DEEP ARMOR

IoT Security Foundation

Achieving Cybersecurity & Compliance Readiness For Healthcare & Medical Devices

Speaker: Sumanth Naropanth

- Founder & CEO — Deep Armor & Gauntlet
- ~20 years of global experience in cybersecurity
- Sun Microsystems, Palm & Intel
- Black Hat, Troopers, AppSec, FIRST, …
- Columbia University alumnus

About Deep Armor

- ★ Experts in product security risk mitigation, automation & vulnerability assessments
- ★ Collaborated with the US FDA & MITRE Corp on several med-tech security initiatives
- ★ Spearheading end-to-end security for 40+ customers worldwide — Fortune 50 enterprises to startups

CSA cloud security alliance®

Customers & Users

EXPLORAMED

MOVANO HEALTH

inito

willow

swasth

Baxter

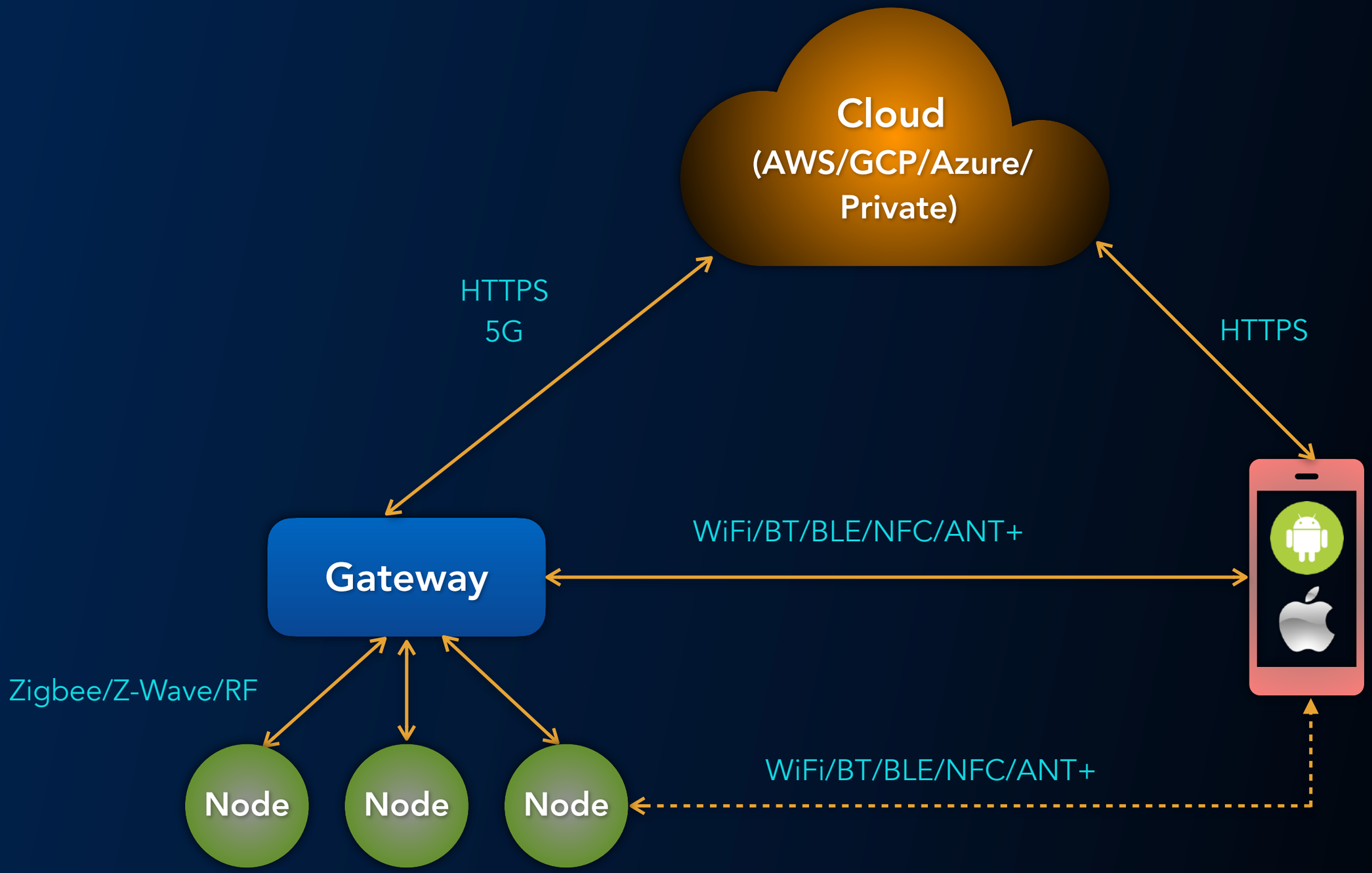
Med-tech Cybersecurity: Why Care?

