

THE MONTHLY PULSE

April 2026

MedTech cybersecurity intel for engineering, quality & regulatory teams.

Published April 30, 2026

IN THIS ISSUE

- 01 From the Editor**
- 02 Where in the World is the Goat?**
- 03 Ask the Goat — the 7 principles of software testing**
- 04 Podcast spotlight — Episode 67**
- 05 Medical device cybersecurity news — April 2026**
- 06 The Blue Goat takeaway**

About this edition. Medtronic cyberattack, expanding device-level threats, tightening FDA expectations, plus our team on the road in Florida and Singapore. Sourced from the Blue Goat Cyber LinkedIn newsletter, The Monthly Pulse.

THE MONTHLY PULSE

April 2026

Medtronic cyberattack, expanding device-level threats, tightening FDA expectations, plus our team on the road in Florida and Singapore.

01

From the Editor

MedTech innovation is accelerating across every front. Connectivity is expanding, AI is advancing, and devices are becoming more integrated into how care is delivered. At the same time, the risk surface is expanding just as fast. This month's edition looks at what that means in practice — from a high-profile Medtronic cyberattack, to rising device-level threats, friction-less device technology, and tightening FDA expectations. The theme is clear: cybersecurity is now foundational to how software-enabled MedTech gets built, approved, and trusted.

02

Where in the World is the Goat?

MedTech World North America 2026 (May 11–13, Hilton West Palm Beach, FL) — Blue Goat Cyber is Title Sponsor. CEO Christian Espinosa will speak on MedTech cybersecurity across the total product lifecycle, joined by VP of Strategic Partnerships Melissa Espinosa and Claudio Salvador (Business Development, LATAM and Spain). Use code **MTWUXCHRISTIAN** for \$150 off your ticket.

LSI Asia '26 (June 30 – July 3, Shangri-La Singapore) — Christian and Melissa will be on the ground June 30 – July 2 as APAC MedTech innovation accelerates and connected-device complexity rises.

03

Ask the Goat — the 7 principles of software testing

They are simple, but they change how you think about risk: testing shows defects, not their absence; exhaustive testing is impossible; test early; defects cluster; tests lose effectiveness over time; testing depends on context; no errors does not mean ready. In MedTech, security is never "proven," only tested. A clean result means nothing was found in that moment and context — not that risk is gone. Treat every validated risk as patient-safety evidence.

04

Podcast spotlight — Episode 67

De-Risking Product Decisions in MedTech Startups with Brent Lavin of Ironwood MedTech Partners. Hospitals are already overloaded — around 14 devices per patient bed, constant alarms, and teams under pressure. If your product adds friction, even slightly, it doesn't matter how advanced it is. The products that stick are the ones that integrate cleanly and become hard to remove. Watch the full episode at youtu.be/qoGs15STxSg.

05

Medical device cybersecurity news — April 2026

Medtronic cyberattack — unauthorized access to corporate IT systems exposed potentially millions of records, with no impact to devices, manufacturing, or patient care. Follow-on reporting suggests up to nine million records may have been accessed by ShinyHunters.

1 in 4 healthcare organizations report device cyberattacks in the past year, many with disruptions to patient care.

FDA raises the bar on cybersecurity requirements — updated guidance pushes deeper SBOM transparency, threat modeling, and lifecycle risk management.

06

The Blue Goat takeaway

A clear pattern is emerging across all three stories: cybersecurity in MedTech encompasses much more than protecting medical devices. It is about protecting systems, data, access, and patient safety across the entire lifecycle. Cybersecurity must be built into both the product and the organization — long before regulators or attackers expose the gaps.

Get the next Pulse in your inbox.

One email a month. MedTech-only. Read every edition at bluegoatcyber.com/resources/pulse or book a strategy session at bluegoatcyber.com/contact.