New Cybersecurity Standards for Hospitals Will Place Software Bill of Materials (SBOMs) In the Limelight

PITTSBURGH, PA, U.S., June 19, 2024 /EINPresswire.com/ -- As the healthcare industry awaits details on cybersecurity standards mandates from the Biden Administration, one thing is clear: software security will be front and center, according to Vigilant Ops, the leading provider of Software Bill of Materials (SBOM) lifecycle management solutions for the healthcare industry.

Vigilant Ops | Leader in SBOM Lifecycle Management

"The $1.6 billion February cyberattack on Change Healthcare highlights why waiting to implement new cyber protections is no longer an option," said Ken Zalevsky, CEO of Vigilant Ops. "Abiding by the upcoming federal cyber requirements is important, but it is just a bare minimum baseline. Healthcare organizations must shore up the holes in their networks that allow hackers in – and that starts with the software that runs healthcare monitors, diagnostic devices, laptops, tablets, and every other connected device."

> We applaud the development of cybersecurity standards to make our healthcare institutions safer and more efficient."
>
> *Ken Zalevsky, CEO at Vigilant Ops*

The new cybersecurity standard will likely require healthcare providers to:

- Conduct regular cybersecurity risk assessments
- Identify vulnerabilities in deployed systems and devices
- Implement more stringent requirements for vendors in their supply chain processes
- Plan to monitor and update risk assessments continuously

These requirements are all prudent and reasonable. However, they are impossible to implement if healthcare institutions have little insight into the components of thousands of commercial and custom software programs that manage their complex Internet of Medical Things (IoMT).

As hospitals increasingly rely on interconnected systems and IoMT devices to deliver healthcare services efficiently, the scope and complexity of this attack vector continues to expand, underscoring the critical need for comprehensive cybersecurity measures to mitigate risks and safeguard patient data and safety.

Yet, hospitals don't have visibility into the inner workings of the software used to manage IoMT devices. Software ingredients aren't printed on the side of the device, like a box of cereal, so when a vulnerability is announced, hospital security officers have no way to determine if the vulnerability is impactful to them.

What does all this mean? Any cybersecurity standard that does not require the deployment of SBOMs for every software product, leaves healthcare institutions open to more attacks.

SBOMs are the foundation of hospital security by providing:
- Visibility and Transparency: SBOMs provide hospitals with insights to identify potential vulnerabilities or security risks associated with each software component.
- Risk Assessment and Prioritization: With SBOMs in place, hospitals can conduct thorough risk assessments to identify vulnerabilities and assess the severity of each risk to prioritize their efforts and allocate resources.
- Patch Management and Vulnerability Remediation: SBOMs facilitate effective patch management and vulnerability remediation processes.
- Compliance and Regulatory Requirements: SBOMs help hospitals demonstrate compliance with regulatory requirements related to software security and risk management. Regulatory bodies such as the FDA and HIPAA require hospitals to ensure compliance when deploying medical devices, which includes maintaining the security of their software components, requiring an accurate inventory to track and manage potential vulnerabilities.
- Vendor Management and Procurement: SBOMs support effective vendor management and procurement practices by enabling hospitals to evaluate the security posture of software vendors and assess the risk associated with using specific software products or services.

"We applaud the development of cybersecurity standards to make our healthcare institutions safer and more efficient," Zalevsky said. "We must look long and hard at software security to ensure that the standards' goals are realized. The threats are too enormous to make this a 'check the box' exercise."

Vigilant Ops offers a comprehensive SBOM lifecycle management solution, enabling hospitals to centralize their SBOMs, automatically identify vulnerabilities, and maintain compliance with industry standards. With Vigilant Ops, every software component is reviewed to ensure that all NTIA minimum elements are captured, every vulnerability is linked, and every SBOM is certified by a cyber expert before it is published. Complete audit trails are captured for quality assurance and regulatory compliance.

For more information about Vigilant Ops, please visit www.vigilant-ops.com or download their

eBook on how hospitals should prepare.

About Vigilant Ops:
Established in 2019, Vigilant Ops has rapidly emerged as a frontrunner in SBOM Lifecycle Management solutions. Our innovative platform empowers organizations to seamlessly generate, monitor, and manage their SBOMs through a unified dashboard while also facilitating the secure sharing of SBOMs. Engage with our SBOM specialists today to discover how Vigilant Ops can enhance your organization's cybersecurity strategy. Please visit www.vigilant-ops.com for more information.

Faye Danis
Vigilant Ops
+1 412-704-4600
faye.danis@vigilant-ops.com
Visit us on social media:
X
LinkedIn
YouTube