- Patient Safety: Medical device vulnerabilities can put lives in danger
- Regulatory Requirements: FDA, CE Mark (MDCG), HIPAA, HITRUST, etc. mandate cybersecurity
- Financial Impact: Average healthcare breach costs millions
- Reputation: One cyber incident can damage years of trust

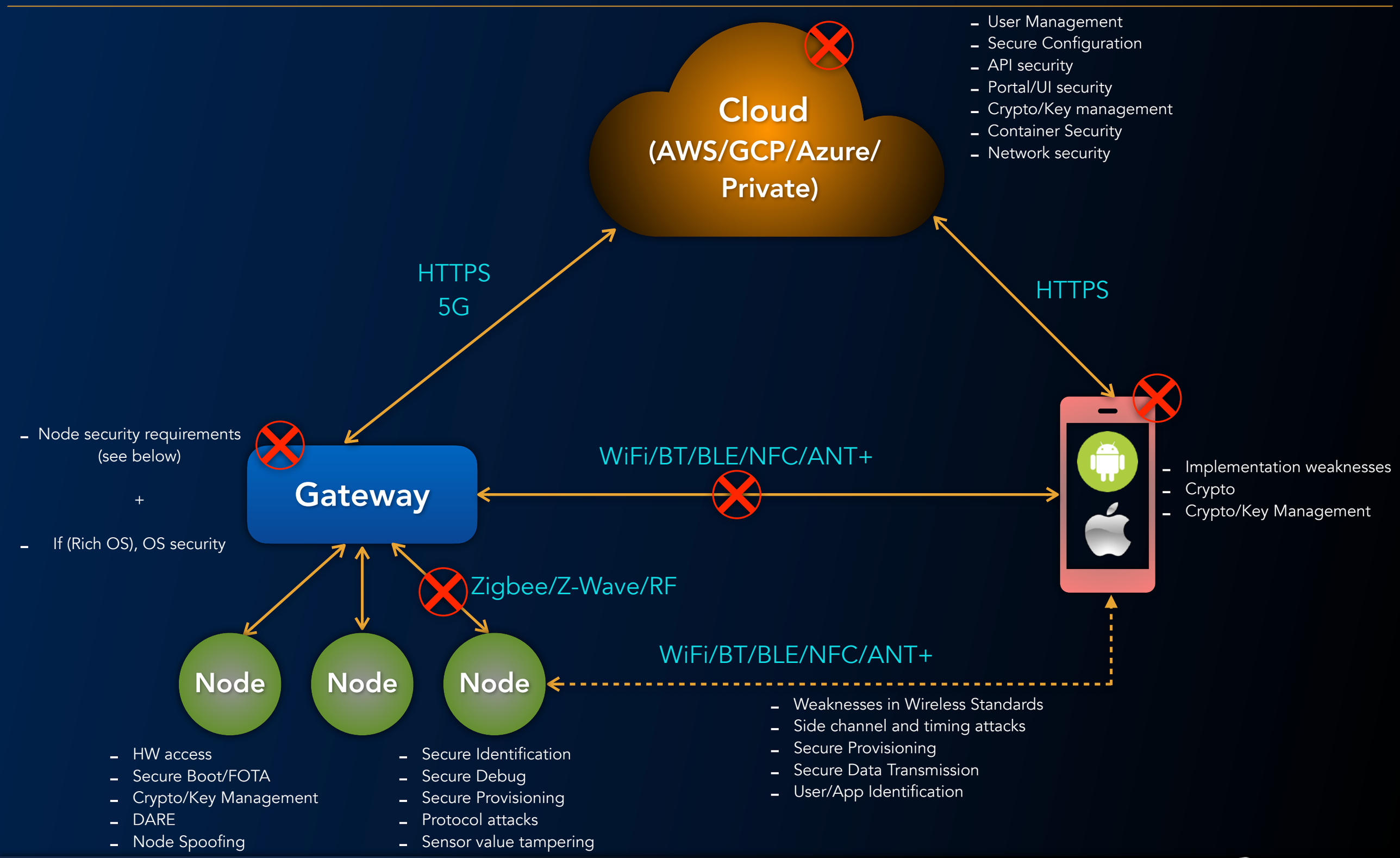
Average breach cost for healthcare in 2024

