BLUE GOAT CYBER

www.bluegoatcyber.com

Cracking the Code: Insider Cybersecurity Insights for Medical Device Premarket Success

Christian Espinosa
Founder and CEO
Blue Goat Cyber

BLUE GOAT CYBER

How confident are you that your device's cybersecurity strategy will meet FDA expectations the first time around?

Introduction

- About Me - Christian Espinosa
  - Involved with medical device cybersecurity since 2014
  - Sold first cybersecurity company, Alpine Security, in 2020
  - Health scare in Feb 2022

CONCLUSION:
Acute deep vein thrombosis (DVT) in the left femoral, left popliteal, left gastrocnemius, left posterior tibial, left peroneal, left soleal veins. There is no evidence of superficial vein thrombophlebitis (SVT) in the proximal saphenous veins.

  - Started Blue Goat Cyber in 2022

About Blue Goat Cyber

- Guided hundreds of manufacturers through FDA premarket submissions and deficiency responses
- Worked with every category of medical devices, such as:
  - Infusion Pumps
  - Blood Glucose Monitors & Insulin Pumps
  - Remote Patient Monitors & Wearable ECGs
  - Implanted Cardiac Devices (Pacemakers, Defibrillators)
  - Ventilators & Critical Care Machines
  - Networked Surgical Robots & Deep Brain Stimulators
- 100% Success Rate
- FDA-Clearance Guarantee

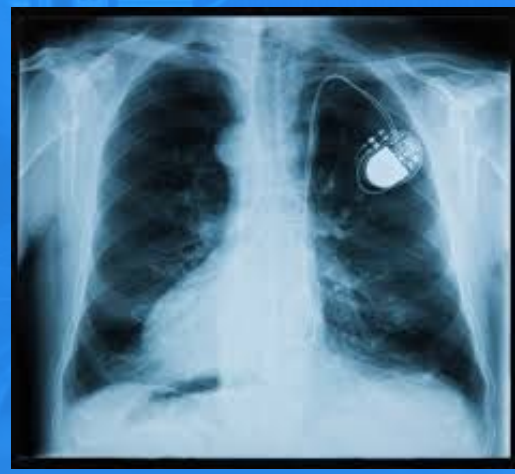
Why Cybersecurity Is No Longer Optional

- **Increasing Connectivity:** By 2025, 68% of medical devices will be network-connected: more entry points for cybercriminals

- **Ransomware Risks:** Ransomware attacks have already disrupted critical hospital systems, impacting devices like infusion pumps, ventilators, and patient monitors

Examples of Medical Device Vulnerabilities

- **Medtronic Insulin Pump Recall**: vulnerabilities allowed attackers to alter insulin delivery remotely, posing life-threatening risks
- **St. Jude Pacemakers:** flaws allowed hackers to interfere with functionality, such as battery depletion or pacing modification
- **WannaCry Ransomware:** attack affected MRI machines and other medical equipment, demonstrating the severe impact of ransomware on connected devices



FDA's Premarket Guidance

- Major cybersecurity update in Sep 2023
- Mandates all connected devices address cybersecurity risks:
  - Threat modeling
  - SBOMs (Software Bill of Materials)
  - SPDF (Secure Product Development Framework)
  - Postmarket monitoring
  - ...and more

Top 5 Cybersecurity Deficiencies in Premarket Submissions

Missing or Inadequate...

1. Comprehensive Threat Modeling
2. SBOM (Software Bill of Materials)
3. Patient Safety-Focused Risk Methodology
4. Early Cybersecurity Engagement in Design
5. Third-Party Penetration Testing

FDA Deficiency Examples

Based on the information provided in your "Software Cybersecurity Repor[redacted], your device meets the definition of a cyber device under Section 524B(c) of the Federal Food, Drug, and Cosmetic Act. However, you did not provide threat modeling documentation. Threat modeling

Based on the information provided in the document Software Cybersecurity Report , your device meets the definition of a cyber device under section 524B(c) of the Federal Food, Drug, and Cosmetic (FD&C) Act. However, you did not provide a software bill of materials (SBOM), including commercial, open-source, and off-the-shelf software components as required by section 524B(b)(3) of the FD&C Act.

