BLUE GOAT CYBER

Complete Medical Device Cybersecurity

Who We Are

At Blue Goat Cyber, we specialize in medical device cybersecurity. We ensure manufacturers meet FDA, EU MDR, and global regulatory compliance while protecting patient safety. With decades of experience, we help MedTech innovators secure their devices against cyber threats and streamline regulatory approval.

- FDA cybersecurity compliance experts
- 100% success rate in FDA cybersecurity submissions
- Fixed-fee pricing with unlimited retests
- Industry leaders in penetration testing, SBOM management, & risk assessments

The Problem We Solve

Medical device manufacturers face increasing cybersecurity challenges:

- Stricter FDA cybersecurity requirements
- Growing cyber threats targeting medical devices.
- Access to professional guidance from seasoned agents.
- Regulatory deficiencies leading to delays & lost revenue.
- Lack of in-house cybersecurity expertise.

Without proper cybersecurity, your device could be vulnerable to attacks, regulatory rejection, or costly delays.

We ensure your cybersecurity meets FDA expectations—preventing delays and securing approval.

How We Help

We guide you through every phase of medical device cybersecurity, ensuring compliance and security from design to postmarket.

Our Services

- Premarket Cybersecurity for FDA Submission
- Medical Device Penetration Testing
- Threat Modeling & Risk Assessments
- Cybersecurity Documentation for FDA & EU MDR Compliance
- Postmarket Security Monitoring & SBOM Tracking

We don't just test—we ensure compliance, risk mitigation, and ongoing security.

BLUE GOAT CYBER

Why Blue Goat Cyber?

Unlike traditional cybersecurity firms, we focus ***exclusively*** on medical device security. Our deep industry knowledge and regulatory expertise set us apart.

Traditional Cybersecurity Firms:

- General IT security testing.
- No regulatory expertise.
- Limited postmarket support.
- Hourly-based pricing with extra fees.

Blue Goat Cyber:

- **FDA & MedTech cybersecurity specialists.**
- **100% focused on regulatory approval & patient safety.**
- **Fixed-fee pricing with unlimited retests.**
- **Continuous postmarket support.**

We don't just find vulnerabilities—we ensure your device is FDA-ready.

Proven Success

We've helped industry leaders secure FDA approval and protect their devices.

Recent clients include: bioMérieux, Inogen, Natera, Nova Biomedical

100% FDA submission success rate.

Accelerating time to market while ensuring security & compliance.

Let's Get Started

Don't risk cybersecurity deficiencies delaying your approval. Work with experts who know how to secure medical devices while meeting FDA expectations.

Schedule a Discovery Session ->

Blue Goat Cyber

Cybersecurity Management Plan - Checklist

Documentation Section	Content Description	Blue Goat Cyber Recommendations, Tips, and Tricks	
Personnel Responsible	Who fills the role of: - Cybersecurity Compliance Officer - Product Owner - Postmarket Management Owner - Authorizing Official	Cybersecurity Compliance Officers are responsible for ensuring that the organization and product are compliant with applicable standards and regulations. They should ensure that the product security team is integrating cybersecurity throughout the total product lifecycle. Product Owners are responsible for the product as a whole and will typically be responsible for overseeing the device at the highest level. They should be responsible for guiding the direction of the product's development. Postmarket Management Owners take responsibility for ongoing efforts with the medical device once it has been fielded. This includes, but is not exclusively limited to the ongoing postmarket monitoring compliance and ensuring that the product remains compliant once cleared. Authorizing Officials can sign off and approve on processes and documentation and should act as the final authority on revisions. This individual should be distinct from any of the other listed roles.	☐
Sources, Methods, and Frequency for Monitoring and Identifying Vulnerabilities	Describes how manufacturers should establish robust methods for continuously monitoring cybersecurity vulnerabilities, including data from security research, threat intelligence, and incident reporting systems.	This section will cover what actions manufacturers must take for vulnerability intake. The intake can vary depending on the product and risk classifications, but at a minimum should include: - SAST: SAST analyzes source code, bytecode, or binaries to detect vulnerabilities early in the development lifecycle before the software is deployed. This proactive approach helps medical device manufacturers meet FDA expectations for secure design by minimizing exploitable flaws at the code level. This testing should occur during any code changes on the new commit. - SBOM Analysis: SBOM analysis inventories all software components, including open-source and third-party libraries, to identify known vulnerabilities and manage supply chain risk. FDA now requires SBOMs in submissions for cyber devices under Section 524B of the FD&C Act, making this a core compliance and transparency tool. SBOM Analysis should be a continuous process for components in the device. - VAPT: VAPT combines vulnerability scanning with simulated attacks to evaluate how effectively a medical device can withstand real-world cyber threats. These tests demonstrate due diligence to regulators by validating security controls and uncovering weaknesses that static analysis or SBOM checks may miss. Vulnerability assessments should be conducted quarterly, with penetration testing conducted annually. - CVD(s): CVD programs provide a structured process for security researchers and stakeholders to report vulnerabilities so manufacturers can assess, remediate, and communicate risks. FDA and CISA strongly endorse CVD as part of postmarket cybersecurity management, ensuring timely mitigations and reducing patient safety risks. - Ext sources (CISA Alerts, FDA Notifications): External threat intelligence sources, such as CISA alerts and FDA safety communications, provide critical updates on emerging vulnerabilities like ransomware or third-party software flaws. Incorporating these into risk management helps manufacturers maintain compliance and respond quickly to evolving cyber risks across the total product lifecycle.	☐
Identifying and Addressing Vulnerabilities Identified in CISA Known Exploited Vulnerabilities Catalog	Manufacturers should regularly monitor and address vulnerabilities listed in the CISA Known Exploited Vulnerabilities Catalog, ensuring prompt remediation of high-risk vulnerabilities.	Monitoring the CISA KEV should be a continuous process referenced against the SBOM. This needs to be done against the latest version of the SBOM, which requires a system in place to maintain that SBOM. Some tools assist with the KEV referencing process, though prioritization often needs to be a manual process. Findings in the KEV should be treated as critical vulnerabilities in most cases with immediate focus on remediation.	☐

