Compliance v. Completeness

A Case Study on SBOMs in Consideration of FDA Premarket Cybersecurity Guidance

Logan Kostick, Michael Rushanan, Tushar Jois

Cybersecurity in Healthcare Workshop 2025 (HealthSec '25) - December 9th, 2025

Cybersecurity Bill of Materials (CBOM) – a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities.

FDA replaces cybersecurity guidance for medical devices, again

Regulatory News | 30 June 2025 | Emily Hayes

Charting FDA's Course: SBOM as the North Star in Cy

"(A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and

"(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;

"(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components; and

Framing Software Component Transparency: Establishing a Software Bill of Materials (SBOM)

Second Edition

TIA Multistakeholder Process on Software Component Transparency
Working Group

3. Software Bill [illegible] Section 524B(b)(3))

Section 524B(b)(3) of the FD&C Act requires manufact[illegible] devices to provide an SBOM, including commercial, open-source, and off-the-shelf softwa[illegible] components. To assist with complying with this requirement, we recommend that a cyber device provide SBOMs that contain the information recommended in Section V.A.4.b.

FDA Medical Device Security SBOMs: While Great, Don't Rely On Them Alone

By Christian Espinosa, Forbes Councils Member.
for Forbes Technology Council, COUNCIL POST | Membership (fee-based)

Published Aug 19, 2024, 08:45am EDT

What is an SBOM?

What is an SBOM?

Software Bill of Materials

"… a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships" [Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)]

Why?

Provide traceability and visibility of the components used to build our ever increasing software stacks

SBOM Composition

NTIA Base Attributes

Author Name

Timestamp

Supplier Name

Component Name

Version String

Component Hash

Unique Identifier

Relationship

Level of Support

End-of-Support Date

Formats

CycloneDX

Developed and maintained by the OWASP Foundation

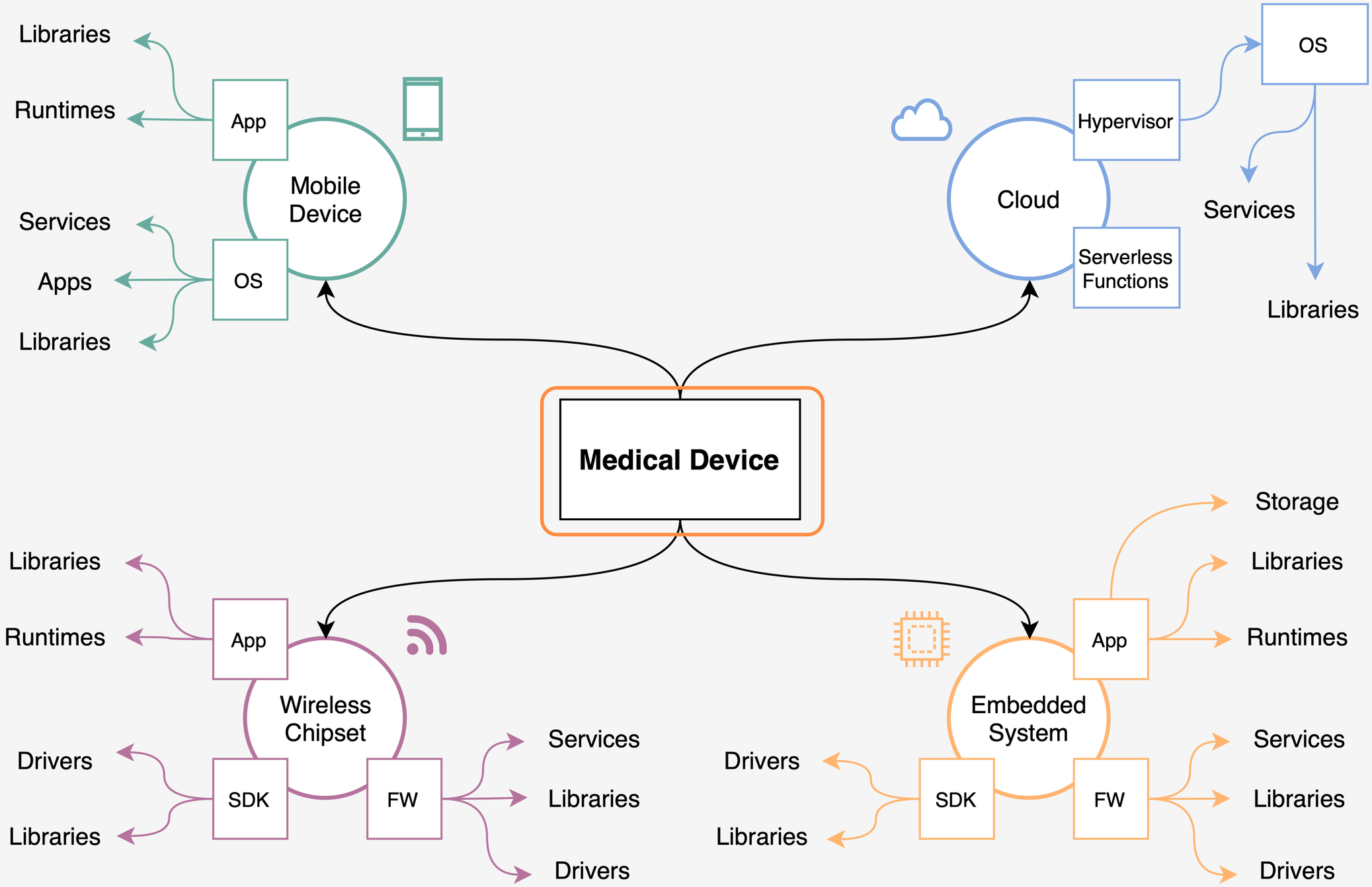
SPDX (Software Package Data Exchange)

