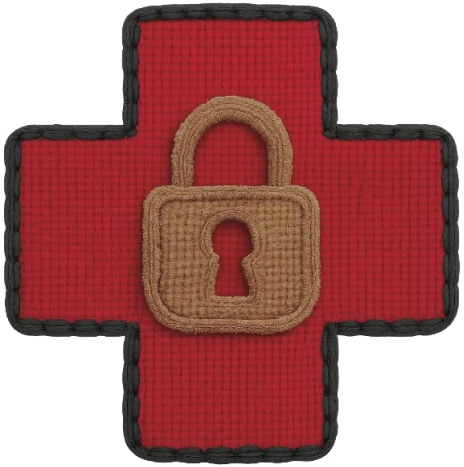
Northeastern University



Medical Device Cybersecurity – Week 12

03/24/2026

Premarket Management – Select Deep Dives

Axel Wirth | Chief Security Strategist | Medcrypt
axel@medcrypt.com

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- Recap – Secure Lifecycle Concept
- Premarket Activities
- Threat Modeling Deep Dive
- Risk Assessment Deep Dive
- Tying it Together

The Secure Development Lifecycle (SDLC) Context

- General Premarket activities
- Postmarket begins after regulatory approval:
  - Release for sale
  - Manufacturing transfer
- Applies to all new products, versions, and updates & patches

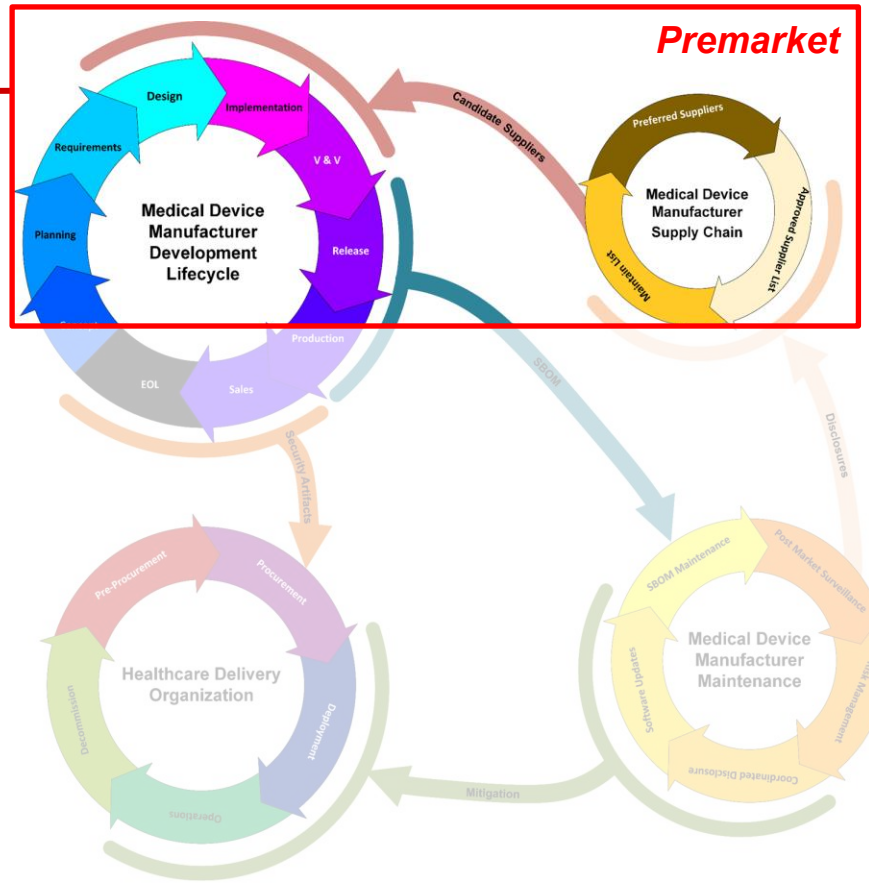
HDO Perspective:
- Procurement
- Onboarding
- Maintenance
- Decommissioning

- Supply Chain Management
- Vulnerability Monitoring
- Contract and relationship management

- Patches and Updates
- Documentation
- Risk Communication
  - Vulnerabilities
  - Threats
  - EOL / EOS

The Secure Development Lifecycle (SDLC) Context

- General Premarket activities
- Postmarket begins after regulatory approval:
  - Release for sale
  - Manufacturing transfer
- Applies to all new products, versions, and updates & patches



- Supply Chain Management
- Vulnerability Monitoring
- Contract and relationship management

