

The Center for Internet Security Community Attack Model

**

The Center for Internet Security

CIS Community Attack Model

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided.   Additionally, if you remix, transform or build upon the CIS Critical Security Controls, you may not distribute the modified materials. Users of the CIS Critical Security Controls framework are also required to refer to (http://www.cisecurity.org/critical-controls.cfm) when referring to the CIS Critical Security Controls in order to ensure that users are employing the most up to date guidance.  Commercial use of the CIS Critical Security Controls is subject to the prior approval of The Center for Internet Security.

# The Center for Internet Security Community Attack Model

## Introduction

The headlines about high profile security breaches are relentless. Massive data losses, theft of intellectual property, credit card breaches, identity theft, threats to our privacy, denial of service – these have become a way of life in cyberspace, affecting governments, companies large and small, and individuals. Business complexity is growing, dependencies are expanding, users are more mobile, and the threats are evolving.

Policy makers and the marketplace have responded with a focus on “threat sharing” and “cyber intelligence” as the keys to success. New threat data companies are hatched to meet the rising demand for data while policy makers forge agreements across government, defense contractors and private sectors to share ever more information. The general notion is that the more information we can gather about attackers and attacks, the better we will be able to defend ourselves.

While we do need more accurate information to drive cyber defense, threat intelligence is not the solution to the problem; it’s a *means to an end* – that of better defenses. Cyber defenders are already overwhelmed by an extraordinary array of security tools and technology, standards, training, certifications, vulnerability databases, threat feeds, best practices, and recommendations. They face very real constraints and challenges: money, time, conflicting guidance, management attention, and multiple sources of oversight. But all of this technology, information, and oversight have become what we call the cybersecurity “Fog of More”: competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action.

So the foundational challenge is not about acquiring more information, it’s the *translation* of information into action.

We all operate in the same environment, use the same technology, and face very similar problems. The Center for Internet Security (CIS) believes the best approach is for the community to work together up-front to identify the key problems we all face and identify the root causes. And then we must share the labor needed to translate this into prioritized, scalable defensive action that can be used by all enterprises.

The Center for Internet Security Critical Security Controls for Effective Cyber Defense Version 6.1 (CIS Controls) is a set of prioritized best practices developed by a community of security experts proven to mitigate the most common threats. Since their inception, the CIS Controls have always approached the prioritization challenge with a basic tenet of *“Offense Informs Defense.”* That is, knowledge of specific attacks that have actually compromised systems (the Bad Guys’ “offense”) must be the key factor to determine the value of specific defensive actions. What are attackers doing to us now, and what are the most useful, scalable actions we can take to stop them? Cyber defense guidance is filled with speculation about what might happen. We choose to make sense of what is actually happening.

The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cyber- security; deliver world-class cyber-security solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace. For additional information, go to <<http://www.cisecurity.org/>>

We apply knowledge of attacks and effective defenses by gathering experts from: every part of the ecosystem (companies, governments, individuals); every role (threat responders and analysts, technologists, vulnerability finders, tool makers, solution providers, defenders, users, policy makers, auditors, etc.); and many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT).

Early versions of the CIS Controls used a simple, informal list of attacks based on the first-hand experience of experts against which to examine possible Controls. In more recent versions we enriched this process by mapping from a well-documented and authoritative source of “real life” data - the Verizon Data Breach Investigations Report (2013, 2014, 2015). After the Verizon team does their primary analysis each year, a volunteer team formed by CIS maps the most important categories or types of attacks seen in the prior year’s data directly to the CIS Controls (at a sub-Control) level, and this map becomes an important part of the Verizon DBIR Recommendations. We repeated this process with several other security vendors, and many others have agreed to do something similar. All of these maps will be made available to the public so that enterprises 1) have confidence that the CIS Controls are based on a large-scale, independent, and authoritative view of the attackers, and 2) can use them as starting point for designing and implementing their own security improvement program.

In this document, we describe the next step of evolution in this process - an open public framework or model into which we can map from multiple authoritative summaries of attack information in a way that naturally supports the identification of high-value defensive action. We call this the CIS Community Attack Model.

