Censinet Launches Wave 4 of The Healthcare Cybersecurity Benchmarking Study

Benchmarking Study Adds The Scottsdale Institute as New Co-Sponsor, Expands Enterprise Assessment and Benchmarking Capabilities to NIST CSF 2.0 and the HPH CPGs

BOSTON, MA, UNITED STATES, September 10, 2024 /EINPresswire.com/ -- Censinet, the leading provider of healthcare risk management solutions, today announced the launch of Wave 4 of The Healthcare Cybersecurity Benchmarking Study. Co-sponsored by KLAS Research, the American Hospital Association (AHA), Health Information Sharing and Analysis Center (Health-ISAC), the Healthcare and Public Health Sector Coordinating Council (HSCC), and new co-sponsor the Scottsdale Institute, Wave 4 of the Benchmarking Study expands and enhances its enterprise assessment, benchmarking, and reporting capabilities to include the NIST Cybersecurity Framework 2.0 (CSF 2.0), the HHS Healthcare and Public Health Cybersecurity Performance Goals (HPH CPGs), the NIST AI Risk Management Framework (AI RMF), Health Industry Cybersecurity Practices 2023 (HICP 2023), and Organizational Metrics. The Healthcare Cybersecurity Benchmarking Study is the industry's only collaborative initiative to establish and maintain robust, objective, and actionable cybersecurity peer benchmarks to improve cyber preparedness, maturity, and resiliency across the health sector. Organizations interested in participating in Wave 4 of the Study should email benchmarks@censinet.com.

> "The Healthcare Cybersecurity Benchmarking Study is more than understanding where your organization stands on cyber maturity, it's about contributing to a broader mission to safeguard our entire sector"
>
> *John Riggi, National Advisor for Cybersecurity and Risk, the AHA*

"Censinet is proud to launch Wave 4 of the Healthcare Cybersecurity Benchmarking Study and we're honored by the ongoing dedication, collaboration, and spirit of community exemplified by participating organizations," said Ed Gaudet, CEO and Founder of Censinet. "Since inception three years ago, the Benchmarking Study has activated a national discussion on healthcare cybersecurity, helped set proposed federal minimum cybersecurity standards, and has brought together hundreds of healthcare organizations in a determined, collective effort to protect our patients from cyber threats."

Wave 4 of the Benchmarking Study contains an expanded set of enterprise assessments, peer benchmarking, and reporting capabilities as well as exclusive benefits available to participants

free of charge, including:
- Enterprise assessments and peer benchmarks for NIST CSF 2.0, HPH CPGs, and Operational Metrics – which are required to be completed by participants
- Enterprise assessments and peer benchmarks for HICP 2023 and the new NIST AI RMF – both are optional for completion by participants
- Board-ready dashboards and summary reporting for all enterprise assessments and benchmarks detailing coverage, compliance, and relative peer group performance
- Access to the Executive Summary and Deep Dive Reports to be published in Q1 2025
- Advanced filtering capabilities for precise peer group refinement and comparison

“The Healthcare Cybersecurity Benchmarking Study is more than just understanding where your organization stands on cyber maturity — it’s about contributing to a broader mission to safeguard our entire sector,” said John Riggi, National Advisor for Cybersecurity and Risk, American Hospital Association. “Ransomware and other cyber threats are becoming more targeted and destructive, putting patient lives at risk. By joining the Benchmarking Study, healthcare organizations can gain the insights they need to bolster their own defenses while also helping to elevate the industry’s collective cybersecurity preparedness and resiliency.”

Wave 4 of the Benchmarking Study includes several product enhancements to expedite assessment completion and accelerate time-to-value, including:
- Ability to “jumpstart” completion of Wave 4 assessments based on previously completed questionnaire responses; for example, participants who have previously completed a NIST CSF 1.1 questionnaire can automatically populate up to 40%+ of NIST CSF 2.0; or, with completed NIST CSF 1.1 (and/or NIST CSF 2.0) and HICP questionnaires, up to 90% of HPH CPG responses can be automatically populated
- Users can assign questions to subject matter experts across the organization to leverage collaborative efforts to accelerate completion and enrich responses
- Question Guidance to identity the source(s) of the question; relevant controls, policies, and procedures; and provide context on the specific risks and threats under evaluation
- Benchmarking results will be available immediately after questionnaire completion, pending availability of a sufficient sample size

Like last year, participation in Wave 4 of the Benchmarking Study is open to a broad set of organizational types across the health sector, including: Healthcare Delivery Organizations (HDOs), Payers, Healthcare Technology Vendors, Pharmaceutical and Lab Companies, Public Health Organizations, Medical Device Manufacturers, Mass Fatality Management Services, and Federal Response & Program Offices.

