CIS Community Defense Model

V1.0

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. 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 and the many contributors to the MITRE ATT&CK Model. 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.

Editors
Joshua M Franklin, EAC

Contributors
Ginger Anderson, CIS
Phil Langlois, Verizon
Robin Regnier, CIS
Thomas Sager, CIS
Tony Sager, CIS

Contents

Executive Summary

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

This paper presents the CIS Community Defense Model (CDM)—our way to bring more rigor, analytics, and transparency to the security recommendations found in the Controls. The CDM leverages the open availability of comprehensive summaries of attacks and security incidents (e.g., the Verizon Data Breach Investigations Report–DBIR), and the industry-endorsed ecosystem that is developing around the MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) Model. In particular, the ATT&CK Model comprehensively lists the Tactics used by attackers (roughly, the steps in an attack) as well as the many Techniques that an attacker could use at each step (Tactic).

The CIS CDM was constructed using the following process:

- From the Verizon DBIR and other sources, we identified the five most important *attack types* we want to defend against: Web-Application Hacking, Insider and Privilege Misuse, Malware, Ransomware, and Targeted Intrusions.
- For each type of attack, we determined an *attack pattern* - the set of ATT&CK Model Techniques required to execute the Tactics used in that attack.
- We identified the specific security value of Safeguards in the CIS Controls against the Techniques found in each attack. We did this by going through the class of Mitigations associated with each Technique.
- We then stood back to examine the security value (in terms of mitigating attacks) of implementing the Sub-Controls comprising the CIS Controls.

IG1 is effective in mitigating 62% of all Techniques in the MITRE ATT&CK model

The CIS Controls (IG1, IG2 and IG3) are effective in mitigating 83% of all Techniques in the MITRE ATT&CK Model

In assessing the security value of the CIS Controls, we started by examining the impact of Implementation Group 1 (IG1)—a prioritized subset of the CIS Controls that we have proposed as "Basic Cyber Hygiene"—security actions that are applicable to even the smallest and least-funded enterprises. Our analysis shows that implementing the Safeguards listed in IG1 is enough to defend against the top five attacks. That is, for each of the five attacks, the Safeguards in IG1 provide mitigation against all of the Techniques found in two or more steps (Tactics) of that attack. In addition to this value against this chosen set of five important attacks, IG1 mitigates against 62% of all ATT&CK Techniques, demonstrating significant value against a wide range of attacks. Taken together, these results strongly reinforce the importance of a relatively small number of well-chosen and basic defensive steps.

More broadly, our analysis shows that implementing the CIS Controls (in total) mitigate approximately 83% of all the Techniques found in ATT&CK. This implies that application of the CIS Controls provides significant security value against a very wide range of potential attacks, even if you don't know any details about those attacks.

The initial version of the CIS CDM is not the final answer for modelling cyber defense. However, we believe that this version represents a major step forward in providing greater rigor to support prudent decision-making regarding cyber defense strategies for organizations.

Overview

In this paper we present the CIS Community Defense Model (CDM). Our goal is to bring another level of rigor and detail to support the development and implementation of the CIS Controls, taking advantage of the industry ecosystem that is developing around the MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) Framework.

The CDM maps CIS Sub-Controls, or Safeguards, to ATT&CK and formalizes the documentation of the specific attack patterns that are mitigated by the CIS Controls.

The CIS CDM was constructed using the following process:

- From the Verizon DBIR and other sources, we identified the five most important *attack types* experienced by organizations in 2019 and, therefore, that we want to defend against: Web-Application Hacking, Insider and Privilege Misuse, Malware, Ransomware, and Targeted Intrusions.
- For each type of attack, we determined an *attack pattern*—the set of ATT&CK Model Techniques required to execute the Tactics used in that attack.
- We identified the specific security value of Safeguards in the CIS Controls against the Techniques found in each attack pattern. We did this by going through the class of Mitigations associated with each Technique.
- We then examined the security value (in terms of mitigating attacks) of implementing the Sub-Controls of the CIS Controls.

This analysis will give enterprises confidence that the Controls:

- are based on a large-scale, independent, industry-supported, and authoritative view of the attackers
- provide specific and analytically-validated defensive value against specific patterns of attack
- can be confidently used as a starting point for designing, prioritizing, and implementing their own security improvement program

At CIS, we believe that the community is best served through a transparent, public framework or model, which provides structure for these activities and translates authoritative summaries of attack information into the identification and prioritization of high-value defensive action. For more information on prior work, please see Appendix B.

We always take a "community-first" approach in our analysis and in our products. That is, we focus on cyber-attacks and issues that are the most common across the entire community, and try to address them in a way that can be used by all enterprises.

Results Summary

The CDM confirms the prioritization and the defensive value of the CIS Controls. In CIS Controls V7.1, CIS introduced a new prioritization scheme called Implementation Groups (IGs). There are three IGs. To develop the IGs, CIS identified a core set of Safeguards (i.e., Sub-Controls) that organizations with limited resources, expertise, and risk exposure should focus on. This is IG1, or "Basic Cyber Hygiene," which combines effective security value with technology and processes that are generally already available. IG1 also provides a basis for more tailored and sophisticated action in situations which call for it. Each IG builds upon the previous one. IG2 identifies additional Safeguards for organizations with more resources and expertise than those in IG1, but also greater risk exposure. Finally, the rest of the Safeguards are included in IG3.

The analysis shows that applying Implementation Group 1 (IG1) Safeguards is enough to defend against the top five most frequently occurring attacks as described in the 2019 Verizon DBIR. That is, for each of the five attack patterns, the Safeguards in IG1 provide mitigation against all of the Techniques found in two or more steps (Tactics) of that attack pattern resulting in complete mitigation of these attack patterns. These attacks are:

- Web-application hacking
- Insider and privilege misuse
- Malware
- Ransomware
- Targeted intrusions

While the Verizon DBIR classified ransomware as a type of malware, CIS chose to analyze ransomware separately due to the motivation, tactics, and outcomes of ransomware attacks. Additionally, the CDM provides evidence that the set of 171 Safeguards in the Controls mitigate the majority of the Techniques in the ATT&CK Model. Specifically, the Controls mitigate approximately 83% of all Enterprise ATT&CK Techniques (the details of this analysis are provided in Appendix A). Furthermore, IG1 mitigates against 62% of all Enterprise ATT&CK Techniques (details are also provided in Appendix A).

Finally, the CDM shows that application of the Controls provides significant security value against a very wide range of attack patterns. In addition, organizations that implement "Basic Cyber Hygiene" are well protected against top attacks.

Methodology

For some time now, frameworks have enabled security professionals to understand the granular steps an attacker must perform in order to obtain unauthorized access to a computer system. The ATT&CK Model provides similar capabilities, and supports a robust data model that is gaining momentum throughout the cybersecurity community. The ATT&CK Model also supports a visualization tool known as the MITRE ATT&CK Navigator that allows a professional to view the steps taken by an attack to access a system all at one time. We refer to a collection of ATT&CK Techniques visualized by the ATT&CK Navigator as an attack pattern.

CIS took the following steps to create the CDM:

1. **Map Safeguards to ATT&CK Mitigations:** The ATT&CK Model contains a list of Mitigations which can be used to associate Enterprise Techniques to the Safeguards.
2. **Map ATT&CK Mitigations to ATT&CK Techniques:** MITRE provides a mapping of Techniques to Mitigations that can be put into the acceptable format for this effort.
3. **Identify Threat Sources:** Choose a specific set of data sources for the CDM.
4. **Analyze and Vet Data Sources:** Understand the background and methodological information for each source.
5. **Identify Attack Patterns:** From the relevant reports and data sources, assess attack patterns and determine their priority for the CDM.
6. **Define Selected Attack Patterns:** Use the ATT&CK Model to select which Enterprise Techniques are associated with specific attack patterns.
7. **Identify Safeguards to Defend Against Attack Patterns:** Using the mappings from Step 2, lists of Safeguards can be created to defend against specific categories of attacks, such as ransomware.

The CIS Controls Mappings to ATT&CK Techniques

The ATT&CK Model includes a series of Mitigations that are mapped to each of the ATT&CK Techniques. CIS manually mapped the Controls to ATT&CK Mitigations. This mapping is then used as a bridge to map between the Controls and the ATT&CK Model. Ultimately, the Controls to ATT&CK Mitigations mappings serves as the foundation for connecting Controls to ATT&CK Techniques, and therefore it is worthwhile to analyze how well the Controls maps to ATT&CK Mitigations.