You provided security testing in your submission, however, the testing did not include vulnerability testing and penetration testing. Adequate cybersecurity testing is important to comply with the requirements specified in section 524B(b)(2) of the Federal Food, Drug, and Cosmetic Act to provide a reasonable assurance that the device and related systems are cybersecure. Verification and validation

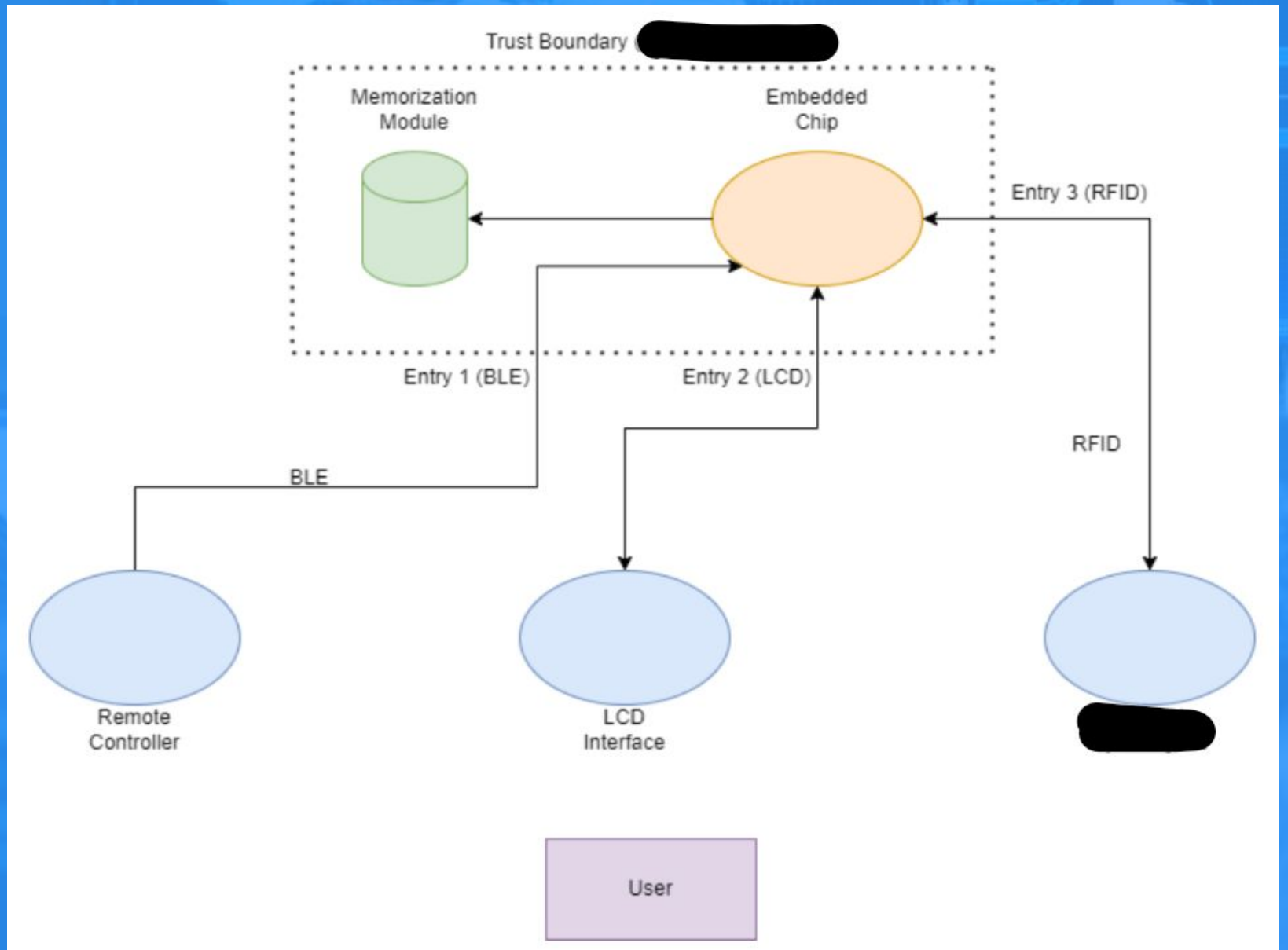
BLUE GOAT CYBER

1. Comprehensive Threat Modeling

Threat Modeling Diagram Example

BLUE GOAT CYBER

Threat Modeling = identifying vulnerabilities and entry points through a trust boundary, aka the “attack surface”



STRIDE Framework

BLUE GOAT CYBER

Threat	Desired property	Threat Definition
Spoofing	Authenticity	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-repudiability	Claiming that you didn't do something or were not responsible; can be honest or false
Information disclosure	Confidentiality	Someone obtaining information they are not authorized to access
Denial of service	Availability	Exhausting resources needed to provide service
Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Threat Modeling Table Example

