1546: Event Triggered Execution
T1133: External Remote Services
T1574: Hijack Execution Flow
T1525: Implant Container Image
T1137: Office Application Startup
T1542: Pre-OS Boot
T1053: Scheduled Task/Job
T1505: Server Software Component
T1205: Traffic Signaling
T1078: Valid Accounts

TA0004: Privilege Escalation
T1548: Abuse Elevation Control Mechanism
T1134: Access Token Manipulation
T1547: Boot or Logon Autostart Execution
T1037: Boot or Logon Initialization Scripts
T1543: Create or Modify System Process
T1543.001: Launch Agent
T1543.004: Launch Daemon
T1543.002: Systemd Service
T1543.003: Windows Service
T1484: Domain Policy Modification
T1546: Event Triggered Execution
T1068: Exploitation for Privilege Escalation
T1574: Hijack Execution Flow
T1574.012: COR_PROFILER
T1574.001: DLL Search Order Hijacking
T1574.002: DLL Side-Loading
T1574.004: Dylib Hijacking
T1574.005: Executable Installer File Permissions Weakness
T1574.006: LD_PRELOAD
T1574.007: Path Interception by PATH Environment Variable
T1574.008: Path Interception by Search Order Hijacking
T1574.009: Path Interception by Unquoted Path
T1574.010: Services File Permissions Weakness
T1574.011: Services Registry Permissions Weakness
T1055: Process Injection
T1053: Scheduled Task/Job
T1078: Valid Accounts

TA0005: Defense Evasion
T1548: Abuse Elevation Control Mechanism
T1134: Access Token Manipulation
T1197: BITS Jobs
T1140: Deobfuscate/Decode Files or Information
T1006: Direct Volume Access
T1484: Domain Policy Modification
T1484.002: Domain Trust Modification
T1484.001: Group Policy Modification
T1480: Execution Guardrails
T1211: Exploitation for Defense Evasion
T1222: File and Directory Permissions Modification
T1564: Hide Artifacts
T1564.005: Hidden File System
T1564.001: Hidden Files and Directories
T1564.002: Hidden Users
T1564.003: Hidden Window
T1564.004: NTFS File Attributes
T1564.006: Run Virtual Instance
T1564.007: VBA Stomping
T1574: Hijack Execution Flow
T1562: Impair Defenses
T1562.008: Disable Cloud Logs
T1562.007: Disable or Modify Cloud Firewall
T1562.004: Disable or Modify System Firewall
T1562.001: Disable or Modify Tools
T1562.002: Disable Windows Event Logging
T1562.003: Impair Command History Logging
T1562.006: Indicator Blocking
T1070: Indicator Removal on Host
T1070.003: Clear Command History
T1070.002: Clear Linux or Mac System Logs
T1070.001: Clear Windows Event Logs
T1070.004: File Deletion
T1070.005: Network Share Connection Removal
T1070.006: Timestomp
T1202: Indirect Command Execution
T1036: Masquerading
T1036.001: Invalid Code Signature
T1036.004: Masquerade Task or Service
T1036.005: Match Legitimate Name or Location
T1036.003: Rename System Utilities
T1036.002: Right-to-Left Override
T1036.006: Space after Filename
T1556: Modify Authentication Process
T1578: Modify Cloud Compute Infrastructure
T1578.002: Create Cloud Instance
T1578.001: Create Snapshot
T1578.003: Delete Cloud Instance
T1578.004: Revert Cloud Instance
T1112: Modify Registry
T1601: Modify System Image
T1599: Network Boundary Bridging
T1027: Obfuscated Files or Information
T1542: Pre-OS Boot
T1055: Process Injection
T1207: Rogue Domain Controller
T1014: Rootkit
T1218: Signed Binary Proxy Execution
T1216: Signed Script Proxy Execution
T1553: Subvert Trust Controls
T1221: Template Injection
T1205: Traffic Signaling
T1127: Trusted Developer Utilities Proxy Execution
T1535: Unused/Unsupported Cloud Regions
T1550: Use Alternate Authentication Material
T1078: Valid Accounts
T1497: Virtualization/Sandbox Evasion
T1600: Weaken Encryption
T1220: XSL Script Processing

TA0006: Credential Access
T1110: Brute Force
T1110.004: Credential Stuffing
T1110.002: Password Cracking
T1110.001: Password Guessing
T1110.003: Password Spraying
T1555: Credentials from Password Stores
T1555.003: Credentials from Web Browsers
T1555.001: Keychain
T1555.002: Securityd Memory
T1212: Exploitation for Credential Access
T1187: Forced Authentication
T1606: Forge Web Credentials
T1056: Input Capture
T1056.004: Credential API Hooking
T1056.002: GUI Input Capture
T1056.001: Keylogging
T1056.003: Web Portal Capture
T1557: Man-in-the-Middle
T1556: Modify Authentication Process
T1040: Network Sniffing
T1003: OS Credential Dumping
T1003.008: /etc/passwd and /etc/shadow
T1003.005: Cached Domain Credentials
T1003.006: DCSync
T1003.004: LSA Secrets
T1003.001: LSASS Memory
T1003.003: NTDS
T1003.007: Proc Filesystem
T1003.002: Security Account Manager
T1528: Steal Application Access Token
T1558: Steal or Forge Kerberos Tickets
T1539: Steal Web Session Cookie
T1111: Two-Factor Authentication Interception
T1552: Unsecured Credentials
T1552.003: Bash History
T1552.005: Cloud Instance Metadata API
T1552.001: Credentials In Files
T1552.002: Credentials in Registry
T1552.006: Group Policy Preferences
T1552.004: Private Keys

