The Monthly Pulse
June 2025

Your Trusted Partner in Navigating MedTech Cybersecurity with Confidence and Clarity.

Welcome to the "Blue Goat Cyber Monthly Pulse,"your trusted source for staying ahead in the rapidly evolving world of medical device cybersecurity.

Each month, we deliver expert insights, regulatory updates, and real-world strategies to help MedTech innovators navigate complex compliance landscapes with clarity and confidence. Whether you're building your first device or scaling globally, our mission is to empower you with the knowledge, tools, and partnerships needed to secure patient safety and maintain regulatory readiness—every step of the way.

Industry Pulse: Key Development in June

Legacy Devices Under Fire: Old operating systems are being targeted in a wave of zero-day exploits. Time to check patchability and isolation of your legacy endpoints.

European MDR + Cyber Rules Tighten: Expect more stringent expectations on premarket cyber documentation and vulnerability disclosure across EU markets.

Postmarket Enforcement Rising: FDA sent warning letters in May citing lack of postmarket patching protocols. Don't be next—prepare now.

Innovator Spotlight: Fujirebio's FDA-Approved Alzheimer's Blood Test

This month, we spotlight Fujirebio Diagnostics, whose Lumipulse test just became the first FDA-cleared blood test to help detect Alzheimer's disease. By measuring key biomarkers through a simple blood draw, it offers a less invasive and more accessible alternative to traditional brain scans—paving the way for earlier intervention and diagnosis. Source – Reuters

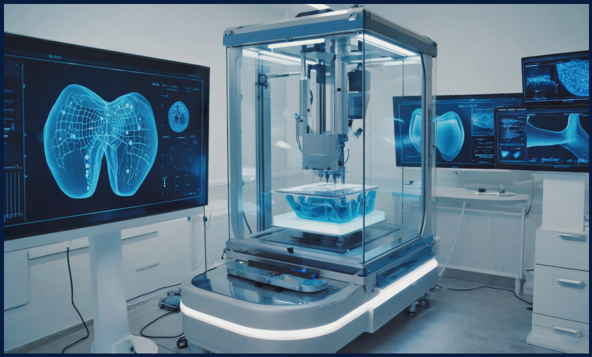
Employee Spotlight: Melissa Espinosa

This month, we're proud to spotlight Melissa Espinosa, our VP of Strategic Partnerships. With a strong background in Nursing and the medical field, she knows first hand how cybersecurity could impact patients lives. Melissa is the driving force behind many of our most impactful client collaborations. Thank you Melissa for your commitment to create meaningful partnerships to safeguard lives!

Blue Goat Cyber in Action!

MedTech World – Bay Area, California

June 26–27, 2025
Christian Espinosa will present: "Cybersecurity best practices for medical device development & Navigating FDA requirements."



Cyber Threat of the Month:

Supply Chain Exploits via Third-Party SDKs

What's Happening: Threat actors are increasingly targeting software supply chains by injecting malicious code into open-source and third-party SDKs. These compromised components can infiltrate applications during development, leading to widespread vulnerabilities.
Quick Tip: Ensure your Software Bill of Materials (SBOM) includes transitive dependencies—those indirect components that your software relies on through other libraries. Comprehensive SBOMs enhance visibility and enable quicker responses to potential threats . Check out this blog to learn more: https://bluegoatcyber.com/blog/the-interplay-of-cbom-and-sbom-in-medical-device-cybersecurity/

Ask the Goat: What is an SBOM and why does it matter?

An SBOM, or Software Bill of Materials, is like an ingredient list for your device's software. It includes all components, versions, and dependencies. This is important because if a vulnerability is found in a third-party library, an SBOM allows you to quickly assess your exposure and respond.

Got a question? Submit yours for the next issue of Ask the Goat!
Email: info@bluegoatcyber.com

THE THREATS ARE EVOLVING BUT SO ARE WE.

Blue Goat Cyber stands ready to help you secure your devices, protect your patients and stay ahead of the curve.

WANT TO CHAT?

Schedule a Discovery Session:

Partner with Us

SDVOSB Service Disabled Veteran Owned Small Business CVE

CONTACT US

www.bluegoatcyber.com