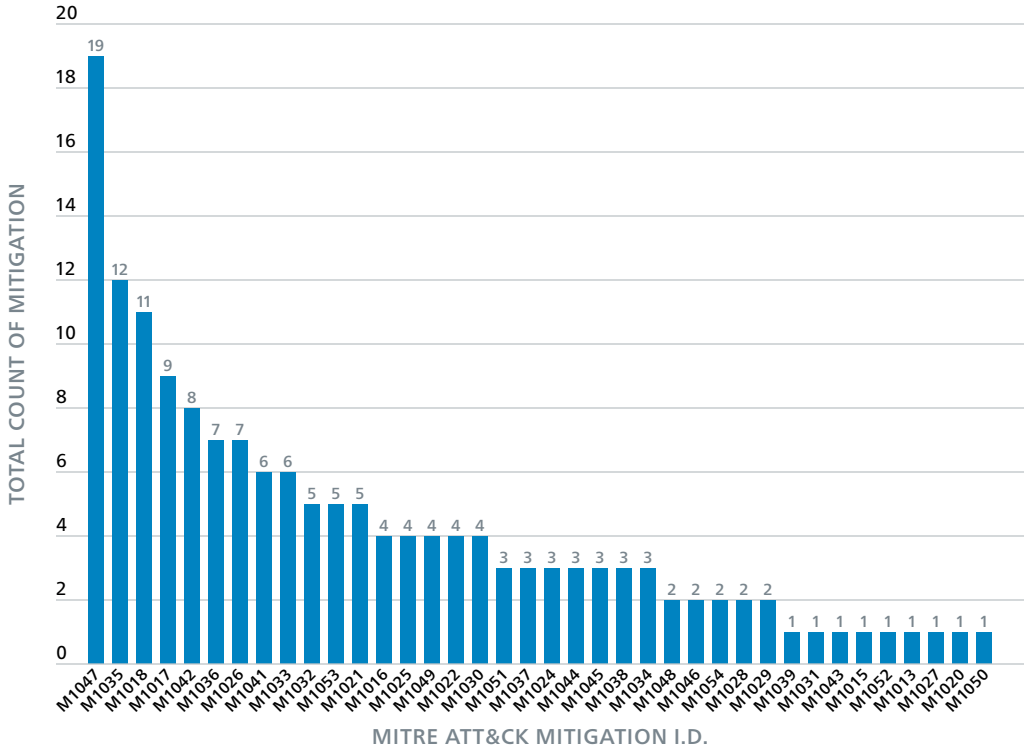
Mitigation Mapping

ATT&CK Mitigations is a list of uniquely numbered defensive mitigations contained within the broader ATT&CK Model. The ATT&CK Mitigations are easily identified as they begin with the letter "M" followed by a unique number (e.g., M1047). These 41 defensive actions are mapped to each of the ATT&CK Techniques and are included as part of the overarching ATT&CK Model. If you view each Mitigation on the ATT&CK webpage, a description is available for the Mitigation. Note that if you view a Technique on the ATT&CK website, you will see a list of Mitigations with unique guidance that assists in defending against a specific Technique. The Controls mapping to ATT&CK Mitigations is available separately from this document within CIS WorkBench and via the CIS website.

An important caveat when considering the ATT&CK Mitigations is that they represent defensive cybersecurity actions at a different level of abstraction than the Controls. Ultimately, this section shows that the Controls cover a larger number of defensive cybersecurity concepts than the ATT&CK Mitigations. This difference in granularity is perhaps best demonstrated by the number of defensive actions within each collection: the Controls contain 171 Safeguards, whereas ATT&CK contains 41 Mitigations.

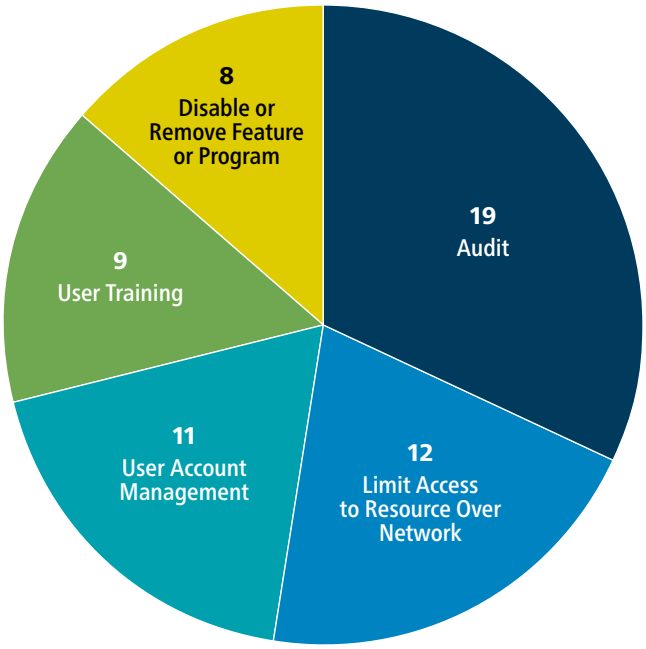
To bolster this analysis, the following graph demonstrates that many ATT&CK Mitigations contain broad concepts that can have many Safeguards mapped to them. There is a N:M relationship between many of the Safeguards and ATT&CK Mitigations. This graph shows that M1047 (Audit) contains the highest number of Safeguard mappings (i.e., 19). This means that there are 19 Safeguards that perform some sort of cybersecurity auditing activity. This chart also shows the ATT&CK Mitigations that have very few or no mappings, which is further discussed below.

Mitigations Applied to Safeguards



Drilling down further, the following chart depicts the top five ATT&CK Mitigations. This chart represents a subset of the same data presented in the preceding graph. As mentioned earlier, M1047 – Audit is the most mapped Mitigation, with a total of 19 Safeguard mappings. This chart also shows that Disabling and Removing Features, User Account Management, and Limiting Access to Network Resources are all also mapped to a large number of Safeguards, demonstrating significant overlap in some areas.

Top 5 Mitigations Applied to Safeguards



Three ATT&CK Mitigations were not included within the CDM, as they were unable to be mapped. They are:

M1040	**Behavior Prevention on Endpoint**	Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc., behavior.
M1055	**Do Not Mitigate**	This category is to associate techniques that mitigation might increase risk of compromise and therefore, mitigation is not recommended.
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.

Behavior Prevention on Endpoint helps to defend against various types of malware and malicious processes exploiting vulnerabilities in a system. Although this goal is achieved through other means via the Controls, the Controls do not explicitly recommend host-based intrusion detection systems or similar capabilities. This area is being examined for inclusion in the upcoming version 8 of the Controls. Another Mitigation not contained within the Controls is the formation and usage of a "Threat Intelligence Program." Finally, the Controls are a collection of specific defensive actions, and do not contain risk-based decisions such as "Do Not Mitigate."

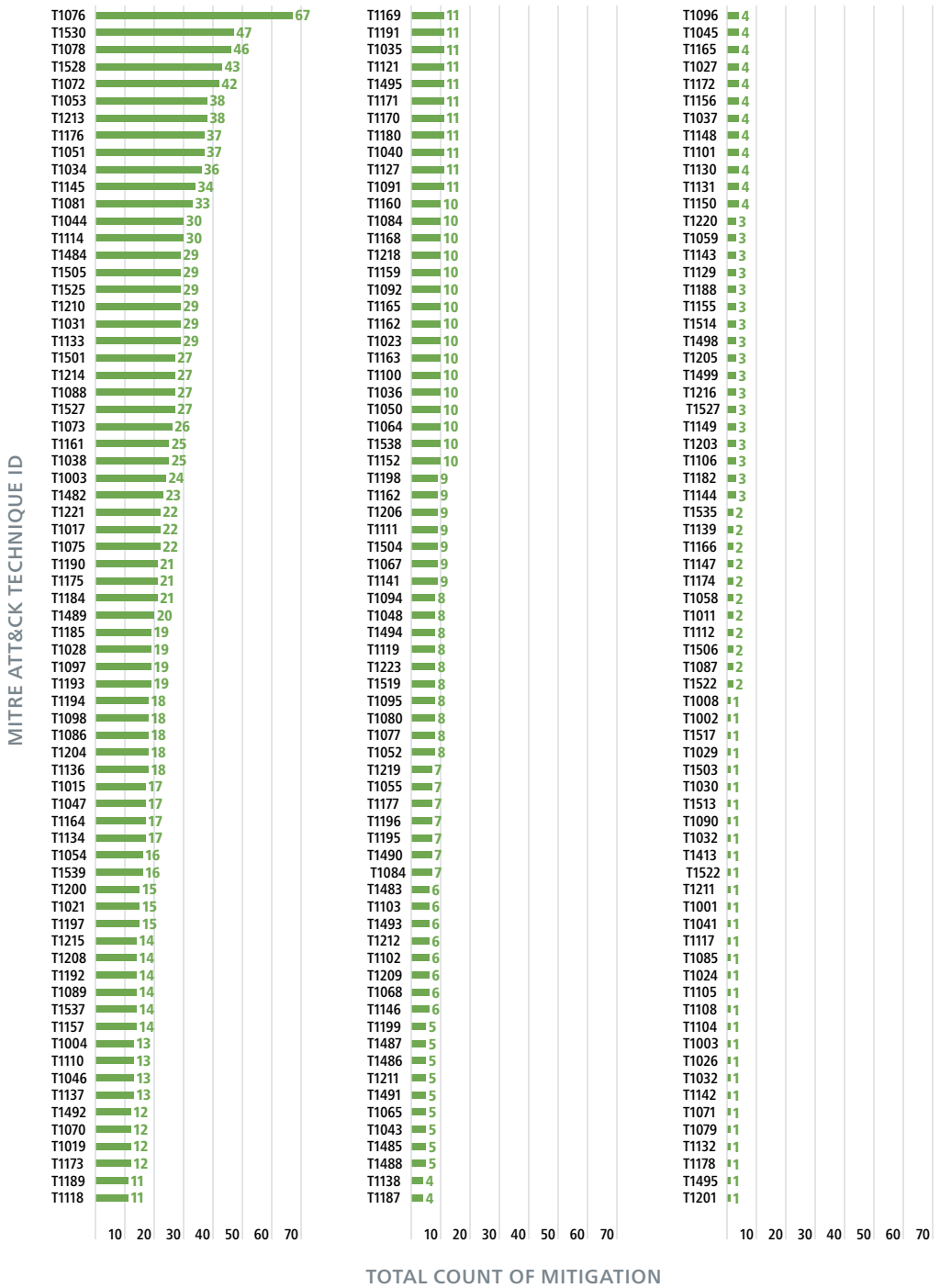
Technique Mapping

ATT&CK Techniques are a list of uniquely numbered attack techniques contained within the broader ATT&CK Model. The 171 Safeguards are mapped to the Mitigations, which are then mapped to the 266 granular Techniques. If you view each Technique on the ATT&CK webpage, a description is available for the specific Technique. The Techniques are easily identified, as they begin with the letter "T" followed by a unique number (e.g., T1076). The collection of the Controls mapped to Techniques is available separately from this document within CIS WorkBench and via the CIS website.