Periodic Security Testing	Ensures that manufacturers implement regular security testing of devices, including penetration testing and vulnerability scanning, to identify and resolve emerging threats.	For each of the below security testing types, the corresponding timelines can act as a strong baseline. It is worth noting that these timelines may be variable depending on device complexity and risk. - Penetration Testing: Annually - SAST: On code change - SBOM Analysis: Continuously - Security Requirements Testing: On major release - Vulnerability Assessments: Quarterly	☐
Timeline to Develop and Release Patches	Establishes a clear and prompt timeline for developing and releasing security patches once vulnerabilities are identified, aiming to minimize the window of exposure to risks.	Patch timelines should be risk-based and documented, with critical vulnerabilities addressed as quickly as possible, typically within 30 days. A tiered approach ensures resources are focused on the most impactful risks first, while medium and low severity issues are scheduled into regular release cycles. Timelines should be clearly tied to internal SLAs and external regulatory expectations, ensuring accountability across engineering and quality teams. A mechanism to accelerate patch release in emergency cases should be built into the process.	☐
Update Processes	Defines secure, efficient processes for delivering updates and patches, ensuring devices can be updated in a timely and secure manner without disrupting functionality.	The patching process should mirror secure development principles, ensuring that all updates are validated, verified, and cryptographically signed before deployment. Updates should be supported through multiple delivery methods (e.g., over-the-air, secure USB, or network-based) to accommodate varied healthcare environments. Automated regression testing is key to reducing risk of disruption while maintaining rapid deployment capabilities. All update steps must be well-documented and communicated to end users to ensure patches are applied correctly and consistently.	☐
Patching Capability	Ensures that devices are designed to support regular patching and updates throughout their lifecycle, preventing security vulnerabilities from remaining unaddressed.	Devices should be designed with built-in mechanisms that make patching practical and reliable across the entire installed base. This includes support for remote patching, clear rollback procedures if issues occur, and modular architectures that allow partial updates without revalidating the entire system. Capability should also include compatibility with hospital IT infrastructures, which often have strict access controls or segmented networks. Ultimately, patching must be secure, transparent, and minimally disruptive to clinical workflows.	☐
Description of Coordinated Vulnerability Disclosure Process	Outlines processes for coordinating vulnerability disclosure with relevant stakeholders, including security researchers, to ensure timely identification and resolution of security issues.	A Coordinated Vulnerability Disclosure (CVD) process should provide external researchers, customers, and partners with a clear channel to report security issues. The process must include defined intake mechanisms, such as a dedicated security email or web portal, with guaranteed acknowledgment within a set timeframe. Reported vulnerabilities should be triaged promptly, prioritized based on clinical impact, and integrated into the organization's risk management system. Transparency with stakeholders and alignment with industry best practices, such as those outlined by CISA, strengthens trust and ensures consistent, timely remediation.	☐
Description of Communicating Forthcoming Remediations, Patches, and Updates to Customers	Establishes methods for clear and timely communication with customers and users regarding upcoming patches, updates, and remediations to maintain trust and ensure systems remain secure.	Communication of forthcoming remediations should be proactive, structured, and tailored to the needs of healthcare environments. Customers should receive advance notice of planned patches or updates, including expected timelines, deployment methods, and potential operational impacts. Updates must be delivered in a clear, non-technical manner for clinical users while also providing technical details for IT and security teams. Leveraging multiple channels—such as customer portals, advisories, and direct notifications—ensures that information reaches the right stakeholders in time to support secure deployment.	☐