Center for Internet Security (CIS) Releases Community Defense Model v2.0 for Cybersecurity

CIS Critical Security Controls are highly effective against the top five attack types found in industry threat data, effectively defending against 86% of the ATT&CK (sub-)techniques in the MITRE ATT&CK framework

EAST GREENBUSH, N.Y., Sept. 29, 2021 – Enterprises naturally want to know how effective the CIS Critical Security Controls® (CIS Controls®) – 18 top-level Controls containing 153 Safeguards that provide a prioritized path to improve an enterprise's cybersecurity posture – are against the most prevalent cyber-attacks. The Center for Internet Security, Inc. (CIS®) answers that question and more through its Community Defense Model (CDM) v2.0, released today.

The model shows that the CIS Controls defend against approximately 86% of all ATT&CK (sub-)techniques found in the MITRE ATT&CK® framework. Furthermore, Implementation Group 1 (IG1) of the Controls, the definition of essential cyber hygiene (formerly basic cyber hygiene), provides enterprises a high level of protection, positioning them to defend against the top five attack types – malware, ransomware, web application hacking, insider privilege and misuse, and targeted intrusions.

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

“This year’s CDM findings strongly reinforce the value of a relatively small number of well-chosen and essential defensive steps found in IG1,” said Curtis Dukes, CIS Executive Vice President and General Manager, Security Best Practices. “As such, enterprises should aim to start with IG1 to obtain the highest value and work up to IG2 and IG3, as appropriate.”

The findings in the CDM demonstrate the security value of the CIS Safeguards against the top five attack types:

- Malware: 77% of Malware ATT&CK (sub-)techniques can be defended through implementation of IG1.
- Ransomware: 78% of Ransomware ATT&CK (sub-)techniques are defended through implementation of IG1.
- Web Application Hacking: 86% of Web Application Hacking ATT&CK (sub-)techniques are defended through implementing IG1 Safeguards.
- Insider Privilege and Misuse: IG1 defends against 86% of the Insider Privilege and Misuse ATT&CK (sub-)techniques.
- Targeted Intrusions: IG1 defends against 83% of Targeted Intrusions ATT&CK (sub-)techniques.

CDM v2.0 also discovered that establishing and maintaining a secure configuration process (CIS Safeguard 4.1) is a linchpin Safeguard for all five attack types. CIS Safeguard 4.1 is most effective

in defending against the top five attack types, reinforcing the importance of secure configurations, such as those contained within the CIS Benchmarks™.

“CDM v2.0 brings another level of rigor and detail to support the development of the CIS Controls, while leveraging industry threat data,” added Dukes. “Our results this year increased our confidence that our conclusions from the first CDM were correct.”

Read the entire Community Defense Model v2.0 white paper here.

About CIS:
The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously refine these standards 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 (SLTT) government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the cybersecurity needs of U.S. election offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

Contact:
Autum Pylant
media@cisecurity.org
518-266-3495