BLUE GOAT CYBER

Entry Point	Threat	Analysis/Test Case	S	T	R	I	D	E	Result	Threat Risk	Mitigation(s)
OS	Attackers may gain unauthorized access to the SSH service	OS-001			X	X		X	System compromise	High	The device implements protections to the SSH service and the password is not easily guessable
[redacted] App	Attackers may execute malicious files on the [redacted] tablet	MAPT-006	X	X	X			X	System compromise	Low	The [redacted] tablet prevents malicious file download and execution
Software Supply Chain	3rd party components may be compromised in a supply chain attack.	SBoM Analysis	X	X	X	X	X	X	System compromise	High	3rd party components are continuously monitored for vulnerabilities
Ethernet	Attackers may intercept Ethernet traffic	ETH-001				X			Information Disclosure	Medium	The device prevents unencrypted Ethernet traffic
Control Logic / [redacted] App	Devices may not receive security updates	N/A	X	X	X	X	X	X	System compromise	High	Users are informed of the importance of regular updates in Cybersecurity Labeling.
WiFi / [redacted] App / HTTP(S)	Device uses insecure communications	HTTP-004				X			Information Disclosure	Medium	Cipher suites are properly configured and the device only uses secure communications
Internal Development Practices	Insecure coding practices expose the device to increased risk.	SAST	X	X	X	X	X	X	System compromise	High	SAST is implemented as part of the CI/CD pipeline.
Device Dismantling	Dismantling of the device allows for access to sensitive internal components.	N/A		X		X		X	System compromise	High	Dismantling a device would require destroying it. Internal components are secured through the device's outer casing.

BLUE GOAT CYBER

2. SBOM (Software Bill of Materials)

SBOM (Software Bill of Materials)

- Focuses on supply chain risk
- SBOM = comprehensive list of all software components included in a device, including open-source, and third-party software
- Provides **transparency** into the software dependencies, similar to how an ingredients list on packaged food discloses what's inside
- The FDA requires an SBOM as part of medical device submissions

Ingredients: Enriched Corn Meal (Corn Meal, Ferrous Sulfate, Niacin, Thiamin Mononitrate, Riboflavin, Folic Acid), Vegetable Oil (Corn, Canola, and/or Sunflower Oil), Cheese Seasoning (Whey, Cheddar Cheese [Milk, Cheese Cultures, Salt, Enzymes], Canola Oil, Maltodextrin [Made from Corn], Natural and Artificial Flavors, Salt, Whey Protein Concentrate, Monosodium Glutamate, Lactic Acid, Citric Acid, Artificial Color [Yellow 6]), and Salt.

SBOM Example

BLUE GOAT CYBER

slack

3rd-Party Software Report for Desktop

The following sets forth attribution notices for third party software that may be contained in portions of the Slack desktop application. We thank the open source community for all of their contributions.

*The following 3rd-party software packages may be used by or distributed with **Desktop**. Any information relevant to third-party vendors listed below are collected using common, reasonable means.*

DATE GENERATED	RELEASE
10/01/21	1.0

@babel/code-frame (7.10.4)

Declared Licenses

MIT

How confident are you that every component in your SBOM is being continuously monitored for vulnerabilities?

