



MEDICAL DEVICE CYBERSECURITY

An Introduction

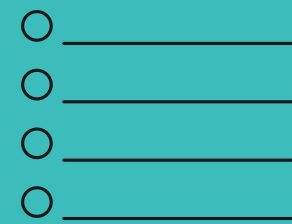
Raj Joshi

MEDICAL DEVICE CYBERSECURITY DISCUSSION TOPICS



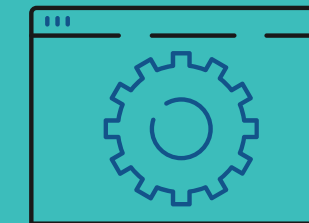
CURRENT CYBER THREATS & STAKEHOLDERS

Examples of threats and risks
impacting different stakeholders



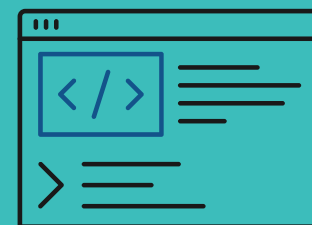
KEY CONCEPTS

Threats, Vulnerabilities, Controls,
Assets, Risks



MEDICAL DEVICE PRODUCT LIFECYCLE

Understand the lifecycle and related
cybersecurity considerations



REGULATORY EXPECTATIONS

How to get ready for regulatory
requirements compliance - FDA focus



ISSUES FACING STARTUPS

Key issues facing MDM startups and
how to address them

Why is Medical Device Security Important?

Threats to whole ecosystem



Medical Device Manufacturers (MDM)

- Cyber incidents can cause loss of consumer confidence / market share
- IP Theft
- Cloning / Counterfeit
- Regulatory action due to non compliance



Hospitals Healthcare Delivery Organizations (HDO)

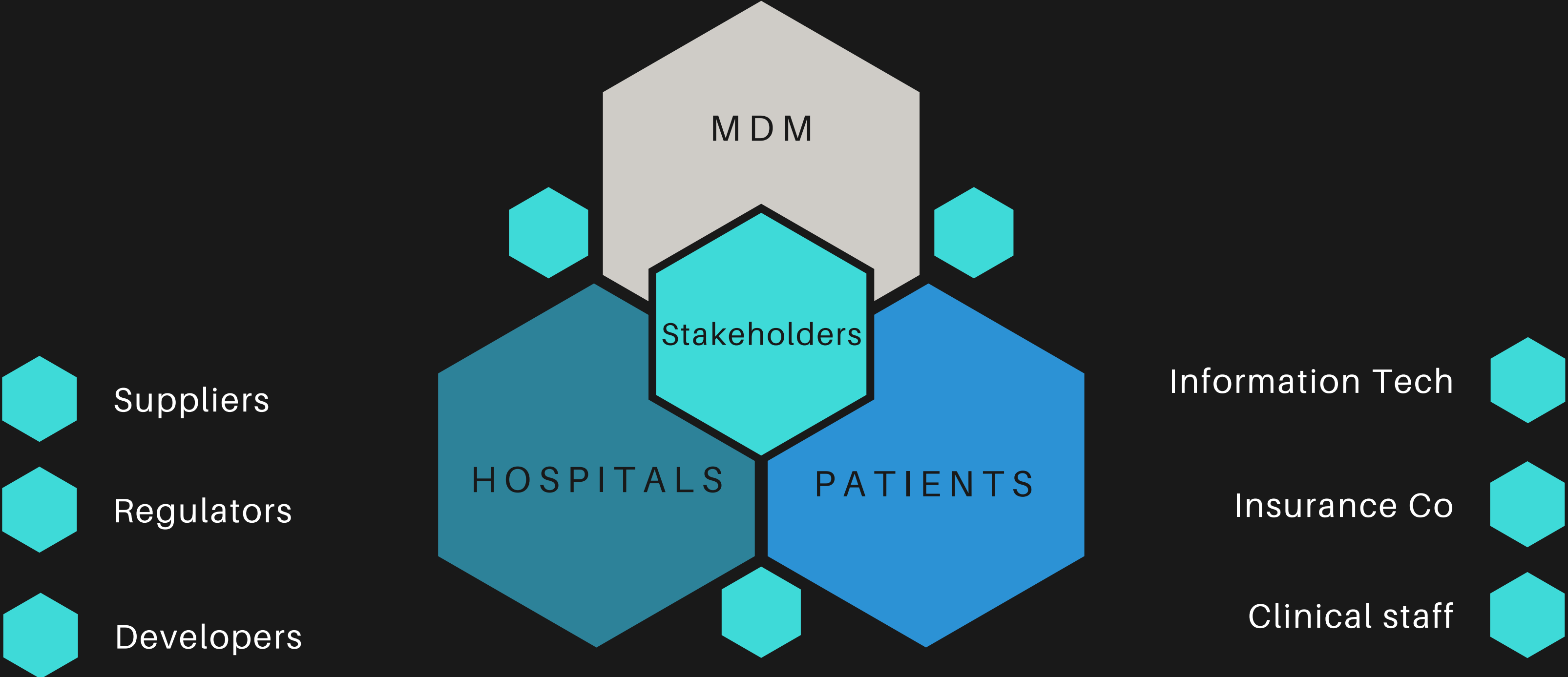
- Prime Targets
- Loss of Patient data
- Reputation damage
- Connected medical device as a attack point
- Ransomware
- Deployment and Maintenance