“KLAS Research is proud to continue our collaboration with Censinet and the other sponsors of the Healthcare Cybersecurity Benchmarking Study,” said Steve Low, President of KLAS Research. “The insights from this study are vital for healthcare organizations seeking to navigate the complex and ever-changing cybersecurity landscape; moreover, participation in the Benchmarking Study helps drive a deeper understanding of an organization's cybersecurity

posture and readily identifies targeted areas for improvement."

The Executive Summary from Wave 3 of the Benchmarking Study is available publicly at no charge and can be found on the KLAS Research website here. The Wave 3 Deep Dive report is also available to Wave 3 participants. In addition, through anonymized data opt-in by participants, analysis from the first two waves of The Healthcare Cybersecurity Benchmarking Study served as a primary input into the Hospital Cyber Resiliency Initiative Landscape Analysis, a key report published by the U.S. Department of Health and Human Services in May 2023. In turn, this report helped inform the Healthcare and Public Health Cybersecurity Performance Goals, proposed by the U.S. Department of Health and Human Services.

"As a continued sponsor of the Healthcare Cybersecurity Benchmarking Study, Health-ISAC is committed to helping our community of healthcare organizations stay ahead of the curve, especially as new threats continue to emerge that threaten patient safety and care operations," said Errol Weiss, Chief Security Officer of Health-ISAC. "With enterprise assessments and benchmarks for 'recognized security practices' like NIST CSF 2.0, the Benchmarking Study gives our members the unique insights they need to better identify and detect these emerging threats, and helps improve their ability to respond and recover to security incidents — this level of guidance is vital as we work to protect both our community members and the patients we serve."

"The Health Sector Coordinating Council is honored once again to sponsor the Healthcare Cybersecurity Benchmarking Study," said Greg Garcia, Executive Director, Health Sector Coordinating Council Cybersecurity Working Group. "As healthcare organizations face new federal cybersecurity requirements in the wake of escalating cyberattacks, such as the HHS Cybersecurity Performance Goals, the Benchmarking Study provides critical guidance and a clear path toward compliance, while also prioritizing the critical long-term investments needed to strengthen cyber preparedness and maturity."

This Wave includes an added sponsor to the Study: The Scottsdale Institute. The Scottsdale Institute aims to advance healthcare's digital transformation within an equitable, consumer-centered, community health framework via collaboration, education and networking Comprising over 70+ not-for-profit health systems and academic medical centers, Members connect through intentionally small, authentic and informal forums with a common objective: Leveraging technology to improve delivery while tackling tough healthcare topics with grace and expertise, thereby strengthening IT-enabled performance, sharing best practices and cultivating deep relationships.

"Scottsdale Institute is delighted to support this initiative and encourage all healthcare organizations to participate in this year's Healthcare Cybersecurity Benchmarking Study," said Janet Guptill, President and CEO of the Scottsdale Institute. "As cyberattacks increasingly jeopardize critical healthcare infrastructure and threaten to disrupt patient care, this industry-specific Benchmarking Study will help deepen our collective understanding of how health

systems and the industry partners they rely upon must collaborate to improve cyber preparedness. We look forward to helping to "raise the bar" across the healthcare industry about the importance of strengthening long-term cyber resiliency to ensure we can all deliver on our collective mission to provide safe, affordable, and equitable care."

There is no cost for qualified health sector organizations to participate in Wave 4 of the Benchmarking Study; however, participation in future Benchmarking Study waves may require a license. Participants in Wave 4 of the Benchmarking Study are guaranteed free access to the next three waves of the Study, including all Benchmarking Study-related benefits and product capabilities. Wave 4 participation is limited to those organizations that complete the required assessments (NIST CSF 2.0, HHS CPGs, Organizational Metrics) by November 15, 2023. If interested in participating in Wave 4 of the Benchmarking Study, please email benchmarks@censinet.com.

About Censinet
Censinet®, based in Boston, MA, takes the risk out of healthcare with Censinet RiskOps, the industry's first and only cloud-based risk exchange of healthcare organizations working together to manage and mitigate cyber risk. Purpose-built for healthcare, Censinet RiskOpsTM delivers total automation across all third party and enterprise risk management workflows and best practices. Censinet transforms cyber risk management by leveraging network scale and efficiencies, providing actionable insight, and improving overall operational effectiveness while eliminating risks to patient safety, data, and care delivery. Censinet is an American Hospital Association (AHA) Preferred Cybersecurity Provider. Find out more about Censinet and its RiskOps platform at censinet.com.

# # #

Justyn Thompson
Censinet
+1 (617) 221-6875
jthompson@censinet.com
Visit us on social media:
Facebook
X
LinkedIn

in today's world. Please see our Editorial Guidelines for more information.