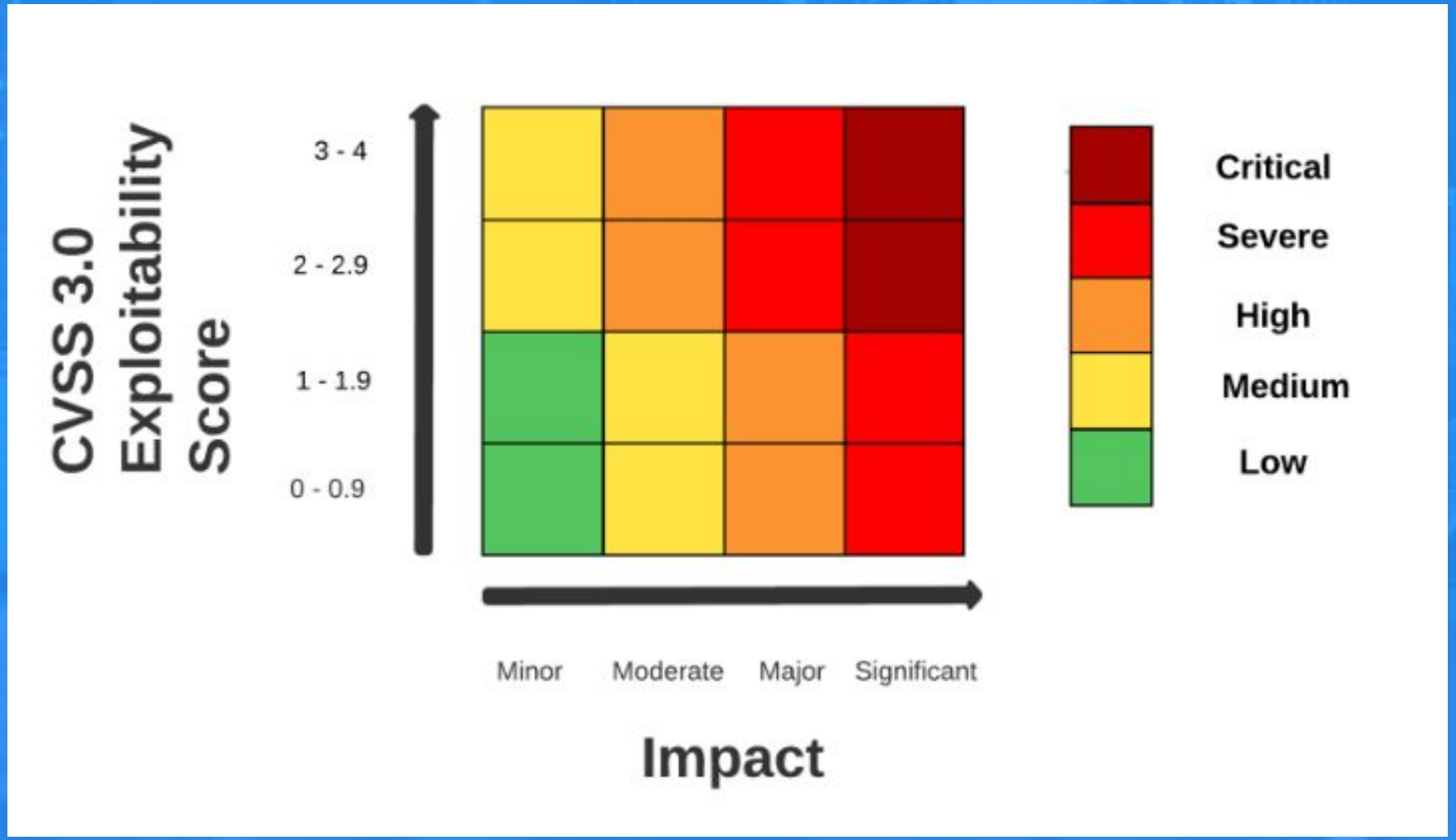
BLUE GOAT CYBER

3. Patient Safety-Focused Risk Methodology

Patient Safety-Focused Risk Methodology

- Cybersecurity risks must align with patient safety outcomes. Not “traditional cybersecurity”
- **Common submission failures:** Risk assessments that focus only on technical issues without linking them to patient harm
- Priority is patient safety, not HIPAA (PHI disclosure)

Example Risk Matrix



Risk Ratings

Risk Rating Definitions

Low

Assigned to situations that may cause temporary discomfort or minor data breaches of non-essential information, these risks have a low probability of occurrence. Their impact is relatively minor, causing limited operational disruption. Low risks warrant standard monitoring and can typically be managed with routine procedures.

Medium

This category includes risks that could lead to temporary injury requiring medical attention or unauthorized access to sensitive, but not critical, patient data. With a moderate likelihood of happening, these risks can cause noticeable disruption and require strategic management to mitigate potential adverse effects on patient trust and regulatory compliance.