The Controls defend against a wide variety of unauthorized intrusion techniques. To that end, a large majority of the Enterprise ATT&CK Techniques were able to be mapped to the Controls. The Controls are also meant to defend against errors, accidents, acts of God, and other scenarios that may not be the consequence of an intelligent adversary. Many of the Safeguards associated with these types of issues did not exhibit a Safeguard mapping. Unmapped Techniques are listed in Appendix F.

The following graph shows the count of the Safeguards mapped to Techniques. The more Safeguards mapped to a Technique results in a higher value. So, Controls are more effective at defending against the Techniques with the higher values shown in the graph. Multiple Safeguards mapping to a Technique also helps to illustrate defense-in-depth. Many Safeguards were mapped to 20 or more Techniques.

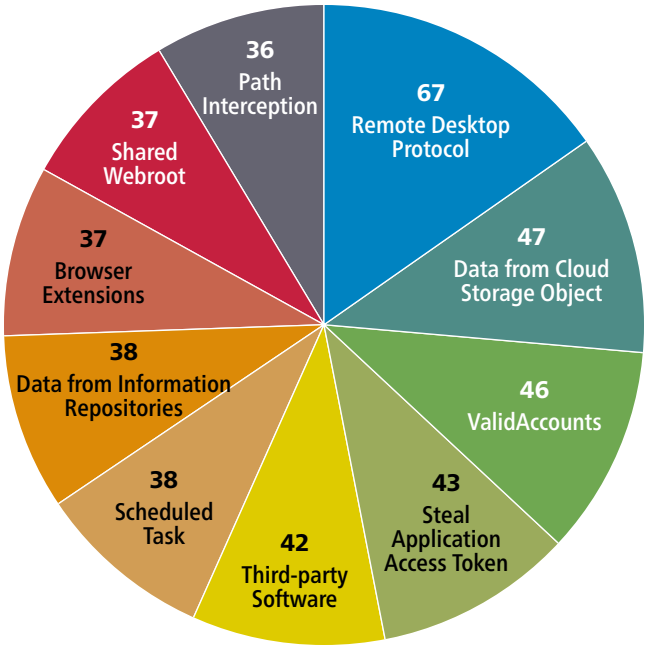
Safeguards Mapped to Techniques



A reference for the Technique name is available on the ATT&CK webpage.

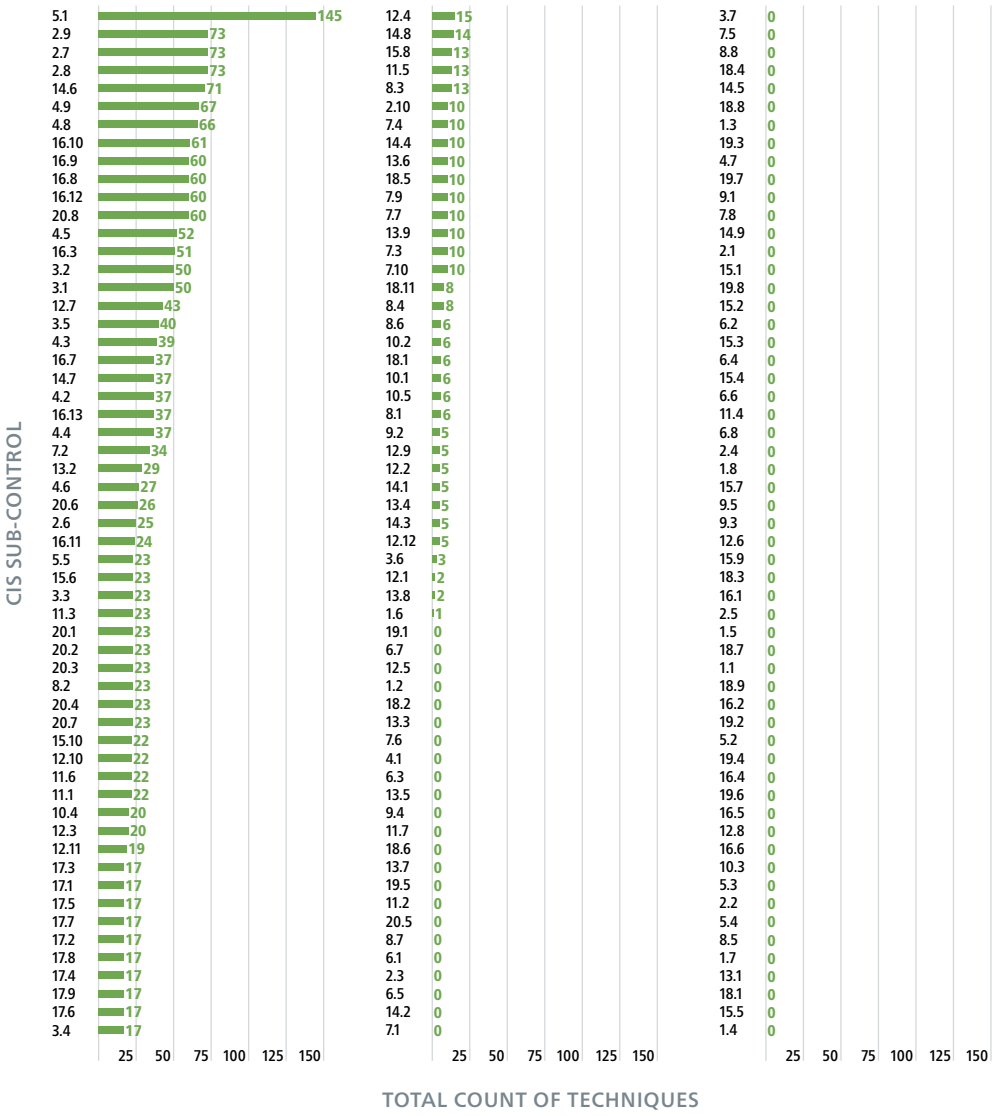
This chart represents a subset of the same data presented in the preceding graph. This pie chart shows the 10 Techniques that are most frequently mapped by Safeguards. Note that this does not mean that *Remote Desktop Protocol* is the most dangerous or frequently occurring Technique. Instead, this indicates that it was the Technique that could be mitigated via the largest number of Safeguards.

Top 10 Techniques Applied to Safeguards



The following graph shows the Safeguards with the highest number of Techniques mapped to them. This only shows frequency, and not a Safeguard's effectiveness at mitigation. However, Safeguard 5.1 – *Establish Secure Configurations,* maps to 145 Techniques and provides the most coverage of a single Safeguard. This illustrates the value of securely configuring hardware, firmware, software, databases, etc.

Number of Techniques Applied to Safeguards



Another takeaway is the percentage of Safeguards that do not map to the ATT&CK Model. The Safeguards that do not map, or map to only one or two Techniques, may in fact be *supportive Safeguards*. Supportive Safeguards may not directly mitigate any attacks, but often times provide guidance to help organizations setup systems and policies that, when implemented, can significantly bolster the effectiveness of other Safeguards in mitigating the impact of a cybersecurity event. The value of supportive Safeguards must be assessed on a case-by-case basis. Other Safeguards not associated with a Technique may be worth considering for deletion from the Controls.

Security Value of Controls

After mapping the Safeguards to the ATT&CK Model, we can now look at the data to determine the security value of the Controls and Implementation Groups. We started by looking at different data sources to find the top attacks, or most frequently occurring, that organizations should defend against. Then, we leveraged the ATT&CK Model by creating attack patterns which allowed us to determine the effectiveness of the Safeguards to defend against top attack types.

Summary of Attack Data

Survey data is subject to a variety of methodological issues, such as responses being drawn from a small number of individuals. The Community Defense Model does not look to utilize survey data.

There is no single authoritative source of data on security incidents and breaches. In fact, many organizations are wary of, or have understandable disincentives to share breach information with the public or outside researchers. Often, even with a particular dataset containing breach information, one may only get a partial piece of the picture.

