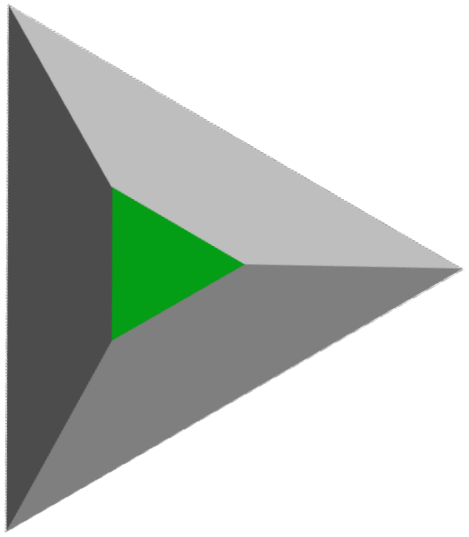
Secure Development Lifecycle and Software Transparency



Velentium

Velentium = **Vel**ocity + Mom**ent**um + Ingen**ium**

Greenlight Guru

MEDICAL DEVICE QUALITY IS ALL WE DO, AND WE'RE ALWAYS AHEAD OF THE GAME.

75
years industry experience

275k
podcast listeners

#1
blog and podcast in the industry

114k
look to us for the latest in quality

FEATURED IN

THE VERGE · TechCrunch · Forbes · QUALITYDIGEST · MDDI · Inc. · MedTech Intelligence · MED DEVICE ONLINE · Medical Design & OUTSOURCING · TNW THE NEXT WEB · Entrepreneur · MPO

"Great eQMS Software..."

"The software is easy to use with little to no customization needed. It has been a great tool for developing our device through design control. The post-market additions have been amazing as well as tasks. **After using multiple types of eQMS software over the years, this is the best by far!"**

"My QMS is world class" ★★★★★

"Design controls lifesaver" ★★★★★

"One-stop shop" ★★★★★

"Fantastic product, even better team" ★★★★★

greenlight guru

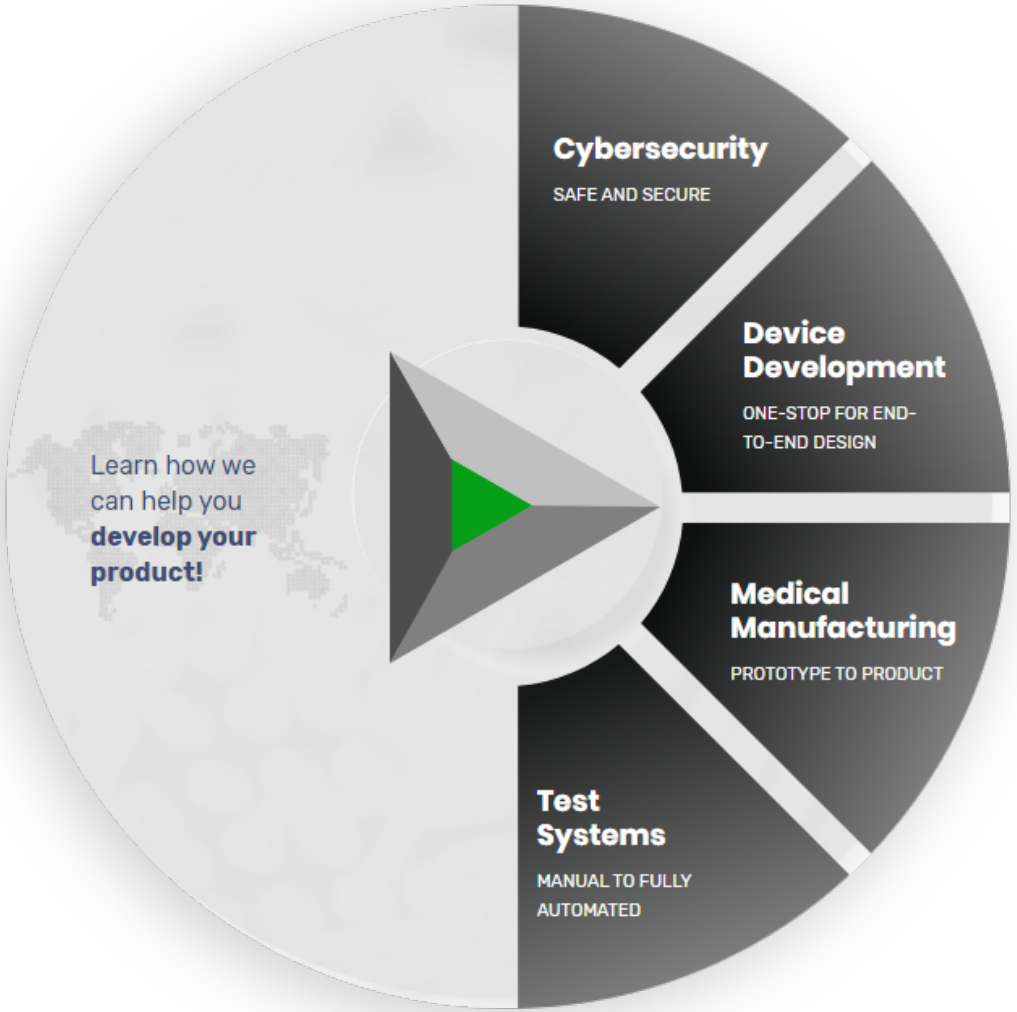
How We Are Different

Cybersecurity

Velentium's depth and breadth of development experience, as well as our ability to navigate the constraints of secure medical device development, makes us an industry leader in device security.

Test Systems

Velentium's Subject Matter Experts can design you a custom test system, ranging from fully manual to fully automatic, and everything in between.



Device Development

We are a one-stop for secure design, development, production, and post-market services. See how we can take your device from IP to commercialized product today!

Medical Manufacturing

Let Velentium meet your manufacturing needs with our ISO 13485-certified lean QMS and our design and development experts within arms' reach at all times.

Medical Device Engineering: Your IP. Designed and Built.

