



BLUE GOAT CYBER
Medical Device Cybersecurity

MEDICAL DEVICE CYBERSECURITY GUIDE

Medical Device Cybersecurity Consulting: Buyer's Guide

Compare medical device cybersecurity consulting partners, retainer scope, deliverables, pricing, and exclusions. Use practical questions before requesting a proposal.

Reviewed 2026-10-30

bluegoatcyber.com

Book a free discovery call
30 minutes with a senior expert
bluegoatcyber.com/discovery-call



IN BRIEF

Choose medical device cybersecurity consulting by the work your product needs. Compare medical device experience, inspectable deliverables, patient-safety reasoning, written scope, and manufacturer decision ownership. Separate ongoing consulting from testing and full submission work before comparing prices. No consultant can promise a regulatory outcome.

This guide is for manufacturers, engineering leaders, and quality and regulatory teams selecting outside product cybersecurity support. It helps you request comparable proposals. It is not a regulatory determination or a substitute for reviewing your device's evidence.

Looking for the offer rather than a comparison checklist? See [medical device cybersecurity consulting](#) for Blue Goat's design-through-postmarket support and monthly retainer.

Start with the work you need to buy

Write down the decision or evidence gap you need help with. A design question, a missing penetration test, and ongoing vulnerability review are different scopes. Buying them under the same vague label makes proposals difficult to compare.

Your situation	Scope to discuss	Boundary to confirm
Intended use and architecture are still taking shape	Threat modeling, security requirements, and architecture review	Which design decisions and documents will be reviewed?
Development is underway	Threat model updates, secure development questions, and document review	What review is included, and who implements changes?
A premarket submission is being assembled	Device-specific evidence gap review or a full premarket package	Is the consultant reviewing existing content or producing the package?
You need independent security testing	A separately scoped penetration-testing engagement	Which build, interfaces, test cases, and retests are covered?
The device is marketed or changing	Vulnerability review, evidence updates, and manufacturer decision support	Who monitors, investigates, approves patches, and communicates?

Use the [premarket cybersecurity deliverables map](#) to discuss document gaps. For testing, compare the [medical device penetration-testing scope](#), not just the number of testing days.

When should consulting begin?

Begin while architecture decisions are still open. Intended use and a sketch showing the device, apps, cloud services, and data flows are enough to start the discussion. Bring existing documents if you have them. Do not wait for a complete documentation package to ask a design question.

If development has already started, identify the decisions that can still change and the evidence that needs review. A consultant should distinguish design recommendations from documentation of the system as built.

For a discussion of timing, listen to [When Should You Start Medical Device Cybersecurity?](#), Episode 89.

Questions to ask a consulting partner

Does the experience fit your product?

Ask how the partner would scope your actual system. Depending on the device, that may include firmware, physical interfaces, wireless transport, mobile applications, cloud services, and third-party components. Ask who will do the work and what medical device experience that person brings.

Generic corporate IT security experience is not the same as product security experience. Ask how the consultant distinguishes data-security impact from potential patient harm and how recommendations connect to the manufacturer's risk management process.

Can you inspect the proposed deliverables?

Request a deliverable list and an anonymized or fictional sample that is clearly labeled. Do not request another manufacturer's confidential documents. A useful proposal identifies inputs, outputs, review responsibilities, and version or build assumptions.

Ask how threats connect to controls and tests. For a testing engagement, ask for the plan, test cases, and report scope. A list of vulnerabilities alone does not explain coverage or the secure behavior that was tested.

Who owns the decisions?

The manufacturer owns risk acceptance, patch, and customer-notice decisions. Its quality team owns and approves the QMS. Ask how recommendations, evidence gaps, and unresolved questions will be recorded for those decision-makers.

Avoid scopes that imply the consultant can accept device risk on your behalf or determine a clinical consequence without device evidence. Consulting supports decisions; it does not transfer manufacturer responsibility.

How are regulations and recommendations distinguished?

Ask the partner to separate applicable statutory duties from guidance recommendations and contractual deliverables. Section 524B addresses cyber devices. The FDA's February 3, 2026 premarket cybersecurity guidance describes recommendations for cybersecurity evidence and lifecycle practices. A proposal should explain applicability rather than label every recommendation a universal legal requirement.

Retainer or fixed-fee project?

A retainer suits recurring questions and agreed review work as your product changes. A project suits a defined deliverable or testing scope. Neither model is inherently more complete. Compare the work included in each.