[Cost of a Data Breach Report 2024 by IBM Security]

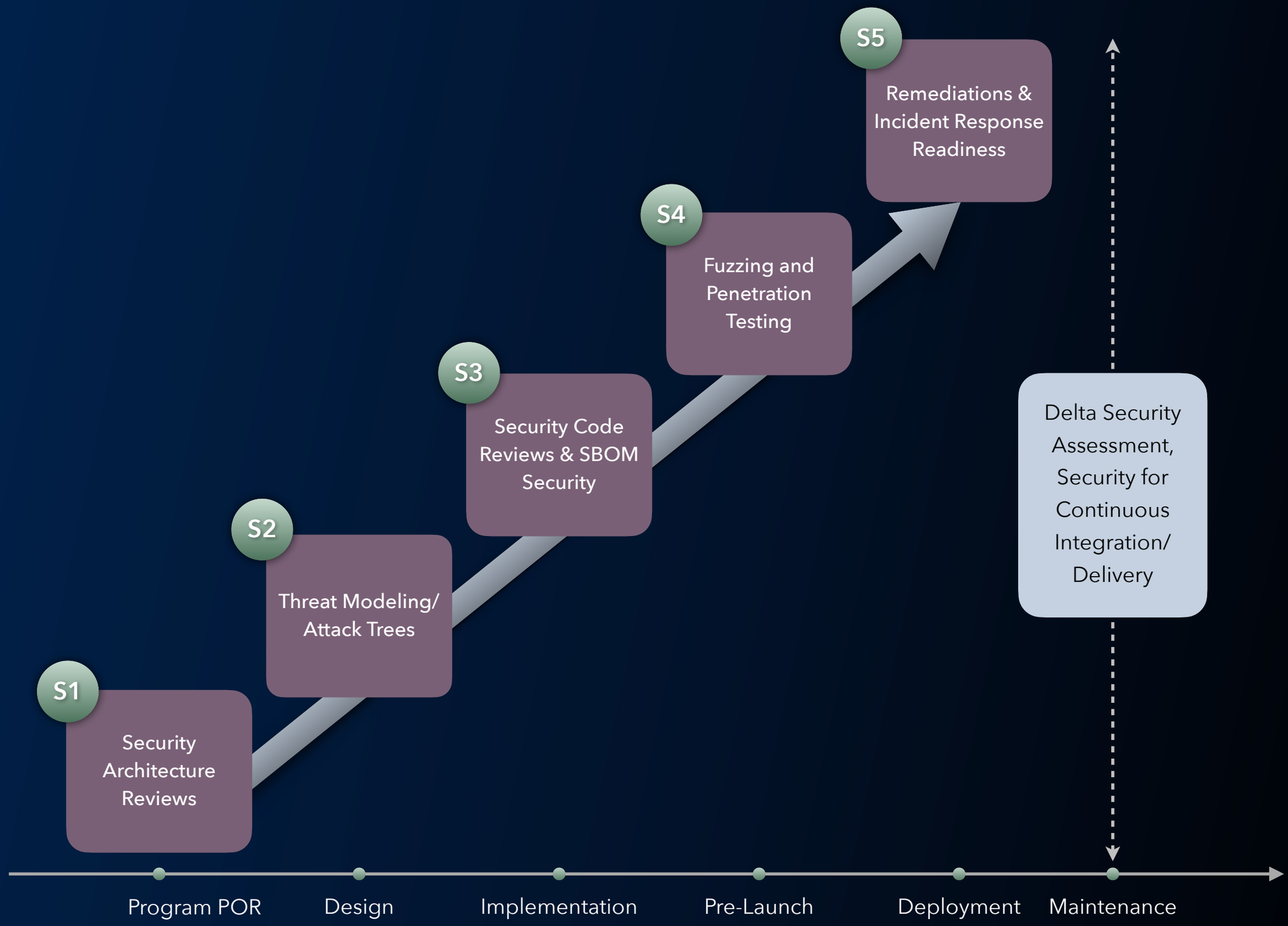
Internet of Medical Things: Product Blueprint