VELENTIUM

We Exist to Help You Change Lives for a Better World

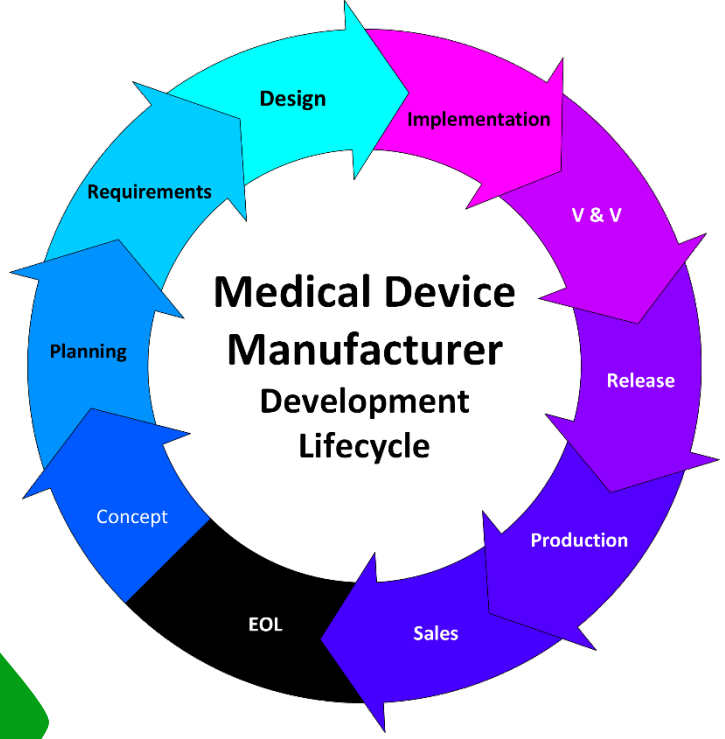
Recent Trends in Medical Device Cybersecurity

- Its easy, just change everything you do in developing your medical device
- Buy our security tool and all your cybersecurity issues are solved

The reality is more complex:

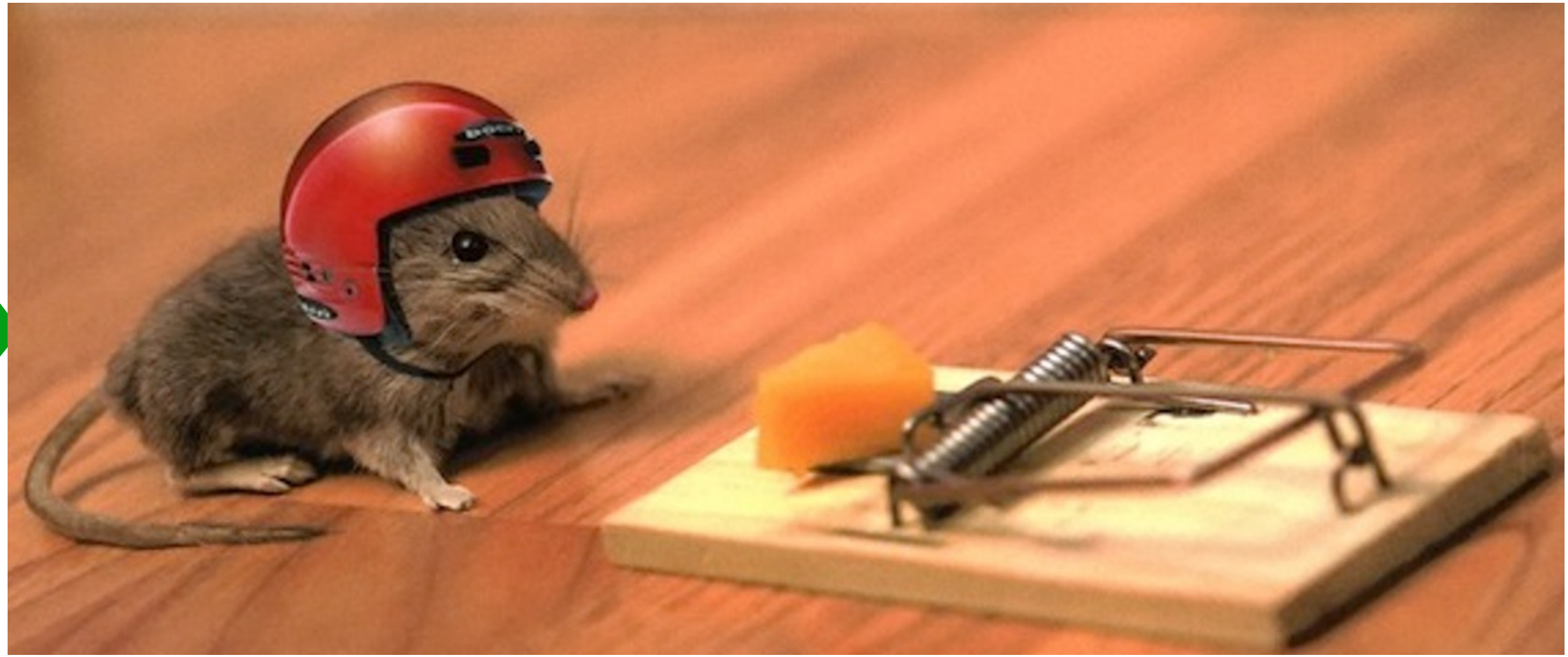
- Train your engineers how to create secure devices.
- Device security starts with a Threat Model
- Utilize a secure development process.
- Security ends at ‘end of support’

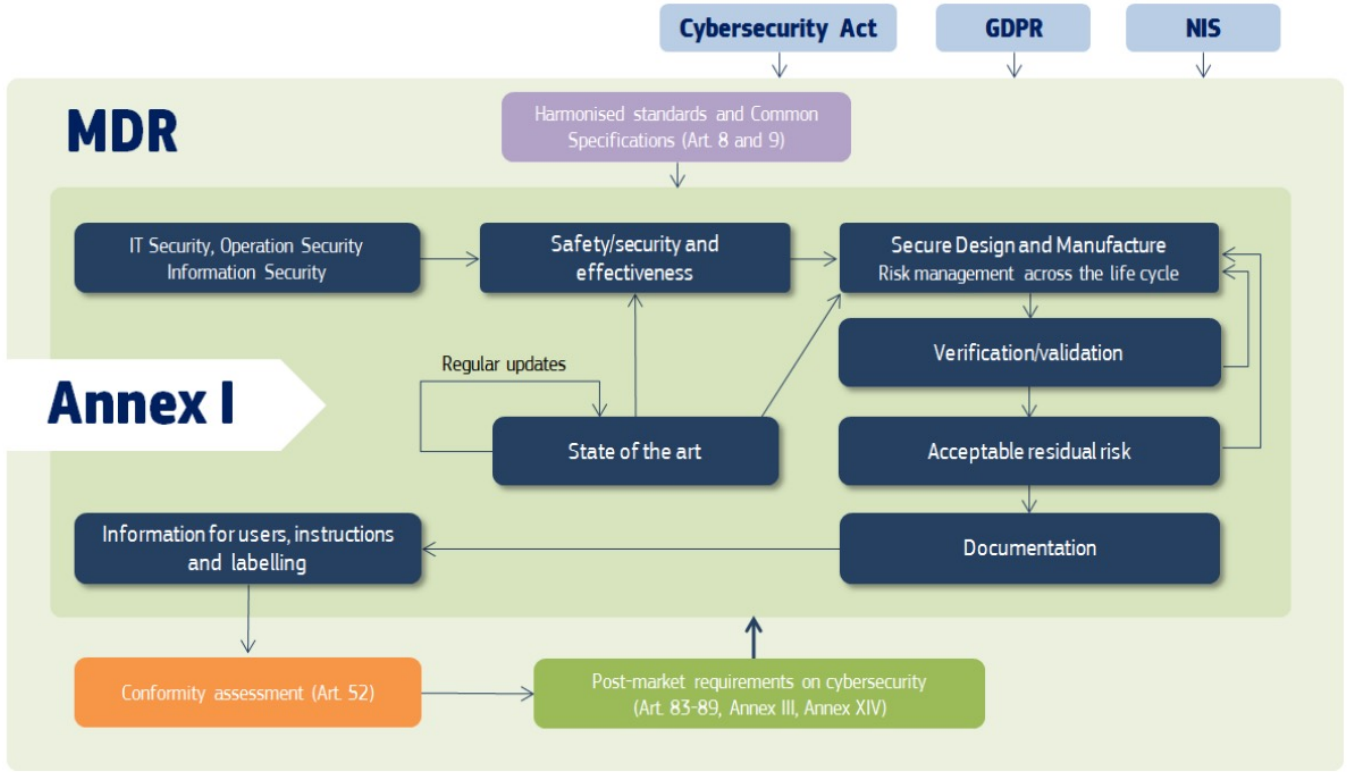
There are no silver bullets!

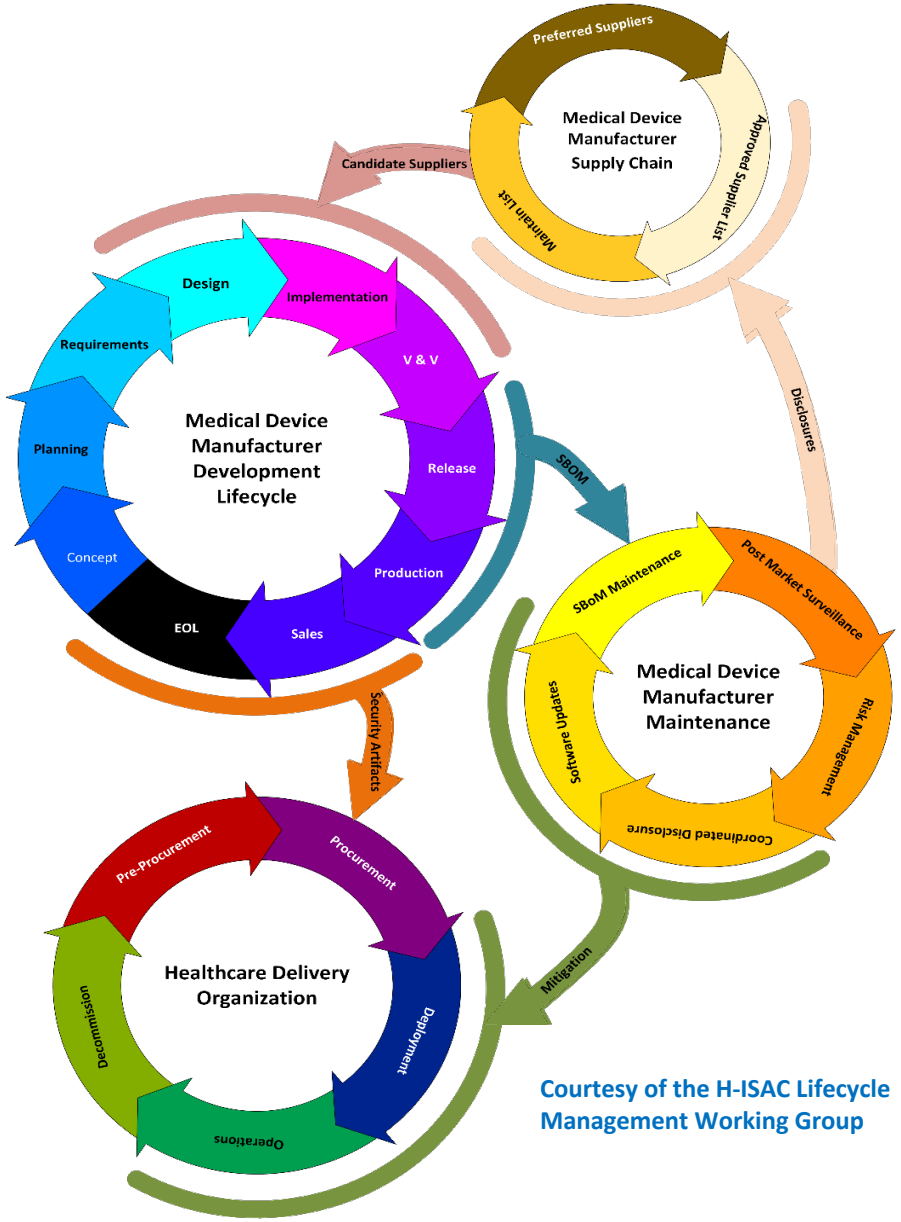


Incorporating Cybersecurity Into the Medical Device Development Lifecycle

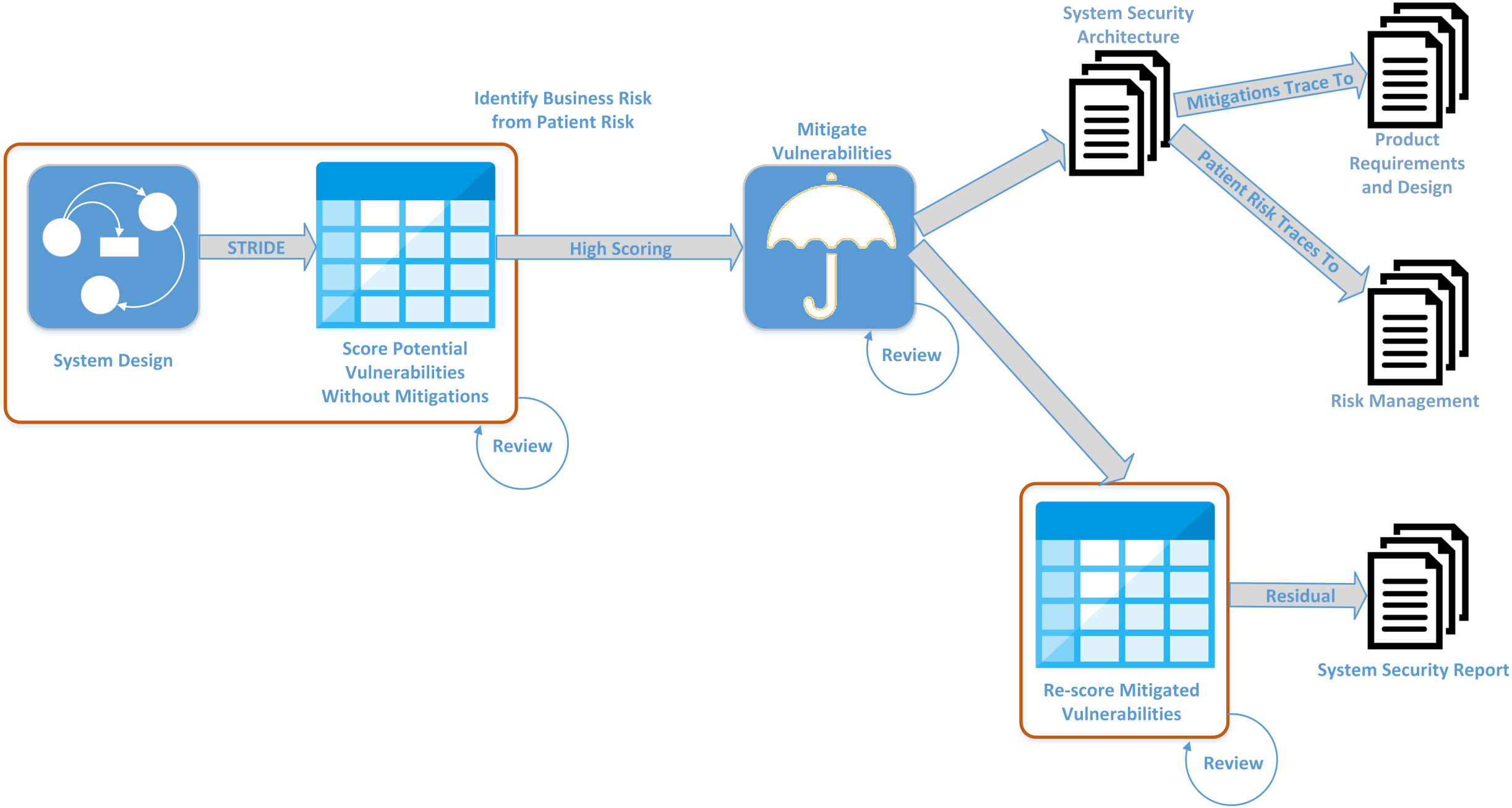
The Risks



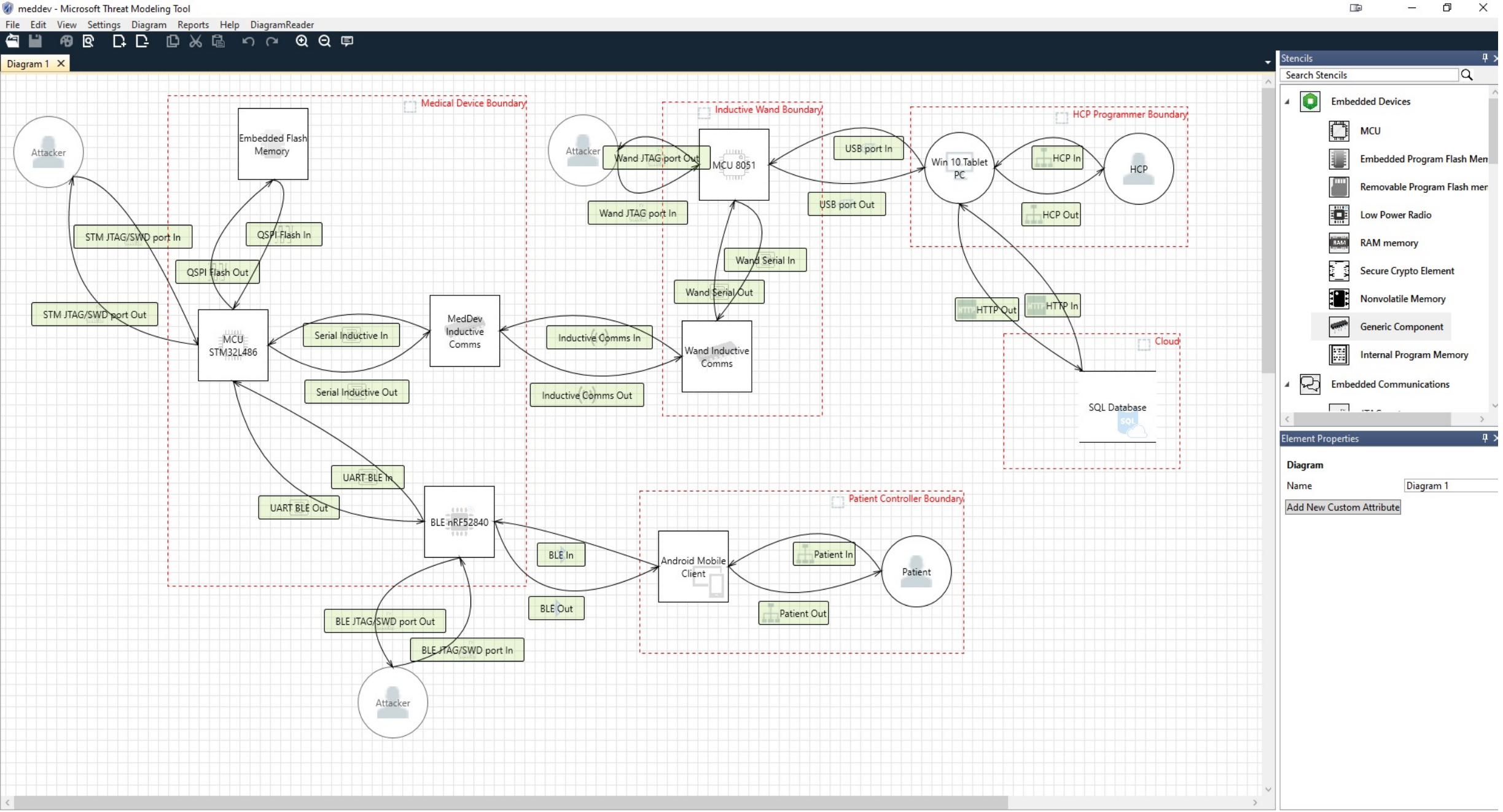


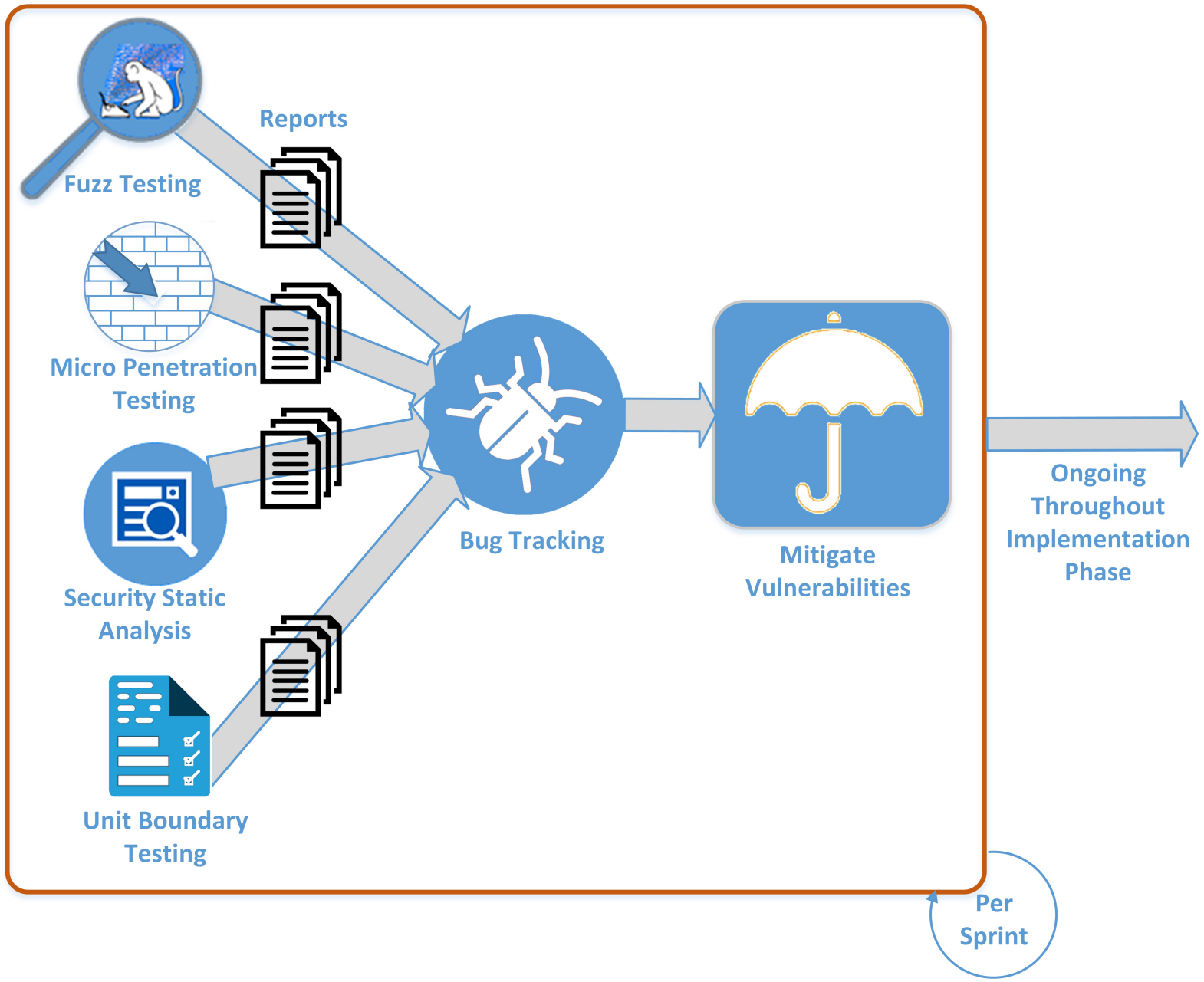


Courtesy of the H-ISAC Lifecycle Management Working Group

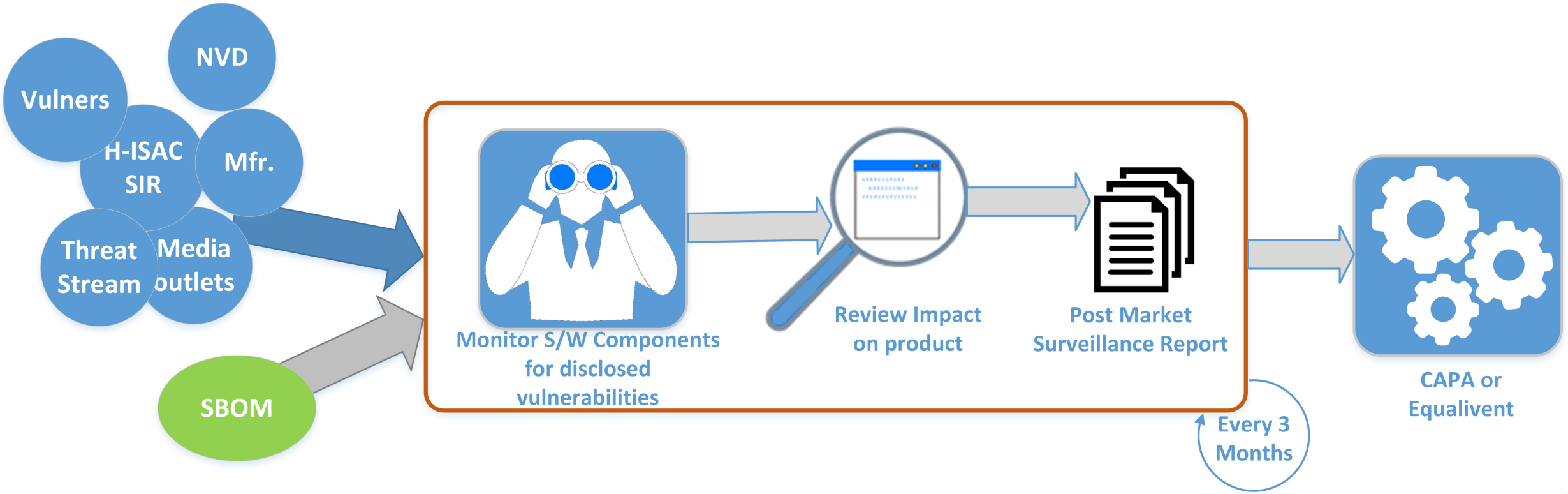


During Design Phase


meddev - Microsoft Threat Modeling Tool
File Edit View Settings Diagram Reports Help DiagramReader
Diagram 1
Medical Device Boundary
Attacker
Embedded Flash Memory
STM JTAG/SWD port In
QSPI Flash In
QSPI Flash Out
STM JTAG/SWD port Out
MCU STM32L486
Serial Inductive In
Serial Inductive Out
MedDev Inductive Comms
Inductive Comms In
Inductive Comms Out
Inductive Wand Boundary
Attacker
Wand JTAG port Out
Wand JTAG port In
MCU 8051
Wand Serial In
Wand Serial Out
Wand Inductive Comms
USB port In
USB port Out
HCP Programmer Boundary
Win 10 Tablet PC
HCP In
HCP
HCP Out
HTTP Out
HTTP In
Cloud
SQL Database
UART BLE In
UART BLE Out
BLE nRF52840
BLE In
BLE Out
Patient Controller Boundary
Android Mobile Client
Patient In
Patient
Patient Out
BLE JTAG/SWD port Out
BLE JTAG/SWD port In
Attacker
Stencils
Search Stencils
Embedded Devices
MCU
Embedded Program Flash Mem
Removable Program Flash mer
Low Power Radio
RAM memory
Secure Crypto Element
Nonvolatile Memory
Generic Component
Internal Program Memory
Embedded Communications
Element Properties
Diagram
Name
Diagram 1
Add New Custom Attribute



During Implementation Phase



For more on SBOMs
Please visit: NTIA.GOV/SBOM

During Release and Post Market Phase

Software Transparency

a.k.a “What's in the Black Box”

“Software Transparency”, allows the end user insight into risks that may be introduced into their environment, via the use of a given device.

- This additional information allows for a faster response by the end user.
- It also enables the end user to self determine their level of acceptable risk.
- Properly implemented, it will also lower the burden on the end user to monitor the devices in their organization.
- SBOM = “Software Bill of Materials” both human and machine readable versions

For more on SBOMs
Please visit: NTIA.GOV/SBOM

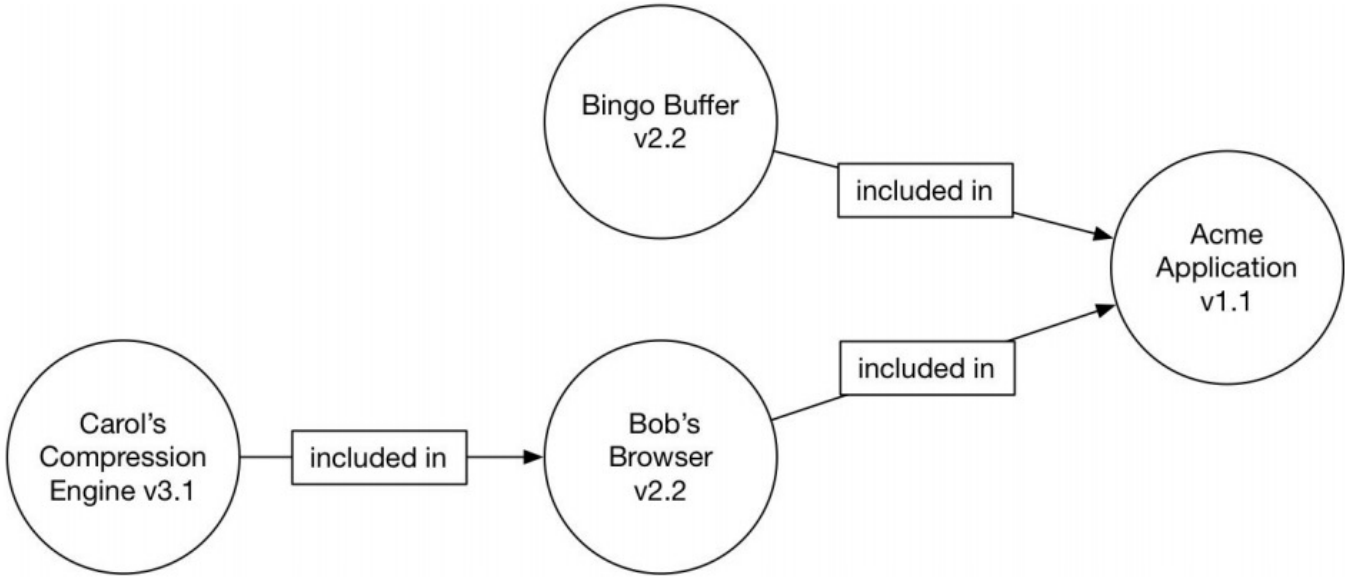
An SBOM can also help a device developer in the following ways:

- Reduce code bloat.
- Adequately understand dependencies within broader complex projects
- Know and comply with license obligations
- Software component end-of-life (EOL)
- Make code easier to review
- Blacklist of banned components or manufacturers
- Insight into legacy device dependencies
- Provide an SBOM to a potential customer during pre-procurement
- Monitor components for disclosed vulnerabilities

There are two predominate SBOM machine readable formats for security:

- SPDX
- CycloneDX

For more on SBOMs
Please visit: NTIA.GOV/SBOM



Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Self
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

For more on SBOMs
Please visit: NTIA.GOV/SBOM

A CycloneDX SBOM (XML) for WebGoat


```xml
<?xml version="1.0" encoding="UTF-8"?><bom serialNumber="urn:uuid:b243b20c-595f-4f43-820c-737b007a1c2d" version="1" xmlns="http://cyclonedx.org/schema/bom/1.2">
  <metadata>
    <timestamp>2021-03-25T03:48:29Z</timestamp>
    <tools>
      <tool>
        <vendor>CycloneDX</vendor>
        <name>CycloneDX Maven plugin</name>
        <version>2.3.0</version>
        <hashes>
          <hash alg="MD5">726f3a7a01e3afd1a62da5aa97d296a6</hash>
          <hash alg="SHA-1">453473640f54a33c7d6b712cc49b77a4833368ef</hash>
          <hash alg="SHA-256">e20af57194bb5c63616a8c9bd24eaf42acc807818e3a4e37493f3825e79208cf</hash>
          <hash alg="SHA-384">781738141c09ba2650dacc6f66e8f3f4f16ea5439a87eaaea453eb4ebe6427ffe9d7281e66d5a8c383088579a7f08389</hash>
          <hash alg="SHA-512">97f992bbe3f1093011b9eecad0d3835f3dd770d22794af2e9c73c655f424ed0230faf9bdfcbca32887f9ea7dd5ba5681fefe339fe4b05c190c9ed939a1c66afa</hash>
          <hash alg="SHA3-256">7698f46ae5ace9d76e3f16915501039524e41701a5224a12d94ecbe051810948</hash>
          <hash alg="SHA3-384">0d1c0eb6b1764d04eb6783811b97e6352af094f664016b6b83820f453aca28a98266caa50887786c267150444a6a4a14</hash>
          <hash alg="SHA3-512">c50b891d349c1227445c4b9cb7ac0119c3b6e533ecf86452fb449df93127fea67fcde8ef8945e96fffd16ebe75003deb4ad2984a23af76d18506d50d5a494bd5</hash>
        </hashes>
      </tool>
    </tools>
    <component type="library" bom-ref="pkg:maven/org.owasp.webgoat/webgoat-container@v8.2.0-SNAPSHOT">
      <group>org.owasp.webgoat</group>
      <name>webgoat-container</name>
      <version>v8.2.0-SNAPSHOT</version>
      <licenses>
        <license>
          <name>GNU General Public License, version 2</name>
          <url>https://www.gnu.org/licenses/gpl-2.0.txt</url>
        </license>
      </licenses>
      <purl>pkg:maven/org.owasp.webgoat/webgoat-container@v8.2.0-SNAPSHOT</purl>
    </component>
  </metadata>
  <components>
    <component type="library" bom-ref="pkg:maven/org.springframework.boot/spring-boot-starter-validation@2.4.0?type=jar">
      <publisher>Pivotal Software, Inc.</publisher>
      <group>org.springframework.boot</group>
      <name>spring-boot-starter-validation</name>
      <version>2.4.0</version>
      <description>Starter for using Java Bean Validation with Hibernate Validator</description>
      <scope>optional</scope>
      <hashes>
        <hash alg="MD5">53b0349f94d4e1488ea3cd429ca2cf93</hash>
        <hash alg="SHA-1">739a3c3d0b08be3c8dfbed08c26b6a633148e186</hash>
        <hash alg="SHA-256">a2968edda2414f0291365f270ceff48888547d3d46fd27a4c52b3f7c7f570276</hash>
        <hash alg="SHA-384">1209a0392075718a0262dd25fc22546ee0af480d60780334c9d0d6ce54fcb01e7b79be0f77f7f310f41a7d4bd75f9f13</hash>
        <hash alg="SHA-512">7c45c6cdeba4548a2b27bde2451b97de6b98e06079a910fc4530e67312bcd78904c5d0128a3c7f8c83354281a61d3ff7e29c6370018274349fcb2ede80d7cfd3</hash>
```


For more on SBOMs Please visit: NTIA.GOV/SBOM

A CycloneDX SBOM (JSON) for WebGoat


```
{
  "bomFormat" : "CycloneDX",
  "specVersion" : "1.2",
  "serialNumber" : "urn:uuid:b243b20c-595f-4f43-820c-737b007a1c2d",
  "version" : 1,
  "metadata" : {
    "timestamp" : "2021-03-25T03:48:29Z",
    "tools" : [ {
      "vendor" : "CycloneDX",
      "name" : "CycloneDX Maven plugin",
      "version" : "2.3.0",
      "hashes" : [ {
        "alg" : "MD5",
        "content" : "726f3a7a01e3afd1a62da5aa97d296a6"
      }, {
        "alg" : "SHA-1",
        "content" : "453473640f54a33c7d6b712cc49b77a4833368ef"
      }, {
        "alg" : "SHA-256",
        "content" : "e20af57194bb5c63616a8c9bd24eaf42acc807818e3a4e37493f3825e79208cf"
      }, {
        "alg" : "SHA-384",
        "content" : "781738141c09ba2650dacc6f66e8f3f4f16ea5439a87eaaea453eb4ebe6427ffe9d7281e66d5a8c383088579a7f08389"
      }, {
        "alg" : "SHA-512",
        "content" : "97f992bbe3f1093011b9eecad0d3835f3dd770d22794af2e9c73c655f424ed0230faf9bdfcbca32887f9ea7dd5ba5681fefe339fe4b05c190c9ed939a1c66afa"
      }, {
        "alg" : "SHA3-256",
        "content" : "7698f46ae5ace9d76e3f16915501039524e41701a5224a12d94ecbe051810948"
      }, {
        "alg" : "SHA3-384",
        "content" : "0d1c0eb6b1764d04eb6783811b97e6352af094f664016b6b83820f453aca28a98266caa50887786c267150444a6a4a14"
      }, {
        "alg" : "SHA3-512",
        "content" : "c50b891d349c1227445c4b9cb7ac0119c3b6e533ecf86452fb449df93127fea67fcde8ef8945e96fffd16ebe75003deb4ad2984a23af76d18506d50d5a494bd5"
      } ]
    } ],
    "component" : {
      "group" : "org.owasp.webgoat",
      "name" : "webgoat-container",
      "version" : "v8.2.0-SNAPSHOT",
      "licenses" : [ {
        "license" : {
          "name" : "GNU General Public License, version 2",
          "url" : "https://www.gnu.org/licenses/gpl-2.0.txt"
        }
      } ],
      "purl" : "pkg:maven/org.owasp.webgoat/webgoat-container@v8.2.0-SNAPSHOT",
```


For more on SBOMs
Please visit: NTIA.GOV/SBOM

But…. An SBOM is not enough!