TA0007: Discovery
T1087: Account Discovery
T1087.004: Cloud Account
T1087.002: Domain Account
T1087.003: Email Account
T1087.001: Local Account
T1010: Application Window Discovery
T1217: Browser Bookmark Discovery
T1580: Cloud Infrastructure Discovery
T1538: Cloud Service Dashboard
T1526: Cloud Service Discovery
T1482: Domain Trust Discovery
T1083: File and Directory Discovery
T1046: Network Service Scanning
T1135: Network Share Discovery
T1040: Network Sniffing
T1201: Password Policy Discovery
T1120: Peripheral Device Discovery
T1069: Permission Groups Discovery
T1069.003: Cloud Groups
T1069.002: Domain Groups
T1069.001: Local Groups
T1057: Process Discovery
T1012: Query Registry
T1018: Remote System Discovery
T1518: Software Discovery
T1518.001: Security Software Discovery
T1082: System Information Discovery
T1016: System Network Configuration Discovery
T1049: System Network Connections Discovery
T1033: System Owner/User Discovery
T1007: System Service Discovery
T1124: System Time Discovery
T1497: Virtualization/Sandbox Evasion

TA0008: Lateral Movement
T1210: Exploitation of Remote Services
T1534: Internal Spearphishing
T1570: Lateral Tool Transfer
T1563: Remote Service Session Hijacking
T1021: Remote Services
T1021.003: Distributed Component Object Model
T1021.001: Remote Desktop Protocol
T1021.002: SMB/Windows Admin Shares
T1021.004: SSH
T1021.005: VNC
T1021.006: Windows Remote Management
T1091: Replication Through Removable Media
T1072: Software Deployment Tools
T1080: Taint Shared Content
T1550: Use Alternate Authentication Material

TA0009: Collection
T1560: Archive Collected Data
T1560.003: Archive via Custom Method
T1560.002: Archive via Library
T1560.001: Archive via Utility
T1123: Audio Capture
T1119: Automated Collection
T1115: Clipboard Data
T1530: Data from Cloud Storage Object
T1602: Data from Configuration Repository
T1213: Data from Information Repositories
T1213.001: Confluence
T1213.002: Sharepoint
T1005: Data from Local System
T1039: Data from Network Shared Drive
T1025: Data from Removable Media
T1074: Data Staged
T1074.001: Local Data Staging
T1074.002: Remote Data Staging
T1114: Email Collection
T1114.003: Email Forwarding Rule
T1114.001: Local Email Collection
T1114.002: Remote Email Collection
T1056: Input Capture
T1185: Man in the Browser
T1557: Man-in-the-Middle
T1113: Screen Capture
T1125: Video Capture

TA0011: Command and Control
T1071: Application Layer Protocol
T1092: Communication Through Removable Media
T1132: Data Encoding
T1001: Data Obfuscation
T1568: Dynamic Resolution
T1573: Encrypted Channel
T1008: Fallback Channels
T1105: Ingress Tool Transfer
T1104: Multi-Stage Channels
T1095: Non-Application Layer Protocol
T1571: Non-Standard Port
T1572: Protocol Tunneling
T1090: Proxy
T1219: Remote Access Software
T1205: Traffic Signaling
T1102: Web Service

TA0010: Exfiltration
T1020: Automated Exfiltration
T1030: Data Transfer Size Limits
T1048: Exfiltration Over Alternative Protocol
T1041: Exfiltration Over C2 Channel
T1011: Exfiltration Over Other Network Medium
T1011.001: Exfiltration Over Bluetooth
T1052: Exfiltration Over Physical Medium
T1052.001: Exfiltration over USB
T1567: Exfiltration Over Web Service
T1567.002: Exfiltration to Cloud Storage
T1567.001: Exfiltration to Code Repository
T1029: Scheduled Transfer
T1537: Transfer Data to Cloud Account

TA0040: Impact
T1531: Account Access Removal
T1485: Data Destruction
T1486: Data Encrypted for Impact
T1565: Data Manipulation
T1565.003: Runtime Data Manipulation
T1565.001: Stored Data Manipulation
T1565.002: Transmitted Data Manipulation
T1491: Defacement
T1561: Disk Wipe
T1561.001: Disk Content Wipe
T1561.002: Disk Structure Wipe
T1499: Endpoint Denial of Service
T1495: Firmware Corruption
T1490: Inhibit System Recovery
T1498: Network Denial of Service
T1496: Resource Hijacking
T1489: Service Stop
T1529: System Shutdown/ Reboot

Targeted Intrusions

Domain: Enterprise ATT&CK v8

Platforms: Linux®, macOS®, Windows®, Office 365®, Azure® AD, IaaS, SaaS, PRE, Network

TA0043: Reconnaissance
- **T1595: Active Scanning**
- **T1592: Gather Victim Host Information**
- **T1589: Gather Victim Identity Information**
- **T1590: Gather Victim Network Information**
- **T1591: Gather Victim Org Information**
  - T1591.002: Business Relationships
  - T1591.001: Determine Physical Locations
  - T1591.003: Identify Business Tempo
  - T1591.004: Identify Roles
- **T1598: Phishing for Information**
- **T1597: Search Closed Sources**
- **T1596: Search Open Technical Databases**
- **T1593: Search Open Websites/ Domains**
- **T1594: Search Victim-Owned Websites**

