Proactive Healthcare Cybersecurity

AI&U - Re-imaging Medical Device Product Security

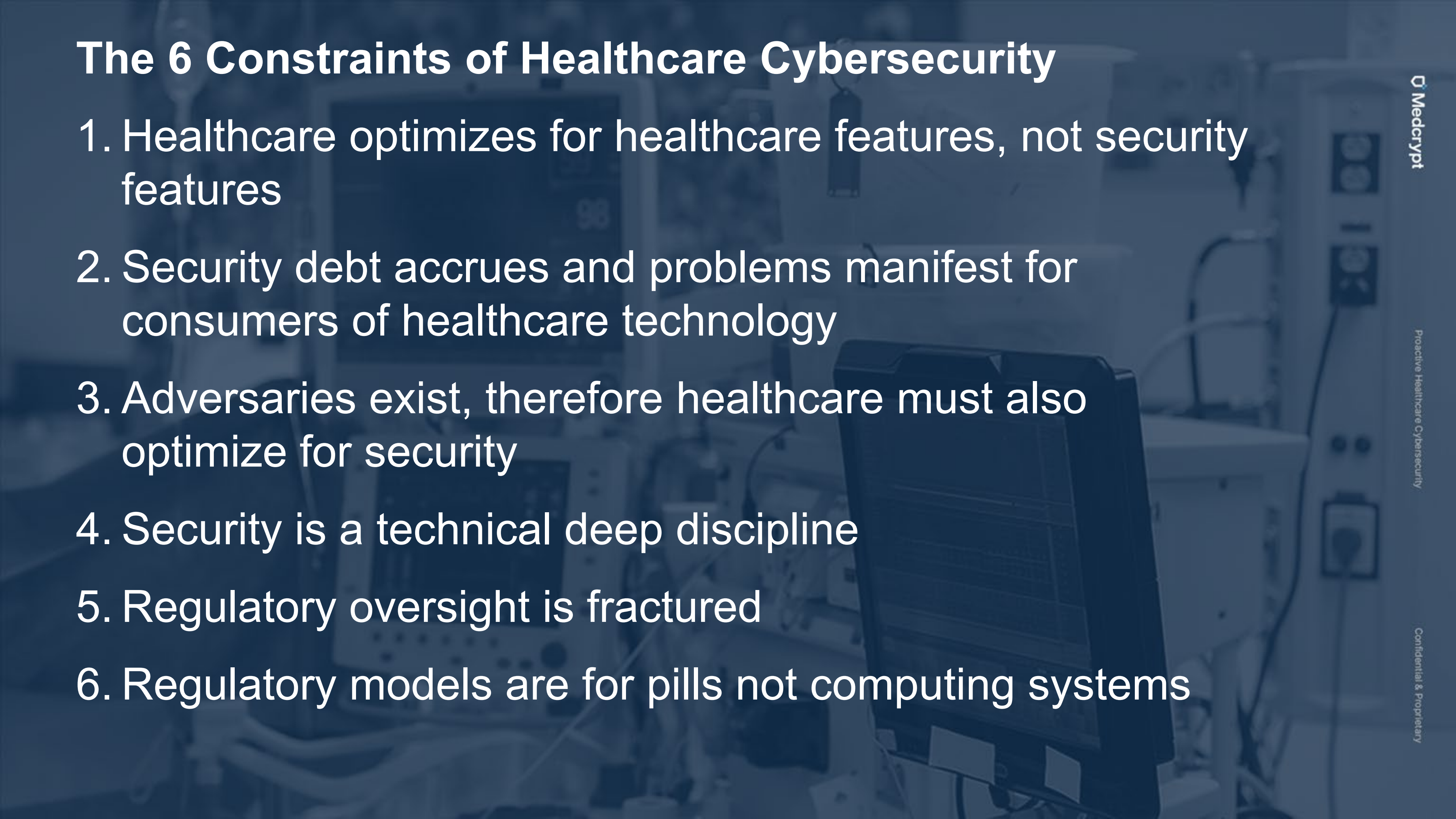
Seth Carmody, VP of Regulatory Strategy

AI Summit - AFDO/RAPS
November 15, 2023

SETH CARMODY

Summary:

- Seth Carmody is the Vice President of Regulatory Strategy at MedCrypt. Drawing on his 12 years of medical device experience, Seth provides strategic direction for cybersecurity products and services for the regulated medical device market.
- Prior to MedCrypt, Seth spent 8 years at FDA, architecting technology policy and laws that impact software-enabled medical devices; namely, the FDA's medical device cybersecurity policies and what would become the Consolidated Appropriations Act of 2022. Seth's industry leadership and strategic direction extends to several high-profile industry frameworks including the Joint Security Plan (HSCC), MITRE's Rubric for Applying CVSS to Medical Devices, and MDIC's Playbook for Threat Modeling Medical Devices. Seth has authored several papers including Building Resilient Medical Technology Supply Chains with a Software Bill of Materials and Why Healthcare Cybersecurity is Hard: Understanding the Constraints of Healthcare Cybersecurity. Seth has also won industry awards including the (ISC)2 Information Security Leadership Award, the Archimedes Center for Medical Device Security's Leadership in Cybersecurity award, and the FDA Commissioner's Special Citation.
- In addition to manifesting more resilient healthcare infrastructure, Seth is currently interested in quantifying ROI for cybersecurity investments and advocating for a new regulatory model for medical devices. He aims to deliver the promise of emerging technology to transform healthcare while balancing public safety.
- Seth received his PhD from Indiana University where he studied the chemical synthesis of peptidoglycan probes in the pursuit of novel antibacterial drugs.



The 6 Constraints of Healthcare Cybersecurity

1. Healthcare optimizes for healthcare features, not security features

2. Security debt accrues and problems manifest for consumers of healthcare technology

3. Adversaries exist, therefore healthcare must also optimize for security

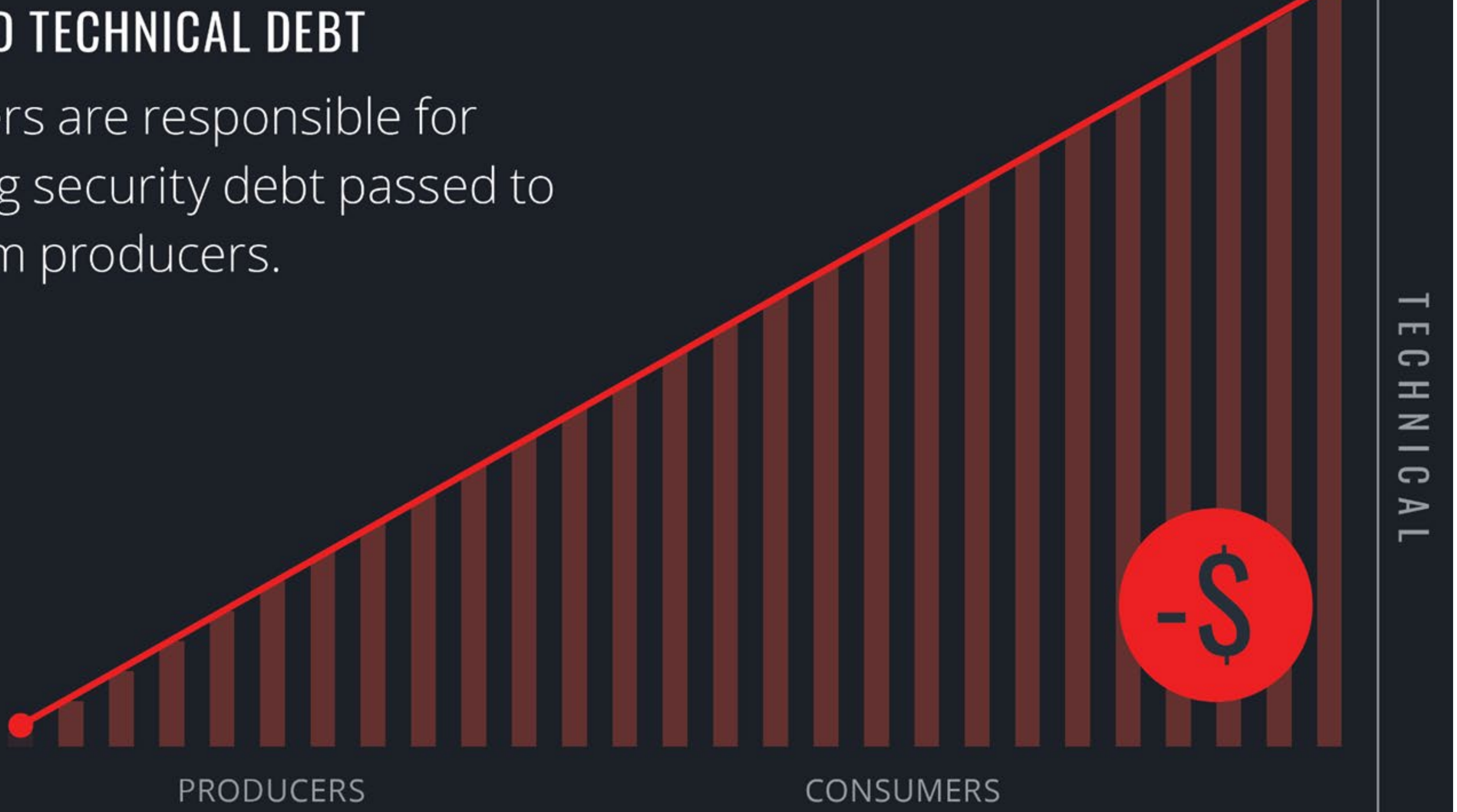
4. Security is a technical deep discipline

