GOATWATCH

Continuous SBOM and Vulnerability Monitoring for Medical Devices

The monitoring platform that keeps your software bill of materials and its risk current, from first submission through end of life.

THE RECORD BEHIND IT

250+	0	Continuous
FDA submissions supported	cybersecurity rejections	CVE and KEV matching

A product of Blue Goat Cyber. Standalone, or included in the postmarket service.

1 What GoatWatch is

GoatWatch is Blue Goat's monitoring platform for medical device software. It takes your software bill of materials, keeps it current, watches every component for newly disclosed vulnerabilities, and tells you which ones actually matter for your device. It runs before submission to give you a clean SBOM, and after clearance to keep watching for the life of the product.

It is purpose-built for medical devices, not general IT. Findings are judged against your device architecture and the patient-harm pathway, not against a raw severity score. The platform does the continuous work; a senior Blue Goat engineer owns the judgment calls that a dashboard cannot make.

GoatWatch is live and in use today. The monitoring, correlation, and triage are running now. The customer portal and reporting are actively being expanded, and we will show you exactly what exists today on a call rather than promise a finished state.

2 What it does

- SBOM ingestion and maintenance. Import a CycloneDX or SPDX bill of materials, or have us build one. Components are normalized and version-resolved, and support status is maintained against FDA's three-tier taxonomy: actively maintained, no longer maintained, and abandoned.
- Continuous vulnerability correlation. Every component is matched against the NIST NVD and upstream supplier advisories, so a new disclosure against your dependency tree surfaces without you going looking for it.
- CISA KEV tracking. Known Exploited Vulnerabilities are treated as a separate, higher-priority signal, because FDA treats them that way. A KEV match on one of your components becomes an explicit action item.
- Device-context triage tied to patient harm. Not every vulnerability matters equally. GoatWatch prioritizes by exploitability in your specific architecture and the harm that reaches the patient, which cuts the noise that raw CVE feeds produce.
- VEX and exportable evidence. Vulnerabilities that do not apply are documented as not affected, with a justification. Findings, decisions, and SBOM change history are exportable as evidence for FDA postmarket and audits.
- End-of-life tracking. Components approaching or past end of support are flagged, because an unmaintained component is a postmarket risk whether or not it has a published vulnerability today.

2.1 How it works

Figure 1. From bill of materials to evidence, continuously.

3 Why the triage is different

The value is not the alert. Anyone can subscribe to a CVE feed. The value is the judgment that turns a raw feed into a decision. GoatWatch scores each finding against your device threat model: whether the vulnerability is exploitable in this architecture, and what harm reaches the patient if it is. That is the same logic FDA reviewers apply, and it is why a component with a high abstract severity score can be correctly deprioritized while a lower-scored one is escalated.

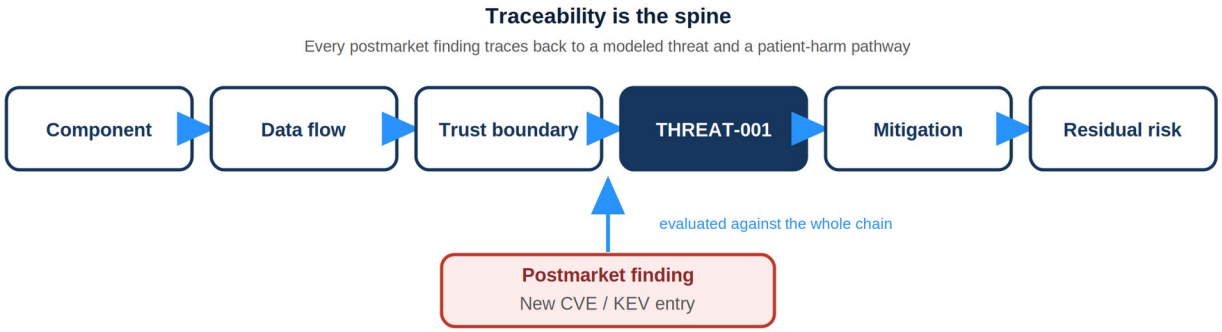

Figure 2. Every finding is judged against the device, not against a database score.

> *Anyone can subscribe to a CVE feed. The value is the judgment that turns a feed into a decision.*

4 Premarket and postmarket

GoatWatch works both sides of the device lifecycle. FDA expects SBOM rigor before clearance and continuous vigilance after launch, and the same platform covers both.

Stage	What GoatWatch provides
Premarket	A submission-ready SBOM: validated component data, resolved unknowns, a known-vulnerability baseline, and documentation aligned to FDA cybersecurity guidance.
Postmarket	Continuous monitoring against NVD, supplier advisories, and CISA KEV; device-context triage; and an exportable evidence trail for postmarket reporting.

5 Platform, plus a named engineer

GoatWatch is a platform, but a medical device is not something you hand to an automated dashboard. Every account is owned by a senior Blue Goat medical device cybersecurity engineer, the same people behind more than 250 FDA submissions. The platform runs the monitoring; the engineer owns the triage, the exploitability judgment, and the regulatory context. You get both, not a login and a wish of luck.

What GoatWatch does not do: it does not patch your device, and it does not make your regulatory reporting decisions for you. It gives you the evidence and the recommendation. The engineering and the decisions stay with you, under your quality system.

6 Standalone or bundled

GoatWatch can be bought on its own to monitor a device you already have, or included as the monitoring engine inside Blue Goat's full postmarket cybersecurity service, where it sits alongside coordinated vulnerability disclosure, incident response, patch validation, and regulatory reporting. If monitoring is all you need, GoatWatch stands alone. If you need the whole postmarket program run for you, GoatWatch is the engine inside it.

7 About Blue Goat

- More than 250 FDA submissions supported, with zero cybersecurity rejections.
- Medical device cybersecurity exclusively. Not a general information security firm with a healthcare practice.
- Senior-led, United States based. A senior engineer owns your account, not an offshore tier-one queue.
- Fixed-fee pricing per device. No hourly billing, no scope creep.
- Service-Disabled Veteran-Owned Small Business.