

THE MONTHLY PULSE

# February 2026

MedTech cybersecurity intel for engineering, quality & regulatory teams.

Published February 27, 2026

IN THIS ISSUE

- 01 From the Editor**
- 02 Where in the World is the Goat?**
- 03 Forbes Technology Council — staying ahead of medical device cyber risk**
- 04 In MedTech History — Brain-Computer Interfaces**
- 05 Ask the Goat — what is cloud penetration testing?**

**About this edition.** LSI USA '26, MedTech Innovator Asia Pacific, Christian's Forbes piece on visibility, and a deep dive on Brain-Computer Interfaces. Sourced from the Blue Goat Cyber LinkedIn newsletter, The Monthly Pulse.

## THE MONTHLY PULSE

# February 2026

*LSI USA '26, MedTech Innovator Asia Pacific, Christian's Forbes piece on visibility, and a deep dive on Brain-Computer Interfaces.*

## 01

## From the Editor

March will be a busy month for Blue Goat Cyber, with our team on the ground and in the conversation globally. We're sponsoring LSI USA '26 in Dana Point, working alongside MedTech innovators and investors focused on accelerating submissions without cybersecurity delays. We're also serving as the Exclusive Cybersecurity Partner and Innovation Partner for MedTech Innovator Asia Pacific, mentoring and judging pitches from early-stage companies in Seoul and Singapore. Together, we can ensure the next generation of medical technology is innovative, secure, resilient, and worthy of patient trust.

## 02

## Where in the World is the Goat?

**LSI USA '26** — Waldorf Astoria Monarch Beach, Dana Point, CA, March 16–20. Jordan John (Director of Regulatory Affairs and Compliance) leads a panel on March 18: "Cybersecurity as a Competitive Advantage: Building Trust, Value, and Safety." Find us on the fifth-floor Monarch Promenade and in our Partnering Lounge in the Pacific 3 ballroom.

**MedTech Innovator Asia Pacific 2026** — Christian and Melissa Espinosa will judge and mentor at MedTech Spotlight: New Impact Korea 2026 (March 19–20, Seoul) and the Singapore pitch event, supporting early- and mid-stage device, digital health, and diagnostic innovators across APAC.

## 03

## Forbes Technology Council — staying ahead of medical device cyber risk

In his recent Forbes Technology Council article, Christian Espinosa addresses a challenge facing both hospitals and manufacturers: visibility. Healthcare systems operate thousands of connected devices; without comprehensive asset visibility and clear risk prioritization, security becomes reactive. He outlines three essential pillars — **Visibility** (SBOM accuracy and asset inventory are nonnegotiable), **Collaboration** (manufacturers and healthcare organizations must coordinate around patching, vulnerability disclosure, and lifecycle risk), and **Guideline Alignment** (security must be operationalized within product architecture, not added during submission preparation).

## 04

## In MedTech History — Brain-Computer Interfaces

We trace BCIs from the landmark 2004 BrainGate clinical trial — when a tiny array of microelectrodes implanted into the motor cortex captured neural firing patterns and translated them into commands controlling a cursor on a screen. Modern BCI platforms now combine implanted hardware, embedded firmware, wireless telemetry, machine learning algorithms, and cloud-based processing environments.

Applications span prosthetic-limb and wheelchair control, stroke neurorehabilitation, treating epilepsy and Parkinson's, and emerging uses in VR and mental-state monitoring. Each step forward increases capability — and each layer of connectivity increases complexity.

05

## Ask the Goat — what is cloud penetration testing?

Cloud penetration testing identifies vulnerabilities that traditional audits often overlook. By simulating realistic attack scenarios, it evaluates cloud-specific risks, misconfigurations, exposed interfaces, and application weaknesses that could put sensitive data at risk. As medical devices increasingly rely on cloud-connected infrastructure, proactive testing is essential to validate security controls, clarify shared-responsibility boundaries, identify configuration errors, and strengthen defenses before incidents occur.

## Get the next Pulse in your inbox.

One email a month. MedTech-only. Read every edition at [bluegoatcyber.com/resources/pulse](https://bluegoatcyber.com/resources/pulse) or book a strategy session at [bluegoatcyber.com/contact](https://bluegoatcyber.com/contact).