Weak Links


Cloud
(AWS/GCP/Azure/
Private)
- User Management
- Secure Configuration
- API security
- Portal/UI security
- Crypto/Key management
- Container Security
- Network security
HTTPS
5G
HTTPS
- Node security requirements
(see below)
+
- If (Rich OS), OS security
Gateway
WiFi/BT/BLE/NFC/ANT+
- Implementation weaknesses
- Crypto
- Crypto/Key Management
Zigbee/Z-Wave/RF
Node
Node
Node
WiFi/BT/BLE/NFC/ANT+
- Weaknesses in Wireless Standards
- Side channel and timing attacks
- Secure Provisioning
- Secure Data Transmission
- User/App Identification
- HW access
- Secure Boot/FOTA
- Crypto/Key Management
- DARE
- Node Spoofing
- Secure Identification
- Secure Debug
- Secure Provisioning
- Protocol attacks
- Sensor value tampering

Security Development Life Cycle



Holistic Approaches to Product Security

Security Architecture Reviews & Risk-based Threat Modeling

- Identify assets, adversaries, trust boundaries, security objectives & non-objectives
- Threat modeling & risk assessment based on exploitability. Comprehensive documents mapping security requirements to threats to vulnerability vectors

Assessments of building blocks & integration touch-points

Hardware/Embedded Device

- Secure boot
- Secure FOTA
- Key management
- Secure debug
- Crypto design
- Protocol security
- Secure port access
- … many others

Securing Wireless Protocols

- Evaluation of communication protocols
  - Eg: Bluetooth, BLE, WiFi, Zigbee, etc.
- Use of custom packet sniffers
- Validation of common security pitfalls in wireless network models

Holistic Approaches (Contd.)

Cloud Infra Security

- Security monitoring of hyperscaler services
- Meet FDA's Continuous Security requirements
- Regulatory and security compliances: HIPAA, CIS, GDPR, etc.
- AI Security Posture Management – new age security threats

Application Security

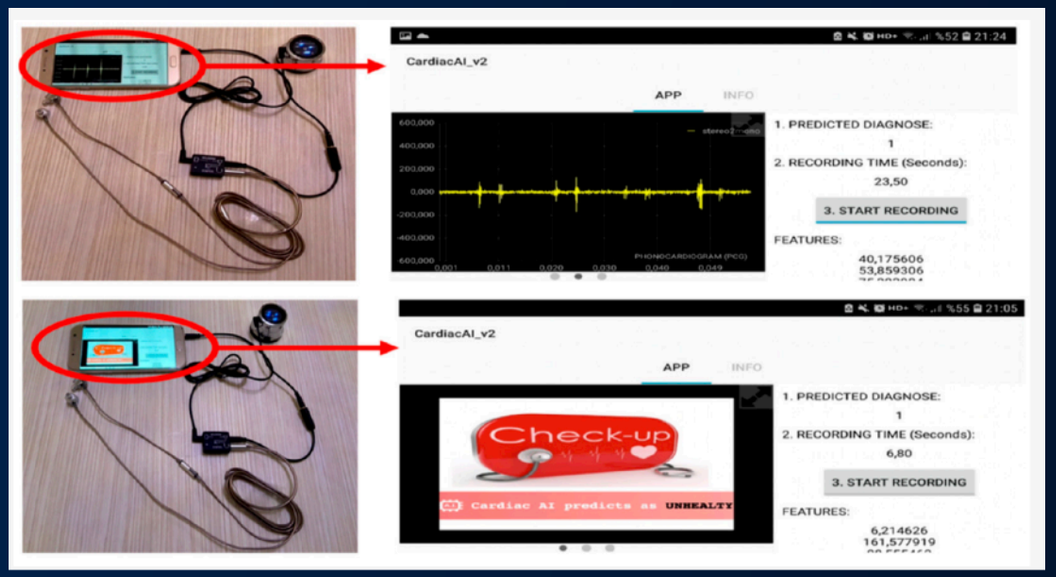
- User Authentication & Authorization
- API parameter sanitization
- Secure implementation of access control (RBAC/ABAC)
- Markup injection attacks
- Business logic evaluation
- Mobile app security best practices (Android & iOS)
- … many other threats