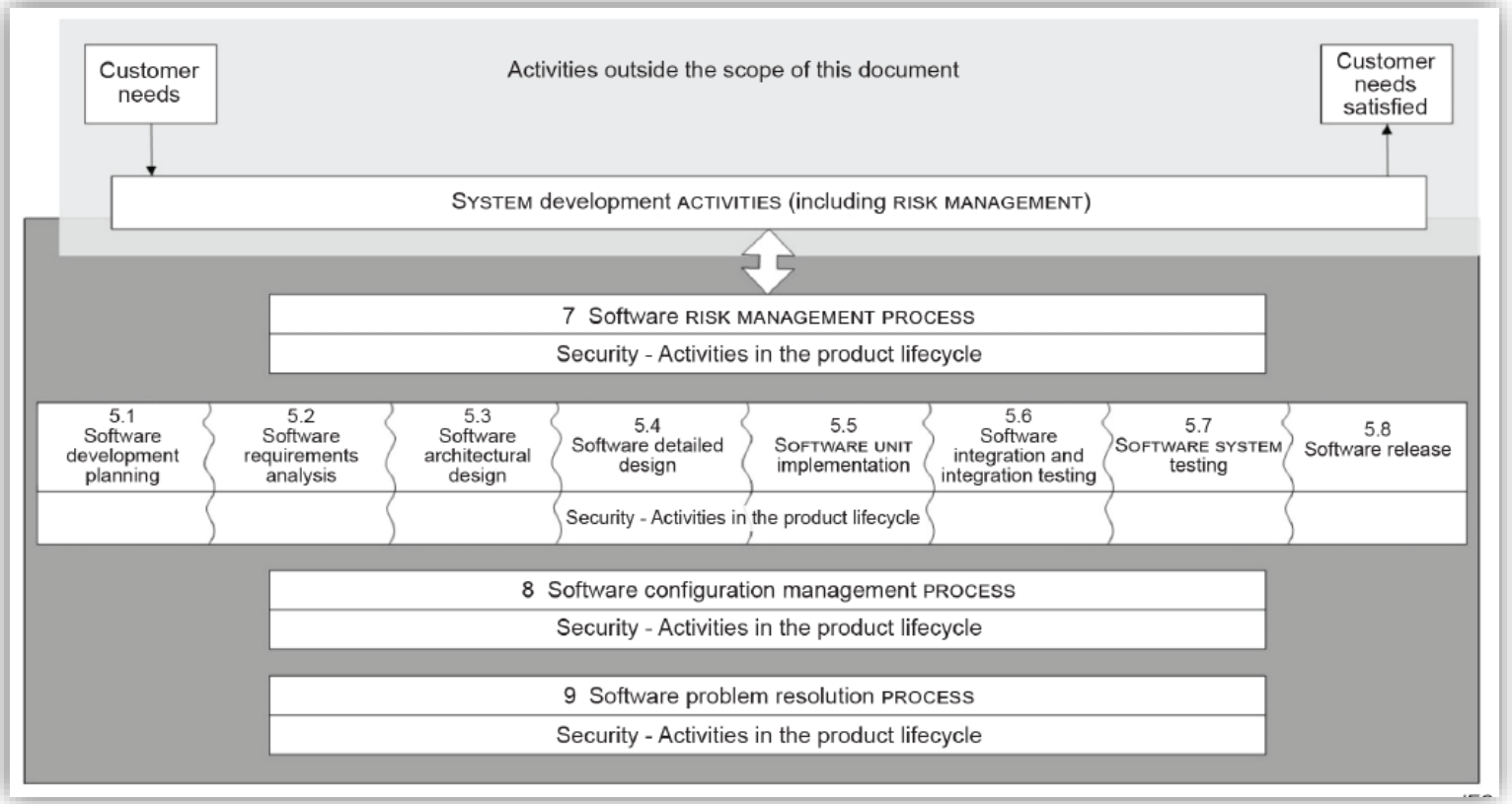
HDO Perspective:
- Procurement
- Onboarding
- Maintenance
- Decommissioning

- Patches and Updates
- Documentation
- Risk Communication
  - Vulnerabilities
  - Threats
  - EOL / EOS

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- Recap – Secure Lifecycle Concept
- Premarket Activities
- Threat Modeling Deep Dive
- Risk Assessment Deep Dive
- Tying it Together

SDLC per IEC 81001-5-1



SDLC per IEC 81001-5-1

5.1 Software development planning
5.1.1 Activities in the life cycle process
5.1.2 Development environment security
5.1.3 Secure coding standards

5.2 Health software requirements analysis
5.2.1 Health software security requirements
5.2.2 Security requirements review
5.2.3 Security risks for required software

5.3 Software architectural design
5.3.1 Defense-in-depth architecture/design
5.3.2 Secure design best practices
5.3.3 Security architectural design review

5.4 Software design
5.4.1 Software design best practices
5.4.2 Secure design
5.4.3 Secure health software interfaces
5.4.4 Detailed design verification for security

5.5 Software unit implementation and verification
5.5.1 Secure coding standards
5.5.2 Security implementation review

5.6 Software integration testing
5.7 Software system testing
5.7.1 Security requirements testing
5.7.2 Threat mitigation testing
5.7.3 Vulnerability testing
5.7.4 Penetration testing
5.7.5 Managing conflicts of interest between testers and developers

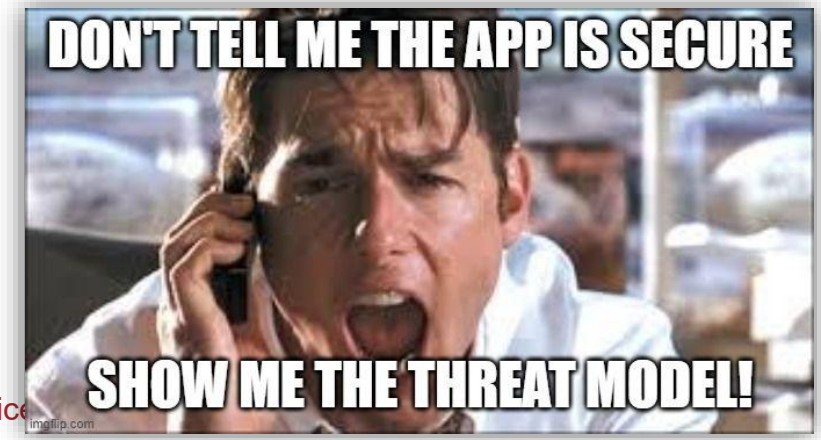
5.8 Software release
5.8.1 Resolve findings prior to release
5.8.2 Release documentation
5.8.3 File integrity
5.8.4 Controls for private keys
5.8.5 Assessing and addressing security-related issues
5.8.6 Activity completion
5.8.7 Secure decommissioning guidelines for health software