5. Regulatory oversight is fractured

6. Regulatory models are for pills not computing systems

INCREASED TECHNICAL DEBT

Consumers are responsible for managing security debt passed to them from producers.



No investment › Tech | MDM › HDO | Clinicians | Patients

REGULATORS: FDA & Congress

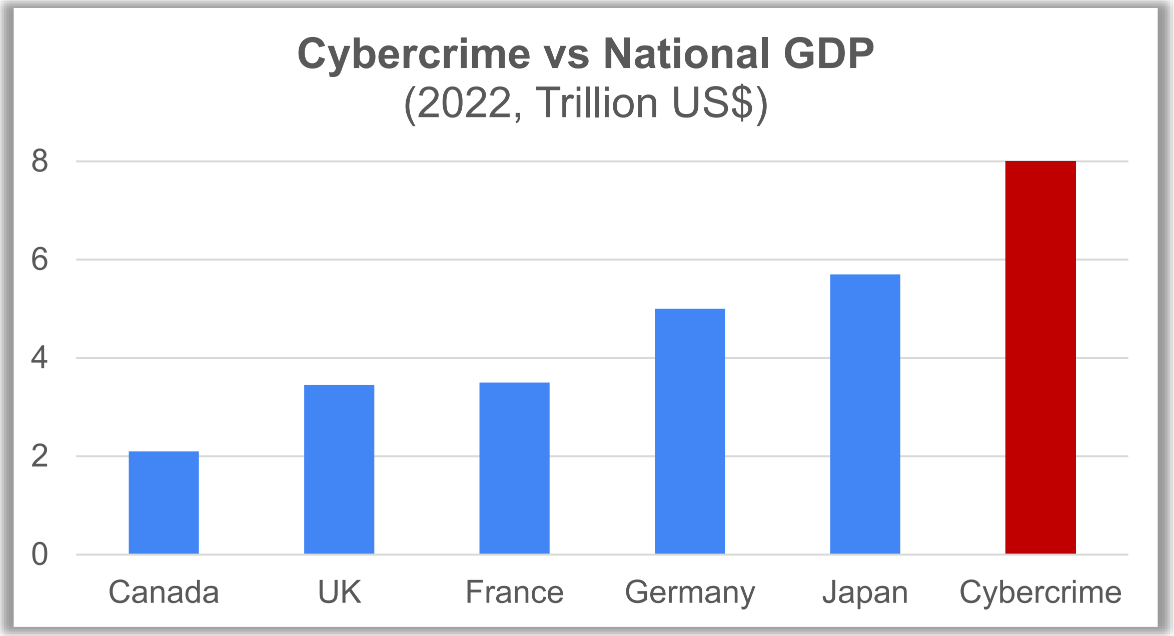
Cybercrime – Understanding the Scope

Global Cybercrime Impact:

- Estimated ~$8T
- 2025 est. ~$10.5T

Cybersecurity Spending:

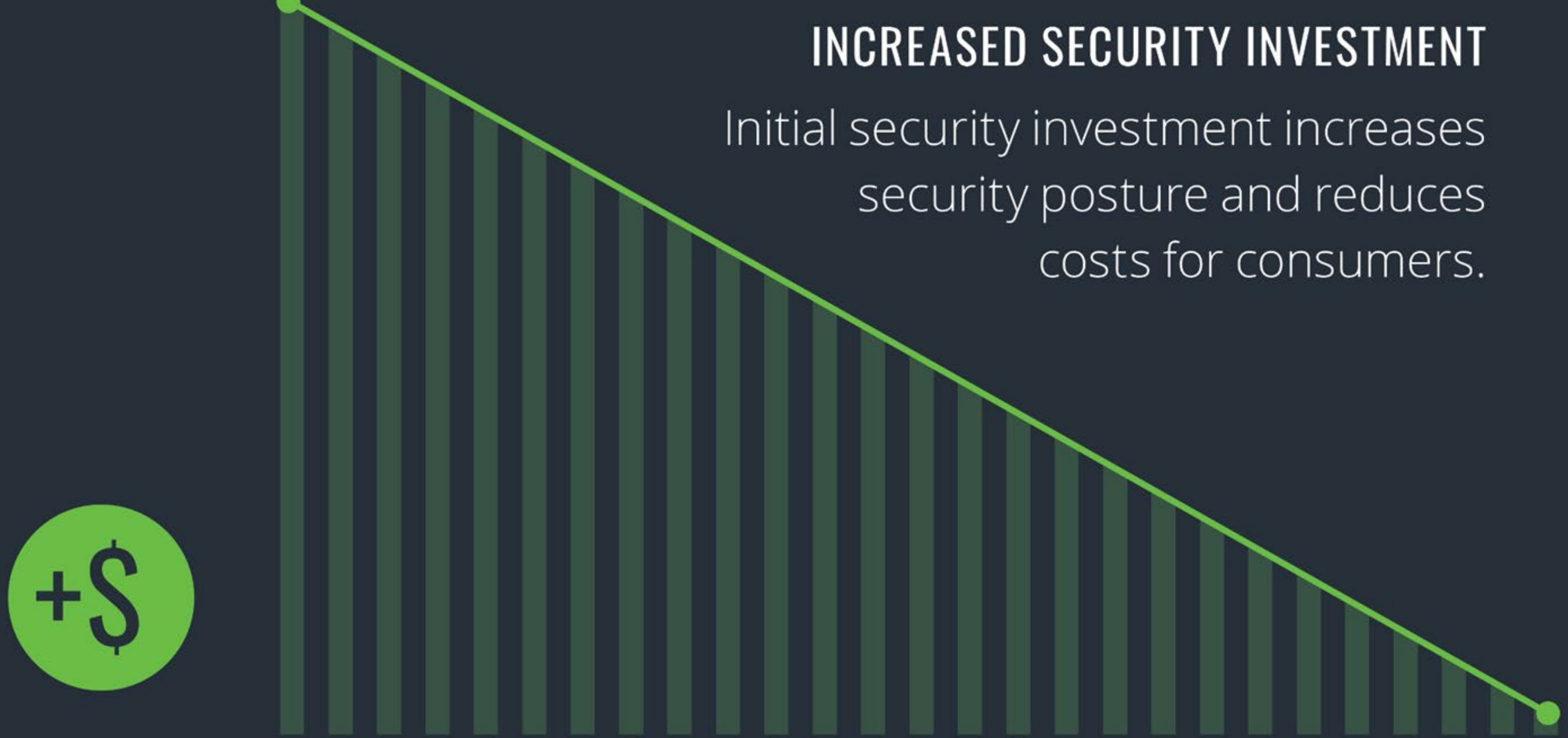
- ~$188B
- Growth ~11%/yr



https://www.sans.org/blog/the-new-financial-metric-for-cybersecurity/

INCREASED SECURITY INVESTMENT

Initial security investment increases security posture and reduces costs for consumers.



