BLUE GOAT CYBER℠
Medical Device Cybersecurity

COMPANY OVERVIEW · 2026

Secure by design. Cleared by the FDA.

The cybersecurity partner medical device manufacturers trust from first 510(k) to postmarket maturity.

Veteran-Owned | FDA 524B (Feb 3, 2026) | AAMI SW96 | AAMI TIR57/97 | IEC 81001-5-1

TRUSTED BY MEDTECH TEAMS AT

INTUITIVE bioMérieux NOVA inogen natera MEDIVIS VitalConnect

250+	100%	12 yrs
FDA submissions supported	Cybersecurity clearance rate	Founders' MedTech security experience

01 · AT A GLANCE

What we do, and why it matters.

Blue Goat Cyber is a specialist medical device cybersecurity firm. We help manufacturers - from pre-seed startups to global Fortune 500 OEMs - design, document, and defend connected medical devices against the FDA's premarket cybersecurity expectations and the real-world adversaries that follow them into the field.

Every engagement is fixed-fee, FDA-aware, and led by senior practitioners. Methodologies map directly to FDA Section 524B (Feb 3, 2026 premarket cybersecurity guidance), AAMI SW96, AAMI TIR57/97, and IEC 81001-5-1. No offshoring. No first-year analysts learning on your submission. No surprise change orders.

250+
FDA submissions supported
510(k), De Novo, and PMA across the SPDF.

100%
Clearance rate on cyber
Across every submission we've supported.

48 hr	Fixed	70+	2015
Deficiency response	**Fee, unlimited revisions**	**Podcast episodes**	**MedTech roots (Alpine)**

"Blue Goat Cyber helped us navigate our first end-to-end cybersecurity testing for our wearable medical device. Their timeline exceeded expectations, and their report helped us achieve FDA clearance without any additional questions."

Anna Norman, VP of Product, InfoBionic.ai

02 · MISSION

Protect patients. Clear submissions. Build trust.

Mission. Make every connected medical device secure by design and ready for FDA review - so that the patients depending on those devices can trust the technology keeping them alive.

Origin. Founder Christian Espinosa, a US Air Force veteran, launched Alpine Security in 2014 and took on the firm's first medical device cybersecurity client in 2015. By 2018 the practice had narrowed exclusively to MedTech. Alpine was acquired by CISO Global in 2020. Shortly after the sale, Christian survived a serious health scare on the receiving side of medical technology - and the experience reframed the work as patient safety with a pulse.

Founding. Blue Goat Cyber was founded in 2022 with a deliberately narrower charter: medical devices only, FDA submissions only, senior practitioners only. No generalist IT audits. No first-year analysts learning on a client's submission.

Today. We support manufacturers across robotic surgery, diagnostics, infusion, imaging, wearables, and SaMD - including Intuitive Surgical, bioMérieux, Nova Biomedical, Inogen, and Natera. Every senior reviewer has either submitted to the FDA or sat on the receiving side of CDRH.

OUR TIMELINE

2014 — **Alpine founded**
Christian Espinosa founds Alpine Security

2018 — **MedTech-only**
Practice narrows exclusively to medical

2020 — **Acquired**
Alpine Security acquired by CISO Global

2022 — **Blue Goat Cyber**
Founded with a sharper MedTech mission

2026 — **Today**
250+ submissions, 100% clearance rate

WHAT MAKES US DIFFERENT

Specialists, not generalists.

We only work on medical devices. Every methodology, template, threat model, and SBOM workflow is purpose-built for FDA Section 524B, the February 3, 2026 premarket cybersecurity guidance, AAMI TIR57/97, IEC 81001-5-1, and the SPDF.

Submission-grade deliverables.

Threat models, SBOMs, VEX statements, pen test reports, and SPDF documentation that map directly to CDRH's review checklist - drafted in the format reviewers expect to see.

Senior-led, no hand-offs.

Every engagement is led day-to-day by a principal who has personally cleared submissions. Average reviewer has 15+ years of MedTech security experience. No analyst hand-offs, no offshore subcontracting.

Fixed fee with unlimited revisions.