High

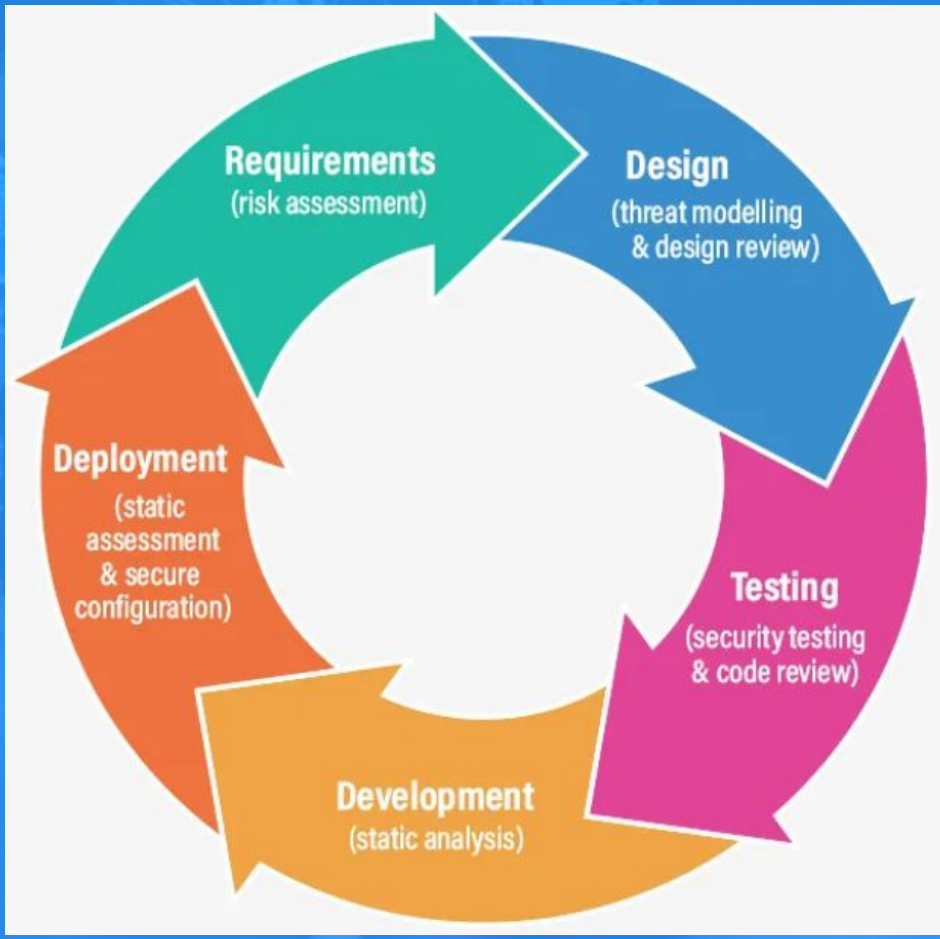
High-risk scenarios involve the potential of life-threatening injury, significant impairment, or major breaches of sensitive data. More liable to occur, these risks can significantly harm

BLUE GOAT CYBER

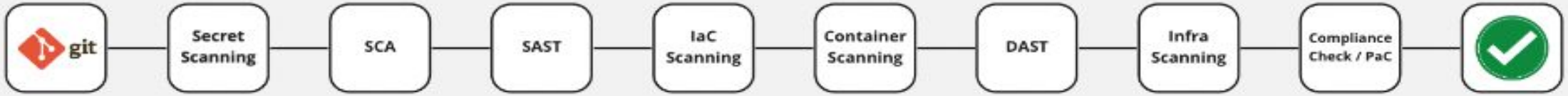
4. Early Cybersecurity Engagement in Design

Build Security into Design—Not After

- Include cybersecurity early in the design phase to avoid costly rework
- Waiting until the final design review leads to delays and design changes
- Set clear cybersecurity milestones early in the product lifecycle
- **Software developers do NOT understand cybersecurity**



OWASP DevSecOps



Initial steps:

At first, we consider to implement the following steps in a basic pipeline:

- Scan git repositories for finding potential credentials leakage.
- SAST (Static Application Security Test)
- SCA (Software Composition Analysis)
- IAST (Interactive Application Security Testing)
- DAST (Dynamic Application Security Test)
- IaC Scanning (Scanning Terraform, HelmChart code to find misconfiguration)
- Infrastructure scanning
- Compliance check

BLUE GOAT CYBER

5. Third-Party Penetration Testing

What Is Penetration Testing?

- Penetration testing is a simulated cyber attack performed on device by white hat hackers
- Vulnerability testing identifies vulnerabilities, penetration testing exploits them
- Provides holistic picture, from chaining vulnerabilities together

Validate Security with Third-Party Penetration Testing

- Third-party penetration testing provides an unbiased assessment of device security
- Independent testing improves submission credibility and identifies overlooked vulnerabilities
- Engage early and often
- Use a firm that specializes in medical device cybersecurity

BLUE GOAT CYBER

Wrap Up

Key Takeaways for Successful Cybersecurity Submissions

- **Start Early:** Engage cybersecurity at the design phase
- **Stay Transparent:** Maintain a complete SBOM throughout the lifecycle
- **Focus on Safety:** Align risk assessments with patient safety
- **Validate Security**: Leverage third-party penetration testing for unbiased assessments
- **Update Continuously:** Refresh threat models and risk assessments regularly

Take Action Today: Build Secure and Compliant Devices

Proactive cybersecurity isn’t just a regulatory requirement—it’s a commitment to patient safety.

Next Steps: Start planning your cybersecurity strategy today—don't let vulnerabilities slow you down.

BLUE GOAT CYBER

Q & A

bluegoatcyber.com