BLUE GOAT CYBER

Case Study

When Traditional Cybersecurity Firms Fail MedTech – Why One Manufacturer Turned to Blue Goat Cyber

How Choosing the Wrong Cybersecurity Partner Led to FDA Rejections, Delays, and Costly Fixes

The High Cost of Choosing the Wrong Cybersecurity Partner

Background

A medical device manufacturer preparing for FDA 510(k) submission needed cybersecurity testing and documentation for compliance. Instead of partnering with a MedTech-focused cybersecurity firm, they chose a traditional IT security company that offered penetration testing at a lower cost.

The result? Dozens of cybersecurity deficiencies flagged by the FDA led to an expensive, months-long scramble to fix their submissions.

⚠ Challenges - When A Traditional Cyber Firm Fails A MedTech Submission

Their chosen cybersecurity firm:

- **Didn't understand the FDA's 2023 cybersecurity guidance**

  Their security tests weren't aligned with regulatory expectations.

- **Only provided generic penetration testing**

  They didn't offer penetration test plans, test cases, fuzz testing, threat modeling, SBOM management, or risk assessments, which are mandatory for FDA approval.

The Outcome: FDA Rejection & Costly Delays

Their submission was rejected with dozens of cybersecurity deficiencies flagged by the FDA.

They lost over 6 months of market time fixing vulnerabilities & missing documentation.

COST

The cost to remediate exceeded $300,000, far outweighing any initial cost savings.

- **Missed critical security documentation**

  The firm didn't prepare security architecture views, postmarket security plans, or interoperability risk assessments.

- **Had no experience with medical device security**

  They applied IT security principles, completely ignoring patient safety risks and the unique security needs of medical devices.

Schedule a Discovery Session ->

Case Study

When Traditional Cybersecurity Firms Fail MedTech – Why One Manufacturer Turned to Blue Goat Cyber

How Choosing the Wrong Cybersecurity Partner Led to FDA Rejections, Delays, and Costly Fixes

After wasting months with a traditional cybersecurity firm, the manufacturer turned to Blue Goat Cyber to get their submission back on track.

The Solution – How Blue Goat Cyber Fixed the FDA Deficiencies

1 ***Full FDA cybersecurity compliance review***

- Identified all gaps and created a remediation roadmap.

2 ***Threat modeling & risk assessments***

- Performed a risk-based approach aligned with patient safety considerations.

3 ***Comprehensive cybersecurity documentation***

- Delivered everything required for FDA submission (security risk management, postmarket surveillance, SBOM support, etc.).

4 ***FDA-ready penetration testing***

- Provided test plans, test cases, and regulatory-aligned reporting.

5 ***Fixed-fee pricing & unlimited retests***

- Ensured no surprises or extra costs until compliance was met.

BLUE GOAT CYBER

The Outcome: Successful FDA Submission & Market Entry ✓

- FDA approved their cybersecurity submission with zero additional deficiencies.
- They regained lost time, securing market entry after a 6-month delay.
- The manufacturer committed to using Blue Goat Cyber for all future medical devices.

Key Takeaways – The Risk of Choosing the Wrong Cybersecurity Partner

- Traditional IT security firms aren't equipped for medical device cybersecurity compliance.
- FDA requires more than penetration testing—documentation, SBOM, and risk assessments are critical.
- The wrong cybersecurity partner can cost manufacturers time, money, and market position.
- Partnering with MedTech cybersecurity experts ensures compliance, security, and faster approval.

Don't Let Cybersecurity Deficiencies Delay Your FDA Submission

- **Get the right cybersecurity partner before it's too late.**
- **Avoid costly rework and lost revenue—secure FDA approval the first time.**

FDA APPROVED ★ FDA ★ FDA APPROVED

Schedule a Discovery Session ->