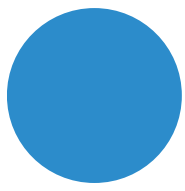


Patients

- Safety
- Loss of personal information
- Effectiveness of diagnosis and treatment

Medical Device Ecosystem



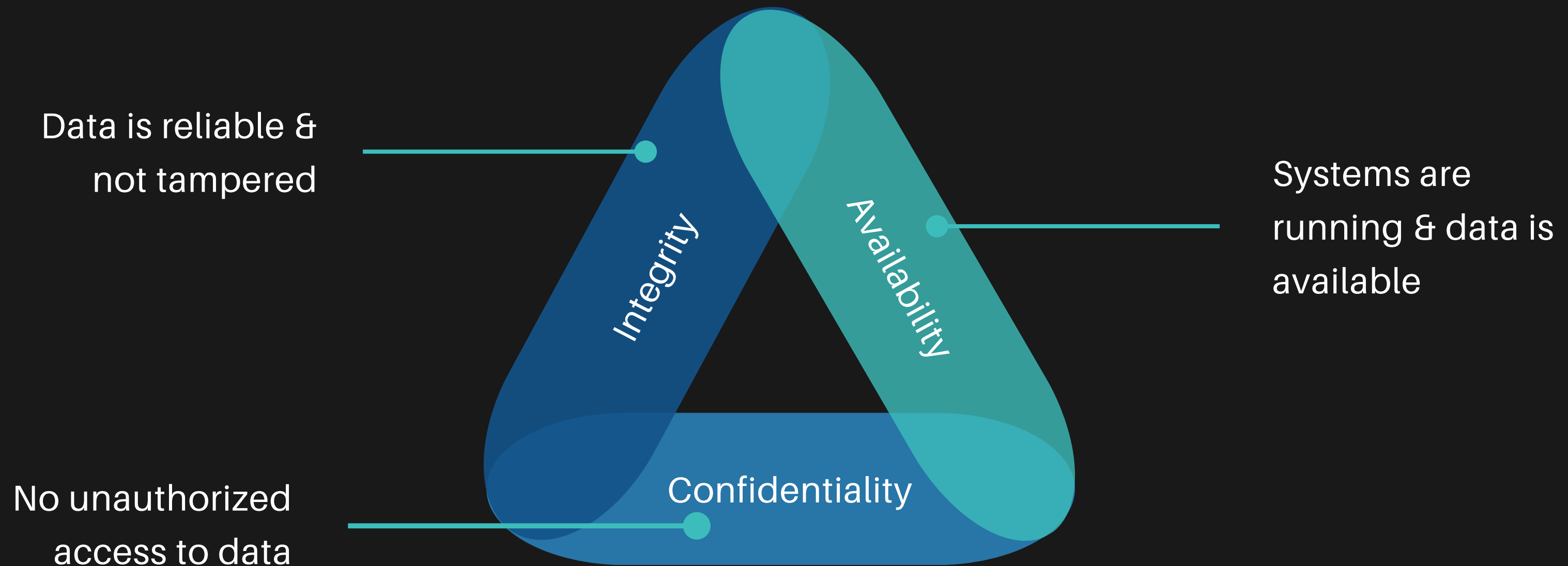


Cybersecurity Concepts

Introduction

WHAT IS CYBERSECURITY?