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- Recap – Secure Lifecycle Concept
- Premarket Activities
- Threat Modeling Deep Dive
- Risk Assessment Deep Dive
- Tying it Together

Threat Modeling as Early-Stage Risk Activity

- How do you identify weaknesses in your architecture and design before you have any code that can be reviewed or tested?
- How do you communicate your design's security properties and resulting risks that may exist at this early stage?
- The answer: Threat Modeling
  (40% art, 40% craft, 20% science)



Threat Modeling Basics

- Threat Modeling allows to examine cyber risk in a methodological and abstracted way. This is particular useful in two scenarios:
  - Early in the SLDC and before actual HW/SW implementation or component selection
  - Later during development or even postmarket when a defined security risk requires system level context, analysis, and understanding.
- The four questions of Threat Modeling:
  - “What are we working on?”
  - “What can go wrong?”
  - “What are we going to do about it?”
  - “Did we do a good job?”
- Threat Modeling is an early-stage risk assessment methodology and helps provide clarity in cross-team communication.

Threat Modeling Basics

1. What are we working on?

Graphical expression of system components, relationships, and behaviors:

- Initial Brainstorming
- Data Flow Diagrams (DFD)
- Trust Boundaries
- Swim Lanes
- State Diagrams

TM lays the initial foundation for Architecture Diagrams – hence, consistency matters.

2. What can go wrong?

Threats don't exist yet, but can be abstracted

Example: STRIDE:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Alternative / complementary:

- Attack Trees (model exploitation paths)
- Kill chains (cyber attack lifecycle)
- Frameworks, ex ATT&CK

3. What are we going to do about it?

1. Eliminate
   - The ideal case
   - TM as tool of choice
   - Ex. avoid data retention
   - May impact features
2. Mitigate
   - Reduce through controls
   - NIST CSF: Protect, detect, respond, recover
3. Accept
   - Reduce to an acceptable level
4. Transfer
   - Labeling (ex. warnings)
   - User acceptance
   - Liability (ex. insurance)

4. Did we do a good job?

Are we confident that all risks are identified and sufficiently addressed?

Did we complete the task (if not, go back and update)?

Did the process work well?

Evaluation criteria:

- Completeness
- Clarity
- Specificity
- Traceability
- Consistency
- Roles and responsibilities
- Assumptions
- Rationales

Requires scoring mechanism such as DREAD, CVSS, or NIST SP 800-30

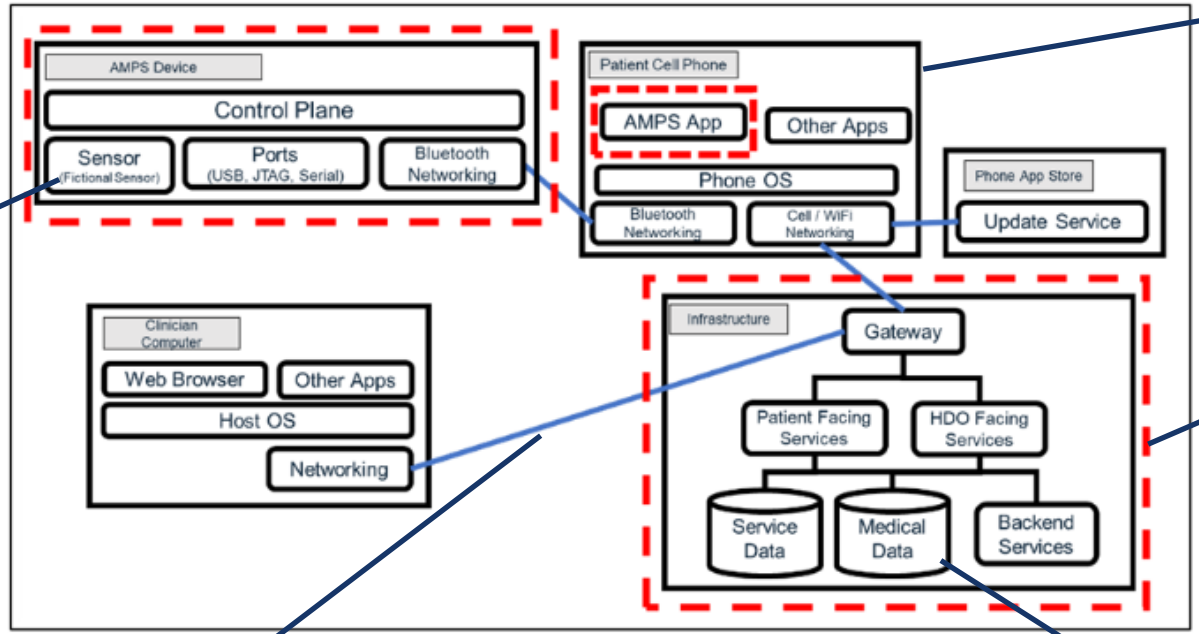
Threat Modeling Methodology - Example

STRIDE Element	*Description*	*Example*
Spoofing	Tricking a system into believing a falsified entity is a true entity	Using stolen or borrowed credentials to log on as another nurse
Tampering	Intentional modification of a system in an unauthorized way	Changing patient data to incorrect values
Repudiation	Disputing the authenticity of an action taken	Denying that a prescribed treatment has been provided to the patient
Information Disclosure	Exposing information intended to have restricted access levels	Health data is sent over an unencrypted Bluetooth connection
Denial of Service (DoS)	Blocking legitimate access or functionality of a system by malicious process(es)	A Bluetooth SpO2 sensor is flooded with bad pairing requests, preventing legitimate connections
Elevation of Privilege (EoP)	Gaining access to functions to which an attacker should not normally have access according to the intended security policy of the product	A patient uses a web portal vulnerability to see all patient data, rather than their own