We quote the scope. We absorb the iteration. If the FDA wants a third round of changes, the meter doesn't restart.

03 · SERVICES

End-to-end medical device cybersecurity.

We cover the full Secure Product Development Framework (SPDF) - from earliest design-input through premarket submission, clearance, and postmarket monitoring. Engage us on the entire lifecycle or drop us in for a single deliverable.

FDA Premarket Package (full-service) - our flagship

End-to-end Section 524B and February 3, 2026 premarket guidance support delivered as a single fixed-fee package: threat modeling, SBOM, security risk management, architecture views, manual pen testing, labeling, and the full submission. Typical timeline: 6-8 weeks. Proposal in 24 hours.

Penetration Testing

Hardware, firmware, mobile/cloud, wireless, and AI/ML attack-surface testing aligned to the FDA's expectations and PWG-T scoping. Reports drafted for CDRH reviewers.

Threat Modeling (STRIDE / Patient Safety)

STRIDE, PASTA, and patient-safety-focused threat models with explicit links to risk management (ISO 14971 / AAMI TIR57) and design controls.

SBOM, VEX & Vulnerability Management

CycloneDX/SPDX generation, VEX statements, KEV monitoring, and a postmarket workflow that keeps your SBOM defensible long after clearance.

FDA Deficiency Response

Surge support for FDA cybersecurity Additional Information letters. Median 48-hour first-pass response; clients have never failed a second round.

Postmarket Cybersecurity

Coordinated vulnerability disclosure (CVD), incident response playbooks, postmarket SBOM/VEX maintenance, and alignment with the FDA's postmarket guidance.

Adjacent programs: EU MDR / Cyber Resilience Act alignment (MDCG 2019-16), SOC 2 Type II, HIPAA, HITRUST, and MDS2 / HSCC procurement disclosures - delivered as MedTech-aware programs, not generic IT audits.

03 · SERVICES (CONT.)

Delivery models built around the FDA clock.

Five engagement shapes — pick what matches your milestone, not what fills a retainer.

Model	Best for	Typical timeline
FDA Premarket Package (flagship)	End-to-end 510(k)/De Novo/PMA cyber submission	6–8 weeks
Single-deliverable	One artifact (pen test, threat model, SBOM)	2–6 weeks
Deficiency surge	Active FDA cybersecurity AI letter	48 hr – 30 days
Postmarket retainer	Cleared device, ongoing obligations	Continuous
Pre-submission diagnostic	Readiness gap assessment	1–2 weeks

Pricing & SLA you can put in front of finance.

- **Fixed-fee, no T&M.** Every package is scoped, quoted, and signed before kickoff — no scope-creep invoices.
- **24-hour proposal SLA.** From scoping call to a complete fixed-fee proposal in your inbox in one business day.
- **Deficiency surge in 48 hours.** Active FDA cyber AI letter? We mobilize in 48 hours and reply within FDA's clock.
- **Submission-ready artifacts.** Everything formatted to eSTAR section structure — drop into the package as-is.
- **Plain-English audit trail.** Reviewer-facing rationale documented so the next 510(k) team isn't starting from zero.

04 · WHERE YOU FIT IN

Find your stage in the medical device lifecycle.

We organize our work by where you are in the FDA medical device lifecycle - not by service category. Pick the stage that matches today, and we'll bring the right deliverables to the table.

STAGE 1
2-7 yrs out

Concept & Design
Build cybersecurity into the architecture before you lock the design. SPDF setup, early threat modeling, SBOM strategy, and Section 524B planning.

STAGE 2
~9 mo out

Premarket Submission
Manual pen testing, reviewer-ready threat model, SBOM, security architecture views, and the Section 524B evidence package - all landing in eSTAR together.

STAGE 3
510(k)/De Novo/PMA

FDA Submission
End-to-end premarket cybersecurity package, eSTAR-ready. Our flagship full-service engagement - 6-8 weeks, fixed fee, senior-led.

STAGE 4
AI letter received

FDA Response
Rapid, reviewer-ready response to FDA cybersecurity Additional Information letters. 48-hour first pass. No client has ever failed a second round.