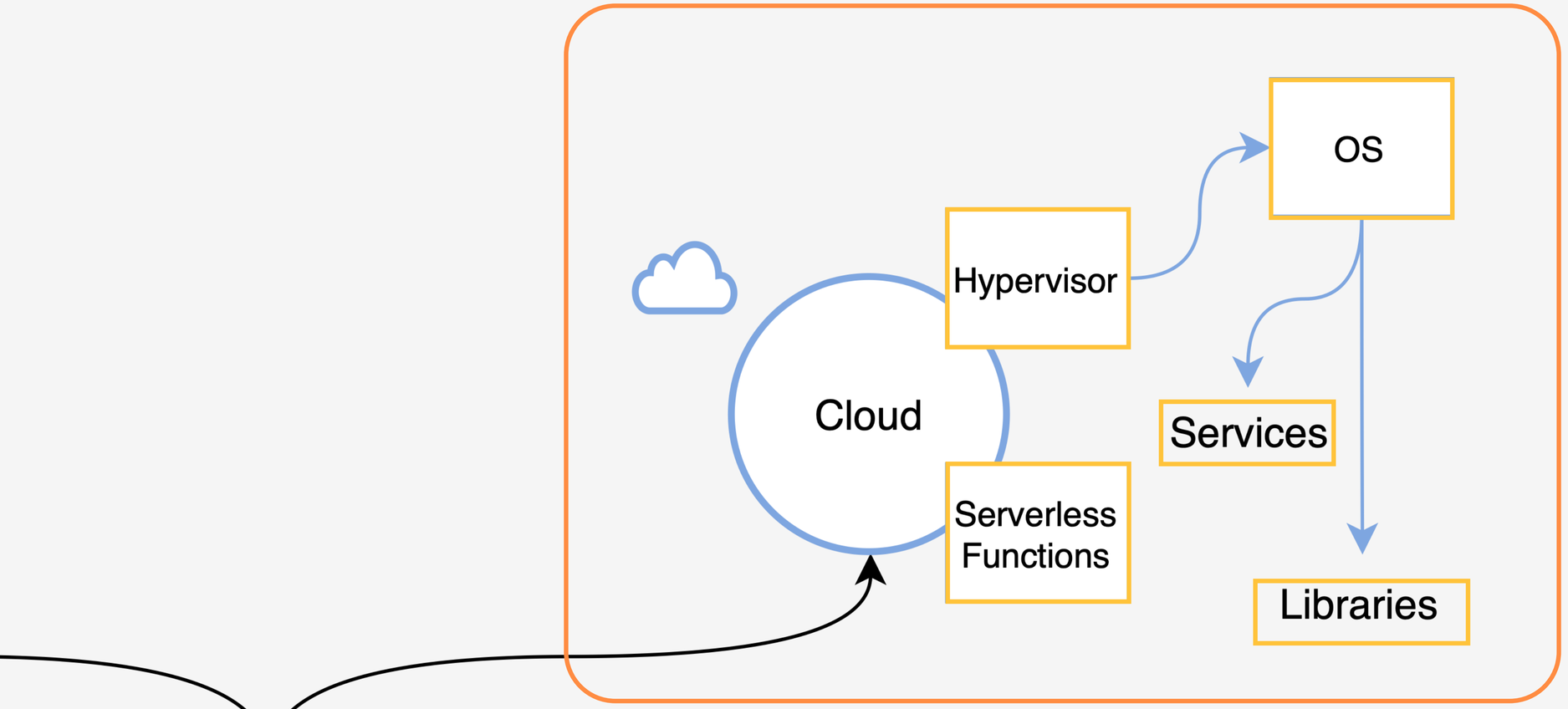
Developed and maintained by the Linux Foundation