Note: STRIDE is a common but not the only methodology

Source: MITRE

Threat Modeling Diagram Example



External Entities

Process

Trust Boundaries

Data Flows

Data Store

Source: MITRE

Threat Modeling Do's and Don'ts

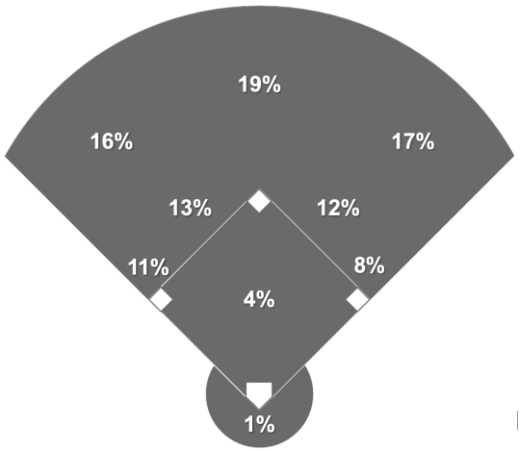
- It can get complex – be organized
- But don't let rigid rules get in the way of creativity
- It's a team effort
- Practice!
- Consider all use cases and scenarios (clinical use, remote access, upgrade …)
- Commercial and open-source tools are readily available
- Training courses are readily available

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- Recap – Secure Lifecycle Concept
- Premarket Activities
- Threat Modeling Deep Dive
- Risk Assessment Deep Dive
- Tying it Together

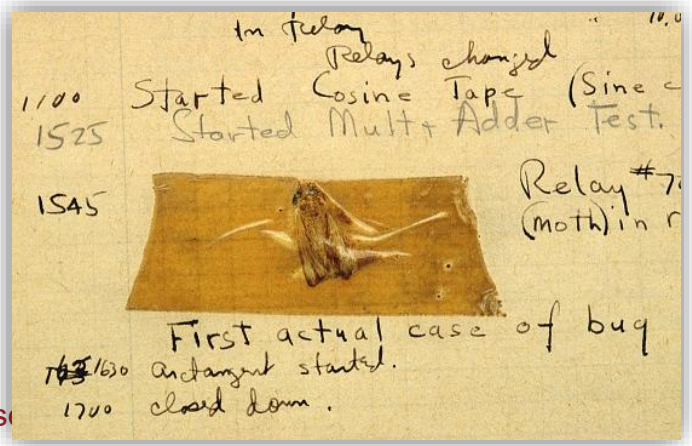
A Word about Risk Assessment

- “Risk” is not a property of a system, the same as “chance of rain” is not a property of a cloud.
- “Risk” and is a forward-looking estimate based on intrinsic and extrinsic factors, more or less determinable, more or less changeable over time.
- Risk management = prioritize highest risks for mitigation to minimize the chance of future exploitation within the given constraints (technical, financial, resources, …) and within a given environment (threats exposure, use case, …).



Risk Assessment in SW Development

- Remember – risks result from vulnerabilities which are a subset of “bugs” (aka anomalies)
- That is why FDA expects a “security assessment of unresolved anomalies”
- Simply put, vulnerabilities manifest themselves in two different ways
  - Via your Supply Chain (open-source, commercial, embedded, contracted)
  - Via your own Code (implementation or configuration)
- Detect via:
  - Reviews (e.g., code review)
  - Analysis (manual or automated, e.g., SAST, DAST)
  - SBOM analysis (
  - Testing (at module level, various integration steps, and final product, e.g., fuzz testing, pen testing)