STAGE 5
Cleared & in field

Postmarket
Coordinated vulnerability disclosure, SBOM/VEX maintenance, KEV monitoring, and incident playbooks aligned with the FDA's postmarket guidance.

Not sure which stage applies? Most first calls are a 30-minute scoping conversation - we'll tell you what evidence you already have, what's missing, and how long it takes to close the gap.

05 · METHODOLOGY

The Blue Goat SPDF - a 5-phase, FDA-aligned framework.

Our engagements follow a five-phase Secure Product Development Framework mapped 1:1 to the FDA's expectations under Section 524B and the February 3, 2026 premarket cybersecurity guidance. Every phase produces evidence the FDA will ask for - in the format reviewers expect.

Design input → Postmarket →

01 **Scope & Threat Model**
Design-input review, asset inventory, STRIDE + patient-safety threat model, and a defensible attack surface map. Output: threat model document and security risk registry.

02 **Architecture & Controls**
Security architecture views, control selection (IEC 81001-5-1), data-flow diagrams, and trust-boundary documentation aligned with risk management file.

03 **Build & Verify**
SBOM generation (CycloneDX/SPDX), VEX statements, static/dynamic analysis, and full penetration testing across hardware, firmware, wireless, mobile, cloud, and AI/ML surfaces.

04 **Submit & Defend**
Submission package drafting, eSTAR mapping, reviewer Q&A, and rapid response to any cybersecurity deficiency letter - typically within 48 hours.

05 **Sustain (Postmarket)**
CVD program, SBOM/VEX maintenance, KEV monitoring, incident playbooks, and annual reassessment aligned with the FDA's postmarket guidance.

06 · PROOF

Track record, clients, and recognition.

We measure ourselves the way our clients measure us: did the device clear, and is it safe in the field? Across more than 250 supported FDA submissions, zero clients have failed clearance because of cybersecurity. The track record runs from solo-founder startups to publicly traded device manufacturers.

REPRESENTATIVE CLIENTS

Intuitive Surgical	bioMérieux	Nova Biomedical	Inogen
Natera	Medivis	VitalConnect	Spiro Health

> *"Blue Goat Cyber takes the burden off our engineers and makes FDA cybersecurity requirements easy to understand. The organized documentation, perfectly formatted for eSTAR, saves us countless hours."*
>
> **Amy Lynn, Chief Compliance Officer, Medivis**

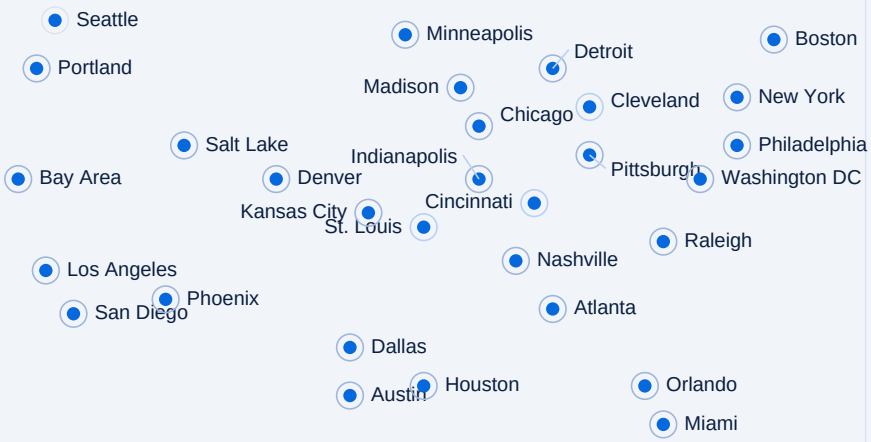
06 · PROOF (CONT.)

Client footprint.

Engagements span MedTech corridors across the US and select international manufacturers operating under both FDA and EU MDR regimes.