Many organizations in industry publish data breach reports. These reports can be categorized as having some combination of the following characteristics:

- **Report Type:** Describes the source of security data. A single report can draw upon multiple types of data sources. The CDM looks across different types of data. Examples include:
  - **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. To obtain this information, a monitoring agent is often installed within an organization's network, or on servers and employee workstations. This data can be very large in volume and scale, but often lacks detail or operational context.
  - **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.
  - **Survey Data:** An organization sends out questions to cybersecurity and analyzes the responses. This report considers responses to survey questions an inadequate source of attack data.
- **Report Longevity:** Denotes how long the report has been under continual development. The CDM attaches higher priority to reports that have been around for longer periods of time, as they often have dedicated staff and budget to perform better data collection and analysis.

- **Access to Underlying Data:** Represents if the underlying data that the report summarizes is available for external analysis. This is typically not possible; however, in certain situations, data is available.

The following is a small subset of reports and other data sources that have been actively published, maintained for some time in the security industry, and that were analyzed to identify attack patterns used to develop the CDM:

- Multi-State Information Sharing and Analysis Center® (MS-ISAC®)
- Verizon Data Breach Investigation Report (DBIR)
- Veris Community Database
- FireEye M-Trends Report
- Symantec Internet Security Threat Report
- IBM X-Force Threat Intelligence Index
- Microsoft Security Intelligence Report

These reports are categorized based on the previously described characteristics.

Name	Type	Longevity	Access to Underlying Data
MS-ISAC Data	Sensor-data, Incident response data	2002	Yes
Verizon DBIR	Self-reported data, Sensor-data, Incident response data	2008	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
FireEye M-Trends Report	Sensor-data, Incident response data	2010	No
Symantec Internet Security Threat Report	Sensor-data	2002	No
IBM X-Force Threat Intelligence Index	Sensor-data, Incident response data	2017	No
CrowdStrike Global Threat Report	Sensor-data, Incident response data	2013	No
Microsoft Security Intelligence Report	Product-usage data, Sensor-data	2008	No

For the first iteration of the CDM, CIS primarily used MS-ISAC, Verizon®, and CrowdStrike® data as these three sources are a mix of report types, as outlined above, from across various sectors. Analysis has shown that the data in these reports does not change dramatically from year to year thus providing confidence in the consistency of the most common attack patterns over time and across a varied population. CIS had a varying degree of data access to include direct access to MS-ISAC and Verizon data and generalized, published trend data from CrowdStrike. CrowdStrike proactively uses their customer data to dissect attacks using the MITRE Framework and publishes the mapping in their yearly report. Additional reports will very likely be added to the CDM in future iterations.

Attack Patterns

These attack patterns are a combination of attacks that lead to both data breaches and computer incidents within the Verizon DBIR. The latter may not necessarily lead to sensitive information being exposed to the public.

The following attack patterns are included within the CDM:

- Web-Application Hacking
- Insider and Privilege Misuse
- Malware
- Ransomware
- Targeted Intrusions

The following sections define each of the attack patterns and justify their inclusion within the overall CDM. These are presented in order of priority based on data from the Verizon DBIR.

Web-Application Hacking

The Verizon DBIR shows that web-application hacking is the top reason for a breach, accounting for over 60% of all breaches. The Verizon DBIR defines this attack pattern as *"any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms,"* (Verizon DBIR, 2019). The report also states that *"Over one-half of breaches in this pattern are associated with unauthorized access of cloud-based email servers."* CIS expanded this attack pattern to include attacks on the underlying platform supporting the web application.

When defining this attack pattern, CIS looked to standards and best practices that help prevent web-application hacking. One such example is the Open Web Application Security Project (OWASP) Top 10. These 10 security issues outline some of the most critical web-application security concerns that developers should understand and defend against. The report is regularly updated and compiled by a team of security experts from all over the world.

The Web-Application Attack Pattern created via the ATT&CK Model can be found in Appendix A (page A2).

Insider and Privilege Misuse

The Verizon DBIR indicates that roughly 15% of data breaches result from authorized users misusing their access. The report defines this category as *"all incidents tagged with the action category of Misuse—any unapproved or malicious use of organizational resources—fall within this pattern,"* (Verizon DBIR, 2019). It's also stated that this attack pattern primarily encompasses *"insider-only misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well."* A selection of Techniques associated with exploiting trust and using existing accounts is included within this pattern.

The Insider and Privilege Misuse Attack Pattern created via the ATT&CK Model can be found in Appendix A (page A3).

Malware

The Verizon DBIR refers to this attack pattern as "crimeware," and it includes all malware-related breaches that did not fit into a more specific pattern. The CIS CDM includes all types of malware, excluding ransomware and destructive malware within this attack pattern. The Verizon DBIR states that 28% of all breaches involved some sort of malware. The Techniques mapped to this attack pattern are identified by the MS-ISAC based on incidents reported and data acquired via Albert sensors during June of 2019. Additional information about the CIS Albert sensors is available on the CIS website. They are based on a snapshot in time and will need to be regularly updated and reviewed in order to reflect the current threat landscape.

The Malware Attack Pattern created via the ATT&CK Model can be found in Appendix A (page A4).

Ransomware

The ransomware attack pattern could be viewed as a subset of the malware attack pattern. Yet, the motivations, tactics, and outcomes exhibited by ransomware and other destructive malware often drastically differ from traditional malware. Ultimately, ransomware was separated into a distinct attack pattern. The Verizon DBIR indicates that around 30% of malware incidents involved ransomware (Verizon DBIR, 2019). Common techniques unique to ransomware are: intentionally encrypting data regardless of who owns the cryptographic key and preventing a system from functioning properly.

The Ransomware Attack Pattern created via the ATT&CK Model can be found in Appendix A (page A5).

Targeted Intrusions

The Verizon DBIR refers to this attack pattern as "cyber-espionage," and it includes *"… unauthorized network or system access linked to state-affiliated actors and/or exhibiting the motive of espionage,"* (Verizon DBIR, 2019). The Verizon DBIR states that cyber-espionage accounts for around 20% of all breaches. Techniques associated with this attack pattern require access to large resources and expert-level knowledge. Information regarding this ATT&CK mapping is sourced from CrowdStrike's 2019 Global Threat Report.

The Targeted Intrusions Attack Pattern created via the ATT&CK Model can be found in Appendix A (page A6).

Assessment of CIS Controls Against Attack Patterns

The ATT&CK Model mapping provides the ability to assess the effectiveness of the Controls to help an organization defend against the top attack patterns previously identified in the *Attack Patterns* portion of the document. The following sections provide insight into how the Controls, with a closer look at IG1 (Basic Cyber Hygiene), mitigate the Techniques at various stages of the attack, for the identified attack patterns. Techniques repeated at various stages of the attack cycle were counted for each respective stage to provide insight into Controls' ability to defend at each stage. As such, the number of Techniques outlined are not unique values of the Techniques identified for the attack pattern. In the graphs below, orange represents Techniques for which a 1:1 mitigation was either unavailable or did not map to a Safeguard; blue represents Techniques for which a 1:1 mitigation and mapping to an IG2 or IG3 Safeguard exists; and green indicates an instance where an IG1 Safeguard mapped.

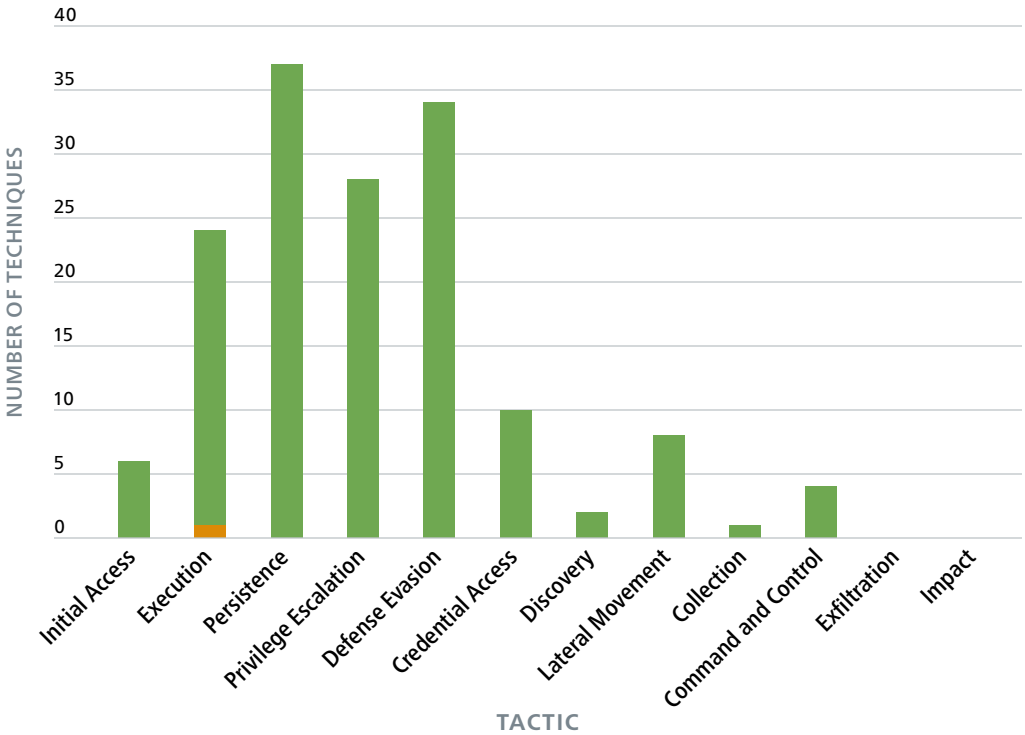
Web-Application Hacking

For the web-application hacking attack pattern, 154 instances of Techniques were identified throughout the attack cycle. As noted by the graph below, 154 of those instances can be defended against by the Controls, and in this case all but one Technique can be defended against by IG1 Safeguards.