TA0042: Resource Development
- **T1583: Acquire Infrastructure**
- **T1586: Compromise Accounts**
- **T1584: Compromise Infrastructure**
- **T1587: Develop Capabilities**
  - T1587.002: Code Signing Certificates
  - T1587.003: Digital Certificates
  - T1587.004: Exploits
  - T1587.001: Malware
- **T1585: Establish Accounts**
- **T1588: Obtain Capabilities**
  - T1588.003: Code Signing Certificates
  - T1588.004: Digital Certificates
  - T1588.005: Exploits
  - T1588.001: Malware
  - T1588.002: Tool
  - T1588.006: Vulnerabilities

TA0001: Initial Access
- **T1189: Drive-by Compromise**
- **T1190: Exploit Public-Facing Application**
- **T1133: External Remote Services**
- **T1200: Hardware Additions**
- **T1566: Phishing**
  - T1566.001: Spearphishing Attachment
  - T1566.002: Spearphishing Link
  - T1566.003: Spearphishing via Service
- **T1091: Replication Through Removable Media**
- **T1195: Supply Chain Compromise**
  - T1195.003: Compromise Hardware Supply Chain
  - T1195.001: Compromise Software Dependencies and Development Tools
  - T1195.002: Compromise Software Supply Chain
- **T1199: Trusted Relationship**
- **T1078: Valid Accounts**
  - T1078.004: Cloud Accounts
  - T1078.001: Default Accounts
  - T1078.002: Domain Accounts
  - T1078.003: Local Accounts

TA0002: Execution
- **T1059: Command and Scripting Interpreter**
  - T1059.002: AppleScript
  - T1059.007: JavaScript/JScript
  - T1059.008: Network Device CLI
  - T1059.001: PowerShell
  - T1059.006: Python
  - T1059.004: Unix Shell
  - T1059.005: Visual Basic
  - T1059.003: Windows Command Shell
- **T1203: Exploitation for Client Execution**
- **T1559: Inter-Process Communication**
- **T1106: Native API**
- **T1053: Scheduled Task/Job**
- **T1129: Shared Modules**
- **T1072: Software Deployment Tools**
- **T1569: System Services**
  - T1569.001: Launchctl
  - T1569.002: Service Execution
- **T1204: User Execution**
  - T1204.002: Malicious File
  - T1204.001: Malicious Link
- **T1047: Windows Management Instrumentation**

TA0003: Persistence
- **T1098: Account Manipulation**
  - T1098.003: Add Office 365 Global Administrator Role
  - T1098.001: Additional Cloud Credentials
  - T1098.002: Exchange Email Delegate Permissions
  - T1098.004: SSH Authorized Keys
- **T1197: BITS Jobs**
- **T1547: Boot or Logon Autostart Execution**
- **T1037: Boot or Logon Initialization Scripts**
- **T1176: Browser Extensions**
- **T1554: Compromise Client Software Binary**
- **T1136: Create Account**
  - T1136.003: Cloud Account
  - T1136.002: Domain Account
  - T1136.001: Local Account
- **T1543: Create or Modify System Process**
- **T1546: Event Triggered Execution**
  - T1546.004: .bash_profile and .bashrc
  - T1546.008: Accessibility Features
  - T1546.009: AppCert DLLs
  - T1546.010: AppInit DLLs
  - T1546.011: Application Shimming
  - T1546.001: Change Default File Association
  - T1546.015: Component Object Model Hijacking
  - T1546.014: Emond
  - T1546.012: Image File Execution Options Injection
  - T1546.006: LC_LOAD_DYLIB Addition
  - T1546.007: Netsh Helper DLL
  - T1546.013: PowerShell Profile
  - T1546.002: Screensaver
  - T1546.005: Trap
  - T1546.003: Windows Management Instrumentation Event Subscription
- **T1133: External Remote Services**
- **T1574: Hijack Execution Flow**
- **T1137: Office Application Startup**
- **T1542: Pre-OS Boot**
- **T1053: Scheduled Task/Job**
- **T1505: Server Software Component**
  - T1505.001: SQL Stored Procedures
  - T1505.002: Transport Agent
  - T1505.003: Web Shell
- **T1205: Traffic Signaling**
- **T1078: Valid Accounts**

TA0004: Privilege Escalation
- **T1548: Abuse Elevation Control Mechanism**
- **T1134: Access Token Manipulation**
  - T1134.002: Create Process with Token
  - T1134.003: Make and Impersonate Token
  - T1134.004: Parent PID Spoofing
  - T1134.005: SID-History Injection
  - T1134.001: Token Impersonation/Theft
- **T1547: Boot or Logon Autostart Execution**
  - T1547.002: Authentication Package
  - T1547.006: Kernel Modules and Extensions
  - T1547.008: LSASS Driver
  - T1547.011: Plist Modification
  - T1547.010: Port Monitors
  - T1547.012: Print Processors
  - T1547.007: Re-opened Applications
  - T1547.001: Registry Run Keys / Startup Folder
  - T1547.005: Security Support Provider
  - T1547.009: Shortcut Modification
  - T1547.003: Time Providers
  - T1547.004: Winlogon Helper DLL
- **T1037: Boot or Logon Initialization Scripts**
- **T1543: Create or Modify System Process**
  - T1543.001: Launch Agent
  - T1543.004: Launch Daemon
  - T1543.002: Systemd Service
  - T1543.003: Windows Service
- **T1484: Domain Policy Modification**
  - T1484.002: Domain Trust Modification
  - T1484.001: Group Policy Modification
- **T1546: Event Triggered Execution**
- **T1068: Exploitation for Privilege Escalation**
- **T1574: Hijack Execution Flow**
- **T1055: Process Injection**
  - T1055.004: Asynchronous Procedure Call
  - T1055.001: Dynamic-link Library Injection
  - T1055.011: Extra Window Memory Injection
  - T1055.002: Portable Executable Injection
  - T1055.009: Proc Memory
  - T1055.013: Process Doppelgänging
  - T1055.012: Process Hollowing
  - T1055.008: Ptrace System Calls
  - T1055.003: Thread Execution Hijacking
  - T1055.005: Thread Local Storage
  - T1055.014: VDSO Hijacking
- **T1053: Scheduled Task/Job**
  - T1053.001: At (Linux)
  - T1053.002: At (Windows)
  - T1053.003: Cron
  - T1053.004: Launchd
  - T1053.005: Scheduled Task
  - T1053.006: Systemd Timers
- **T1078: Valid Accounts**