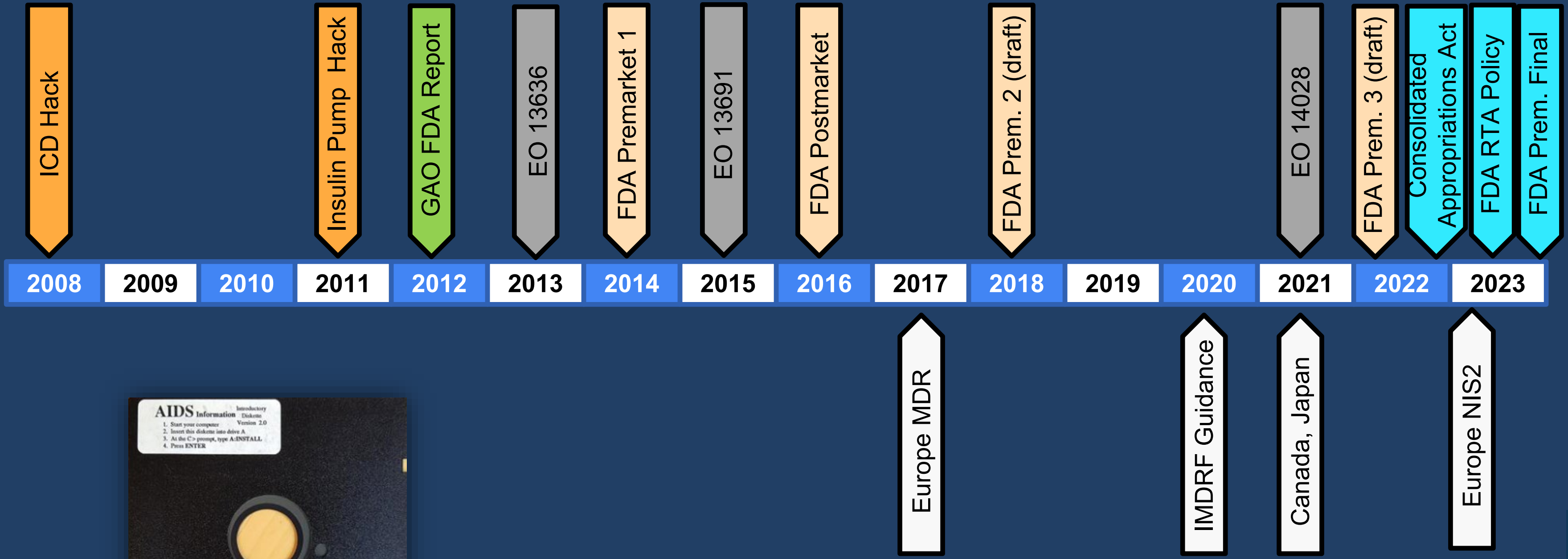
PRODUCERS | CONSUMERS

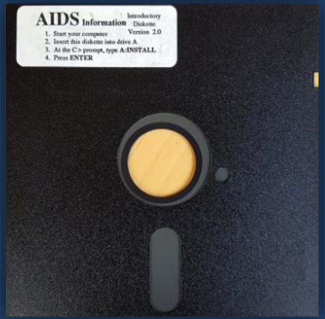
+Investment > Tech | MDM > HDO | Clinicians | Patients

REGULATORS: FDA & Congress

TECHNICAL

Regulators’ and Lawmakers’ Response





AIDS MS-DOS Trojan
1989

Looking at the Big Picture

WH Security Strategy

A Path to Resilience in Cyberspace

- Meet needs of national security and public safety.
- Shift liability onto those entities that fail to take reasonable precautions.
- Enhanced cooperation between CISA and critical infrastructure.
- Coordinated cyber defense operations.

CISA Security Strategy

Secure-by-Design and Secure-by-Default

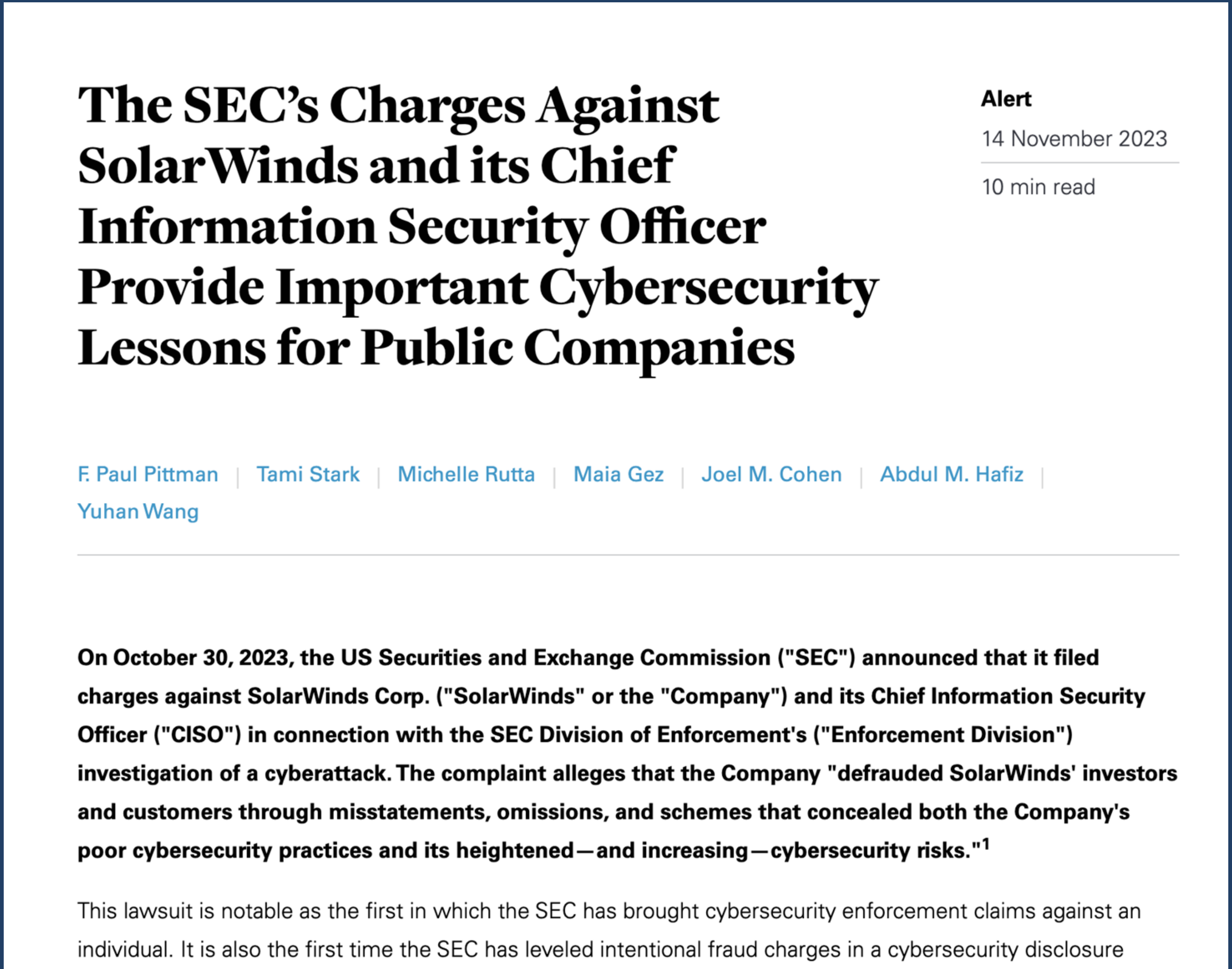
- Embrace transparency and accountability.
- Build organizational structure and leadership.
- Meetings with company executive leadership.
- Importance of security to business success.
- Use a tailored threat model during development.

SEC Rule

Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

- Report material cyber incidents within 4 days.
- Report when immaterial cyber incidents become material in the aggregate.
- Policies for management of cyber risks.
- Describe cyber risk governance.

Moving away from user-owned security – “shift left” and “shift up”



The SEC's Charges Against SolarWinds and its Chief Information Security Officer Provide Important Cybersecurity Lessons for Public Companies

Alert

14 November 2023

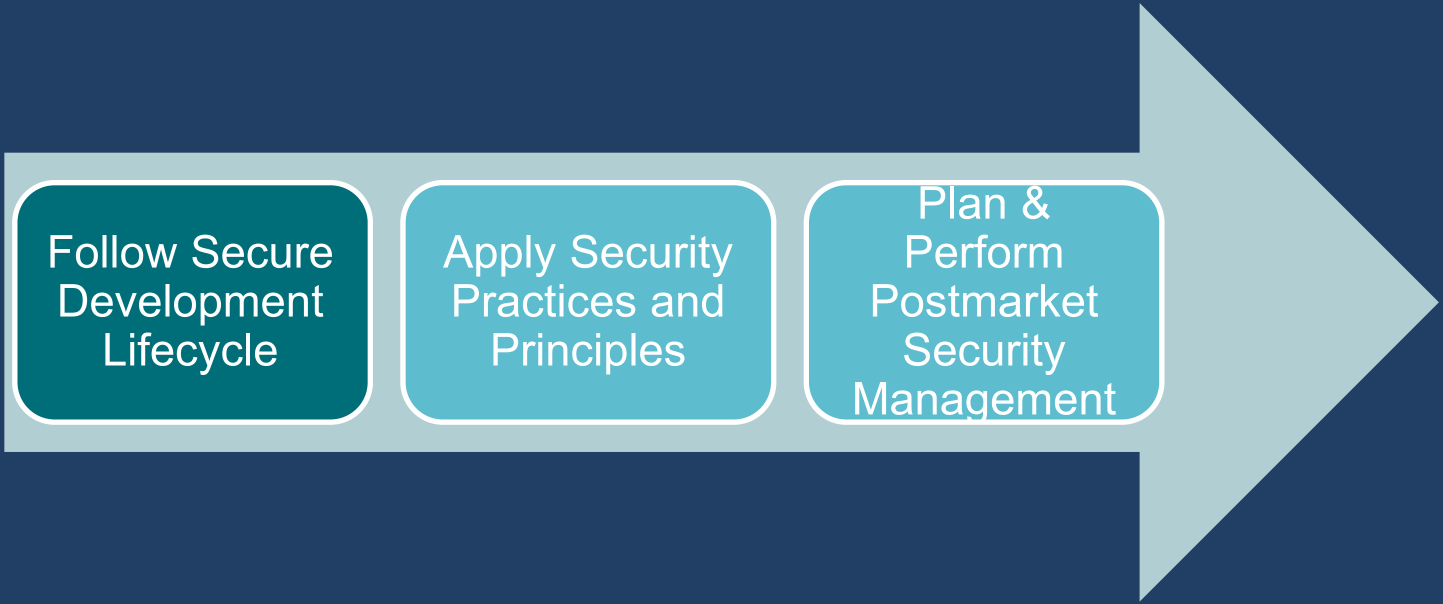
10 min read

F. Paul Pittman | Tami Stark | Michelle Rutta | Maia Gez | Joel M. Cohen | Abdul M. Hafiz | Yuhan Wang

On October 30, 2023, the US Securities and Exchange Commission ("SEC") announced that it filed charges against SolarWinds Corp. ("SolarWinds" or the "Company") and its Chief Information Security Officer ("CISO") in connection with the SEC Division of Enforcement's ("Enforcement Division") investigation of a cyberattack. The complaint alleges that the Company "defrauded SolarWinds' investors and customers through misstatements, omissions, and schemes that concealed both the Company's poor cybersecurity practices and its heightened—and increasing—cybersecurity risks."[1]

This lawsuit is notable as the first in which the SEC has brought cybersecurity enforcement claims against an individual. It is also the first time the SEC has leveled intentional fraud charges in a cybersecurity disclosure

Cybersecurity Program Objective:
“Provide Reasonable Assurance of Patient Safety”



Follow Secure Development Lifecycle

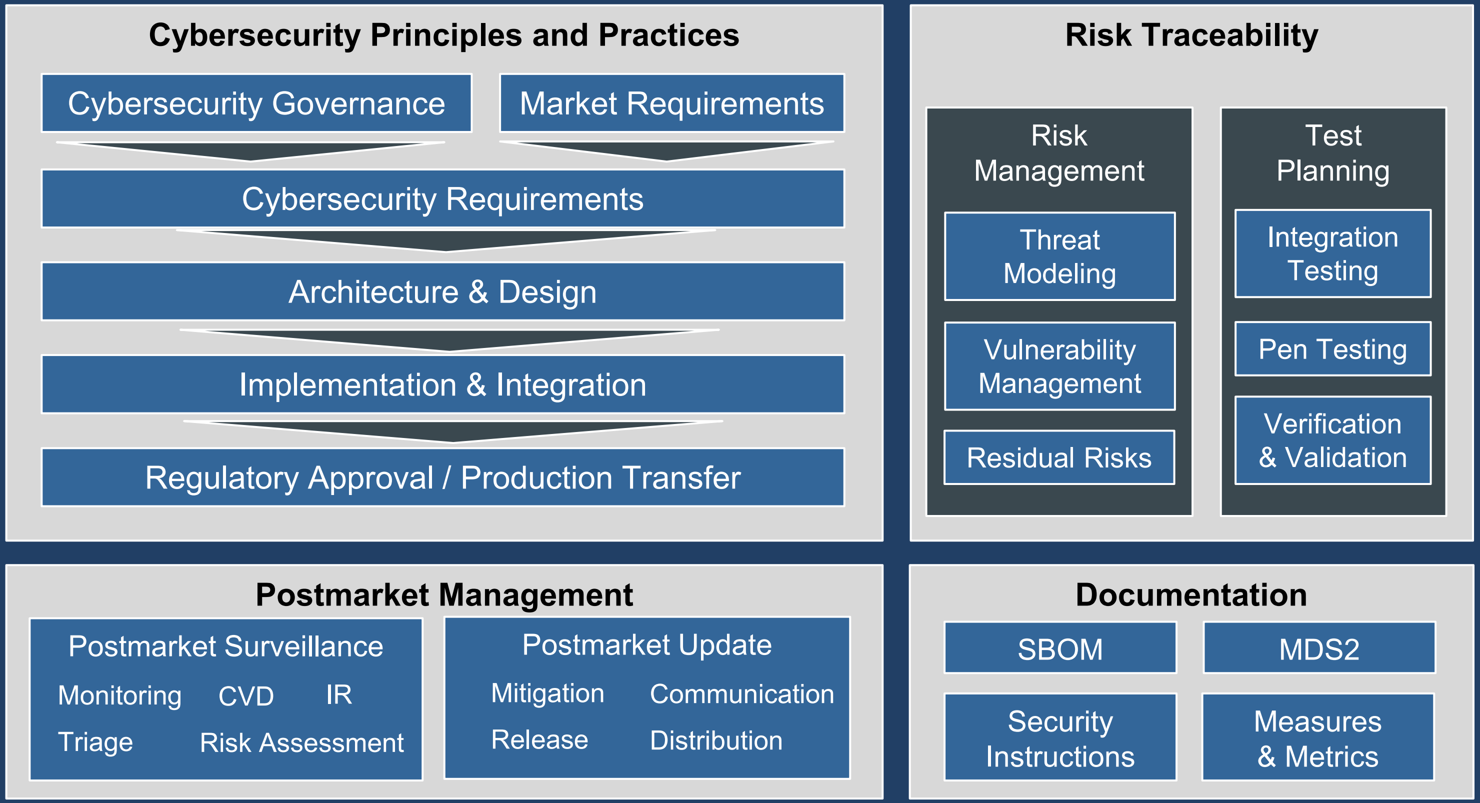
Apply Security Practices and Principles

Plan & Perform Postmarket Security Management

Objectives:

1. Secure Lifecycles: Reduce the number and severity of vulnerabilities
2. Risk Management: Assess for and fix vulnerabilities with higher risk
3. Defense in Depth: Reduce attack surface, maintain security posture

Integrating Cybersecurity into your QMS



Cybersecurity Principles and Practices

- Cybersecurity Governance
- Market Requirements
- Cybersecurity Requirements
- Architecture & Design
- Implementation & Integration
- Regulatory Approval / Production Transfer

Risk Traceability

- Risk Management
  - Threat Modeling
  - Vulnerability Management
  - Residual Risks
- Test Planning
  - Integration Testing
  - Pen Testing
  - Verification & Validation

Postmarket Management

- Postmarket Surveillance
  - Monitoring
  - CVD
  - IR
  - Triage
  - Risk Assessment
- Postmarket Update
  - Mitigation
  - Communication
  - Release
  - Distribution

Documentation

- SBOM
- MDS2
- Security Instructions
- Measures & Metrics

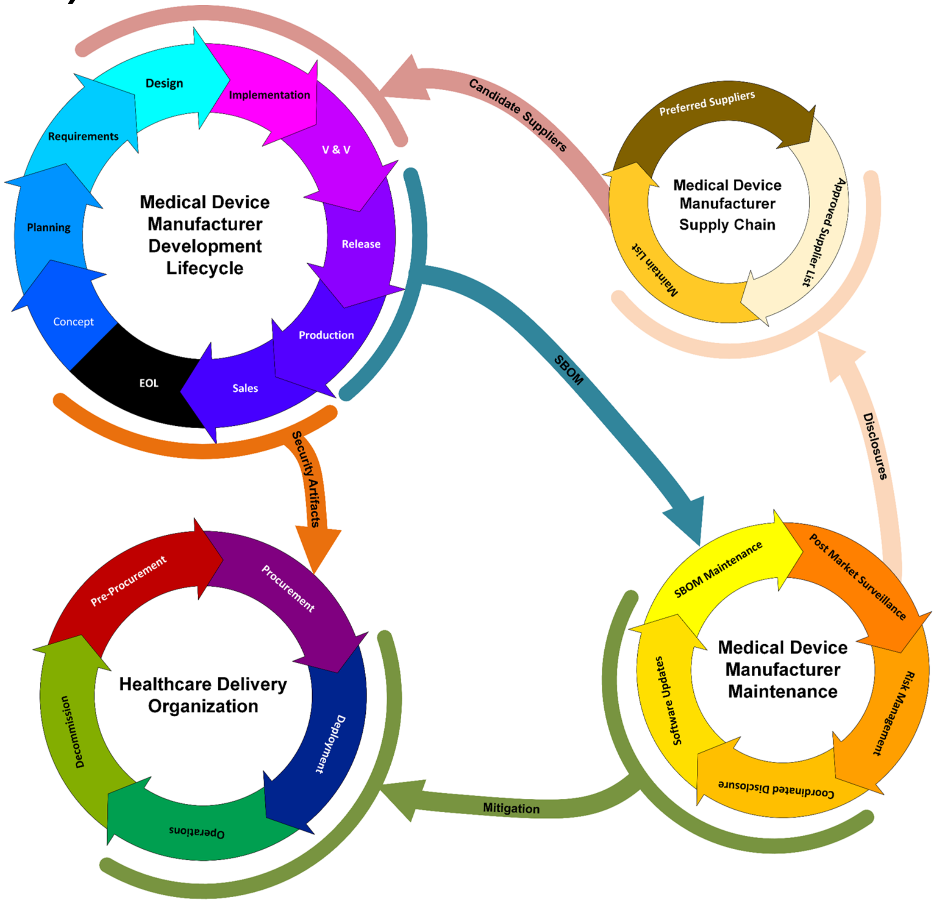
Medcrypt

Proactive Healthcare Cybersecurity

Secure Software Development Lifecycle (SSDLC)

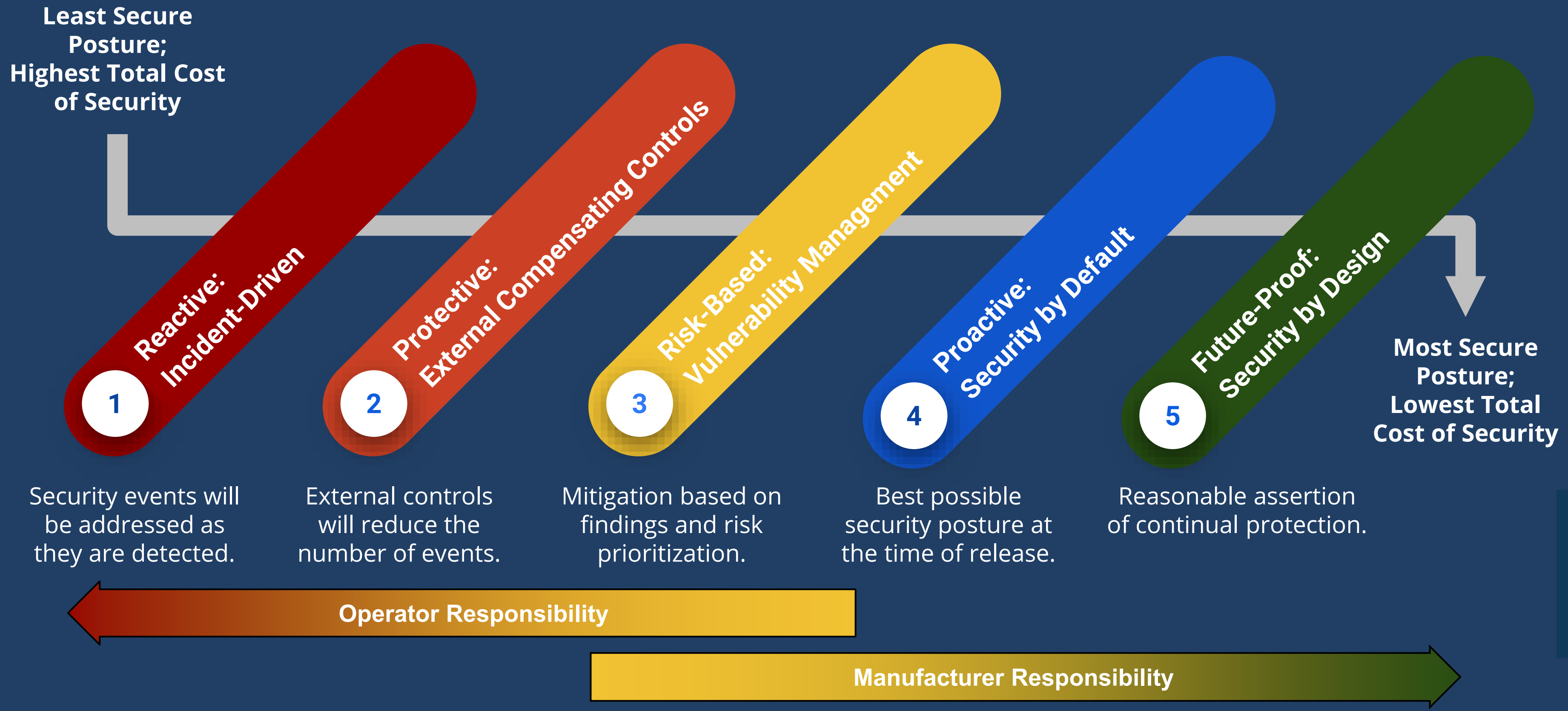
Various Secure Software Development Lifecycle (SDLC) models exist. However, many are not suited outside of the pure software space and may not be helpful to meet medical device regulator expectations; others are misguided or overly simplified.

The H-ISAC approach seems to be the most appropriate model to adopt in the medical device space and can be used as a basis for a Secure Product Development Framework (SPDF)



https://h-isac.org/medical-device-cybersecurity-lifecycle-management/

Cybersecurity: Current State vs. Desired Future State



Least Secure Posture; Highest Total Cost of Security

1 **Reactive: Incident-Driven**

Security events will be addressed as they are detected.

2 **Protective: External Compensating Controls**

External controls will reduce the number of events.

3 **Risk-Based: Vulnerability Management**

Mitigation based on findings and risk prioritization.

4 **Proactive: Security by Default**

Best possible security posture at the time of release.

5 **Future-Proof: Security by Design**

Reasonable assertion of continual protection.

Most Secure Posture; Lowest Total Cost of Security

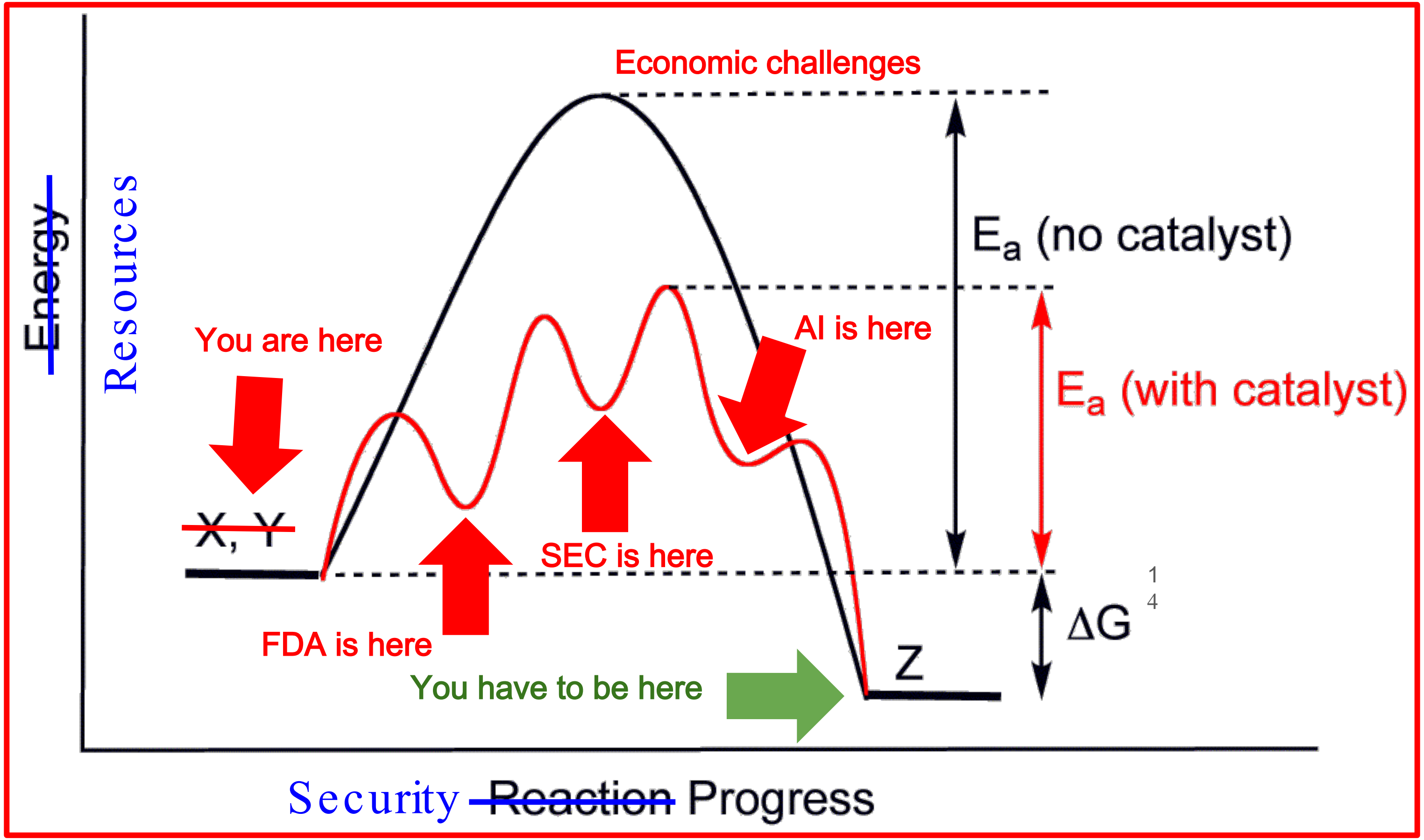
Operator Responsibility

Manufacturer Responsibility

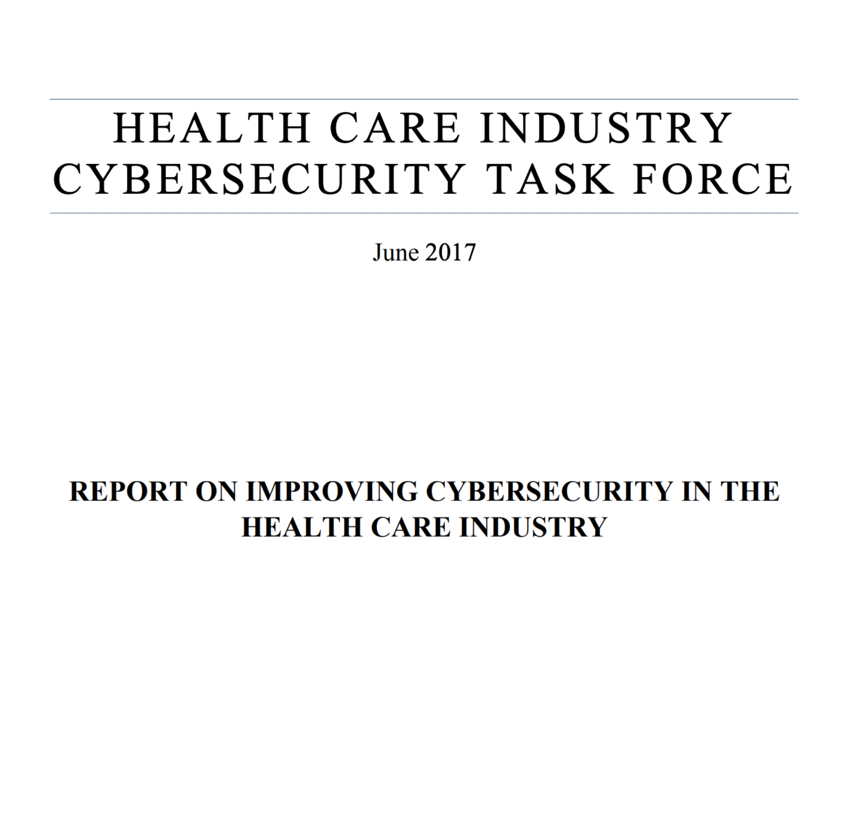
Medcrypt

Proactive Healthcare Cybersecurity

Where are Your ~~Chemistry~~ Security Catalysts?



Who is going to do the work?



HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

June 2017

REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

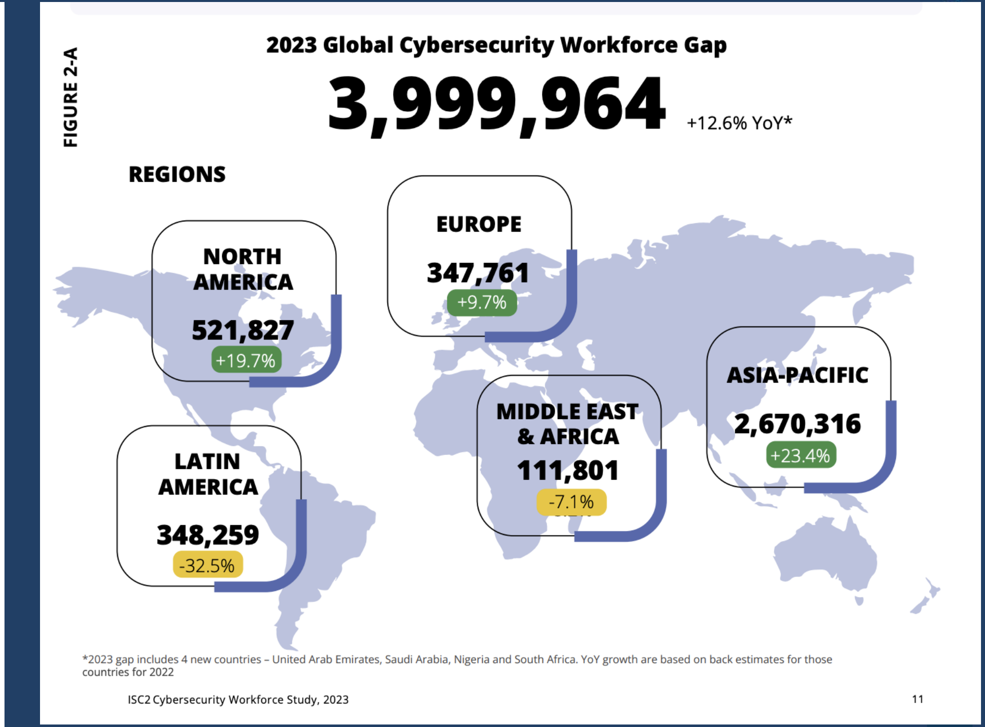


FIGURE 2-A

2023 Global Cybersecurity Workforce Gap

3,999,964 +12.6% YoY*

REGIONS

NORTH AMERICA 521,827 +19.7%

EUROPE 347,761 +9.7%

LATIN AMERICA 348,259 -32.5%

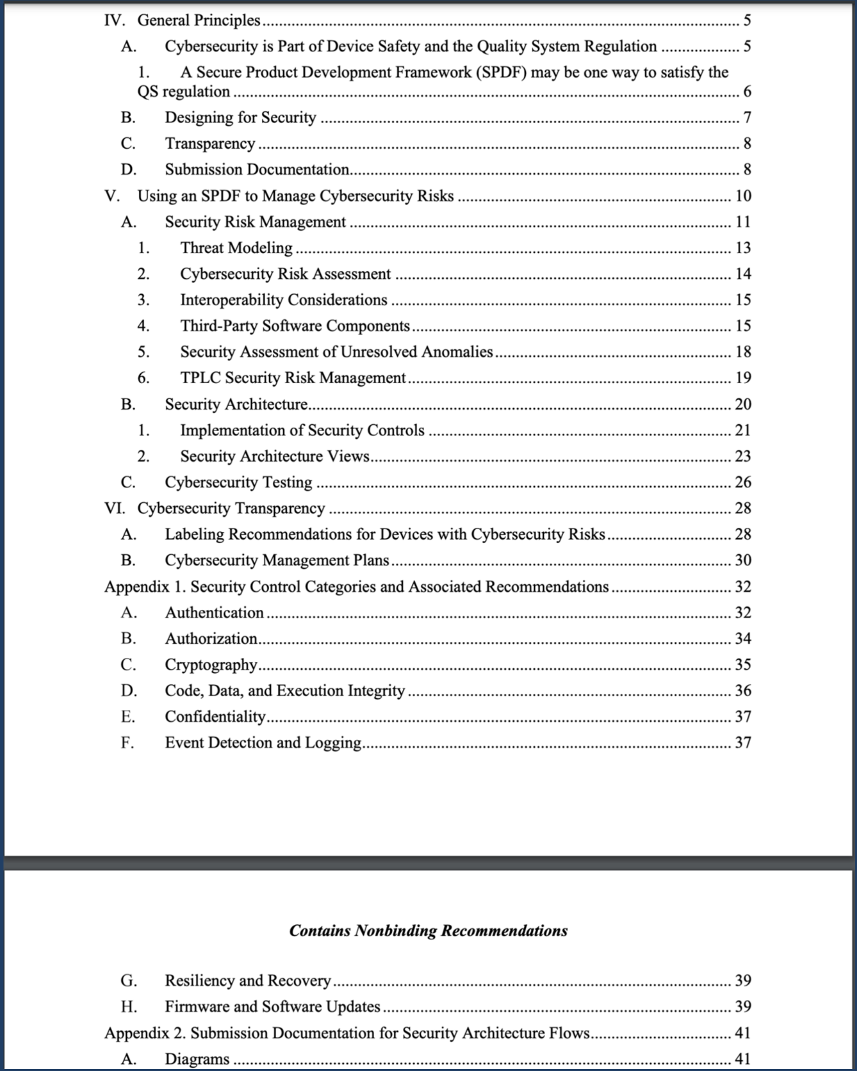
MIDDLE EAST & AFRICA 111,801 -7.1%

ASIA-PACIFIC 2,670,316 +23.4%

*2023 gap includes 4 new countries – United Arab Emirates, Saudi Arabia, Nigeria and South Africa. YoY growth are based on back estimates for those countries for 2022

ISC2 Cybersecurity Workforce Study, 2023 11

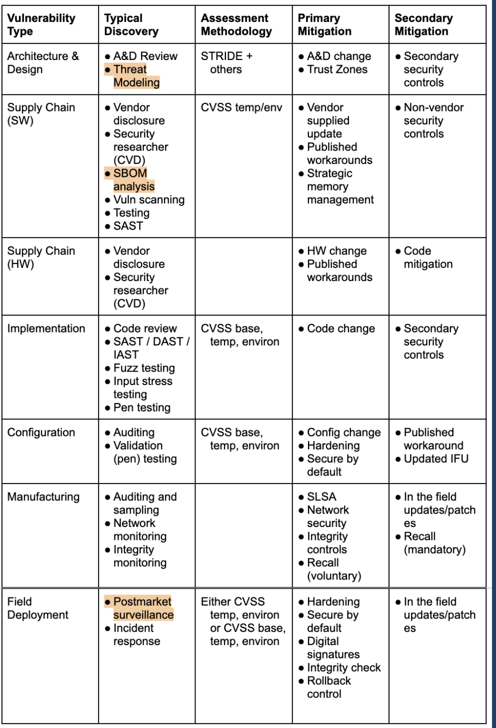
The Data Set



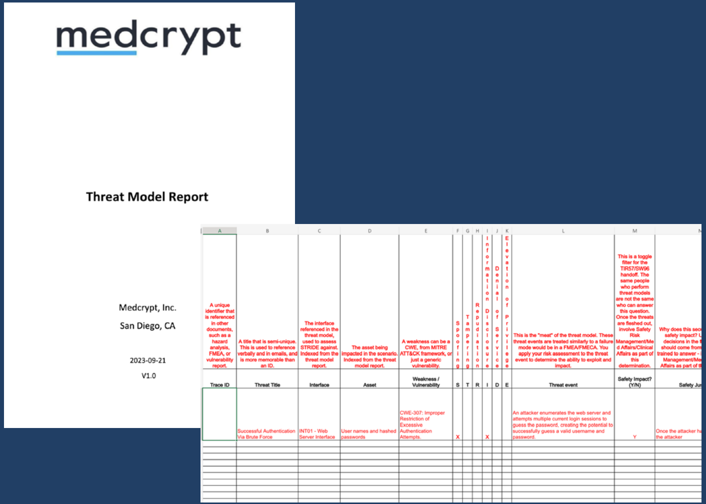
Contains Nonbinding Recommendations

Medcrypt

Proactive Healthcare Cybersecurity



Vulnerability Type	Typical Discovery	Assessment Methodology	Primary Mitigation	Secondary Mitigation
Architecture & Design	• A&D Review • Threat Modeling	STRIDE + others	• A&D change • Trust Zones	• Secondary security controls
Supply Chain (SW)	• Vendor disclosure • Security researcher (CVD) • SBOM analysis • Vuln scanning • Testing • SAST	CVSS temp/env	• Vendor supplied update • Published workarounds • Strategic memory management	• Non-vendor security controls
Supply Chain (HW)	• Vendor disclosure • Security researcher (CVD)		• HW change • Published workarounds	• Code mitigation
Implementation	• Code review • SAST / DAST / IAST • Fuzz testing • Input stress testing • Pen testing	CVSS base, temp, environ	• Code change	• Secondary security controls
Configuration	• Auditing • Validation (pen) testing	CVSS base, temp, environ	• Config change • Hardening • Secure by default	• Published workaround • Updated IFU
Manufacturing	• Auditing and sampling • Network monitoring • Integrity monitoring		• SLSA • Network security • Integrity controls • Recall (voluntary)	• In the field updates/patches • Recall (mandatory)
Field Deployment	• Postmarket surveillance • Incident response	Either CVSS temp, environ or CVSS base, temp, environ	• Hardening • Secure by default • Digital signatures • Integrity check • Rollback control	• In the field updates/patches



medcrypt

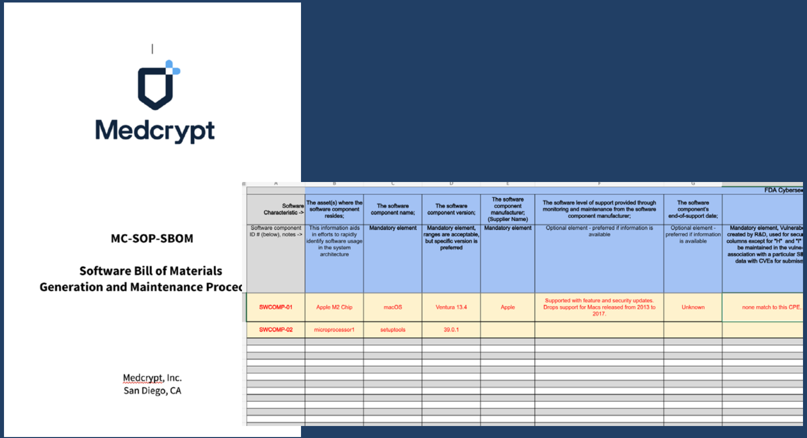
Threat Model Report

Medcrypt, Inc.
San Diego, CA

2023-09-21

V1.0

A	B	C	D	E	F	G	H	I	J	K	L	M	N
A unique identifier that is referenced in other documents, such as a hazard analysis, FMEA, or vulnerability report.	A title that is semi-unique. This is used to reference verbally and in emails, and is more memorable than an ID.	The interface referenced in the threat model, used to assess STRIDE against. Indexed from the threat model report.	The asset being impacted in the scenario. Indexed from the threat model report.	A weakness can be a CWE, from MITRE ATT&CK framework, or just a generic vulnerability.	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege	This is the "meat" of the threat model. These threat events are treated similarly to a failure mode would be in a FMEA/FMECA. You apply your risk assessment to the threat event to determine the ability to exploit and impact.	This is a toggle filter for the TIR57/SW96 handoff. The same people who perform threat models are not the same who can answer this question. Once the threats are fleshed out, involve Safety Risk Management/Med Affairs/Clinical Affairs as part of this determination.	Why does this sec safety impact? U decisions in the f should come from trained to answer - I Management/Me Affairs as part of th
Trace ID	Threat Title	Interface	Asset	Weakness / Vulnerability	S	T	R	I	D	E	Threat event	Safety Impact? (Y/N)	Safety Jus
	Successful Authentication Via Brute Force	INT01 - Web Server Interface	User names and hashed passwords	CWE-307: Improper Restriction of Excessive Authentication Attempts.	X			X			An attacker enumerates the web server and attempts multiple current login sessions to guess the password, creating the potential to successfully guess a valid username and password.	Y	Once the attacker ha the attacker