SBOM & Secrets Scanning

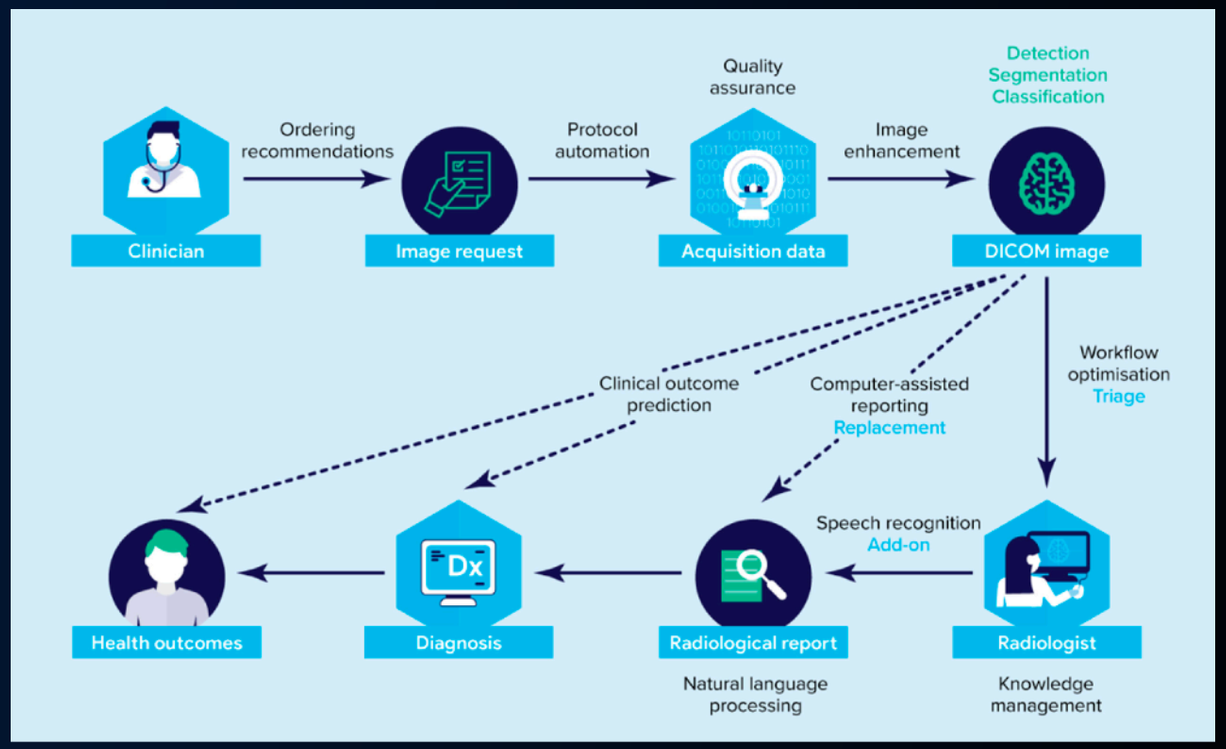
- Security code reviews and tool-based analysis
  - Front-end code for black-box engagements
  - Complete source code for white-box engagements
- Review of CVEs (for 3rd party and open source libraries)
- Exploitability & risk evaluation of affected CVEs

SaMD (Software as a Medical Device)

"Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device."



Mobile apps that diagnose heart conditions



AI-driven radiology image analysis tools

Attacks Against SaMD

Breaking News: Major SaMD Breach Exposes Patient Data

Date: October 2022

In a significant data breach, a leading Software as a Medical Device (SaMD) provider has exposed sensitive patient health information. The incident was traced back to inadequate encryption practices, raising urgent concerns about data protection in medical software.

Urgent Alert: Ransomware Attack Disrupts Medical Software Services

Date: September 2021

A ransomware attack has struck a prominent medical software company, severely disrupting essential services and patient care. The attack underscores the critical need for robust cybersecurity measures to safeguard medical software from emerging threats.