UNITED STATES

Engagements concentrated in MedTech corridors



INTERNATIONAL

Cross-border MedTech

- United Kingdom
- France
- Germany
- Ireland
- Switzerland
- Israel
- UAE
- Singapore

20+ states & countries served

RECOGNITION & PRESENCE

- Featured speakers at DeviceTalks Boston/West, LSI USA, LSI Europe, MedTech World Asia, and AMDM.
- Host of The Med Device Cyber Podcast — 70+ episodes interviewing MedTech leaders, FDA reviewers, and investors.
- Publisher of The Monthly Pulse — the newsletter that reads like the FDA cybersecurity guidance, decoded.
- Authors of the 2026 FDA Premarket Cybersecurity Decoder and the SBOM/VEX Field Guide for Medical Devices.

07 · LEADERSHIP

Senior practitioners — no junior intake, no handoffs.

Every engagement is led by someone on this page. The same people who scope your project are the ones writing your threat model, running your pen test, and defending your submission.

Christian Espinosa

Founder & CEO

MBA, CISSP

U.S. Air Force Academy graduate and veteran with 30+ years in cybersecurity. Founded Alpine Security in 2014 (acquired by CISO Global in 2020), then Blue Goat Cyber in 2022. Supported 250+ FDA medical device submissions; no client has failed to clear due to cybersecurity.

Myles Kellerman

CTO

Leads device and IoMT cybersecurity services, application security, red-team and physical assessments, and product security consulting. 18+ years in IT, 13+ in cybersecurity. Previously Principal Consultant at Cerberus Sentinel and led pen testing at Alpine Security.

Melissa Espinosa

VP, Strategic Partnerships

Builds and grows Blue Goat's channel and partner network. Former cardiac stepdown nurse — brings clinical insight to MedTech partnerships with consultants, regulatory experts, and technology vendors.

Kristy Kennedy

VP, Sales

Global commercial leader with 25+ years across life sciences, medical device, and MedTech. Background spans sales, marketing, business development, and operations — including product launches and go-to-market strategy.

Sarah Beach

Senior Project Manager

Owns engagement timelines, deliverables, and FDA interactions end-to-end. Keeps threat models, pen tests, SBOMs, and submission packages on rails so engineering and regulatory teams stay aligned without surprises.

Michelle Hughes

Senior Project Manager

Senior project manager driving complex MedTech cybersecurity engagements from kickoff through FDA clearance. Coordinates technical, QA, and regulatory workstreams to keep submissions moving and clients informed.

08 · HOW TO ENGAGE

From first call to FDA clearance — a predictable arc.

Every engagement follows the same five-step rhythm. Fixed-fee scope, senior-led delivery, submission-grade evidence in the format CDRH reviewers expect.

01
Discovery call
30 min
Scope, device class, timeline, and current evidence.

02
Proposal
24 hr
Fixed fee, fixed scope, delivery dates. No change-order roulette.

03
Kickoff
Week 1
Senior team assigned. Working sessions, not status calls.

04
Delivery
6-8 wks
Threat model, SBOM, pen test, architecture views, 524B package.

05
Submission & beyond
Ongoing
eSTAR-ready handoff, deficiency coverage, postmarket monitoring.

THREE WAYS TO START

Pre-submission diagnostic
1-2 week readiness assessment mapped to the Feb 3, 2026 premarket guidance. Tells you what's defensible, what's missing, what reviewers will challenge.

Best when: 3-9 months from submission

Full FDA Premarket Package
Our flagship: end-to-end 524B evidence in 6-8 weeks. Threat model, SBOM, pen test, architecture views, labeling, and the full submission - eSTAR-ready.

Best when: submitting in next 12 months

Deficiency surge
FDA cyber deficiency letter in hand? We respond within 48 hours, own the rewrite, and hand back a reviewer-ready package. Never lost a second round.

Best when: clock is already running

READY WHEN YOU ARE

Let's talk before your next submission.

Most first conversations take 30 minutes. We'll tell you whether we're the right fit, and if we're not, who is.

YOUR FIRST CALL

A senior MedTech practitioner
30-minute scoping call. Principal-led, no junior intake. Proposal turned around within 24 hours.

info@bluegoatcyber.com · bluegoatcyber.com/contact

CONTACT

Web bluegoatcyber.com

Email info@bluegoatcyber.com

Book bluegoatcyber.com/contact

LinkedIn /company/blue-goat-cyber

Scan to book

Veteran-owned · US-based senior team