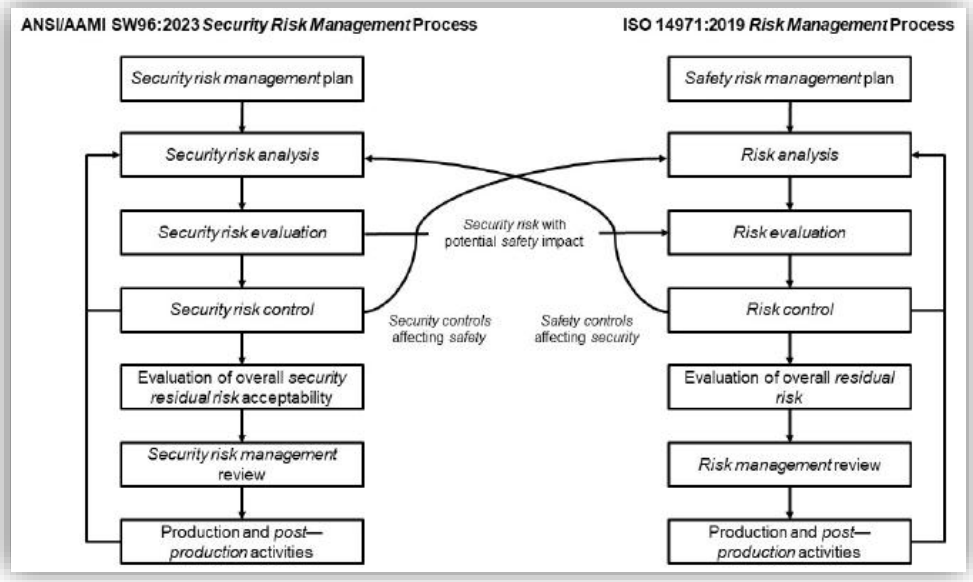


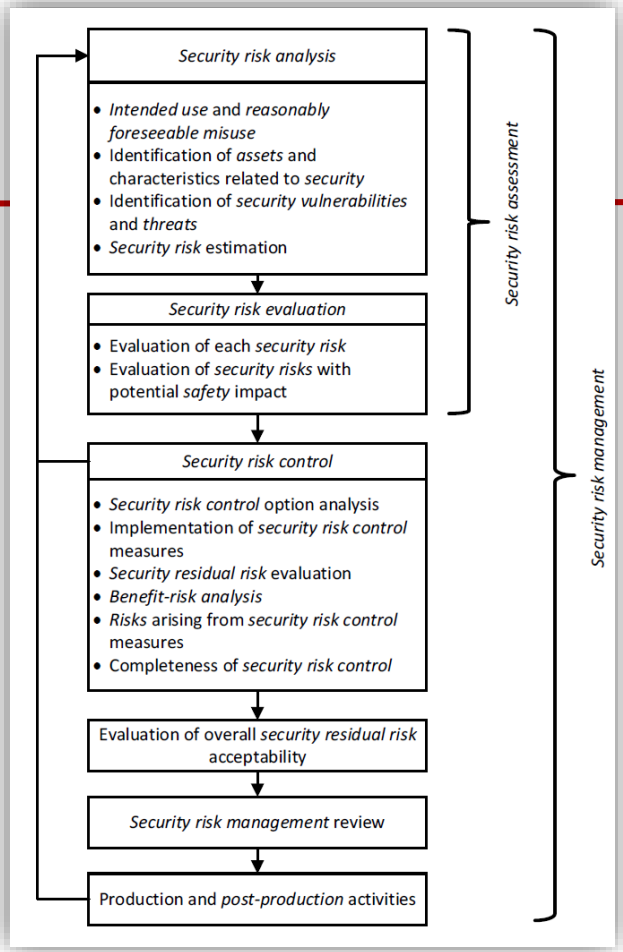
Identifying and Scoring Risk – Never Easy

- Assembly of all identified and known risks in a Risk Register:
  - Residual Risks from Threat Model
  - Risks identified during Code Reviews and Analysis
  - Risks based on SBOM Analysis
  - Risks based on vulnerabilities uncovered in Testing (at the various stages)
- All Risks need to be tracked, but security-based Safety Risks need to be linked to your separate Safety Risk Management (of all Safety Risks).

Impact (of harm) \ Likelihood (of harm)	Improbable 1	Remote 2	Occasional 3	Probable 4
Catastrophic 4	4	8	12	16
Critical 3	3	6	9	12
Marginal 2	2	4	6	8
Negligible 1	1	2	3	4

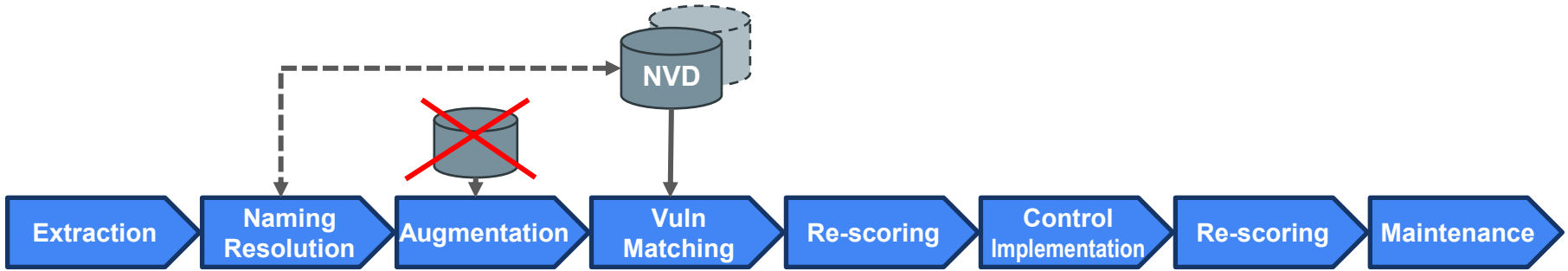
For Example





Source: AAMI SW 96

SBOM-Based Risk Analysis



Sources:
- Supplier
- SCA-Tool
- Binary Analysis

Mismatched or un-resolved CPEs

- Component EOL/EOS
- License info
- Export controls

Match CPEs against known CVEs

Reassess based on context (implementation and use case)

Mitigate based on assessed risk (exploitability, impact)

Reassess after control implementation

Postmarket

SBOM standards:
- CycloneDx
- SPDX

Naming standards:
- CPE (NVD)
- PURL

Vuln Scoring:
- CVSS (NVD)
- CISA KEV
- EPSS
- ….

