EINPRESSWIRE

Blue Goat Cyber Launches Legacy Medical Device Cybersecurity Service with Advanced Monitoring and Testing

Blue Goat Cyber offers cybersecurity services for legacy medical devices, including assessments, SBOM analysis, penetration testing, & vulnerability disclosure.

SCOTTSDALE, AZ, UNITED STATES, October 30, 2024 /EINPresswire.com/ -- Blue Goat Cyber, a medical device cybersecurity solutions leader, has announced a new service dedicated to [securing legacy medical devices](). Aimed at addressing the unique vulnerabilities of aging healthcare technology, this service begins with a thorough cybersecurity assessment, including Static Application Security Testing (SAST), Software Bill of Materials (SBOM) generation, and penetration testing. Following the initial assessment, Blue Goat Cyber offers a postmarket management contract featuring SBOM monitoring, routine penetration testing, and a Coordinated Vulnerability Disclosure (CVD) portal, ensuring long-term device protection and regulatory compliance.

> Securing legacy devices is about protecting patient safety and supporting manufacturers in meeting modern security requirements.”
>
> *Christian Espinosa, Blue Goat Cyber Founder and CEO*

Legacy medical devices, often operating on outdated software and hardware, pose heightened cybersecurity risks that can affect patient safety and regulatory compliance. Blue Goat Cyber’s new service delivers a tailored approach to securing these devices, providing a clear roadmap for addressing vulnerabilities and enabling manufacturers to maintain security standards over time.

"Securing legacy devices is about protecting patient safety and supporting manufacturers in meeting modern security requirements,” said Christian Espinosa, Founder and CEO of Blue Goat Cyber. “Our service is designed to help manufacturers gain control over cybersecurity risks while remaining compliant with regulatory demands.”

In-Depth Initial Assessment for Legacy Device Security

The initial assessment of Blue Goat Cyber’s legacy device service is structured around three core evaluations: SAST, SBOM creation, and penetration testing, offering a robust analysis of potential security gaps.

- Static Application Security Testing (SAST) scans the device’s source code, identifying hidden vulnerabilities that attackers could exploit. SAST is particularly crucial for legacy devices, where code structures may lack modern security features.

- Software Bill of Materials (SBOM) creation offers a comprehensive inventory of all software components within the device, including third-party and open-source libraries. By identifying components with outdated or unsupported software, the SBOM provides a foundation for ongoing vulnerability management, addressing hidden risks often found in legacy systems.

- Penetration Testing simulates real-world cyberattacks, exposing the device’s vulnerabilities in its current state and testing its resilience against potential threats. This phase offers manufacturers a clear picture of their device’s security posture and serves as a foundation for building a targeted and effective security strategy.

These assessments culminate in a gap analysis report that identifies and prioritizes vulnerabilities, paired with a customized security roadmap for addressing identified risks. This roadmap provides manufacturers with a clear path to enhance device security, balancing regulatory compliance with practical, resource-conscious steps.

Postmarket Management: SBOM Monitoring, Routine Testing, and Vulnerability Disclosure

Blue Goat Cyber’s postmarket cybersecurity management contract builds on the initial assessment, providing continuous security support to protect legacy devices over their operational lifespan. The postmarket services include SBOM monitoring, regular penetration testing, and access to a Coordinated Vulnerability Disclosure (CVD) portal.

- SBOM Monitoring ensures ongoing visibility of all software components in the device, alerting manufacturers to potential vulnerabilities as they arise. This proactive approach is essential for legacy devices that rely on components from multiple vendors, some of which may introduce new vulnerabilities over time.

- Routine Penetration Testing is conducted regularly, simulating new and evolving cyber threats to ensure that devices remain resilient against the latest attack methods. This routine testing allows Blue Goat Cyber to continually refine the device’s security posture, helping manufacturers stay one step ahead of cyber threats.

- The Coordinated Vulnerability Disclosure (CVD) Portal provides a secure, structured way for healthcare providers, researchers, and manufacturers to report and track vulnerabilities in legacy devices. This centralized system supports transparent communication among stakeholders, ensuring vulnerabilities are addressed quickly and thoroughly while maintaining regulatory compliance.

"Our postmarket services extend security beyond the initial assessment," said Espinosa. "SBOM monitoring, routine testing, and the CVD portal create a robust defense, ensuring legacy devices remain secure against both current and emerging threats."

Aligning Legacy Device Security with Regulatory Standards

Blue Goat Cyber’s legacy device service aligns closely with the cybersecurity requirements outlined by the FDA and EU MDR. By adhering to these regulatory frameworks, Blue Goat Cyber provides manufacturers a streamlined process for ensuring compliance while maintaining security standards.

"Regulatory compliance is a cornerstone of our approach,” said Espinosa. “Through our detailed assessments and postmarket support, we help manufacturers uphold the security and integrity of their devices, reinforcing their commitment to patient safety."

About Blue Goat Cyber

Founded by cybersecurity expert Christian Espinosa, Blue Goat Cyber specializes in protecting medical devices from cybersecurity threats. Its services span risk assessment, regulatory compliance, and postmarket management. Blue Goat Cyber’s mission is to ensure that all medical devices—whether newly developed or legacy models—meet the highest security standards, empowering manufacturers to deliver safe, resilient healthcare solutions.

For more information, visit https://bluegoatcyber.com.

Melissa Reeves
Blue Goat Cyber
+1 (844) 939-4628
email us here
Visit us on social media:
Facebook
X
LinkedIn
Instagram
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/755176717