THE PRACTICE OF ENSURING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF INFORMATION BY PROTECTING NETWORKS, DEVICES, PEOPLE AND DATA FROM UNAUTHORIZED ACCESS OR CRIMINAL EXPLOITATION



Medical Device Security - Key Terms

Learn the language



01

ASSETS

Something of value
Money, PII Data,
Reputation etc.



02

THREATS

Event that has a
potential to adversely
impact assets,
operations e.g.
Robbery, Hacking,
Ransomware



03

VULNERABILITIES

Weakness that
renders an
organization open to
exploitation e.g.
unlocked door,
software bugs



04

RISKS

Potential of an
unwanted outcome
determined by:
Impact of loss (Rs) x
likelihood (%) of
exploitation






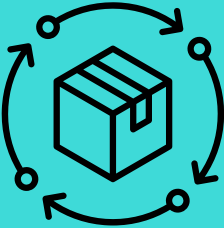

05

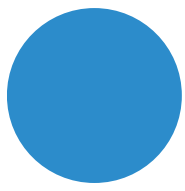
CONTROLS

Safeguards
prescribed to protect
"CIA" of assets e.g.
Cameras, OTP, locks,
encryption,
authentication

Medical Device Security Key Terms (contd.)

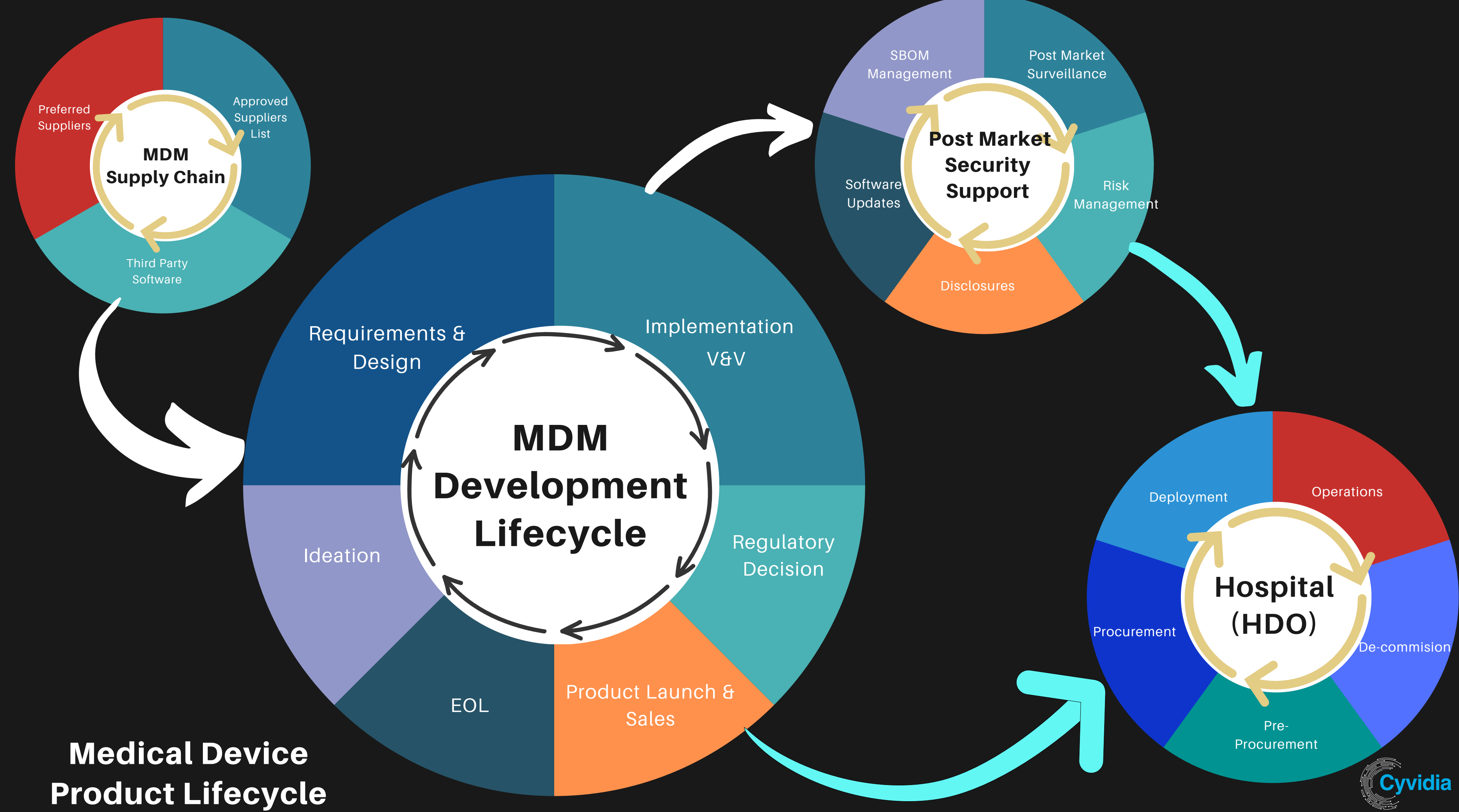
Learn the language

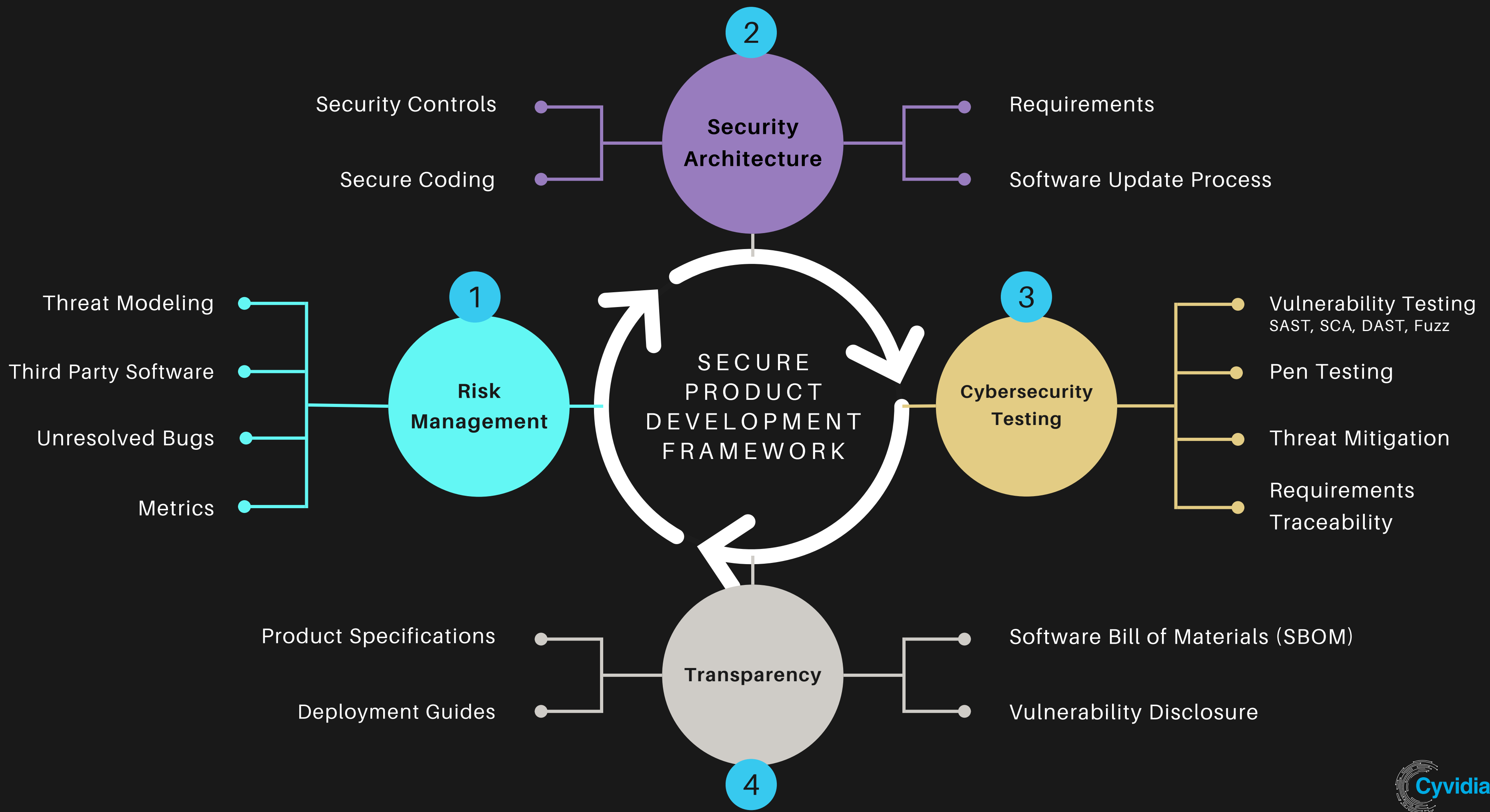
 06	 07	 08	 09	 10
<p data-bbox="219 874 626 1084">PERSONALLY IDENTIFIABLE INFORMATION (PII) AND PHI</p> <p data-bbox="219 1174 679 1376">Patient name, Identifiers, Address, Credit Card Number</p>	<p data-bbox="819 874 1286 1028">SOFTWARE BILL OF MATERIALS (SBOM)</p> <p data-bbox="819 1174 1306 1542">List of ingredients in the software to help with license compliance and vulnerability analysis</p>	<p data-bbox="1419 874 1636 915">LABELING</p> <p data-bbox="1419 1174 1872 1617">Device security information, diagrams, software update instructions, infrastructure requirements</p>	<p data-bbox="2019 874 2385 1028">TPLC (TOTAL PRODUCT LIFECYCLE)</p> <p data-bbox="2019 1174 2505 1301">Product lifecycle from concept to end-of-life</p>	<p data-bbox="2618 874 3002 1028">QUALITY MANAGEMENT SYSTEM</p> <p data-bbox="2618 1174 3105 1778">QMS is a formalized system that documents processes, procedures, and responsibilities toward achieving the company quality objectives.</p>



Medical Device Security Lifecycle

Introduction







Regulations

If you start with good security,
regulatory compliance is easy.



Process for FDA Approval

CYBERSECURITY VIEW

1 Classify the Device

2 Pick Pre-market Submission Type

3 Prepare information

4 Submit to FDA

5 Complete registration



Cybersecurity Documentation

Key examples

**"Things you are submitting today, better
be able to operationalize"**
Chris Reed
VP of Product Security at Medtronic

01	Threat Model
02	Cyber Risk Assessment
03	Software Bill of Materials
04	Security Architecture
05	Security Testing
06	Transparency Artifacts

Identify potential security risks that could impact safety and effectiveness. FDA recommends that threat modeling documentation include sufficient information to assess and review the security features built into the device

FDA recommends that the cybersecurity risk assessment provided in premarket submissions should capture the risks and controls identified from the threat model

SBOM are needed for software components for which a manufacturer cannot claim complete control of the software lifecycle. Manufacturers should provide machine-readable SBOMs consistent with the minimum elements

The objective in providing security architecture information in premarket submissions is to provide to the FDA the security context and trust-boundaries of the medical device system in terms of the interfaces, interconnections, and interactions that the medical device system has with external entities.

Vulnerability Testing, Software Composition Analysis Penetration Testing etc.

Labeling including relevant security information for users, Disclosure process, Patch Management procedures. Manufacturer Disclosure Statement for Medical Device Security (MDS2) may address requirements

How to Start on the Security Journey?