TA0005: Defense Evasion
- **T1548: Abuse Elevation Control Mechanism**
  - T1548.002: Bypass User Account Control
  - T1548.004: Elevated Execution with Prompt
  - T1548.001: Setuid and Setgid
  - T1548.003: Sudo and Sudo Caching
- **T1134: Access Token Manipulation**
- **T1197: BITS Jobs**
- **T1140: Deobfuscate/Decode Files or Information**
- **T1006: Direct Volume Access**
- **T1484: Domain Policy Modification**
- **T1480: Execution Guardrails**
- **T1211: Exploitation for Defense Evasion**
- **T1222: File and Directory Permissions Modification**
  - T1222.002: Linux and Mac File and Directory Permissions Modification
  - T1222.001: Windows File and Directory Permissions Modification
- **T1564: Hide Artifacts**
  - T1564.005: Hidden File System
  - T1564.001: Hidden Files and Directories
  - T1564.002: Hidden Users
  - T1564.003: Hidden Window
  - T1564.004: NTFS File Attributes
  - T1564.006: Run Virtual Instance
  - T1564.007: VBA Stomping
- **T1574: Hijack Execution Flow**
  - T1574.012: COR_PROFILER
  - T1574.001: DLL Search Order Hijacking
  - T1574.002: DLL Side-Loading
  - T1574.004: Dylib Hijacking
  - T1574.005: Executable Installer File Permissions Weakness
  - T1574.006: LD_PRELOAD
  - T1574.007: Path Interception by PATH Environment Variable
  - T1574.008: Path Interception by Search Order Hijacking
  - T1574.009: Path Interception by Unquoted Path
  - T1574.010: Services File Permissions Weakness
  - T1574.011: Services Registry Permissions Weakness
- **T1562: Impair Defenses**
  - T1562.004: Disable or Modify System Firewall
  - T1562.001: Disable or Modify Tools
  - T1562.002: Disable Windows Event Logging
  - T1562.003: Impair Command History Logging
  - T1562.006: Indicator Blocking
- **T1070: Indicator Removal on Host**
  - T1070.003: Clear Command History
  - T1070.002: Clear Linux or Mac System Logs
  - T1070.001: Clear Windows Event Logs
  - T1070.004: File Deletion
  - T1070.005: Network Share Connection Removal
  - T1070.006: Timestomp
- **T1202: Indirect Command Execution**
- **T1036: Masquerading**
  - T1036.001: Invalid Code Signature
  - T1036.004: Masquerade Task or Service
  - T1036.005: Match Legitimate Name or Location
  - T1036.003: Rename System Utilities
  - T1036.002: Right-to-Left Override
  - T1036.006: Space after Filename
- **T1556: Modify Authentication Process**
- **T1112: Modify Registry**
- **T1601: Modify System Image**
- **T1599: Network Boundary Bridging**
- **T1027: Obfuscated Files or Information**
  - T1027.001: Binary Padding
  - T1027.004: Compile After Delivery
  - T1027.005: Indicator Removal from Tools
  - T1027.002: Software Packing
  - T1027.003: Steganography
- **T1542: Pre-OS Boot**
- **T1055: Process Injection**
- **T1207: Rogue Domain Controller**
- **T1014: Rootkit**
- **T1218: Signed Binary Proxy Execution**
  - T1218.003: CMSTP
  - T1218.001: Compiled HTML File
  - T1218.002: Control Panel
  - T1218.004: InstallUtil
  - T1218.005: Mshta
  - T1218.007: Msiexec
  - T1218.008: Odbcconf
  - T1218.009: Regsvcs/Regasm
  - T1218.010: Regsvr32
  - T1218.011: Rundll32
  - T1218.012: Verclsid
- **T1216: Signed Script Proxy Execution**
- **T1553: Subvert Trust Controls**
  - T1553.002: Code Signing
  - T1553.001: Gatekeeper Bypass
  - T1553.004: Install Root Certificate
  - T1553.003: SIP and Trust Provider Hijacking
- **T1221: Template Injection**
- **T1205: Traffic Signaling**
- **T1127: Trusted Developer Utilities Proxy Execution**
- **T1550: Use Alternate Authentication Material**
  - T1550.001: Application Access Token
  - T1550.002: Pass the Hash
  - T1550.003: Pass the Ticket
  - T1550.004: Web Session Cookie
- **T1078: Valid Accounts**
- **T1497: Virtualization/Sandbox Evasion**
  - T1497.001: System Checks
  - T1497.003: Time Based Evasion
  - T1497.002: User Activity Based Checks
- **T1600: Weaken Encryption**
- **T1220: XSL Script Processing**

TA0006: Credential Access
- **T1110: Brute Force**
  - T1110.004: Credential Stuffing
  - T1110.002: Password Cracking
  - T1110.001: Password Guessing
  - T1110.003: Password Spraying
- **T1555: Credentials from Password Stores**
  - T1555.003: Credentials from Web Browsers
  - T1555.001: Keychain
  - T1555.002: Securityd Memory
- **T1212: Exploitation for Credential Access**
- **T1187: Forced Authentication**
- **T1606: Forge Web Credentials**
  - T1606.002: SAML Tokens
  - T1606.001: Web Cookies
- **T1056: Input Capture**
  - T1056.004: Credential API Hooking
  - T1056.002: GUI Input Capture
  - T1056.001: Keylogging
  - T1056.003: Web Portal Capture
- **T1557: Man-in-the-Middle**
- **T1556: Modify Authentication Process**
- **T1040: Network Sniffing**
- **T1003: OS Credential Dumping**
  - T1003.008: /etc/passwd and /etc/shadow
  - T1003.005: Cached Domain Credentials
  - T1003.006: DCSync
  - T1003.004: LSA Secrets
  - T1003.001: LSASS Memory
  - T1003.003: NTDS
  - T1003.007: Proc Filesystem
  - T1003.002: Security Account Manager
- **T1528: Steal Application Access Token**
- **T1558: Steal or Forge Kerberos Tickets**
  - T1558.004: AS-REP Roasting
  - T1558.001: Golden Ticket
  - T1558.003: Kerberoasting
  - T1558.002: Silver Ticket
- **T1539: Steal Web Session Cookie**
- **T1111: Two-Factor Authentication Interception**
- **T1552: Unsecured Credentials**
  - T1552.003: Bash History
  - T1552.001: Credentials In Files
  - T1552.002: Credentials in Registry
  - T1552.006: Group Policy Preferences
  - T1552.004: Private Keys

TA0007: Discovery
- **T1087: Account Discovery**
  - T1087.004: Cloud Account
  - T1087.002: Domain Account
  - T1087.003: Email Account
  - T1087.001: Local Account
- **T1010: Application Window Discovery**
- **T1217: Browser Bookmark Discovery**
- **T1538: Cloud Service Dashboard**
- **T1526: Cloud Service Discovery**
- **T1482: Domain Trust Discovery**
- **T1083: File and Directory Discovery**
- **T1046: Network Service Scanning**
- **T1135: Network Share Discovery**
- **T1040: Network Sniffing**
- **T1201: Password Policy Discovery**
- **T1120: Peripheral Device Discovery**
- **T1069: Permission Groups Discovery**
  - T1069.003: Cloud Groups
  - T1069.002: Domain Groups
  - T1069.001: Local Groups
- **T1057: Process Discovery**
- **T1012: Query Registry**
- **T1018: Remote System Discovery**
- **T1518: Software Discovery**
  - T1518.001: Security Software Discovery
- **T1082: System Information Discovery**
- **T1016: System Network Configuration Discovery**
- **T1049: System Network Connections Discovery**
- **T1033: System Owner/User Discovery**
- **T1007: System Service Discovery**
- **T1124: System Time Discovery**
- **T1497: Virtualization/Sandbox Evasion**

TA0008: Lateral Movement
- **T1210: Exploitation of Remote Services**
- **T1534: Internal Spearphishing**
- **T1570: Lateral Tool Transfer**
- **T1563: Remote Service Session Hijacking**
- **T1021: Remote Services**
  - T1021.003: Distributed Component Object Model
  - T1021.001: Remote Desktop Protocol
  - T1021.002: SMB/Windows Admin Shares
  - T1021.004: SSH
  - T1021.005: VNC
  - T1021.006: Windows Remote Management
- **T1091: Replication Through Removable Media**
- **T1072: Software Deployment Tools**
- **T1080: Taint Shared Content**
- **T1550: Use Alternate Authentication Material**

TA0009: Collection
- **T1560: Archive Collected Data**
  - T1560.003: Archive via Custom Method
  - T1560.002: Archive via Library
  - T1560.001: Archive via Utility
- **T1123: Audio Capture**
- **T1119: Automated Collection**
- **T1115: Clipboard Data**
- **T1602: Data from Configuration Repository**
- **T1213: Data from Information Repositories**
- **T1005: Data from Local System**
- **T1039: Data from Network Shared Drive**
- **T1025: Data from Removable Media**
- **T1074: Data Staged**
  - T1074.001: Local Data Staging
  - T1074.002: Remote Data Staging
- **T1114: Email Collection**
  - T1114.003: Email Forwarding Rule
  - T1114.001: Local Email Collection
  - T1114.002: Remote Email Collection
- **T1056: Input Capture**
- **T1185: Man in the Browser**
- **T1557: Man-in-the-Middle**
- **T1113: Screen Capture**
- **T1125: Video Capture**

TA0011: Command and Control
- **T1071: Application Layer Protocol**
  - T1071.004: DNS
  - T1071.002: File Transfer Protocols
  - T1071.003: Mail Protocols
  - T1071.001: Web Protocols
- **T1092: Communication Through Removable Media**
- **T1132: Data Encoding**
  - T1132.002: Non-Standard Encoding
  - T1132.001: Standard Encoding
- **T1001: Data Obfuscation**
  - T1001.001: Junk Data
  - T1001.003: Protocol Impersonation
  - T1001.002: Steganography
- **T1568: Dynamic Resolution**
  - T1568.003: DNS Calculation
  - T1568.002: Domain Generation Algorithms
  - T1568.001: Fast Flux DNS
- **T1573: Encrypted Channel**
  - T1573.002: Asymmetric Cryptography
  - T1573.001: Symmetric Cryptography
- **T1008: Fallback Channels**
- **T1105: Ingress Tool Transfer**
- **T1104: Multi-Stage Channels**
- **T1095: Non-Application Layer Protocol**
- **T1571: Non-Standard Port**
- **T1572: Protocol Tunneling**
- **T1090: Proxy**
  - T1090.004: Domain Fronting
  - T1090.002: External Proxy
  - T1090.001: Internal Proxy
  - T1090.003: Multi-hop Proxy
- **T1219: Remote Access Software**
- **T1205: Traffic Signaling**
- **T1102: Web Service**

TA0010: Exfiltration
- **T1020: Automated Exfiltration**
- **T1030: Data Transfer Size Limits**
- **T1048: Exfiltration Over Alternative Protocol**
- **T1041: Exfiltration Over C2 Channel**
- **T1011: Exfiltration Over Other Network Medium**
- **T1052: Exfiltration Over Physical Medium**
- **T1567: Exfiltration Over Web Service**
- **T1029: Scheduled Transfer**

TA0040: Impact
- **T1531: Account Access Removal**
- **T1485: Data Destruction**
- **T1486: Data Encrypted for Impact**
- **T1565: Data Manipulation**
  - T1565.003: Runtime Data Manipulation
  - T1565.001: Stored Data Manipulation
  - T1565.002: Transmitted Data Manipulation
- **T1491: Defacement**
- **T1561: Disk Wipe**
- **T1499: Endpoint Denial of Service**
- **T1495: Firmware Corruption**
- **T1490: Inhibit System Recovery**
- **T1498: Network Denial of Service**
- **T1496: Resource Hijacking**
- **T1489: Service Stop**
- **T1529: System Shutdown/ Reboot**

APPENDIX H

Unmapped ATT&CK (Sub-)Techniques to CIS Safeguards Within an Attack Pattern

The following are ATT&CK (sub-)techniques that were used within an attack pattern, and assigned to an ATT&CK mitigation, but could not be defended against by a CIS Safeguard in the master mapping.

ATTACK TYPE	ATT&CK (SUB-) TECHNIQUE ID	ATT&CK (SUB-)TECHNIQUE NAME
Malware	T1583	Acquire Infrastructure
Malware	T1583.005	Botnet
Malware	T1584	Compromise Infrastructure
Malware	T1584.001	Domains
Malware	T1586.002	Email Accounts
Malware	T1587	Develop Capabilities
Malware	T1587.003	Digital Certificates
Malware	T1588.004	Digital Certificates
Malware	T1592	Gather Victim Host Information
Malware	T1592.002	Software
Ransomware	T1480	Execution Guardrails
Ransomware	T1583	Acquire Infrastructure
Ransomware	T1583.005	Botnet
Ransomware	T1584	Compromise Infrastructure
Ransomware	T1585	Establish Accounts
Ransomware	T1587.001	Malware
Ransomware	T1587.002	Code Signing Certificates
Ransomware	T1588.001	Malware
Ransomware	T1588.002	Tool
Ransomware	T1588.003	Code Signing Certificates
Ransomware	T1588.004	Digital Certificates
Ransomware	T1588.005	Exploits
Ransomware	T1589.001	Credentials
Ransomware	T1589.003	Employee Names

ATTACK TYPE	ATT&CK (SUB-) TECHNIQUE ID	ATT&CK (SUB-)TECHNIQUE NAME
Ransomware	T1592	Gather Victim Host Information
Ransomware	T1592.004	Client Configurations
Web App Hacking	T1583.006	Web Services
Web App Hacking	T1584.006	Web Services
Web App Hacking	T1596.005	Scan Databases
Insider and Privilege Misuse	T1587.001	Malware
Insider and Privilege Misuse	T1588.001	Malware
Insider and Privilege Misuse	T1589	Gather Victim Identity Information
Insider and Privilege Misuse	T1589.001	Credentials
Insider and Privilege Misuse	T1591	Gather Victim Org Information
Insider and Privilege Misuse	T1591.002	Business Relationships
Insider and Privilege Misuse	T1592	Gather Victim Host Information
Insider and Privilege Misuse	T1592.001	Hardware
Insider and Privilege Misuse	T1592.002	Software
Insider and Privilege Misuse	T1592.003	Firmware
Insider and Privilege Misuse	T1592.004	Client Configurations
Targeted Intrusions	T1480	Execution Guardrails
Targeted Intrusions	T1587	Develop Capabilities
Targeted Intrusions	T1587.001	Malware
Targeted Intrusions	T1588	Obtain Capabilities
Targeted Intrusions	T1588.001	Malware
Targeted Intrusions	T1591	Gather Victim Org Information
Targeted Intrusions	T1591.001	Determine Physical Locations
Targeted Intrusions	T1592	Gather Victim Host Information

APPENDIX I

ATT&CK (Sub-)Techniques With No ATT&CK Mitigation Mapped Within an Attack Pattern

The following are ATT&CK (sub-)techniques that had no assignment to an ATT&CK mitigation (and therefore, were not mapped to a CIS Safeguard); however, they were used within an attack pattern.

ATTACK TYPE	ATT&CK (SUB-) TECHNIQUE ID	ATT&CK (SUB-)TECHNIQUE NAME
Malware	T1005	Data from Local System
Malware	T1007	System Service Discovery
Malware	T1012	Query Registry
Malware	T1016	System Network Config. Discovery
Malware	T1018	Remote System Discovery
Malware	T1027.001	Binary Padding
Malware	T1027.003	Steganography
Malware	T1027.004	Compile After Delivery
Malware	T1027.005	Indicator Removal from Tools
Malware	T1033	System Owner/User Discovery
Malware	T1036.004	Masquerade Task or Service
Malware	T1039	Data from Network Shared Drive
Malware	T1049	System Network Conn. Discovery
Malware	T1056	Input Capture
Malware	T1056.001	Keylogging
Malware	T1056.004	Credential API Hooking
Malware	T1057	Process Discovery
Malware	T1069	Permission Groups Discovery
Malware	T1069.001	Local Groups
Malware	T1069.002	Domain Groups
Malware	T1070.004	File Deletion
Malware	T1070.005	Network Share Conn. Removal
Malware	T1074	Data Staged
Malware	T1074.001	Local Data Staging
Malware	T1082	System Information Discovery
Malware	T1083	File and Directory Discovery
Malware	T1087.003	Email Account
Malware	T1113	Screen Capture
Malware	T1115	Clipboard Data
Malware	T1124	System Time Discovery
Malware	T1125	Video Capture
Malware	T1140	Deobfuscate/Decode Files or Info.
Malware	T1202	Indirect Command Execution
Malware	T1496	Resource Hijacking
Malware	T1497	Virtualization/Sandbox Evasion
Malware	T1505.003	Web Shell
Malware	T1518	Software Discovery
Malware	T1518.001	Security Software Discovery
Malware	T1529	System Shutdown/Reboot
Malware	T1531	Account Access Removal
Malware	T1546	Event Triggered Execution
Malware	T1547	Boot or Logon Autostart Exec.
Malware	T1547.001	Registry Run Keys/Startup Folder
Malware	T1553.002	Code Signing
Malware	T1564	Hide Artifacts
Malware	T1564.001	Hidden Files and Directories
Malware	T1568.001	Fast Flux DNS
Ransomware	T1005	Data from Local System
Ransomware	T1007	System Service Discovery
Ransomware	T1012	Query Registry
Ransomware	T1016	System Network Config. Discovery
Ransomware	T1018	Remote System Discovery
Ransomware	T1020	Automated Exfiltration
Ransomware	T1027.001	Binary Padding
Ransomware	T1027.003	Steganography
Ransomware	T1027.004	Compile After Delivery
Ransomware	T1027.005	Indicator Removal from Tools
Ransomware	T1036.002	Right-to-Left Override
Ransomware	T1036.004	Masquerade Task or Service
Ransomware	T1039	Data from Network Shared Drive
Ransomware	T1049	System Network Conn. Discovery
Ransomware	T1056	Input Capture
Ransomware	T1056.001	Keylogging
Ransomware	T1057	Process Discovery
Ransomware	T1069.002	Domain Groups
Ransomware	T1070.004	File Deletion
Ransomware	T1082	System Information Discovery
Ransomware	T1083	File and Directory Discovery
Ransomware	T1113	Screen Capture
Ransomware	T1120	Peripheral Device Discovery
Ransomware	T1123	Audio Capture
Ransomware	T1124	System Time Discovery
Ransomware	T1134.004	Parent PID Spoofing
Ransomware	T1140	Deobfuscate/Decode Files or Info.
Ransomware	T1202	Indirect Command Execution
Ransomware	T1497	Virtualization/Sandbox Evasion
Ransomware	T1497.001	System Checks
Ransomware	T1497.002	User Activity Based Checks
Ransomware	T1497.003	Time Based Evasion
Ransomware	T1518	Software Discovery
Ransomware	T1518.001	Security Software Discovery
Ransomware	T1529	System Shutdown/Reboot
Ransomware	T1534	Internal Spearphishing
Ransomware	T1546.015	Comp. Object Model Hijacking
Ransomware	T1547	Boot or Logon Autostart Exec.
Ransomware	T1547.001	Registry Run Keys/Startup Folder
Ransomware	T1553.002	Code Signing
Ransomware	T1555.002	Securityd Memory

ATTACK TYPE	ATT&CK (SUB-) TECHNIQUE ID	ATT&CK (SUB-)TECHNIQUE NAME
Ransomware	T1560.002	Archive via Library
Ransomware	T1560.003	Archive via Custom Method
Ransomware	T1564.001	Hidden Files and Directories
Ransomware	T1600	Weaken Encryption
Ransomware	T1600.002	Disable Crypto Hardware
Web App Hacking	T1007	System Service Discovery
Web App Hacking	T1016	System Network Config. Discovery
Web App Hacking	T1018	Remote System Discovery
Web App Hacking	T1033	System Owner/User Discovery
Web App Hacking	T1036.006	Space after Filename
Web App Hacking	T1056	Input Capture
Web App Hacking	T1056.004	Credential API Hooking
Web App Hacking	T1057	Process Discovery
Web App Hacking	T1069	Permission Groups Discovery
Web App Hacking	T1082	System Information Discovery
Web App Hacking	T1083	File and Directory Discovery
Web App Hacking	T1120	Peripheral Device Discovery
Web App Hacking	T1124	System Time Discovery
Web App Hacking	T1134.004	Parent PID Spoofing
Web App Hacking	T1202	Indirect Command Execution
Web App Hacking	T1497	Virtualization/Sandbox Evasion
Web App Hacking	T1505.003	Web Shell
Web App Hacking	T1542.002	Component Firmware
Web App Hacking	T1546.005	Trap
Web App Hacking	T1546.012	Image File Exec. Options Injection
Web App Hacking	T1546.015	Comp. Object Model Hijacking
Web App Hacking	T1547.010	Port Monitors
Web App Hacking	T1564.001	Hidden Files and Directories
Insider and Privilege Misuse	T1005	Data from Local System
Insider and Privilege Misuse	T1007	System Service Discovery
Insider and Privilege Misuse	T1012	Query Registry
Insider and Privilege Misuse	T1014	Rootkit
Insider and Privilege Misuse	T1016	System Network Config. Discovery
Insider and Privilege Misuse	T1018	Remote System Discovery
Insider and Privilege Misuse	T1020	Automated Exfiltration
Insider and Privilege Misuse	T1025	Data from Removable Media
Insider and Privilege Misuse	T1033	System Owner/User Discovery
Insider and Privilege Misuse	T1039	Data from Network Shared Drive
Insider and Privilege Misuse	T1056	Input Capture
Insider and Privilege Misuse	T1056.001	Keylogging
Insider and Privilege Misuse	T1056.004	Credential API Hooking
Insider and Privilege Misuse	T1057	Process Discovery
Insider and Privilege Misuse	T1069	Permission Groups Discovery
Insider and Privilege Misuse	T1069.001	Local Groups
Insider and Privilege Misuse	T1069.002	Domain Groups
Insider and Privilege Misuse	T1069.003	Cloud Groups
Insider and Privilege Misuse	T1070.004	File Deletion
Insider and Privilege Misuse	T1074	Data Staged
Insider and Privilege Misuse	T1074.001	Local Data Staging
Insider and Privilege Misuse	T1074.002	Remote Data Staging
Insider and Privilege Misuse	T1082	System Information Discovery
Insider and Privilege Misuse	T1083	File and Directory Discovery
Insider and Privilege Misuse	T1087.003	Email Account
Insider and Privilege Misuse	T1113	Screen Capture

ATTACK TYPE	ATT&CK (SUB-) TECHNIQUE ID	ATT&CK (SUB-)TECHNIQUE NAME
Insider and Privilege Misuse	T1115	Clipboard Data
Insider and Privilege Misuse	T1120	Peripheral Device Discovery
Insider and Privilege Misuse	T1123	Audio Capture
Insider and Privilege Misuse	T1125	Video Capture
Insider and Privilege Misuse	T1518	Software Discovery
Insider and Privilege Misuse	T1518.001	Security Software Discovery
Insider and Privilege Misuse	T1560.002	Archive via Library
Insider and Privilege Misuse	T1560.003	Archive via Custom Method
Insider and Privilege Misuse	T1564	Hide Artifacts
Insider and Privilege Misuse	T1564.001	Hidden Files and Directories
Insider and Privilege Misuse	T1564.005	Hidden File System
Targeted Intrusions	T1005	Data from Local System
Targeted Intrusions	T1007	System Service Discovery
Targeted Intrusions	T1012	Query Registry
Targeted Intrusions	T1016	System Network Config. Discovery
Targeted Intrusions	T1018	Remote System Discovery
Targeted Intrusions	T1027.003	Steganography
Targeted Intrusions	T1027.004	Compile After Delivery
Targeted Intrusions	T1027.005	Indicator Removal from Tools
Targeted Intrusions	T1033	System Owner/User Discovery
Targeted Intrusions	T1036.004	Masquerade Task or Service
Targeted Intrusions	T1039	Data from Network Shared Drive
Targeted Intrusions	T1049	System Network Conn. Discovery
Targeted Intrusions	T1056	Input Capture
Targeted Intrusions	T1056.001	Keylogging
Targeted Intrusions	T1057	Process Discovery
Targeted Intrusions	T1069	Permission Groups Discovery
Targeted Intrusions	T1069.001	Local Groups
Targeted Intrusions	T1069.002	Domain Groups
Targeted Intrusions	T1070.004	File Deletion
Targeted Intrusions	T1070.005	Network Share Conn. Removal
Targeted Intrusions	T1070.006	Timestomp
Targeted Intrusions	T1074	Data Staged
Targeted Intrusions	T1074.001	Local Data Staging
Targeted Intrusions	T1074.002	Remote Data Staging
Targeted Intrusions	T1082	System Information Discovery
Targeted Intrusions	T1083	File and Directory Discovery
Targeted Intrusions	T1113	Screen Capture
Targeted Intrusions	T1124	System Time Discovery
Targeted Intrusions	T1134.004	Parent PID Spoofing
Targeted Intrusions	T1140	Deobfuscate/Decode Files or Info.
Targeted Intrusions	T1207	Rogue Domain Controller
Targeted Intrusions	T1497.001	System Checks
Targeted Intrusions	T1497.003	Time Based Evasion
Targeted Intrusions	T1505.003	Web Shell
Targeted Intrusions	T1518	Software Discovery
Targeted Intrusions	T1518.001	Security Software Discovery
Targeted Intrusions	T1529	System Shutdown/Reboot
Targeted Intrusions	T1546	Event Triggered Execution
Targeted Intrusions	T1546.012	Image File Exec. Options Injection
Targeted Intrusions	T1547	Boot or Logon Autostart Exec.
Targeted Intrusions	T1547.001	Registry Run Keys/Startup Folder
Targeted Intrusions	T1553.002	Code Signing
Targeted Intrusions	T1564	Hide Artifacts

CIS Center for Internet Security®

CIS Controls

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
TheCISecurity
cisecurity