Compliance in MedTech

- MedTech compliance ensures the safety, efficacy, and regulatory adherence of medical devices throughout their lifecycle
    - MDCG: Oversees MDR and IVDR implementation in the EU
    - ISO 13485: Quality management systems for medical devices
    - CLIA: Ensures accuracy in lab testing
    - HIPAA: Protects patient data privacy

FDA Overview: Regulates devices for safety & effectiveness


FDA

Overview - 3 Facets of FDA Submissions

Pre-Sub

A

Early engagement with the FDA to get feedback on high-level cybersecurity strategy to be adopted for product development

Pre-Market

B

Detailed review of the product design, manufacturing, and clinical data to ensure safety and efficacy before market approval

Post-Market

C

Continuous oversight of product safety and effectiveness through real-world performance monitoring and addressing any arising issues

Pre-Market (510k) – FDA's Requirements & Expectations

- End-to-end security assessment for product design & implementation
- Threat modeling (STRIDE/MDIC) documentation for all the building blocks
- Cybersecurity risk assessment documentation
- Continuous security assurance
- Documentation on the cybersecurity controls designed into the device and related systems
- SBOM Security Report
- Security Assessment Report
- Cybersecurity management plan
- Narrative/Reviewer Guide

Post-market: Overview

"Post-market" procedures refer to the ongoing processes and activities that occur after a medical device has been approved and is available on the market

- Risk Management & Quality Systems
- Vulnerability Disclosure & Mitigation
- Monitoring & Addressing Vulnerabilities
- FDA Reporting Requirements
- NIST Cybersecurity Framework

Summary: Tactical Security for IoMT

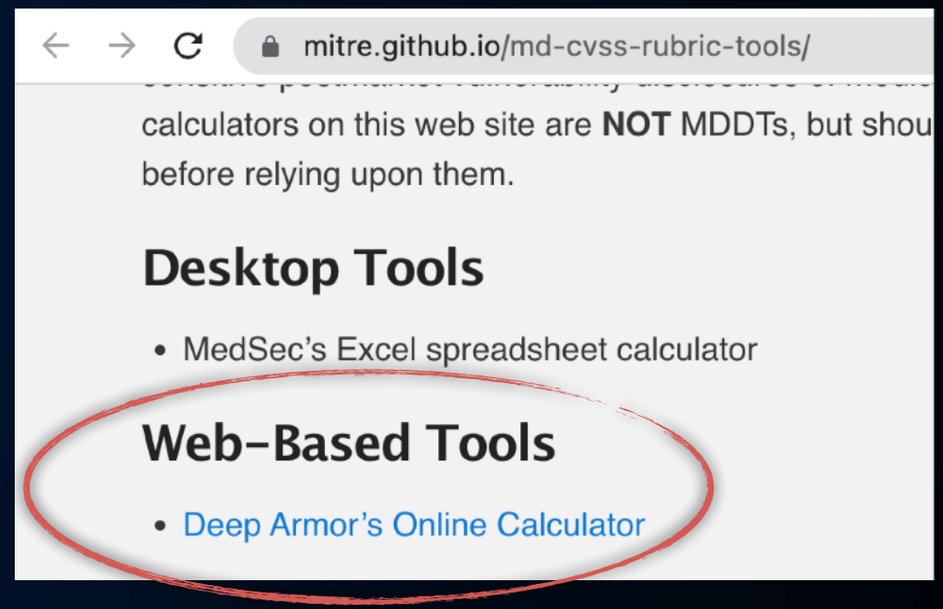
- **Start early** (especially if you're not a med-tech giant)
  - Regulatory audits can be EXCRUCIATING
  - *(They are figuring out a lot of stuff themselves)*

- Medical devices are no longer about the "device"
  - Software stack is an easy target for attackers
  - Secure the building blocks; Secure the integration touch-points

