The Monthly Pulse
September 2025

BLUE GOAT CYBER

Your Trusted Partner in Navigating MedTech Cybersecurity

Welcome to the Blue Goat Cyber Monthly Pulse—your trusted source for navigating the rapidly evolving world of medical device cybersecurity.

Industry Pulse: Key Developments:

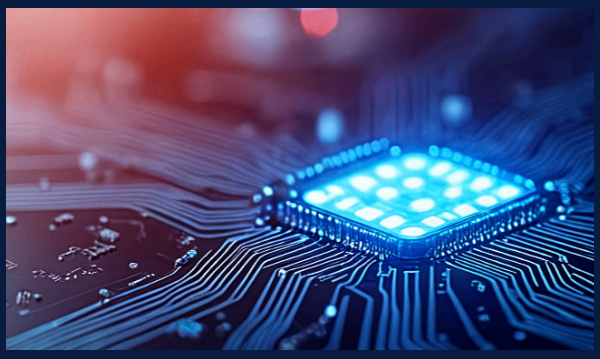
The FDA's new agency-wide AI tool, "Elsa" launched earlier this summer. Elsa is poised to revolutionize medical device oversight by accelerating regulatory reviews, enhancing transparency, and strengthening postmarket monitoring. For MedTech cybersecurity, this means identifying vulnerabilities in devices is expedited, more effective risk analysis, and stricter compliance with evolving safety standards, reducing threats. Read more here: FDA AI News

Innovator Spotlight:

Strokes remain one of the deadliest health crises—claiming over 3M lives each year and affecting 7.8M U.S. adults in 2025. Yet up to 80% are preventable with better diagnostics and timely care.
Vena Medical is tackling this with the Vena MicroAngioscope™—the first device to deliver real-time, full-color imaging directly inside veins and arteries. This breakthrough helps physicians precisely navigate vascular anatomy, detect clots faster, and improve neurovascular outcomes. Its FDA Breakthrough Device designation underscores both its clinical potential and path to rapid adoption. Learn more here: Vena Medical

Employee Spotlight:

Jordan John, H.BSc, RAC, MBA, leads global regulatory compliance and authors FDA cybersecurity submissions for advanced medical device technologies. With over a decade in Regulatory Affairs & Quality Assurance at both startups and multinationals—and experience co-developing postgraduate programs and teaching Regulatory Affairs & Cybersecurity Compliance—Jordan brings unmatched expertise. We're grateful to have Jordan on the Blue Goat team!



Blue Goat Cyber in Action!

MedTech World Singapore, October 1st.
AdvaMed MedTech Conference: October 5th–8th, San Diego, CA
Device Talks West: October 15th-16th, 2025, Santa Clara, CA.
MedTech World Malta, November 12th–14th, Valetta, Malta

Cyber Threat of the Month:

What's Happening:

Nearly 200K IoT-enabled medical devices were recently found vulnerable due to default passwords and open internet access—leaving hospitals exposed to remote hijacking, data tampering, and care disruptions.
Reported Sept 5–9 by HHS, the threat underscores the need for vigilance. Clinicians, IT teams, and manufacturers must secure firmware, close open ports, and adopt Zero Trust and regular audits as urged by the FDA to protect patient safety.
Read more: HHS Report

Ask the Goat:

Q: Many MedTech innovators design for performance and compliance—but what's the biggest cybersecurity blind spot in medical device development that could still put patients at risk?

The Goat: The danger usually isn't in your code—it's in the third-party components you didn't build. Most devices rely on open-source libraries or vendor modules, but without a complete SBOM (Software Bill of Materials), you have no idea what vulnerabilities are lurking inside. If even one of those components is exploited, your device—and your patients—are exposed. You can't patch what you don't know exists.

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

THE THREATS ARE EVOLVING.
WE ARE VIGILANT.
WE'VE GOT YOUR BACK.

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

WANT TO CHAT?

Schedule a Discovery Session:

Partner with Us

CONTACT US

www.bluegoatcyber.com