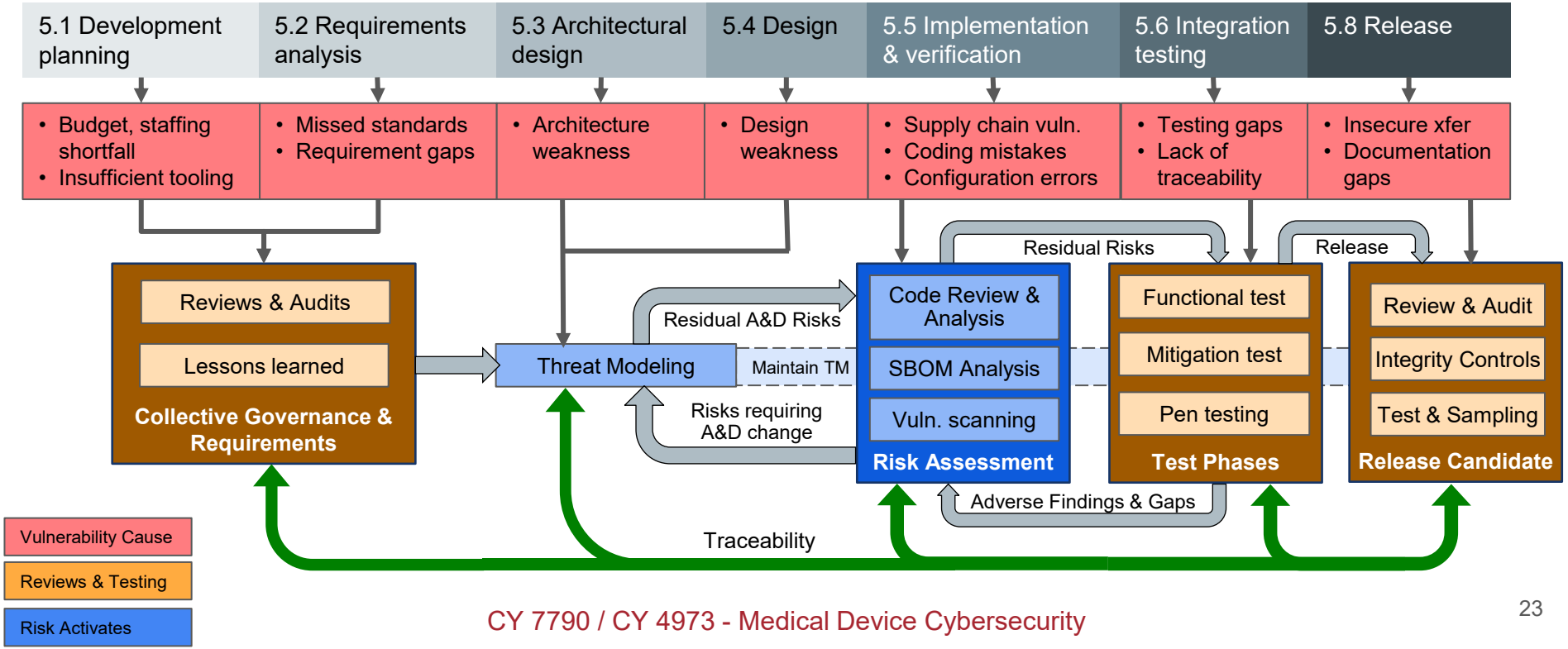
Important Things about CVSS and NVD

- It is an abstract score of the severity of a vulnerability.
- It lacks implementation and use case context.
- It should not be used as a sole assessment of risk (says the CVSS specification)
- It is mainly exploitability scoring but with some impact consideration
- Multiple sources: NVD, EUVD. SW vendor, commercial, CISA KEV
- Note that NVD includes SW component as well as device data
- Alternative methods are emerging, e.g., EPSS
- NVD data is messy (e.g., inconsistent name spelling in CPE)
- NVD uses CVSS for scoring but obviously CVSS can be used in any context (e.g., your own code)

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

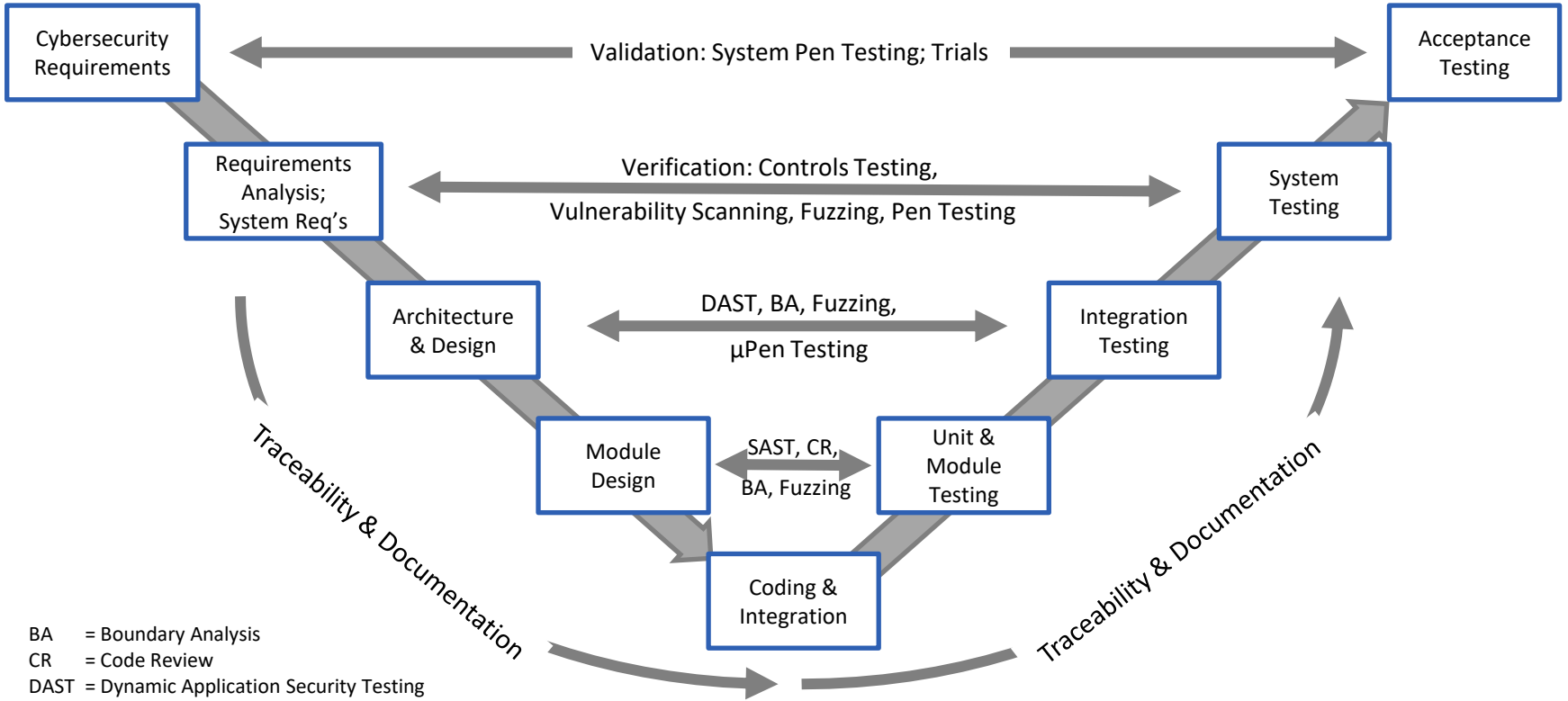
- Recap – Secure Lifecycle Concept
- Premarket Activities
- Threat Modeling Deep Dive
- Risk Assessment Deep Dive
- Tying it Together