## A Community Approach to Understanding Attacks

What do we mean by a Community Attack Model? It is a process to gather lots of relevant real-life information about successful attacks, and organize it in a way that helps enterprises make good choices about the most effective defensive actions they can take. It assimilates the Fog of More into something meaningful and actionable. Its primary purpose is to use the information to update the CIS Controls and ensure that they are based on the most current and relevant threat knowledge. “Community” refers to the breadth of the participants and information sources, and also to the shared labor that operates this process. The Model acknowledges that these are risks that the entire Community faces – the documented, specific successes of attackers. Every enterprise (and its partners, suppliers, customers, etc.) has to deal with these problems, and so the most effective strategy is for the Community to share ideas, knowledge, and action up-front. This approach is fundamental to the work of the Center for Internet Security.

The Community Attack Model has a number of essential attributes. It is:

* driven by data from multiple authoritative, publicly available summaries of attacks (e.g., the Verizon Data Breach Investigations Report, the Symantec ISTR);
* focused on characterizing and summarizing attacks by class or type, not on trying to capture complex, nuanced, and highly targeted actions;
* based on a well-defined process to translate from attacks to action (Controls) in a way that supports prioritization and is consistent with formal Risk Management Frameworks;
* updated on an ongoing “refresh cycle” to validate prior defensive choices, and to assess the impact of new information on the Model;
* low/shared cost to create, operate, and use;
* support views and discussions at multiple levels, including executive, planning, operational, and technical; and
* openly demonstrable to others, since your risk is always shared with other enterprises and must be negotiated.

For us, a Community Attack Model is a very pragmatic, grassroots activity. Rather than start from scratch, we chose to work from the many great ideas, sources, and models already in the literature. So the creation of our Model is more about “composition” than “creation.” Some of the references we found most useful are listed in Appendix B.

## Description of the CIS Community Attack Model - Structure

The basic structure of the CIS Attack Model consists of:

* columns representing stages in the life cycle of attacks;
* rows matching the Core Functions found in the NIST Cybersecurity Framework; and
* cells populated with applicable CIS Controls and countermeasures (e.g. Host Intrusion Detection, Patching, Anti-Malware, Firewall Access Control Lists, Security Configurations, Honeypots, Application Control/whitelisting).



*Each cell contains controls that*

*Identify, Protect, Detect, Respond, Recover against specific attack stages*

**Figure 1. The CIS Community Attack Model - Structure**

This matrix provides a way to discuss the ***capability*** of specific defensive actions against specific ***stages*** of an attack. Intuitively, you could ask questions like, “What are my options for *Detecting* an attack at the *Exploitation* stage? How can I *Prevent* their *Lateral Movement*?” If you populate a parallel matrix with your current mix of defensive tools and technologies, you could also raise the discussion to a strategy level, and ask “Am I over-invested in *Protection* and *Delivery* against attacks, but not investing enough to deal with attacks when they get through?”

This basic approach is suggested in the original Lockheed Martin paper. However, they map the stages in their Cyber Kill Chain against specific “Courses of Action” as defined in DOD Joint Publication 3-13 (2006): Detect, Deny, Disrupt, Degrade, Deceive, Destroy. We opted to use the Functions found in the NIST Cybersecurity Framework instead, which gives a more universally known and comprehensive way to identify potential enterprise actions.

There are several enterprises that already use a similar approach for their cyberdefense planning and implementation. Some use the Lockheed Model, with some additional stages or some form of grouping of the stages. Others use “rows” that include just “Protect, Defend, Respond,” or some other variation. Some create multiple versions of the columns that correspond to different types of attackers (e.g., Nation-State, Criminal), or partition the rows for different types of defensive enterprises (e.g., government, commercial).

But they all share the same intuitive notion: get above the noise of massive numbers of incidents and summarize the nature of attacks by category and stages; and organize a defensive plan by choosing countermeasures that provide desirable capability to defenders, at multiple points in the attacker’s lifecycle.