- Continuous Security

- Jumping on to the AI bandwagon? A whole new world of security threats

Deep Armor – FDA/MITRE Free Tool

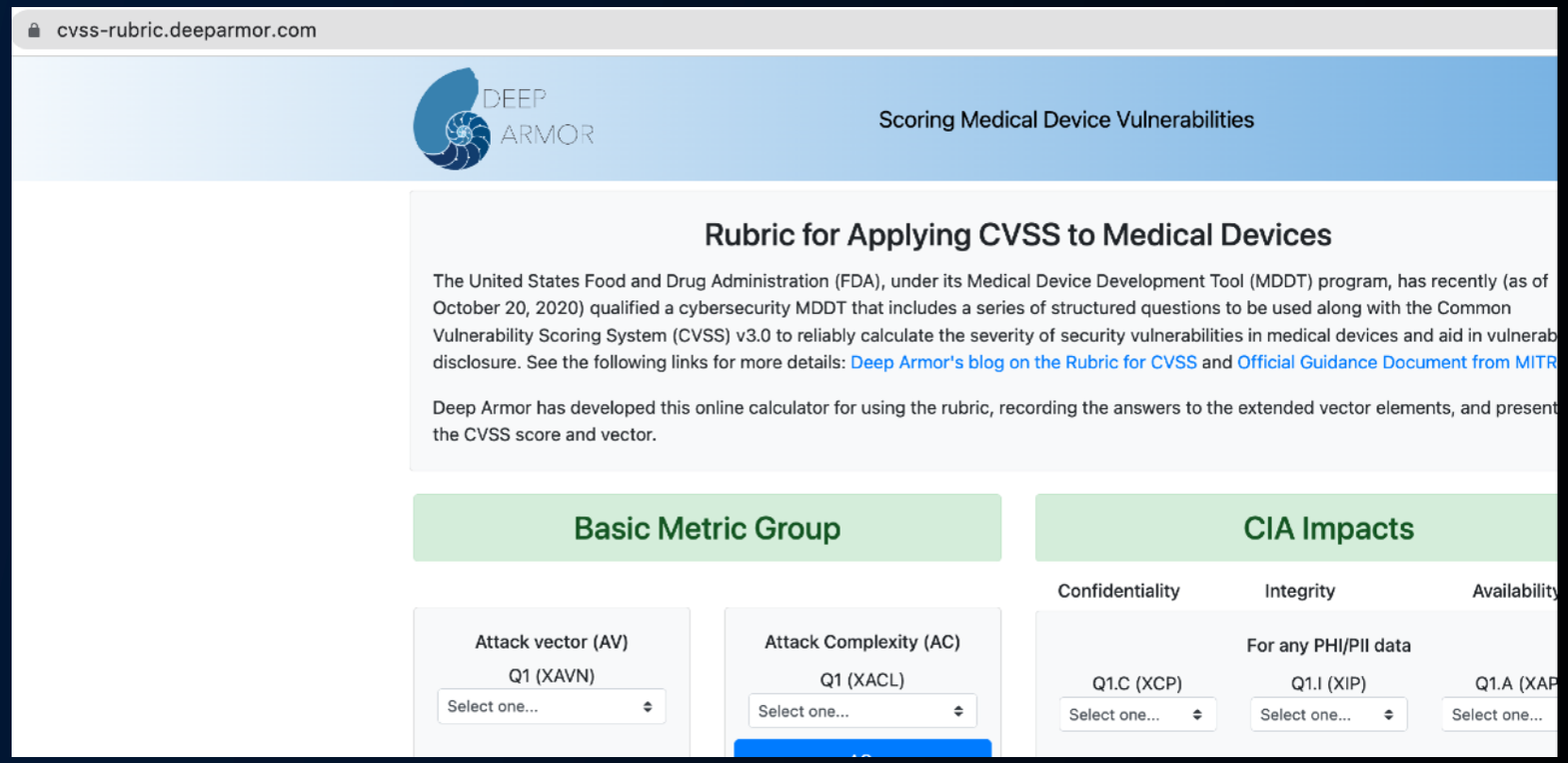


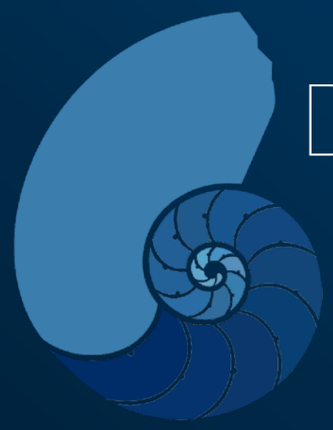
GE HealthCare

IBEX Trusted Cancer Diagnostics for All

SIEMENS Healthineers

stryker





DEEP ARMOR

Cloud Security Solutions

Vulnerability Assessments

Security Consulting

CISO Services

www.deeparmor.com | @deep_armor | services@deeparmor.com