Prioritizing Best Practices for the Level 2 and Level 3 maturities

Level 2 and Level 3 Maturities

More mature organizations should take a more sophisticated approach to prioritizing best practice implementation.

The CIS Community Defense Model

To help organizations determine where to invest their next dollar in cybersecurity, CIS developed the Community Defense Model (CDM). The CDM was created to help answer that and other questions about the value of the CIS Controls based on currently available threat data from industry reports. Ready more about the CIS Controls in the CIS Controls best practice. In short, the Community Defense Model is a data-driven, prioritized approach to building yourself up to a defense-in-depth posture.

Using authoritative data sources like the Verizon Data Breach Investigations Report, CIS identified the top attack types that enterprises should defend against.

For CDM 2.0, the top five attack types are:

1. Malware
2. Ransomware
3. Web Application Hacking
4. Insider and Privilege Misuse
5. Targeted Intrusions

Certain techniques are used to execute each of these types of attacks. The CDM uses the MITRE ATT&CK framework to cateogize these techniques and sub-techniques. These are mapped to mitigations, such as the Safeguards contained with the CIS Controls and the actions within this Guide's best practices, that protect against one or more sub-technique.

Using real world data, the CDM determines which Safeguards are the most efficient–the Safeguards that mitigate the most sub-techniques and thus, when implemented, are most likely to stop any given attack.

In the table below, we map the highest efficiency Safeguards from the CIS Controls to the best practices in this Guide to establish the priority best practices. For more details on the efficiency rankings, see Figure 13 of the CDM 2.0.

This efficiency ranking drives the ordering of the best practices in this Guide, with some exceptions particular to elections. While we recommend following the prescribed order, do what's best for your environment and, most importantly, keep making progress!

Mapping of the Most Efficient Safeguards to Priority Best Practices

Rank	Safeguard	Safeguard Title	Essential Guide Best Practice
1	4.1	Establish and Maintain a Secure Configuration Process	Managing Infrastructure
2	4.7	Manage Default Accounts on Enterprise Assets and Software	Managing Infrastructure
3	5.3	Disable Dormant Accounts	User Management
4	6.1	Establish an Access Granting Process	User Management
5	6.2	Establish an Access Revoking Process	User Management
6	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Managing Infrastructure
7	18.3	Remediate Penetration Test Findings	Remediate Pen Test Findings
8	18.5	Perform Periodic Internal Penetration Tests	Internal Pen Testing
9	6.8	Define and Maintain Role-Based Access Control	User Management
10	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Managing Infrastructure
11	3.12	Segment Data Processing and Storage Based on Sensitivity	Network Segmentation
12	5.2	Use Unique Passwords	User Management
13	6.4	Require MFA for Remote Network Access	Managing Remote Connections
14	6.5	Require MFA for Administrative Access	User Management
15	12.8	Maintain Dedicated Computing Resources for All Administrative Work	Managing Infrastructure
16	2.3	Address Unauthorized Software	Asset Management
17	2.5	Allowlist Authorized Software	Asset Management
18	4.2	Maintain a Secure Configuration Process for Network Infrastructure	Managing Infrastructure
19	4.4	Implement and Manage a Firewall on Servers	Firewalls and Port Restrictions
20	6.3	Require MFA for Externally-Exposed Applications	User Management

The best practices in the right column are listed as priority actions in the best practice index and should be implemented first for the Level 2 and Level 3 maturities.

Copyright © 2024, Center for Internet Security
Made with Sphinx and @pradyunsg's Furo
Last updated on Apr 04, 2023