CIS Launches Updated Community Defense Model

New analysis identifies the safeguards that provide the greatest security value against today's most prevalent attacks

CLIFTON PARK, NY, UNITED STATES, September 21, 2026 / EINPresswire.com/ -- The Center for Internet Security, Inc. (CIS®) today announced the release of the CIS Community Defense Model (CDM) v3.0, the latest version of its data-driven framework that helps enterprises prioritize cybersecurity actions based on real-world threats. Built on attack data, threat intelligence, and MITRE ATT&CK® mappings, CDM v3.0 helps enterprises identify which CIS Critical Security Controls® (CIS Controls®) Safeguards provide the greatest defensive value against the attacks they are most likely to face.

> CDM v3.0 helps defenders cut through the noise by identifying the actions that will have the greatest security value against today's most prevalent threats."
>
> *Curt Dukes, EVP and GM of Security Best Practices at CIS*

The CIS Community Defense Model is grounded in the principle of collective defense, recognizing that enterprises often face similar cyber threats and can benefit from shared defensive knowledge. By connecting real-world attacker behavior directly to the CIS Controls, CDM v3.0 provides practical, data-driven guidance that helps enterprises reduce risk, strengthen cyber resilience, and maximize the impact of their cybersecurity investments.

"Enterprises continue to face difficult decisions about where to focus limited cybersecurity resources," said Curt Dukes, Executive Vice President and General Manager of Security Best Practices at CIS. "CDM v3.0 helps defenders cut through the noise by identifying the actions that will have the greatest security value against today's most prevalent threats."

Among its key findings, CDM v3.0 reinforces the value of Implementation Group 1 (IG1) of the CIS Controls, also known as essential cyber hygiene. The analysis found that enterprises

implementing IG1 can achieve coverage against:

- 89% of System Intrusion techniques
- 86% of Social Engineering techniques
- 88% of Basic Web Application Attack techniques
- 84% of Privilege Misuse techniques
- 88% of Denial of Service (DoS) techniques

These findings demonstrate that a relatively small set of prioritized cybersecurity actions can provide broad protection against today's most common attack types and reinforce CIS guidance that every enterprise should start with essential cyber hygiene.

The analysis also found that enterprises implementing all CIS Controls Safeguards can defend against 99% to 100% of techniques used across the five attack categories studied, further validating the CIS Controls as an effective foundation for modern cyber defense.

New in this release, the CIS Controls Active Defense Lifecycle™ provides a defender-focused capability that reinforces the value of layered defense and understanding where safeguards can disrupt attacker activity before impact occurs. By aligning safeguards to stages of attacker behavior, enterprises can identify defensive strengths, uncover potential gaps, and strengthen defense-in-depth strategies.

CDM v3.0 also identified CIS Safeguard 4.1: Establish and Maintain a Secure Configuration Process as the most effective individual safeguard across all five attack categories, reinforcing the critical role of secure configuration as a foundation for cyber defense.

The report further concludes that while artificial intelligence is increasing the speed, scale, and accessibility of cyber attacks, foundational cybersecurity practices continue to provide effective protection against many AI-enabled attack paths.

Ultimately, CDM v3.0 helps enterprises answer one of cybersecurity's most pressing questions: What should we do first? By identifying the CIS Safeguards that provide the greatest security value against real-world threats, the model transforms threat intelligence into prioritized, actionable defense strategies.

The CIS Community Defense Model (CDM) v3.0 is available now at www.cisecurity.org.

###

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 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. election offices. To learn more, visit or follow us on X: @CISecurity.

Kelly Wyland
Center for Internet Security
+1 518-256-6978
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/943436082

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.