SDLC – Vulnerability Methodologies



MDM Premarket Activities

Alignment of Development and Testing



BA = Boundary Analysis
CR = Code Review
DAST = Dynamic Application Security Testing
SAST = Static Application Security Testing
µPen = Pen Testing at the subsystem level

Risk Detection and Scoring Methodologies

Where vulnerabilities get introduced:

- Missed requirements
- Faults in architecture or design
- Inherited from 3rd party code (supply chain)
- Mistakes in code, configuration, or integration

Where risks get identified and scored:

- Reviews (at earliest stages, but continues throughout (e.g., code review)
- Threat Modeling (review architecture and design, maintain throughout the lifecycle)
- Risk Assessment (assess all vulnerabilities and resulting risks)

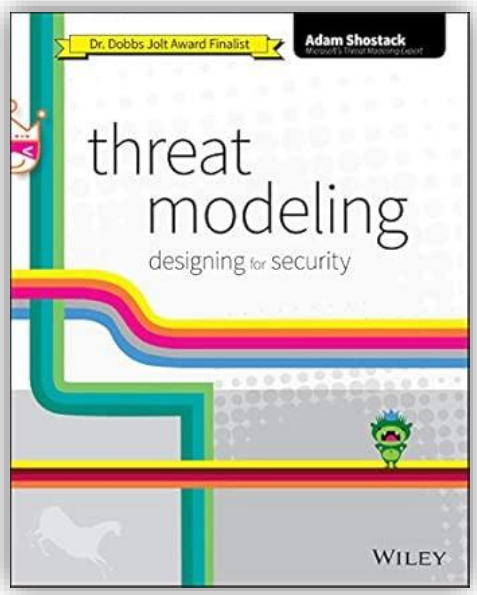
Two-fold Purpose of Testing

- Confirm identified risks have been mitigated and that controls work as intended
- Find unidentified risks that may have slipped through (esp. pen testing)

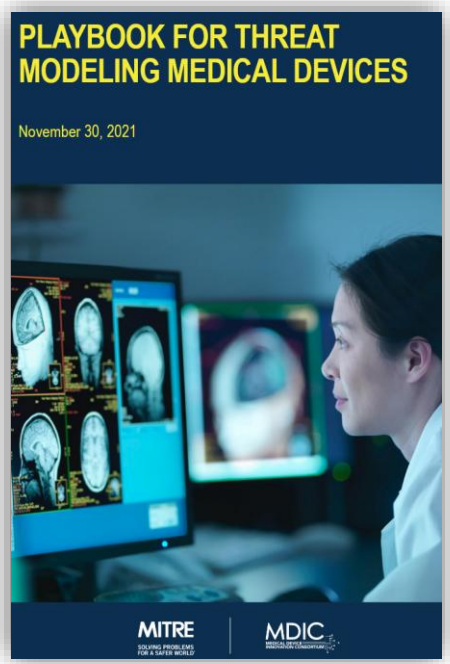
Thank you!

axel@medcrypt.com

Threat Modeling

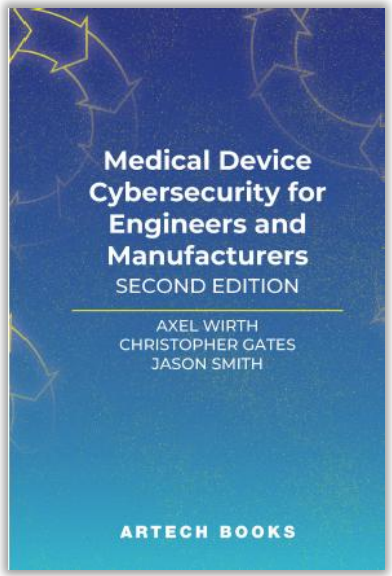


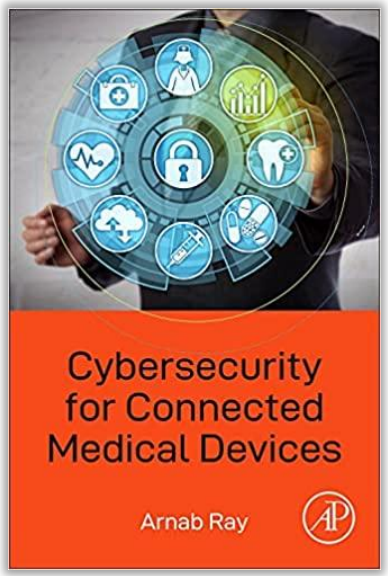
https://shostack.org/books/threat-modeling-book