SWID (Software Identification) Tag

ISO-defined standard

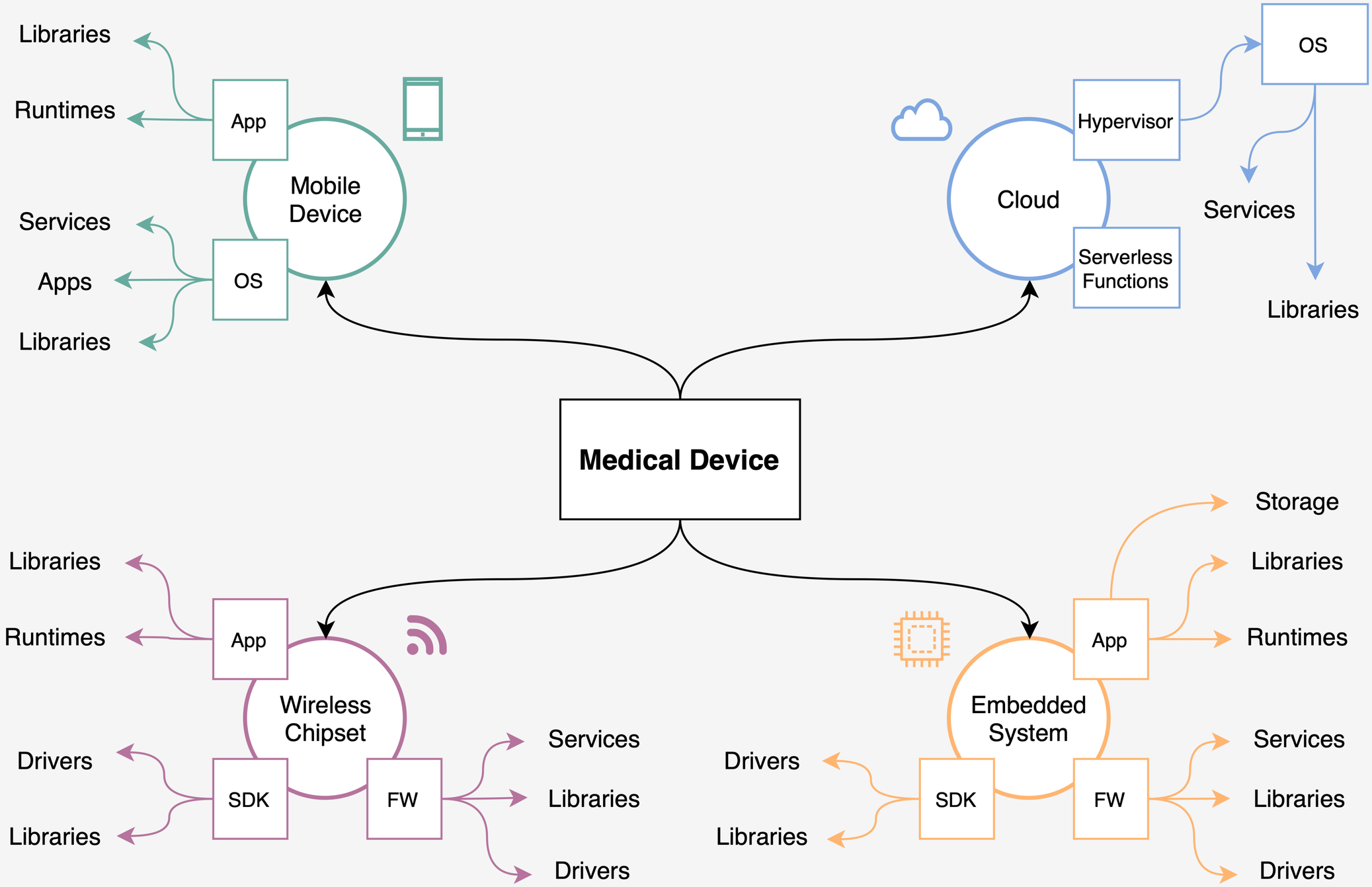
Spreadsheets?