ESTABLISH GOVERNANCE

Develop objectives, identify product security leader and cross functional team, policy creation

BUILD SECURITY SKILLS

Develop Cybersecurity skills in product leaders and developers.

REGULATORY GUIDANCE

Align to market specific guidance and appropriate frameworks e.g. FDA, ISO 81001-5 etc.

DOCUMENT

Design reviews, code reviews, risk analysis, vulnerability management, SBOM creation, Disclosures

MONITOR & OPTIMIZE

Define continuous maturity process. Identify maturity areas e.g. security automation

DON'T FORGET

Crawl...Walk...Run

Built-in NOT Bolt-on security

Plenty of available resources



CHALLENGES FACED BY MDM STARTUPS

Lack of early cybersecurity focus creates long terms costs



REGULATORY COMPLIANCE

Multiple standards across geography, post market readiness, external audits

Regulatory resources for FDA and EU MDR



SECURITY RESOURCES

Lack of security resources and mindset is a barrier to building security by design

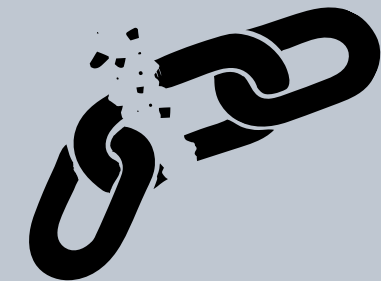
Start early, Available training, External advisors



COUNTERFEITS

Can cause patient safety issues and reputation / financial damage.

Anti-counterfeiting methods e.g. Tamper-evident packaging



SUPPLY CHAIN RISKS

Choosing the right suppliers who are building secure and resilient supplies is critical

Build redundancies in the supply chain, collaborate

Resources

US Food and Drug Administration
Premarket and Post Market Guidance



Central Drugs Standard Control Organization
www.cdsc.gov.in/



Joint Security Plan
www.healthsectorcouncil.org/the-joint-security-plan/



NTIA SBOM Resources
<https://www.ntia.gov/page/software-bill-materials>



CompTIA
www.comptia.org/certifications/security



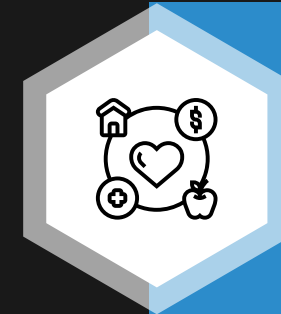
Various sites
Hacker News
Dark Reading

5 TAKEAWAYS

Start early and Stay Consistent



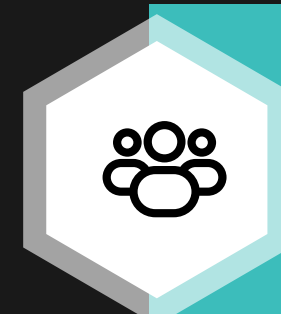
Cybersecurity protects your business model



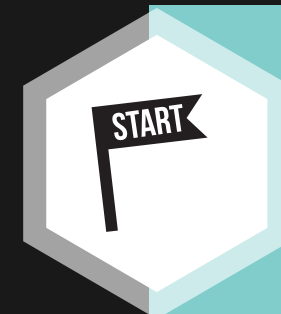
Need security mindset at all levels



Cybersecurity skills are critical
(Threat Modeling, Secure Coding, Risk assessment)



Creat a plan for the whole lifecycle



Document, Document, Document



Questions?



info@cyvidia.com



Our solutions

Building trust and efficiencies in the cyber supply chain



Contract & Regulatory Compliance

Test Once, Comply with many. Cyvidia's Predictive AI unifies Regulatory, Customer and Policy Cybersecurity Requirements to streamline multi-audit readiness and build a holistic security and compliance view.



Cyber supply chain program build

Dashboards, policies, training, 3rd party assessment tools, scoring and incidence response plans



Secure Product Development

Product and Application security program assessment, risk score cards, SBOM implementation, training curriculum development



Customer Due Diligence Support

Using AI and machine learning to answer due diligence questions from customers to speed up sales processes, provide more accurate information, and improve customer confidence.



www.cyvidia.com