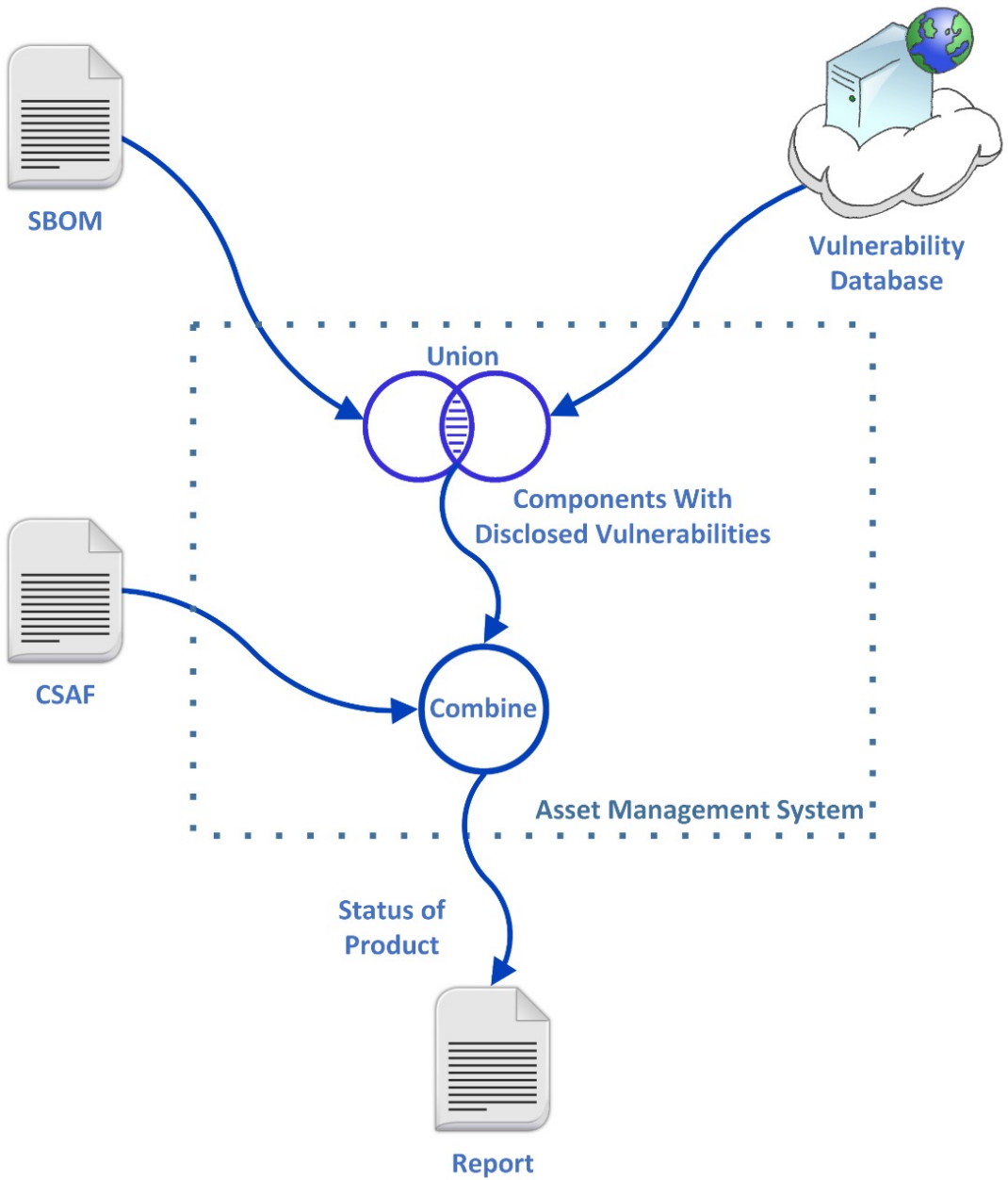
Exposing the software components in a black box, results in a high quantity of false positive results. As only a small percentage of disclosed vulnerabilities can be exploited*.

The NTIA SBOM working groups are working with the Oasis Open standard body to utilize their “Common Security Advisory Framework” (i.e. CSAF) version 2.0 to convey the device manufacturer’s position on the exploitability of given vulnerabilities in their devices via a machine readable format.

This will result, in an improved level of trust of the risks being posed to an end user.

Both BSI (British Standards Institution) and Germany are creating standards to address the use of the CSAF.

*For more on this topic see the Sonatype “2020 State of the Software Supply Chain Report” and the RSA 2019 “How Understanding Risk is Changing for Open Source Components” presentation.


SBOM
Vulnerability Database
Union
Components With Disclosed Vulnerabilities
CSAF
Combine
Asset Management System
Status of Product
Report

Level 1

Core: 3 Days

2-Year Certification

Evaluating designs, assessing vulnerabilities, and constructing SBOMs

- ★ Why Invest in Cybersecurity?
- ★ Basic Hacking Tutorials
- ★ Introduction to Secure Development
- ★ Post-Market Surveillance

Level 2

Intermediate: 3 Days

3-Year Certification

Identifying, selecting, and implementing cybersecurity solutions

- ★ Design Choices with respect to Hardware Selection, ASL, Device EOL, Field Updates & Secure Production Considerations
- ★ Implementation of Secure Coding, Cryptography, and making use of Secure Hardware
- ★ Hardening of Commercial OTS Products

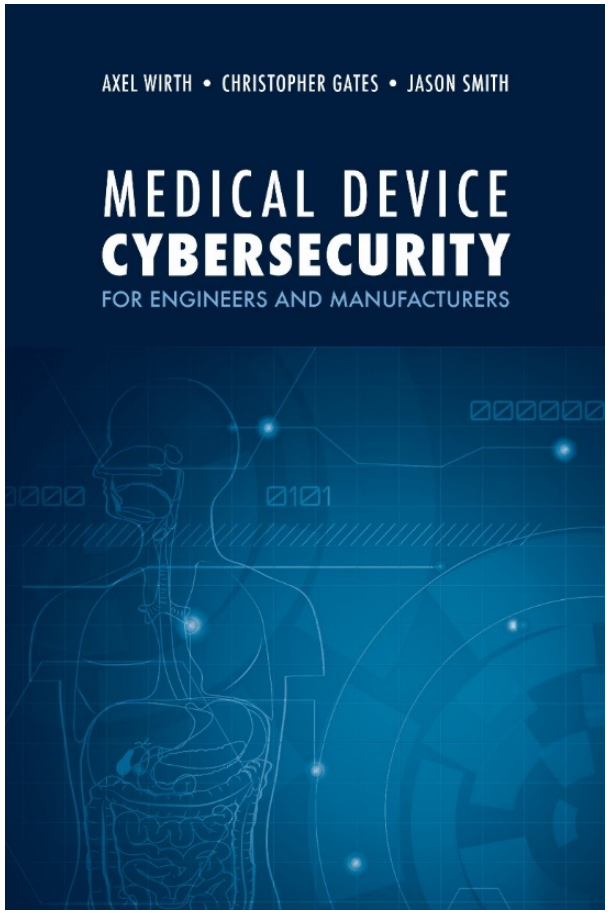
Level 3

Advanced: 3 Days

5-Year Certification

Crafting custom security solutions and system security engineering

- ★ Third-party Software Components
- ★ Worldwide Security Regulation
- ★ Creating a Security-minded Culture
- ★ Communicating Cybersecurity to Senior Leadership Teams



The first and only book devoted to Medical Device Cybersecurity. Available in all the usual places, and cybersecurity book of the year 2020

VELENTIUM

chris.gates@velentium.com

greenlight guru