Web-application Hacking Mapping

Each IG builds upon the previous level

- IG1
- IG2 or IG3
- No Mapping to Controls



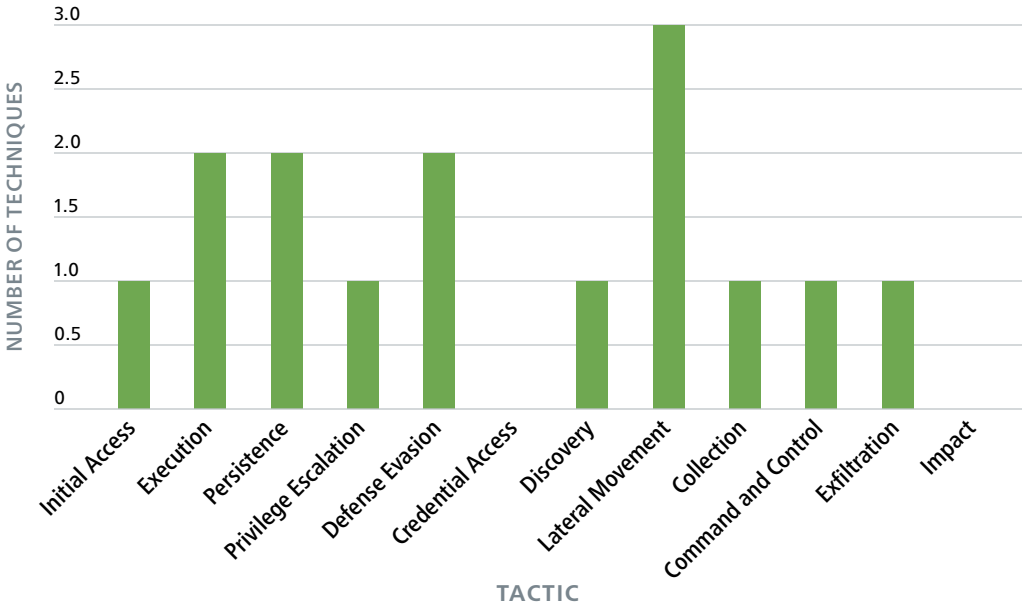
Insider and Privilege Misuse

Fifteen Techniques at various attack stages mapped to the insider and privilege misuse attack pattern. In this attack pattern, all Techniques can be defended against by properly implementing IG1 Safeguards.

Insider and Privilege Misuse Mapping

Each IG builds upon the previous level

- IG1
- IG2 or IG3
- No Mapping to Controls



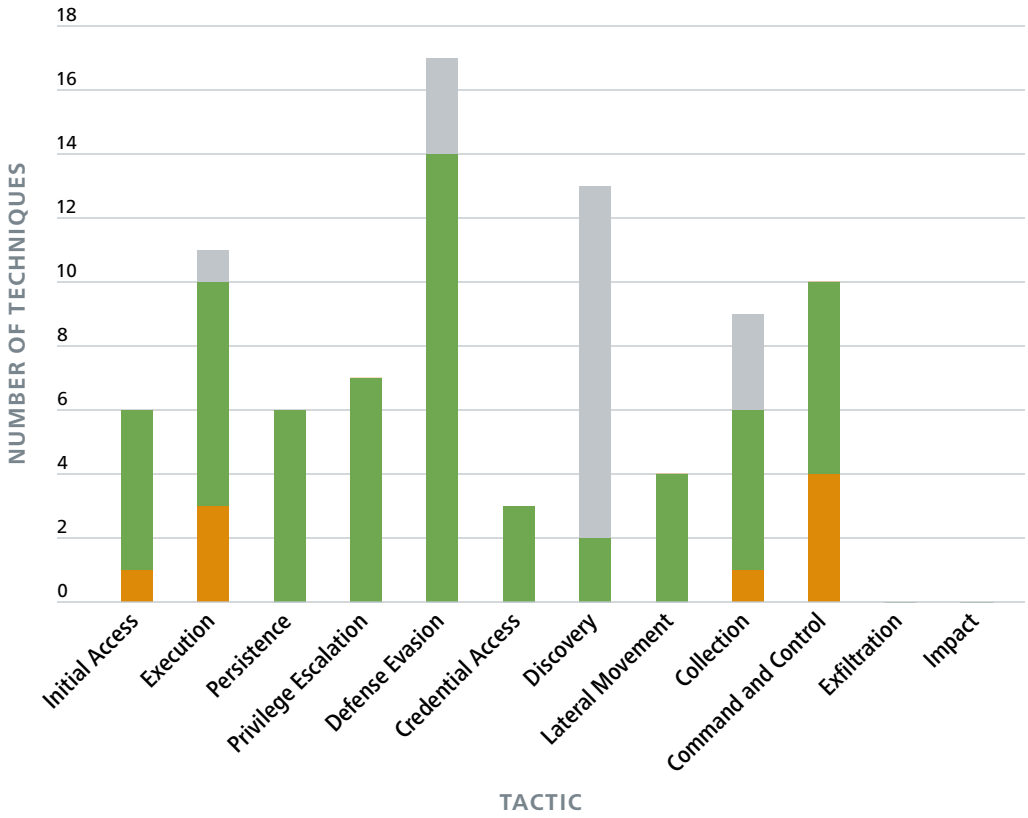
Malware

The malware attack pattern contained 86 Techniques at various stages of the attack cycle. Of those 86 Techniques, approximately 21% (18) of the Techniques did not have a Mitigation mapping to any Safeguards. The majority of those Techniques are within the Discovery stage of the attack cycle and Defense Evasion. Based on current mapping, 68 Techniques can be defended against by the Safeguards, with approximately 79% of those Safeguards contained within IG1.

Malware Mapping

Each IG builds upon the previous level

- IG1
- IG2 or IG3
- No Mapping to Controls



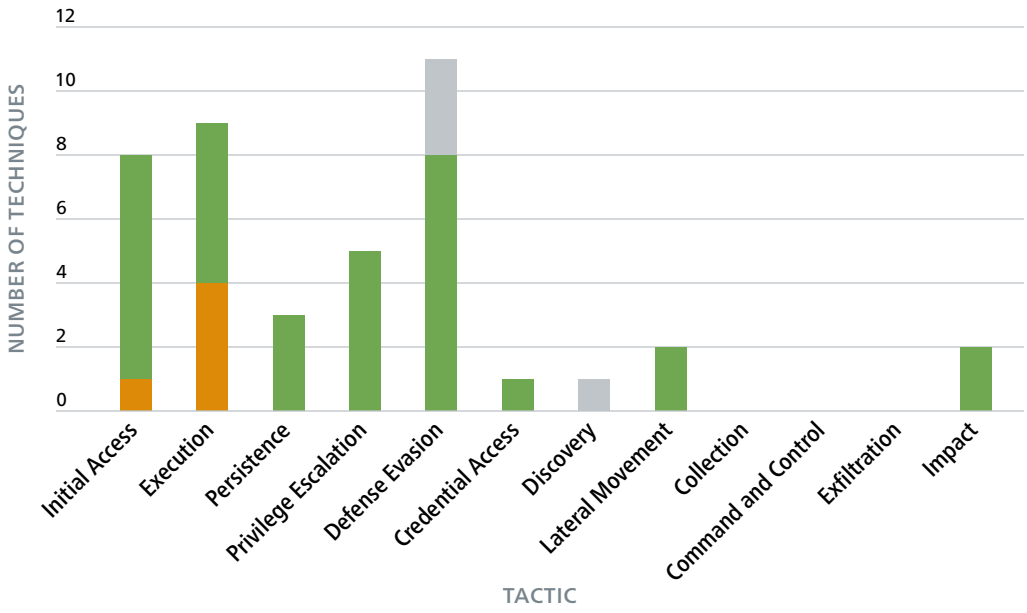
Ransomware

Within the ransomware attack pattern mapping, 42 Technique instances were identified throughout the attack cycle. The Safeguards map to Mitigations that defend against approximately 90% (38) of the Techniques identified for this attack pattern. Approximately 87% are IG1 Safeguards. Of significant importance, Techniques used to gain initial access, execute, and minimize impacts associated with ransomware can be defended against through the Controls. Based on current mapping, Defensive Evasion and Discovery stages are currently not defended against through the Controls.

Ransomware Mapping

Each IG builds upon the previous level

- IG1
- IG2 or IG3
- No Mapping to Controls



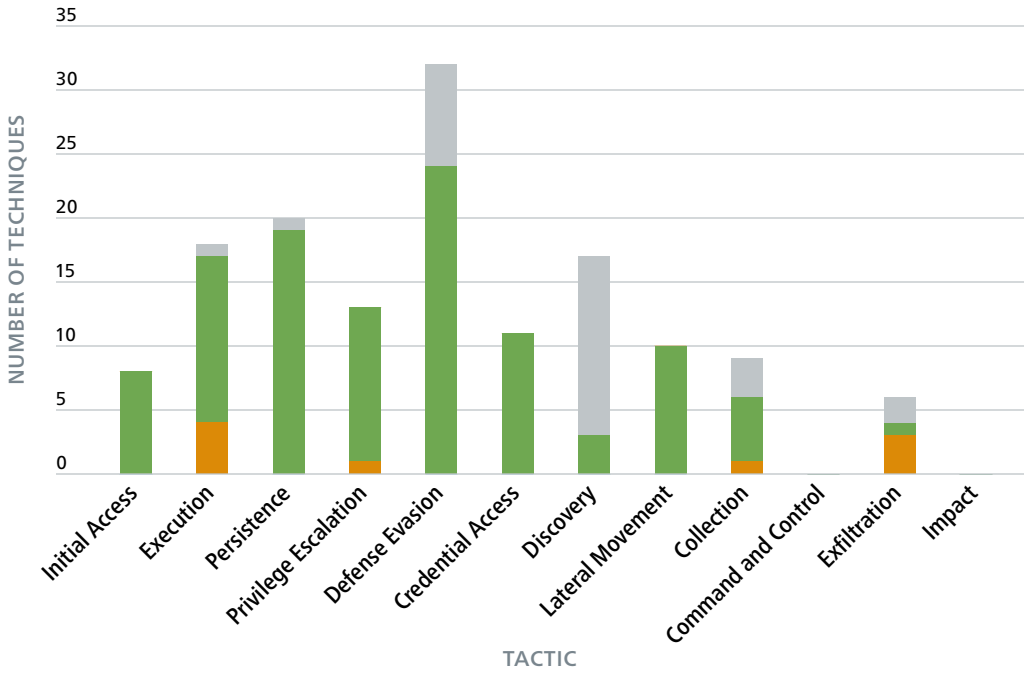
Targeted Intrusion

For the targeted intrusion attack pattern, 144 Techniques were identified at various stages of the attack cycle. The Controls help defend against approximately 80% (115) of those Techniques, with IG1 Safeguards covering 109 Techniques. Unmapped Techniques primarily fall within the Defense Evasion and Discovery phases of the attack cycle.

Targeted Intrusions Mapping

Each IG builds upon the previous level

- IG1
- IG2 or IG3
- No Mapping to Controls



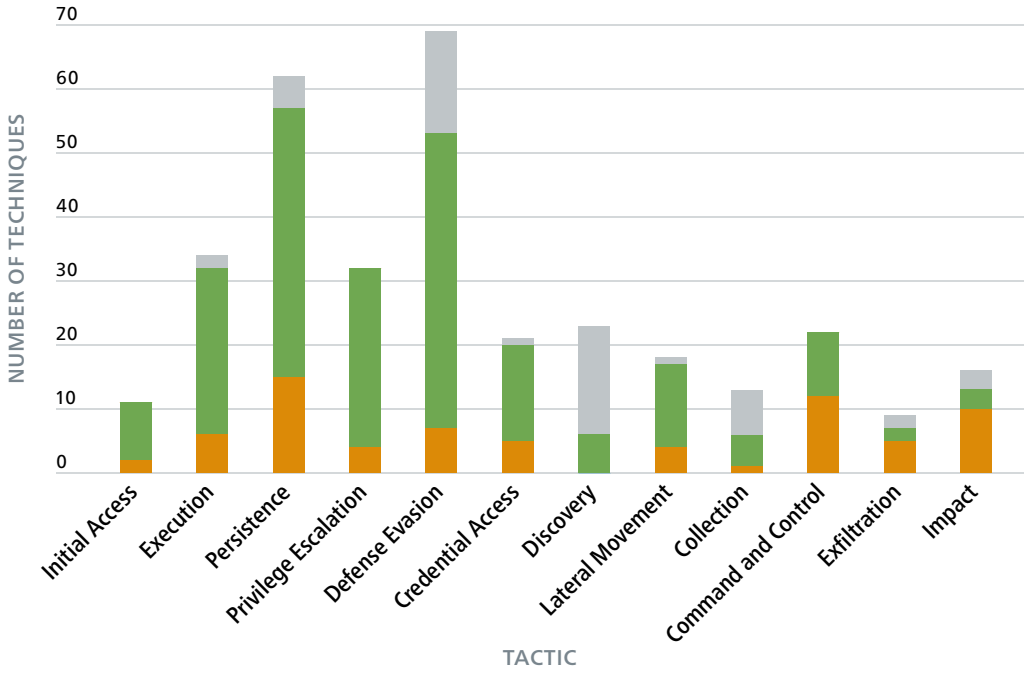
Mapping Summary

This effort is meant to help prioritize and identify the Controls and Safeguards that organizations should look to implement within their networks first. Note that accidents, acts of God, and physical attacks generally are not covered within the ATT&CK Model and are not reflected within the CDM. The CDM is also meant to assess IG1 or Basic Cyber Hygiene. IG1 provides defense against approximately 62% of the Techniques identified in the ATT&CK Model with a focus on the Initial Access, Execution, Persistence, Privilege Escalation, and Defense Evasion of the top attack patterns—stages in which, if successfully defended, organizations can mitigate subsequent impacts of the attack.

Overall Mapping

Each IG builds upon the previous level

- IG1
- IG2 or IG3
- No Mapping to Controls



Future Work

While this is not an "easy button" for cyber defense, we believe that the CDM significantly advances our goal of bringing more rigor, data, and transparency to the establishment of specific security value to the selection of individual controls, and to control strategies and frameworks. For the near term, this CDM will be used to bolster CIS Recommendations for Basic Cyber Hygiene, and to help develop Safeguard recommendations and prioritization in the next version of the CIS Controls.

This work is also the basis for some exciting future projects at CIS, and by others, including those described below.

- Future iterations of the CDM will integrate a broader selection of data and reports about current attacks.
- Specific communities of interest with insight about attacks relevant to them (e.g., critical sectors, ISACs, closed sharing groups) could build upon the CDM to fine-tune their collective priorities and security control strategies.
- By identifying control implementation options (e.g., configuration choices, architectures, tools, processes) and their associated costs, we could start to support economic decision-making, e.g., "For my enterprise, what are my lowest-cost options to get the security-value of IG1," "How much would it cost to mitigate the top 10 attacks seen in my sector last year?"
- CIS is now an active member of the Center for Threat-Informed Defense, the center within MITRE that is responsible for the maintenance and evolution of the MITRE ATT&CK Model. We are focused on improving the mapping from attack patterns to control choices. This will also help us illustrate the security value found in a variety of security and regulatory frameworks. Additionally, Safeguards will be associated directly to Techniques and not just through the Mitigations.

Finally, the CDM will be used to help prioritize which Safeguards should be within different IGs.

- As with all CIS products, readers are encouraged to reach out to controlsinfo@cisecurity.org to participate and make this effort stronger.

The ATT&CK matrix and all other matrices for the attack patterns are available within the CIS Community Defense Model space within CIS WorkBench and via the CIS website in both JavaScript Object Notation (JSON) and Excel formats. The master ATT&CK Model can be found in Appendix A (page A7).

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 document 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

CIS Controls®

Appendix A

ATT&CK Model Applied to Attack Patterns Included in the CDM

These attack patterns are presented in order of priority based on the findings from the Verizon DBIR and represent attacks that led to data breaches, computer incidents, or a combination of both. The tables on pages A2–A7, in general, depict the ATT&CK Model to include all Tactics and applicable Techniques within the Tactics.

Techniques highlighted in blue indicate the Techniques applicable to the attack pattern.

Appendix A

ATT&CK Model Applied to Attack Patterns Included in the CDM

CIS Controls®

Web-App-Cam-v3

FILTERS | **Stages:** Act | **Platforms:** Windows, Linux, MacOS

Techniques highlighted in blue indicate the Techniques applicable to the attack pattern.

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Component Object Model and Distributed COM
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trap
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

Persistence
- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- Emond
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Launch Agent
- Launch Daemon
- Launchctl
- LC_LOAD_DYLIB Addition
- Local Job Scheduling
- Login Item
- Logon Scripts
- LSASS Driver
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Plist Modification
- Port Knocking
- Port Monitors
- PowerShell Profile
- Rc.common
- Re-opened Applications
- Redundant Access
- Registry Run Keys / Startup Folder
- Scheduled Task
- Screensaver
- Security Support Provider
- Server Software Component
- Service Registry Permissions Weakness
- Setuid and Setgid
- Shortcut Modification
- SIP and Trust Provider Hijacking
- Startup Items
- System Firmware
- Systemd Service
- Time Providers
- Trap
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

Privilege Escalation
- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Elevated Execution with Prompt
- Emond
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Parent PID Spoofing
- Path Interception
- Plist Modification
- Port Monitors
- PowerShell Profile
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- Setuid and Setgid
- SID-History Injection
- Startup Items
- Sudo
- Sudo Caching
- Valid Accounts
- Web Shell

Defense Evasion
- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Connection Proxy
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File and Directory Permissions Modification
- File Deletion
- File System Logical Offsets
- Gatekeeper Bypass
- Group Policy Modification
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- HISTCONTROL
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Launchctl
- LC_MAIN Hijacking
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Parent PID Spoofing
- Plist Modification
- Port Knocking
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Packing
- Space after Filename
- Template Injection
- Timestomp
- Trusted Developer Utilities
- Valid Accounts
- Virtualization/Sandbox Evasion
- Web Service
- XSL Script Processing

Credential Access
- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials from Web Browsers
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Steal Web Session Cookie
- Two-Factor Authentication Interception

Discovery
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
- AppleScript
- Application Deployment Software
- Component Object Model and Distributed COM
- Exploitation of Remote Services
- Internal Spearphishing
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- System Shutdown/Reboot
- Transmitted Data Manipulation

Appendix A

ATT&CK Model Applied to Attack Patterns Included in the CDM

CIS Controls®

PrivilegeMisuse-v1

FILTERS | **Stages:** Act | **Platforms:** Windows, Linux, MacOS

Initial Access

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Techniques highlighted in blue indicate the Techniques applicable to the attack pattern.