For a retainer, confirm:

- Included expert access and how priorities are agreed.
- Whether meetings, preparation, document review, and written follow-up use that access.
- Who your advisor is and how work is handed over.
- How additional work is approved and priced.
- Whether unused access carries forward, and what termination terms apply. Ask for these terms; do not assume them.
- Which testing, submission, QMS, and implementation activities are excluded.

For a project, confirm the deliverables, system boundaries, dependencies, review rounds, retest terms where applicable, and change-control process. Request a schedule based on those inputs, not a promised regulatory decision date.

Pricing: compare scope before fees

There is no single useful price for every medical device cybersecurity consulting scope. Architecture, existing evidence, interfaces, requested outputs, and team responsibilities affect the work. Compare proposals against the same inputs and exclusions.

Blue Goat's Fractional Product Security Officer retainer provides up to 20 hours a month of expert access.

Starting at \$5,000 a month. Final monthly fee is fixed after scoping. This is Blue Goat's offer, not a market-wide pricing benchmark.

Within agreed scope, the retainer supports design questions, threat modeling, security architecture reviews, document review, and CI/CD and secure development pipeline help. It can also support evidence updates and vulnerability review. Penetration testing, full submission packages, deficiency responses, and larger QMS integration projects are scoped separately. Additional help is agreed before work begins.

See the [consulting retainer scope and exclusions](#) before requesting a quote. Corporate IT security, full QMS implementation, and general software validation are not this product cybersecurity offer.

Red flags in a proposal

- A promised clearance or approval outcome instead of defined work.
- A generic scope that does not identify your device, interfaces, or evidence inputs.
- Vulnerability severity presented as patient risk without device-specific analysis.
- Testing described as included without a build, coverage, or reporting scope.
- Unlimited access implied by a retainer with no written capacity terms.

- QMS integration assumed to be included without reviewing existing procedures.
- No explanation of who approves recommendations or handles unresolved findings.

Prepare a comparable request for proposals

Provide your intended use, system sketch, development stage, relevant markets, open questions, and requested outputs. Identify existing threat models, SBOMs, risk files, architecture documents, or test reports. Share confidential evidence only through an agreed secure process.

Ask each partner to respond with included work, excluded work, required inputs, deliverables, responsibilities, fees, and scheduling dependencies. Separate recurring support from larger projects in the comparison. This makes a lower fee meaningful only when the scopes are genuinely comparable.

Frequently asked questions

Is medical device cybersecurity consulting the same as penetration testing?

No. Consulting can support design decisions, architecture review, evidence upkeep, and vulnerability review. Penetration testing evaluates a defined system and build through separately scoped testing. Confirm whether any testing is actually included in the proposal.

Do we need a prototype to start?

No. Intended use and a system sketch are enough to discuss design-stage consulting. Testing access and build requirements are agreed separately when testing is needed.

Does a retainer include a full FDA submission package?

Not automatically. Blue Goat scopes full submission packages, penetration testing, and deficiency responses separately. Confirm the boundary between document review and production of a complete package in writing.

Can the consultant accept cybersecurity risk for us?

No. The manufacturer owns risk acceptance and decisions about patches and customer notices. A consultant provides analysis and recommendations for manufacturer review.

What does Blue Goat's retainer cost?

Starting at \$5,000 a month. Final monthly fee is fixed after scoping. The retainer provides up to 20 hours a month of expert access for agreed product cybersecurity work. Additional help and larger projects require prior agreement.

Discuss your consulting scope

Bring your intended use and system sketch to [discuss the consulting retainer](#). Blue Goat provides product cybersecurity support from design through postmarket. The manufacturer retains its decisions and responsibilities.

Sources and related resources

- [The FDA: Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions, February 3, 2026](#)
- [21 U.S.C. 360n-2: FD&C Act Section 524B](#)
- [Secure Product Development Framework consulting](#)
- [Download this buyer's guide as a PDF](#)

Current web guide: bluegoatcyber.com/guides/medical-device-cybersecurity-consulting-buyers-guide

Talk to a senior medical device cybersecurity expert

Book a free 30-minute discovery call. Scan the code or visit bluegoatcyber.com/discovery-call. You get a written quote within 24 hours.



Informational material. Confirm requirements for your device and market. The manufacturer owns risk decisions, QMS approvals, and regulatory submissions. No regulatory outcome is promised.