Libraries
Runtimes
App
Mobile Device
Services
Apps
OS
Libraries
Cloud
Hypervisor
OS
Services
Serverless Functions
Libraries
Medical Device
Libraries
Runtimes
App
Wireless Chipset
Drivers
SDK
FW
Libraries
Services
Libraries
Drivers
Storage
Libraries
Runtimes
App
Embedded System
Drivers
SDK
FW
Libraries
Services
Libraries
Drivers



Medical Device

Storage


Libraries
Runtimes
App
Mobile Device
Services
Apps
OS
Libraries
Hypervisor
OS
Cloud
Services
Serverless Functions
Libraries
Medical Device
Libraries
Runtimes
App
Wireless Chipset
Drivers
SDK
FW
Libraries
Services
Libraries
Drivers
Storage
Libraries
Runtimes
App
Embedded System
Drivers
SDK
FW
Libraries
Services
Libraries
Drivers

FDA Guidance

FD&C Guidance Section 524B (Consolidated Appropriations Act, 2023)

- Calls out the need for a “software bill of materials”

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (June 2025)

- Descriptive guidance, points to NTIA as the baseline

Goal: Identify risk in the premarket submission and use the SBOM for monitoring postmarket.

Case Study

Methodology

Used a real medical device submitted to the FDA for review

- The submission included full scope of components (extended SBOM)

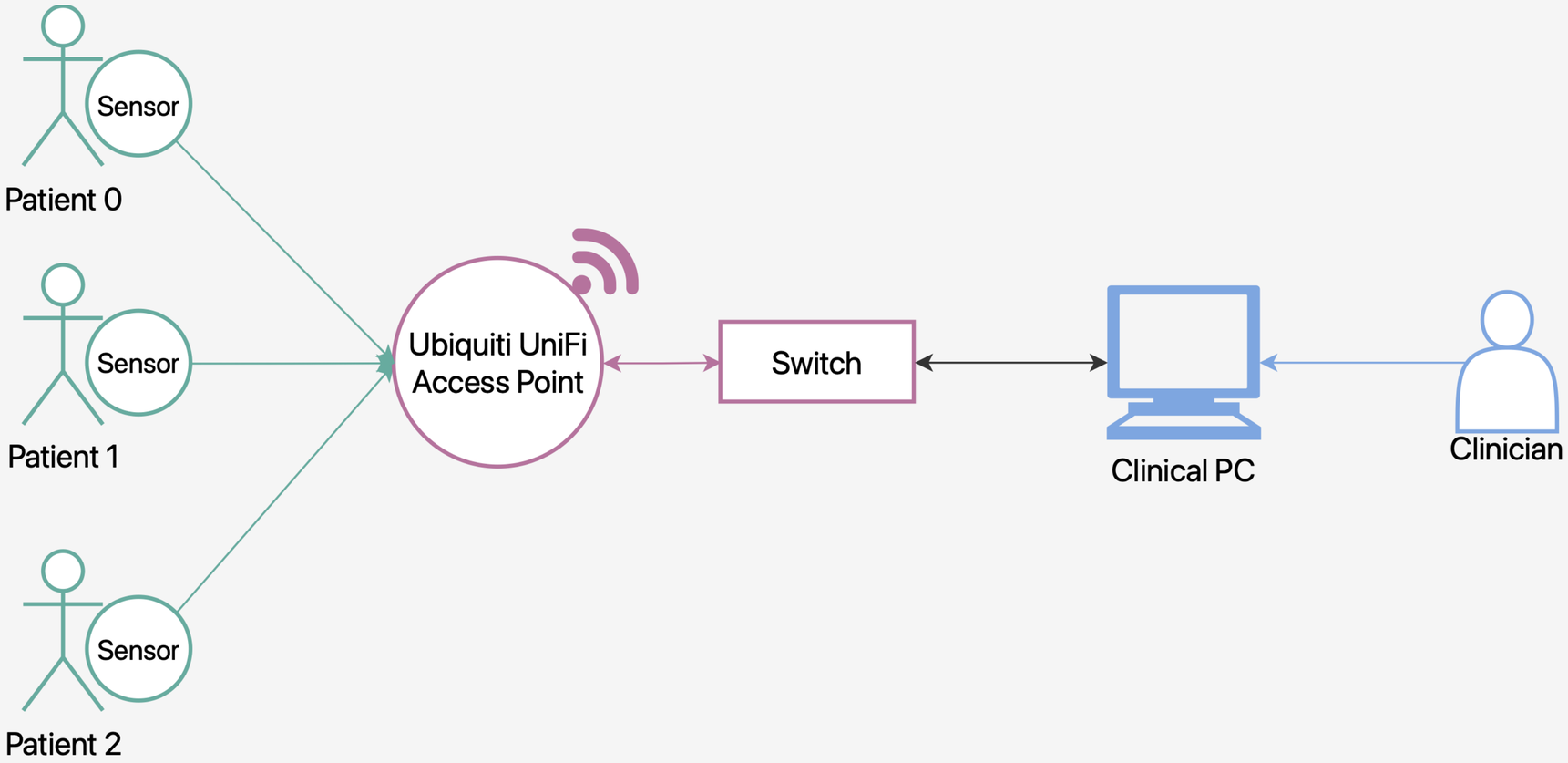
SBOM Anonymization

- Script to remove manufacturer information (deidentify)