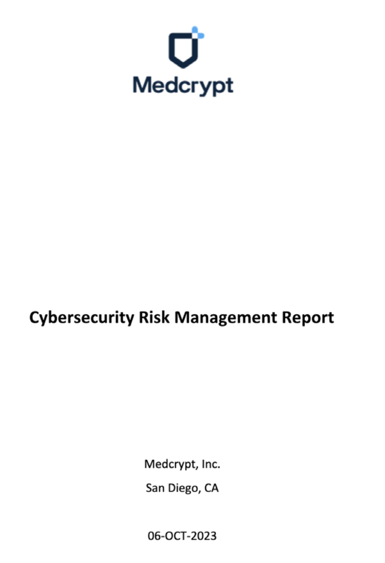
Medcrypt

MC-SOP-SBOM

Software Bill of Materials
Generation and Maintenance Procec

Medcrypt, Inc.
San Diego, CA

A	B	C	D	E	F	G	H
							FDA Cyberse
Software Characteristic ->	The asset(s) where the software component resides;	The software component name;	The software component version;	The software component manufacturer; (Supplier Name)	The software level of support provided through monitoring and maintenance from the software component manufacturer;	The software component's end-of-support date;	
Software component ID # (below), notes ->	This information aids in efforts to rapidly identify software usage in the system architecture	Mandatory element	Mandatory element, ranges are acceptable, but specific version is preferred	Mandatory element	Optional element - preferred if information is available	Optional element - preferred if information is available	Mandatory element, Vulnerab created by R&D, used for secu columns except for "H" and "I" be maintained in the vulne association with a particular SE data with CVEs for submiss
SWCOMP-01	Apple M2 Chip	macOS	Ventura 13.4	Apple	Supported with feature and security updates. Drops support for Macs released from 2013 to 2017.	Unknown	none match to this CPE.
SWCOMP-02	microprocessor1	setuptools	39.0.1				



Medcrypt

Cybersecurity Risk Management Report

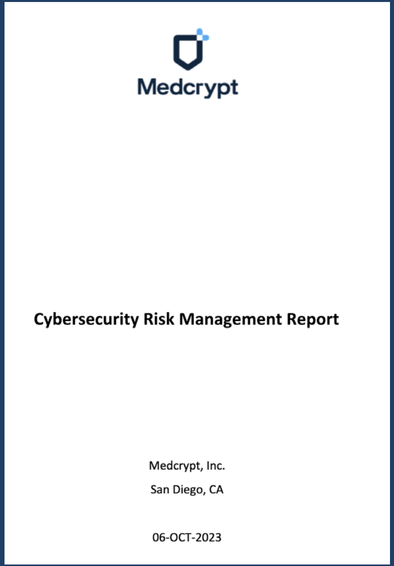
Medcrypt, Inc.
San Diego, CA

06-OCT-2023

- Reject, Redesign to eliminate
- Reject, Apply standard mitigations
- Reject, Develop new mitigations
- Accept vulnerability in design
- Accept and monitor in the field
- Reject and sunset device

Medcrypt

Proactive Healthcare Cybersecurity



Medcrypt

Cybersecurity Risk Management Report

Medcrypt, Inc.
San Diego, CA

06-OCT-2023

FDA U.S. FOOD & DRUG ADMINISTRATION

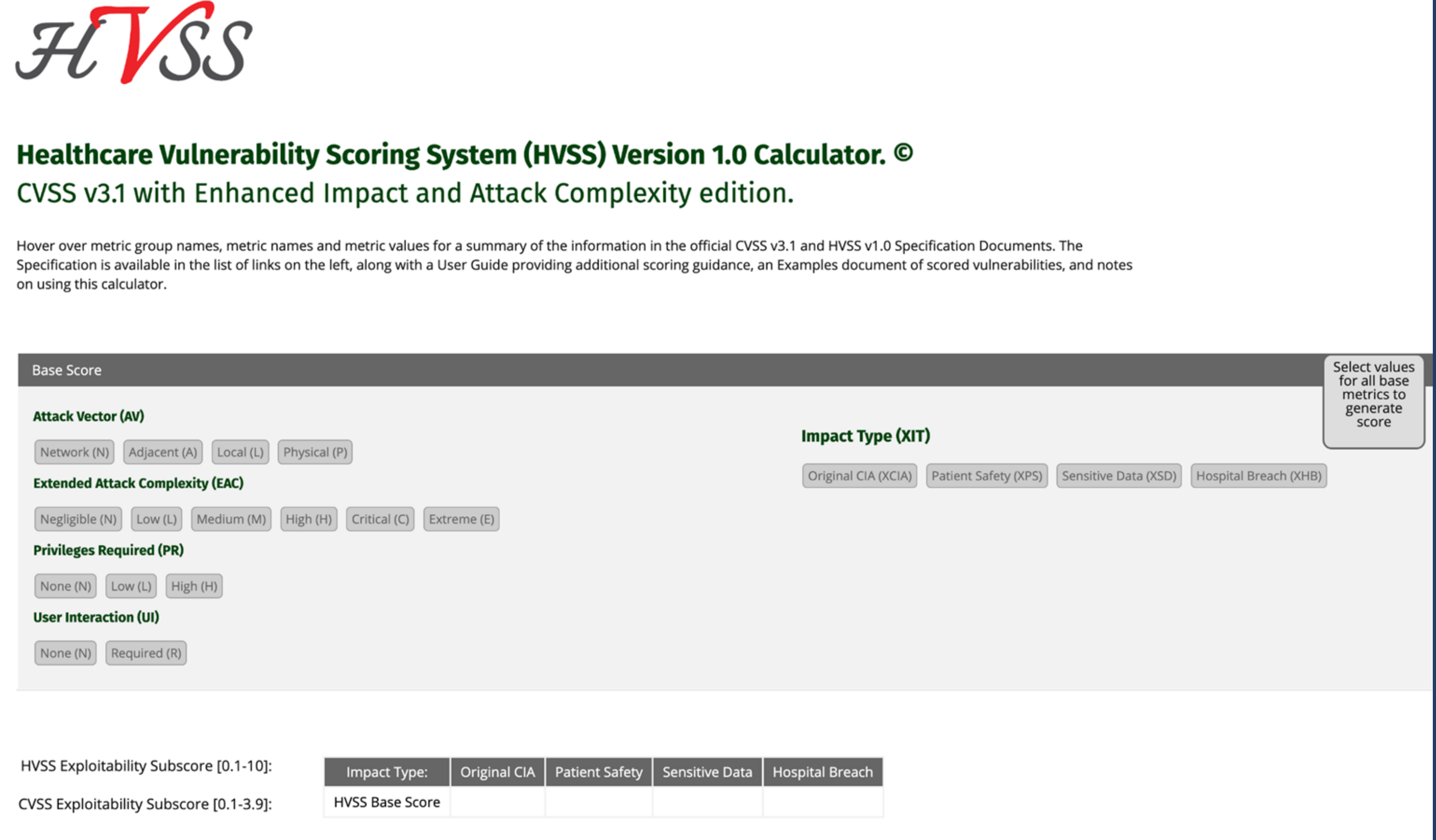
1. Reasonably safe and effective
2. Benefits outweigh the risks

Medcrypt

MC-PLAN-Postmarket Cybersecurity Mitigation, Management, and Communication

Quality Management System Cybersecurity Template

Medcrypt, Inc.
San Diego, CA



HVSS

Healthcare Vulnerability Scoring System (HVSS) Version 1.0 Calculator. ©

CVSS v3.1 with Enhanced Impact and Attack Complexity edition.

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 and HVSS v1.0 Specification Documents. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator.

Base Score

Select values for all base metrics to generate score

Attack Vector (AV)

Network (N) Adjacent (A) Local (L) Physical (P)

Extended Attack Complexity (EAC)

Negligible (N) Low (L) Medium (M) High (H) Critical (C) Extreme (E)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Impact Type (XIT)

Original CIA (XCIA) Patient Safety (XPS) Sensitive Data (XSD) Hospital Breach (XHB)

HVSS Exploitability Subscore [0.1-10]:

CVSS Exploitability Subscore [0.1-3.9]:

Impact Type:	Original CIA	Patient Safety	Sensitive Data	Hospital Breach
HVSS Base Score				

Medcrypt

Thank you!

seth@medcrypt.com