Execution

- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Component Object Model and Distributed COM
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trap
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

Persistence

- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- Emond
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Launch Agent
- Launch Daemon
- Launchctl
- LC_LOAD_DYLIB Addition
- Local Job Scheduling
- Login Item
- Logon Scripts
- LSASS Driver
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Plist Modification
- Port Knocking
- Port Monitors
- PowerShell Profile
- Rc.common
- Re-opened Applications
- Redundant Access
- Registry Run Keys / Startup Folder
- Scheduled Task
- Screensaver
- Security Support Provider
- Server Software Component
- Service Registry Permissions Weakness
- Setuid and Setgid
- Shortcut Modification
- SIP and Trust Provider Hijacking
- Startup Items
- System Firmware
- Systemd Service
- Time Providers
- Trap
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

Privilege Escalation

- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Elevated Execution with Prompt
- Emond
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Parent PID Spoofing
- Path Interception
- Plist Modification
- Port Monitors
- PowerShell Profile
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- Setuid and Setgid
- SID-History Injection
- Startup Items
- Sudo
- Sudo Caching
- Valid Accounts
- Web Shell

Defense Evasion

- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Connection Proxy
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File and Directory Permissions Modification
- File Deletion
- File System Logical Offsets
- Gatekeeper Bypass
- Group Policy Modification
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- HISTCONTROL
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Launchctl
- LC_MAIN Hijacking
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Parent PID Spoofing
- Plist Modification
- Port Knocking
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Packing
- Space after Filename
- Template Injection
- Timestomp
- Trusted Developer Utilities
- Valid Accounts
- Virtualization/Sandbox Evasion
- Web Service
- XSL Script Processing

Credential Access

- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials from Web Browsers
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Steal Web Session Cookie
- Two-Factor Authentication Interception

Discovery

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement

- AppleScript
- Application Deployment Software
- Component Object Model and Distributed COM
- Exploitation of Remote Services
- Internal Spearphishing
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection

- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control

- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- System Shutdown/Reboot
- Transmitted Data Manipulation

Appendix A

ATT&CK Model Applied to Attack Patterns Included in the CDM

CIS Controls®

MS-ISAC Top 10

FILTERS | **Stages:** Act | **Platforms:** Windows, Linux, MacOS

Techniques highlighted in blue indicate the Techniques applicable to the attack pattern.

Initial Access

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution

- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Component Object Model and Distributed COM
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trap
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

Persistence

- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- Emond
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Launch Agent
- Launch Daemon
- Launchctl
- LC_LOAD_DYLIB Addition
- Local Job Scheduling
- Login Item
- Logon Scripts
- LSASS Driver
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Plist Modification
- Port Knocking
- Port Monitors
- PowerShell Profile
- Rc.common
- Re-opened Applications
- Redundant Access
- Registry Run Keys / Startup Folder
- Scheduled Task
- Screensaver
- Security Support Provider
- Server Software Component
- Service Registry Permissions Weakness
- Setuid and Setgid
- Shortcut Modification
- SIP and Trust Provider Hijacking
- Startup Items
- System Firmware
- Systemd Service
- Time Providers
- Trap
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

Privilege Escalation

- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Elevated Execution with Prompt
- Emond
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Parent PID Spoofing
- Path Interception
- Plist Modification
- Port Monitors
- PowerShell Profile
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- Setuid and Setgid
- SID-History Injection
- Startup Items
- Sudo
- Sudo Caching
- Valid Accounts
- Web Shell

Defense Evasion

- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Connection Proxy
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File and Directory Permissions Modification
- File Deletion
- File System Logical Offsets
- Gatekeeper Bypass
- Group Policy Modification
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- HISTCONTROL
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Launchctl
- LC_MAIN Hijacking
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Parent PID Spoofing
- Plist Modification
- Port Knocking
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Packing
- Space after Filename
- Template Injection
- Timestomp
- Trusted Developer Utilities
- Valid Accounts
- Virtualization/Sandbox Evasion
- Web Service
- XSL Script Processing

Credential Access

- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials from Web Browsers
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Steal Web Session Cookie
- Two-Factor Authentication Interception

Discovery

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement

- AppleScript
- Application Deployment Software
- Component Object Model and Distributed COM
- Exploitation of Remote Services
- Internal Spearphishing
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection

- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control

- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- System Shutdown/Reboot
- Transmitted Data Manipulation

Appendix A

ATT&CK Model Applied to Attack Patterns Included in the CDM

CIS Controls®

Ransomware-v1

FILTERS | **Stages:** Act | **Platforms:** Windows, Linux, MacOS

Techniques highlighted in blue indicate the Techniques applicable to the attack pattern.

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Component Object Model and Distributed COM
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trap
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

Persistence
- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- Emond
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Launch Agent
- Launch Daemon
- Launchctl
- LC_LOAD_DYLIB Addition
- Local Job Scheduling
- Login Item
- Logon Scripts
- LSASS Driver
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Plist Modification
- Port Knocking
- Port Monitors
- PowerShell Profile
- Rc.common
- Re-opened Applications
- Redundant Access
- Registry Run Keys / Startup Folder
- Scheduled Task
- Screensaver
- Security Support Provider
- Server Software Component
- Service Registry Permissions Weakness
- Setuid and Setgid
- Shortcut Modification
- SIP and Trust Provider Hijacking
- Startup Items
- System Firmware
- Systemd Service
- Time Providers
- Trap
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

Privilege Escalation
- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Elevated Execution with Prompt
- Emond
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Parent PID Spoofing
- Path Interception
- Plist Modification
- Port Monitors
- PowerShell Profile
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- Setuid and Setgid
- SID-History Injection
- Startup Items
- Sudo
- Sudo Caching
- Valid Accounts
- Web Shell

Defense Evasion
- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Connection Proxy
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File and Directory Permissions Modification
- File Deletion
- File System Logical Offsets
- Gatekeeper Bypass
- Group Policy Modification
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- HISTCONTROL
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Launchctl
- LC_MAIN Hijacking
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Parent PID Spoofing
- Plist Modification
- Port Knocking
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Packing
- Space after Filename
- Template Injection
- Timestomp
- Trusted Developer Utilities
- Valid Accounts
- Virtualization/Sandbox Evasion
- Web Service
- XSL Script Processing

Credential Access
- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials from Web Browsers
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Steal Web Session Cookie
- Two-Factor Authentication Interception

Discovery
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
- AppleScript
- Application Deployment Software
- Component Object Model and Distributed COM
- Exploitation of Remote Services
- Internal Spearphishing
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- System Shutdown/Reboot
- Transmitted Data Manipulation

Appendix A

ATT&CK Model Applied to Attack Patterns Included in the CDM

CIS Controls®

CrowdStrike Heat Map

FILTERS | **Stages:** Act | **Platforms:** Windows, Linux, MacOS

Initial Access

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Techniques highlighted in blue indicate the Techniques applicable to the attack pattern.

Execution

- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Component Object Model and Distributed COM
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trap
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

Persistence

- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- Emond
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Launch Agent
- Launch Daemon
- Launchctl
- LC_LOAD_DYLIB Addition
- Local Job Scheduling
- Login Item
- Logon Scripts
- LSASS Driver
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Plist Modification
- Port Knocking
- Port Monitors
- PowerShell Profile
- Rc.common
- Re-opened Applications
- Redundant Access
- Registry Run Keys / Startup Folder
- Scheduled Task
- Screensaver
- Security Support Provider
- Server Software Component
- Service Registry Permissions Weakness
- Setuid and Setgid
- Shortcut Modification
- SIP and Trust Provider Hijacking
- Startup Items
- System Firmware
- Systemd Service
- Time Providers
- Trap
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

Privilege Escalation

- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Elevated Execution with Prompt
- Emond
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Parent PID Spoofing
- Path Interception
- Plist Modification
- Port Monitors
- PowerShell Profile
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- Setuid and Setgid
- SID-History Injection
- Startup Items
- Sudo
- Sudo Caching
- Valid Accounts
- Web Shell

Defense Evasion

- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Connection Proxy
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File and Directory Permissions Modification
- File Deletion
- File System Logical Offsets
- Gatekeeper Bypass
- Group Policy Modification
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- HISTCONTROL
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Launchctl
- LC_MAIN Hijacking
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Parent PID Spoofing
- Plist Modification
- Port Knocking
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Packing
- Space after Filename
- Template Injection
- Timestomp
- Trusted Developer Utilities
- Valid Accounts
- Virtualization/Sandbox Evasion
- Web Service
- XSL Script Processing

Credential Access

- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials from Web Browsers
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Steal Web Session Cookie
- Two-Factor Authentication Interception

Discovery

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement

- AppleScript
- Application Deployment Software
- Component Object Model and Distributed COM
- Exploitation of Remote Services
- Internal Spearphishing
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection

- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control

- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- System Shutdown/Reboot
- Transmitted Data Manipulation

ATT&CK Model Applied to Attack Patterns Included in the CDM

CIS Controls®

Mapping Master

FILTERS | **Stages:** Act | **Platforms:** Windows, Linux, MacOS

Techniques highlighted in blue indicate the Techniques applicable to the attack pattern.