A fully populated version of the CIS Community Attack Model is presented here.



**Figure 2. The CIS Community Attack Model – With General Defensive Controls**

## The CIS Community Attack Model and the CIS Critical Security Controls

The primary use of the CIS Community Attack Model is to support the development and maintenance of the CIS Controls. This gives us a consistent and repeatable way to guide our discussions with numerous threat intelligence vendors and other sources of attack summaries, and then select controls that provide the best defensive value against the composite view of attackers. This becomes the basis for the publication of the CIS Controls.

The mapping from the Model into the CIS Critical Security Controls (Version 6.1) is presented below.



**Figure 3. The CIS Community Attack Model – Mapped to the CIS Controls (V6.0)**

This makes it easy for enterprises that use the CIS Controls to describe their work in terms of the NIST Cybersecurity Framework.

## Making the CIS Community Attack Model an Operational Process

The CIS Model helps bring order to the creation and maintenance of the CIS Controls, which can be the basis for major security improvement programs. But given the rapid changes in attack methods, defensive tools, and practices, we also have to make sure that the Model stays valid, and that adopters of the resulting recommendations (the CIS Controls) are informed about anything that could affect their priorities.

* We’ll continue to work with numerous sources of threat intelligence and attack summaries, mapping their results into the CIS Controls. Numerous vendors and analysts have already agreed to participate in this process, which will give us a diverse and representative sample of what is being seen across the cyber ecosystem. Some vendors (like the Verizon DBIR) use the CIS Controls directly in their final published report. For those and for others, CIS will make these mappings available to adopters of the CIS Controls.
* CIS will host a teleconference with a panel of participating companies and invited analysts. We believe that we can create a meaningful, but simple, low-cost event focused on a handful of questions like, “Has anyone seen attacks that **don’t** fit our Model,” and “Has anyone seen attacks or changes in attacker behavior that **do** fit our Model, but would lead adopters of the CIS Controls to reconsider their priority of implementation?”
* We will also work with a number of “closed” communities to adapt our Model for internal use. Every Enterprise or community of Enterprises has data about attacks that is unique, closely held, or encumbered by classification or legal agreement, but still should be factored into an overall risk assessment. For example, the MS-ISAC has agreed to provide a technical member to the CIS Attack Model Panel. This allows them to be part of the primary process and validate how the CIS Model reflects the concerns of their Community. The MS-ISAC can also set up a complementary internal process in which they consider closely held data about attacks in the same Model. This allows them to leverage the CIS process to deal with the very large-scale body of mass-market attack reporting, easily map what they are seeing into effective controls, and focus their attention on problems unique to their Community.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial (SLTT) governments.

## Summary

The CIS Community Attack Model is a way for our community overall to makes sense of large amounts of summarized attack data and organize it in a way that can be naturally mapped into countermeasures, and is consistent with security frameworks (like the NIST Cybersecurity Framework). CIS will use this to drive the evolution of the CIS Controls, and make it available to support other cyberdefense initiatives.

At a human level, it also provides a simple means to bring together a large number of experienced people around a shared problem, shared labor, and shared insight, and translate them into positive, constructive action that we can each take to improve cyber defense.

## Appendix A: The CIS Critical Security Controls (Version 6.1)

### CSC 1: Inventory of Authorized and Unauthorized Devices

### CSC 2: Inventory of Authorized and Unauthorized Software

### CSC 3: Secure Configuration of End user devices

### CSC 4: Continuous Vulnerability Assessment and Remediation

### CSC 5: Controlled Use of Administrative Privileges

### CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

### CSC 7: Email and Web Browser Protections

### CSC 8: Malware Defense

### CSC 9: Limitation and Control of Network Ports, Protocols, and Service

### CSC 10: Data Recovery Capability

### CSC 11: Secure Configuration of Network Devices

### CSC 12: Boundary Defense

### CSC 13: Data Protection

### CSC 14: Controlled Access Based on Need to Know

### CSC 15: Wireless Access Control

### CSC 16: Account Monitoring and Control

### CSC 17: Security Skills Assessment and Appropriate Training

### CSC 18: Application Software Security

### CSC 19: Incident Response and Management

### CSC 20: Penetration Tests and Red Team Exercises

## Appendix B: Annotated References

1. E. M. Hutchins, M. J. Cloppert, R. M. Amin, Lockheed Martin Corporation. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”.