Vulnerability Analysis

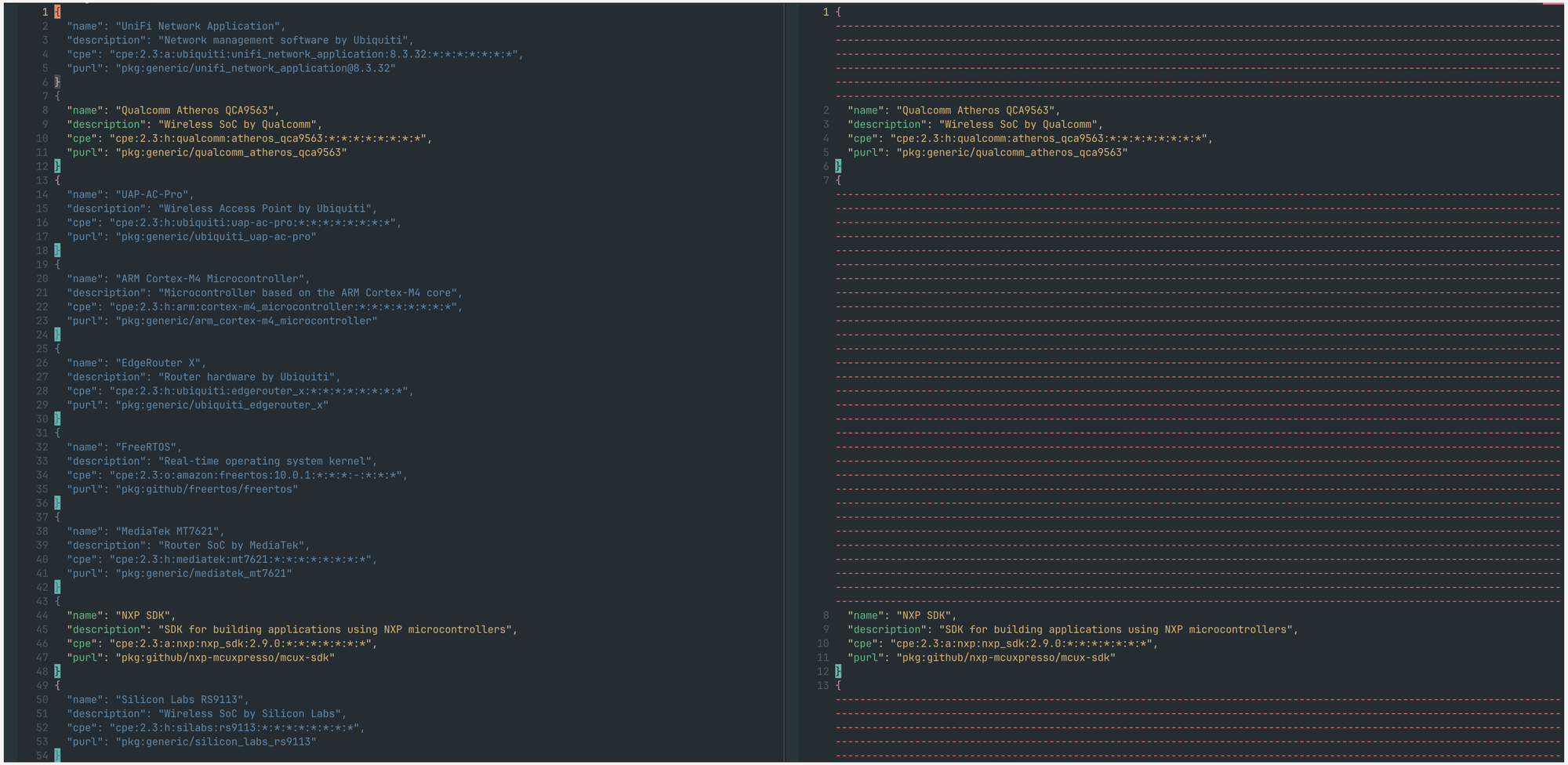
- OWASP Dependency Track and manual research of hardware and OTS components

The Device


Sensor
Patient 0
Sensor
Patient 1
Sensor
Patient 2
Ubiquiti UniFi
Access Point
Switch
Clinical PC
Clinician