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Component Object Model and Distributed COM
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Space after Filename
- Third-party Software
- Trap
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management
- XSL Script Processing

Persistence
- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- Emond
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Launch Agent
- Launch Daemon
- Launchctl
- LC_LOAD_DYLIB Addition
- Local Job Scheduling
- Login Item
- Logon Scripts
- LSASS Driver
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Plist Modification
- Port Knocking
- Port Monitors
- PowerShell Profile
- Rc.common
- Re-opened Applications
- Redundant Access
- Registry Run Keys / Startup Folder
- Scheduled Task
- Screensaver
- Security Support Provider
- Server Software Component
- Service Registry Permissions Weakness
- Setuid and Setgid
- Shortcut Modification
- SIP and Trust Provider Hijacking
- Startup Items
- System Firmware
- Systemd Service
- Time Providers
- Trap
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

Privilege Escalation
- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Elevated Execution with Prompt
- Emond
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Parent PID Spoofing
- Path Interception
- Plist Modification
- Port Monitors
- PowerShell Profile
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- Setuid and Setgid
- SID-History Injection
- Startup Items
- Sudo
- Sudo Caching
- Valid Accounts
- Web Shell

Defense Evasion
- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Connection Proxy
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File and Directory Permissions Modification
- File Deletion
- File System Logical Offsets
- Gatekeeper Bypass
- Group Policy Modification
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- HISTCONTROL
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Launchctl
- LC_MAIN Hijacking
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Parent PID Spoofing
- Plist Modification
- Port Knocking
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Packing
- Space after Filename
- Template Injection
- Timestomp
- Trusted Developer Utilities
- Valid Accounts
- Virtualization/Sandbox Evasion
- Web Service
- XSL Script Processing

Credential Access
- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials from Web Browsers
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL
- Private Keys
- Securityd Memory
- Steal Web Session Cookie
- Two-Factor Authentication Interception

Discovery
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
- AppleScript
- Application Deployment Software
- Component Object Model and Distributed COM
- Exploitation of Remote Services
- Internal Spearphishing
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Command And Control
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- System Shutdown/Reboot
- Transmitted Data Manipulation

Appendix B

Background

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

The earliest versions of the 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 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; and the mapping from summaries and patterns of attack to the Controls was still informal and based on the judgment of relatively few people.

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

1. steps of the attacker's life-cycle (similar to the well-known Lockheed Martin Cyber Kill Chain) and
2. categories of defensive effect, for which we used the Core Functions of the National Institute of Standards and Technology (NIST) Cyber Security Framework.

This approach helped CIS focus on questions like, "What types of countermeasures could help prevent the Delivery phase of an attacker's life-cycle?" 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 succeeds?" 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.

CIS Controls®

Appendix C

Acronyms and Abbreviations

ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CDM	Community Defense Model
CIS	Center for Internet Security
DBIR	Data Breach Investigations Report
IBM	International Business Machines
ICS	Industrial Control Systems
IG	Implementation Group
ISAC	Information Sharing and Analysis Center
IT	Information Technology
JSON	JavaScript Object Notation
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
VCDB	VERIS Community Database
VERIS	Vocabulary for Event Recording and Incident Sharing

Appendix D

Links and Resources

- CIS Controls
  https://www.cisecurity.org/controls/
- CIS Controls Navigator
  https://www.cisecurity.org/controls/cis-controls-implementation-groups
- CrowdStrike Threat Report
  https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
- FireEye M-Trends Report
  https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
- IBM X-Force Threat Intelligence Index
  https://www.ibm.com/security/resources/xforce/xfisi
- Lockheed Martin Killchain
  https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- Microsoft Security Intelligence Report
  https://www.microsoft.com/en-us/security/business/security-intelligence-report
- MITRE ATT&CK
  https://attack.mitre.org
- MS-ISAC
  https://www.cisecurity.org/ms-isac/
- MS-ISAC Top 10 Malware June 2019
  https://www.cisecurity.org/blog/top-10-malware-june-2019
- M-Trends Turns 10: A Retrospective
  https://www.fireeye.com/blog/executive-perspective/2019/02/m-trends-turns-ten.html
- OWASP Top 10
  https://owasp.org/www-project-top-ten
- SANS Institute
  https://www.sans.org/findtraining/
- Symantec Internet Security Threat Report
  https://www.symantec.com/security-center/threat-report
- 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
- Verizon Data Breach Investigations Report
  https://enterprise.verizon.com/resources/reports/dbir/

Appendix E

Mapping CIS Safeguards to ATT&CK Techniques

The following are the MITRE ATT&CK Techniques that have no mapping at all to the CIS Safeguards.

- Account Access Removal
- AppCert DLLs
- AppInit DLLs
- AppleScript
- Application Shimming
- Application Window Discovery
- Authentication Package
- Binary Padding
- Bootkit
- Browser Bookmark Discovery
- Browser Extensions
- Change Default File Association
- CMSTP
- Compile After Delivery
- Compiled HTML File
- Component Firmware
- Connection Proxy
- Control Panel Items
- Credentials from Web Browsers
- Custom Command and Control Protocol
- Data Destruction
- Data Encoding
- Data from Removable Media
- DCShadow
- Disk Content Wipe
- Disk Structure Wipe
- Domain Fronting
- Domain Generation Algorithms
- Dylib Hijacking
- Dynamic Data Exchange
- Elevated Execution with Prompt
- Emond
- Endpoint Denial of Service
- Execution Guardrails
- Exfiltration Over Other Network Medium
- Extra Window Memory Injection
- File System Logical Offsets
- Firmware Corruption
- Forced Authentication
- Gatekeeper Bypass
- Hardware Additions
- Hidden Users
- Hidden Window
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Indirect Command Execution
- Input Prompt
- Install Root Certificate
- Internal Spearphishing
- Kernel Modules and Extensions
- Launch Agent
- Launchctl
- LC_LOAD_DYLIB Addition
- LC_MAIN Hijacking
- LLMNR/NBT-NS Poisoning and Relay
- Login Item
- LSASS Driver
- Multiband Communication
- Multilayer Encryption
- Multi-Stage Channels
- Network Denial of Service
- NTFS File Attributes
- Office Application Startup
- Parent PID Spoofing
- Pass the Ticket
- Password Filter DLL
- Plist Modification
- Port Knocking
- Port Monitors
- PowerShell Profile
- Process Doppelgänging
- Rc.common
- Regsvcs/Regasm
- Re-opened Applications
- Resource Hijacking
- Runtime Data Manipulation
- Screensaver
- Security Support Provider
- Securityd Memory
- Service Execution
- Service Stop
- Shared Webroot
- SID-History Injection
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Discovery
- Source
- Spearphishing via Service
- SSH Hijacking
- Standard Non-Application Layer Protocol
- Startup Items
- Stored Data Manipulation
- Sudo
- Sudo Caching
- System Firmware
- System Shutdown/Reboot
- Systemd Service
- Taint Shared Content
- Template Injection
- Time Providers
- Transmitted Data Manipulation
- Trap
- Virtualization/Sandbox Evasion
- Winlogon Helper DLL
- XSL Script Processing

Appendix F

Unmapped Techniques within Attack Patterns

The following MITRE Enterprise ATT&CK Techniques were associated with attack patterns in the Community Defense Model efforts. These were unable to be associated with CIS Sub-Controls. Specifically, most of the techniques listed below were provided with a mitigation stating *"This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features."*

T1123	Audio Capture
T1115	Clipboard Data
T1116	Code Signing
T1122	Component Object Model Hijacking
T1140	Deobfuscate/Decode Files or Information
T1083	File and Directory Discovery
T1222	File and Directory Permissions Modification
T1107	File Deletion
T1061	Graphical User Interface
T1158	Hidden Files and Directories
T1066	Indicator Removal from Tools
T1128	Netsh Helper DLL
T1126	Network Share Connection Removal
T1135	Network Share Discovery
T1120	Peripheral Device Discovery
T1057	Process Discovery
T1093	Process Hollowing
T1012	Query Registry
T1018	Remote System Discovery
T1113	Screen Capture
T1063	Security Software Discovery
T1151	Space after Filename
T1082	System Information Discovery
T1016	System Network Configuration Discovery
T1049	System Network Connections Discovery
T1125	Video Capture

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 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. elections 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