A foundational work that developed the basic model of advanced attackers, often referenced in cybersecurity literature. Although its focus is on deep understanding of attackers, it also suggests the use of Courses Of Actions (COAs) from Department of Defense Joint Publication 3-13 (2006; now outdated): Detect, Deny, Disrupt, Degrade, Deceive, Destroy.

2. Invincea, Inc. (2015). “Know Your Adversary: An Adversary Model for Mastering Cyber Defense Strategies”. [White Paper]. Available (with registration**):** [**http://www.invincea.com**](http://www.invincea.com)

This paper presents a comprehensive model with many elements in common with the CIS CAM. They add a couple of excellent refinements: “Playbooks” for different types of attackers and defenders; and a notion of using the model for “game play” or simulation matching defensive strategy against adversary tactics.

3. C. Sanders, “Making the Mandiant APT1 Report Actionable”. [Blog posting]. Available:

[**http://www.appliednsm.com/making-mandiant-apt1-report-actionable/**](http://www.appliednsm.com/making-mandiant-apt1-report-actionable/)

The author describes a similar model based on the Mandiant APT-1 report (instead of the Lockheed Martin Cyber Kill Chain), and also using the COAs from DoD Joint Publication 3-13. This creates a “Course of Action” matrix which is populated with controls.

4. D. Mechaber, “APT: How to Defend Your Network Against Advanced Persistent Threats”. Available: [**http://www.tomsitpro.com/articles/IDS-Antil-Malware-IT\_Security-e-crime-advanced\_persistent\_threats,2-438.html**](http://www.tomsitpro.com/articles/IDS-Antil-Malware-IT_Security-e-crime-advanced_persistent_threats%2C2-438.html)

This article uses the Mandiant APT-1 Report for its attacker model, but partitions defensive options into “Inhibit, Detect, Respond” (instead of the NIST Framework or the DoD Joint Publication COAs, etc).

5. J. Tarala, K. Tarala, Enclave Security. “Open Threat Taxonomy”, Version 1.1, 2015. Available: [**http://www.enclavesecurity.com/**](http://www.enclavesecurity.com/)

This is a community volunteer project to produce and maintain a “free, community driven, open source taxonomy of potential threats to information systems”. This is not a model, but a way to comprehensively enumerate and organize the full range of threat actions that can affect information and systems, which can be used as input to decision models like the CIS CAM.

6. National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0”, February 12, 2014. Available: [**http://www.nist.gov/cyberframework/**](http://www.nist.gov/cyberframework/)

7. The Center for Internet Security, “The CIS Critical Security Controls for Effective Cyber Defense, Version 6.1”. Available (with registration**):** [**http://www.cisecurity.org**](http://www.cisecurity.org)

8. MITRE ATT&CK Matrix, MITRE Corporation, “Adversarial Tactics, Techniques, and Common Knowledge. [Web Site]. Available: [**https://attack.mitre.org/wiki/Main\_Page**](https://attack.mitre.org/wiki/Main_Page)

This is a “model and framework for describing the actions an adversary may take while operating within an enterprise network. “ From the point of initial exploitation onwards (“the right of Boom”), it lists the attackers basic *tactics* (derived from the Lockheed Martin Cyber Kill Chain) and then lists in very specific detail the *techniques* used by attackers (e.g., “Pass the Hash”, Indicator removal from tools) in support of those tactics. This can provide much finer ability to assess specific defensive tools against attacker techniques.

9. The Verizon Data Breach Investigations Report. Available (with registration): [**http://www.verizonenterprise.com/DBIR/**](http://www.verizonenterprise.com/DBIR/)

NOTE: In addition to the specific references above, we gratefully acknowledge the ideas, feedback, and insight received from numerous people across the industry and government.