Case Study

The Differences

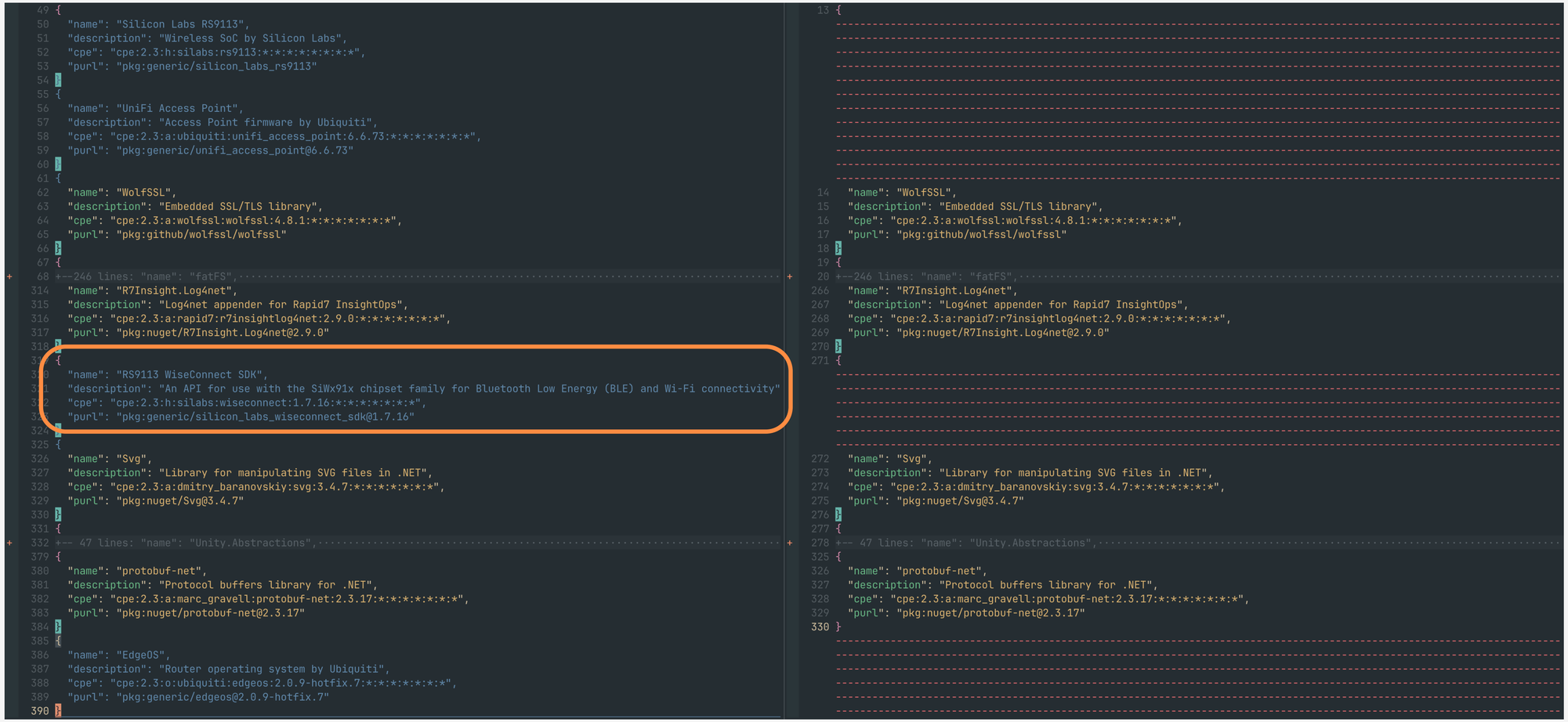


```
{
  "name": "UniFi Network Application",
  "description": "Network management software by Ubiquiti",
  "cpe": "cpe:2.3:a:ubiquiti:unifi_network_application:8.3.32:*:*:*:*:*:*:*",
  "purl": "pkg:generic/unifi_network_application@8.3.32"
}
{
  "name": "Qualcomm Atheros QCA9563",
  "description": "Wireless SoC by Qualcomm",
  "cpe": "cpe:2.3:h:qualcomm:atheros_qca9563:*:*:*:*:*:*:*:*",
  "purl": "pkg:generic/qualcomm_atheros_qca9563"
}
{
  "name": "UAP-AC-Pro",
  "description": "Wireless Access Point by Ubiquiti",
  "cpe": "cpe:2.3:h:ubiquiti:uap-ac-pro:*:*:*:*:*:*:*:*",
  "purl": "pkg:generic/ubiquiti_uap-ac-pro"
}
{
  "name": "ARM Cortex-M4 Microcontroller",
  "description": "Microcontroller based on the ARM Cortex-M4 core",
  "cpe": "cpe:2.3:h:arm:cortex-m4_microcontroller:*:*:*:*:*:*:*:*",
  "purl": "pkg:generic/arm_cortex-m4_microcontroller"
}
{
  "name": "EdgeRouter X",
  "description": "Router hardware by Ubiquiti",
  "cpe": "cpe:2.3:h:ubiquiti:edgerouter_x:*:*:*:*:*:*:*:*",
  "purl": "pkg:generic/ubiquiti_edgerouter_x"
}
{
  "name": "FreeRTOS",
  "description": "Real-time operating system kernel",
  "cpe": "cpe:2.3:o:amazon:freertos:10.0.1:*:*:*:-:*:*:*",
  "purl": "pkg:github/freertos/freertos"
}
{
  "name": "MediaTek MT7621",
  "description": "Router SoC by MediaTek",
  "cpe": "cpe:2.3:h:mediatek:mt7621:*:*:*:*:*:*:*:*",
  "purl": "pkg:generic/mediatek_mt7621"
}
{
  "name": "NXP SDK",
  "description": "SDK for building applications using NXP microcontrollers",
  "cpe": "cpe:2.3:a:nxp:nxp_sdk:2.9.0:*:*:*:*:*:*:*",
  "purl": "pkg:github/nxp-mcuxpresso/mcux-sdk"
}
{
  "name": "Silicon Labs RS9113",
  "description": "Wireless SoC by Silicon Labs",
  "cpe": "cpe:2.3:h:silabs:rs9113:*:*:*:*:*:*:*:*",
  "purl": "pkg:generic/silicon_labs_rs9113"
}
```

```
{
  "name": "Qualcomm Atheros QCA9563",
  "description": "Wireless SoC by Qualcomm",
  "cpe": "cpe:2.3:h:qualcomm:atheros_qca9563:*:*:*:*:*:*:*:*",
  "purl": "pkg:generic/qualcomm_atheros_qca9563"
}
{
  "name": "NXP SDK",
  "description": "SDK for building applications using NXP microcontrollers",
  "cpe": "cpe:2.3:a:nxp:nxp_sdk:2.9.0:*:*:*:*:*:*:*",
  "purl": "pkg:github/nxp-mcuxpresso/mcux-sdk"
}
{
```

Case Study

The Differences



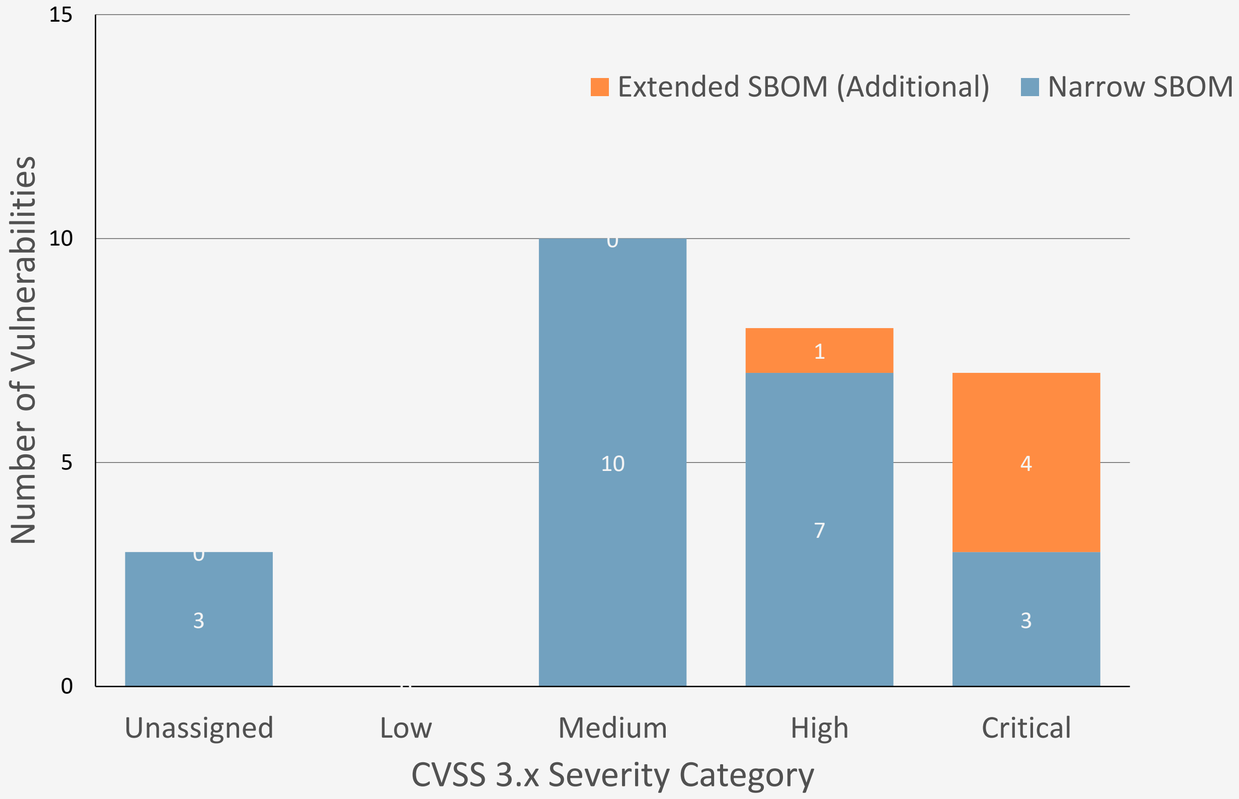
Results

Extended SBOM included 10 additional components — primarily embedded systems

- EdgeRouter X with EdgeOS
- Ubiquiti UniFi Access Point

One CVE found manually

Increased CVE identification by 21%



Discussion

OTS Components

Non-clinicial components can play a key role in functionality e.g. Ubiquiti Access Point

- OTS Components are shipped and sold with the medical device

Treat OTS components as a system within a system-of-systems

Not considering OTS components does not change the risk

Discussion

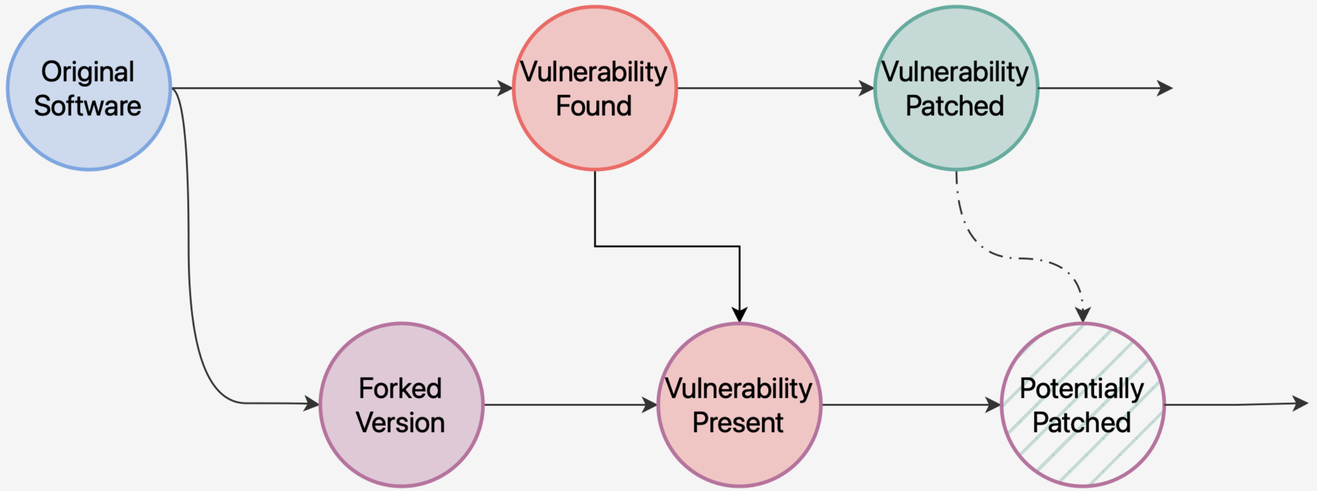
Software Derivatives

Forking and renaming of software creates an issue for traceability

FreeRTOS vs. OPENRTOS — license change but functionality equivalent*

Embedded SDKs fork open source software such as mbedtls

Nordic NRF SDK forks mbedtls with its own library mbedtls-nrf



Need visibility to identify a vulnerability to determine exploitability

Wrapping Up

The Key Players

Industry: FDA compliance does not ensure complete cybersecurity

Regulators: Recommend inclusion of OTS hardware components in submission guidelines.

Academics: A fragmented ecosystem, how can we better understand the landscape?

Healthcare Providers: Ask MDMs about a device's required hardware or infrastructure and cybersecurity risk measures.

Patients: Cybersecurity controls for medical devices impact real people.

Thank you! :)

Contact me!
Logan Kostick
lkostic1@jh.edu, LinkedIn, Bluesky
kostick.dev