The Monthly Pulse
August 2025

BLUE GOAT CYBER

Your Trusted Partner in Navigating MedTech Cybersecurity

Welcome to the Blue Goat Cyber Monthly Pulse—your go-to source for expert insights, new innovations on the market, regulatory updates, and practical strategies in medical device cybersecurity. Whether you're launching your first device or scaling globally, we're here to help you navigate compliancecand protect patient safety confidently.

Industry Pulse: Key Developments:

The EU AI Act, introduced in 2024 and updated this month, is the world's first comprehensive AI framework. By 2026, it will reshape how AI is developed and regulated.
For MedTech, AI-powered devices are now high-risk, requiring strict compliance—risk mitigation, quality data, transparency, and oversight. Without early planning, startups risk costly delays or rejection.
At the center is cybersecurity: secure data, trustworthy AI, and strong oversight are essential for approval and patient safety.
Read more here: EU AI Act

Innovator Spotlight: A Historic Milestone in Surgical Robotics.

Cornerstone Robotics, together with The Chinese University of Hong Kong, has achieved the world's first clinical validation of autonomous surgery using the Sentire Endoscopic Surgical System—published in Science Robotics. This milestone shows how embodied intelligence can bring unprecedented precision, consistency, and safety to robot-assisted procedures, setting the stage for a new era in surgical innovation.
Read More Here

Employee Spotlight:

We're proud to spotlight Myles Kellerman, our Director of MedTech Cybersecurity. With nearly two decades of IT experience and 13+ years in cybersecurity, Myles leads penetration testing and application security for our clients worldwide. Every day, he works closely with MedTech startups and manufacturers to rigorously test and secure their devices. His expertise and relentless commitment to patient safety make him a cornerstone of our team and mission.

Cyber Threat of the Month:

What's Happening:
Data Leak from Misconfigured Medical Devices

Researchers uncovered that over 1.2 million internet-connected healthcare devices—including MRI and X-ray machines—are exposed online due to misconfigurations and weak passwords, jeopardizing patient privacy and device integrity.

Why It's Critical:
Leaked scans and medical data can fuel identity theft, blackmail, or targeted phishing. Attackers may even impersonate providers to trick patients. This makes active asset mapping, strong vulnerability management, and a proactive cybersecurity culture essential in MedTech.
Read more: Cyber News Wire

Blue Goat Cyber in Action!

LSI Europe 2025: September 7th-11th, in London, UK.

Device Talks West: October 15th-16th, 2025 in Santa Clara, CA.

Ask the Goat:

Q: Is Medical Device Penetration Testing Enough?

A: Penetration testing is vital, but it's only one piece of the puzzle. A single test gives you a snapshot—how attackers might exploit known vulnerabilities at a given moment. But medical devices face constant, evolving threats.
That's why true security requires layers: vulnerability assessments to spot weaknesses early, static and dynamic analysis to catch coding flaws, fuzz testing to uncover zero-days, and continuous monitoring to stay ahead of new risks. At Blue Goat Cyber, we remind clients—penetration testing should be the final check, never the only check.

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.
Trust. Security. Compliance.

WANT TO CHAT?

Schedule a Discovery Session:

Partner with Us

CONTACT US

www.bluegoatcyber.com