https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf

General Resources - For Medical Device Manufacturers

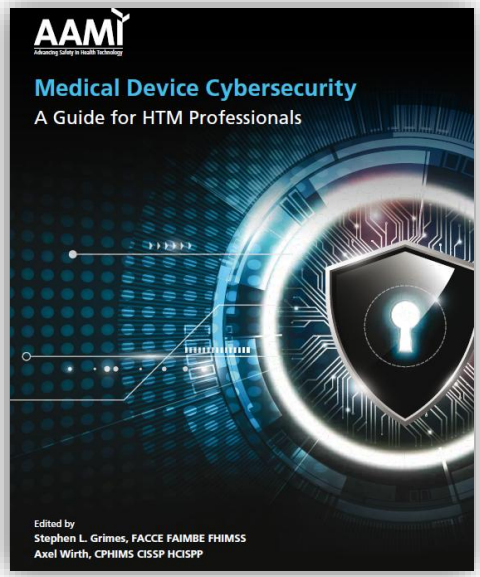




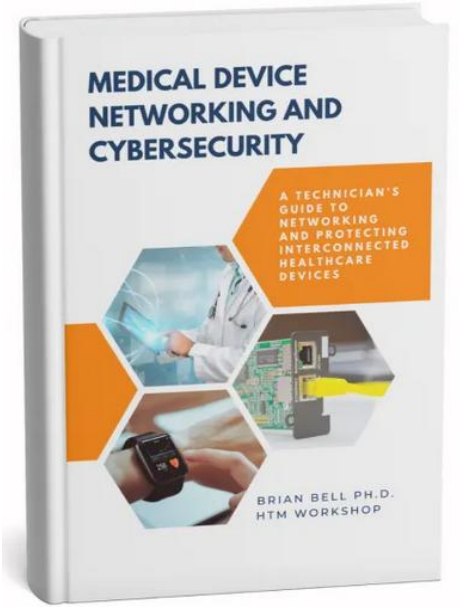
US: https://us.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2416.aspx
UK: https://uk.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2354.aspx

https://www.amazon.com/Cybersecurity-Connected-Medical-Devices-Arnab/dp/0128182628/ref=sr_1_4

General Resources - For Healthcare Delivery Organization

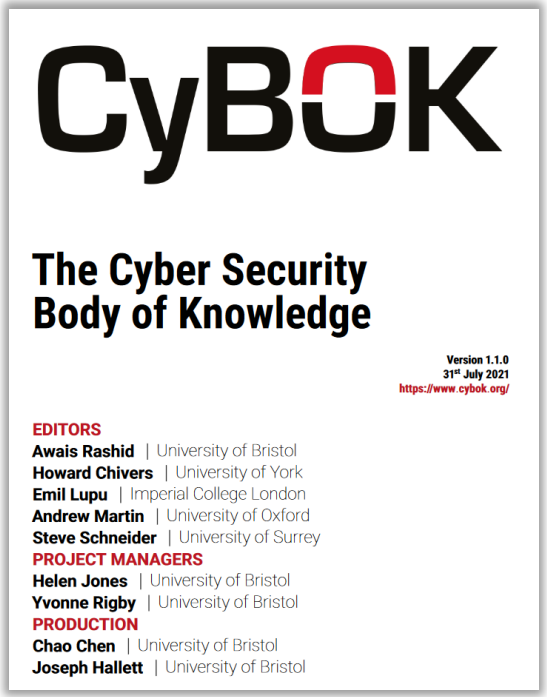


https://store.aami.org/s/store#/store/browse/detail/a152E000006j66qQAA



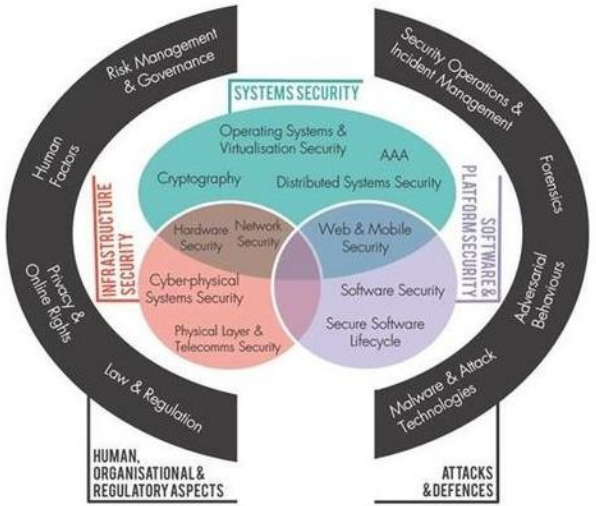
https://htm-workshop.com/shop/medical-device-networking-and-cybersecurity/

General Resources - CyBOK



The Cyber Security Body of Knowledge v1.1,
https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

CyBOK Knowledge Base
https://www.cybok.org/knowledgebase1_1/



Staying Informed on the Day-to-Day

- Security briefs and threat alerts via Health Sector Cybersecurity Coordination Center (HC3) https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- US Department of Homeland Security's Industrial Control Systems—Cyber Emergency Response Team (ICS-CERT) medical device alerts (ICSMA) https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A96
- Healthcare and Public Sector Highlights - Cybersecurity (via HHS) https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare
- CISA HPH Sector https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector