CIS. Center for Internet Security®

Essential Cyber Hygiene

Enterprises that adopt the CIS Critical Security Controls (CIS Controls) have repeatedly asked: “What should we do first?” While there are a multitude of activities that any enterprise *could* do to defend itself, the imperative question is: *what are the most important, most* ***CRITICAL*** *activities that every enterprise should do to get started, based on what attackers are doing?*

In response to these questions, CIS categorized the Safeguards within the CIS Controls into three Implementation Groups based on their difficulty and cost to implement.

The first group, aptly named *Essential Cyber Hygiene*, is the group that is least costly and least difficult to implement. This group is comprised of the Safeguards CIS asserts that every enterprise should deploy. Enterprises that face more sophisticated attacks or that must protect more critical data or systems, would consider deploying additional Safeguards from the other Implementation Groups.

Enterprises naturally also want to know “How effective are the CIS Controls against the most prevalent types of attacks?” CIS’s Community Defense Model (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.

To underpin CDM, CIS Safeguards were assessed against attack techniques (as defined in the MITRE ATT&CK Framework) used in the most prevalent attacks (Malware, Ransomware, Web Application Hacking, Insider Privilege and Misuse, Targeted Intrusions). The results of this analysis were clear: CIS Controls, and specifically the Safeguards defined as Essential Cyber Hygiene, are a robust foundation for any cybersecurity program. The Essential Cyber Hygiene Safeguards provide mitigation against all the top five attack types mentioned above.

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