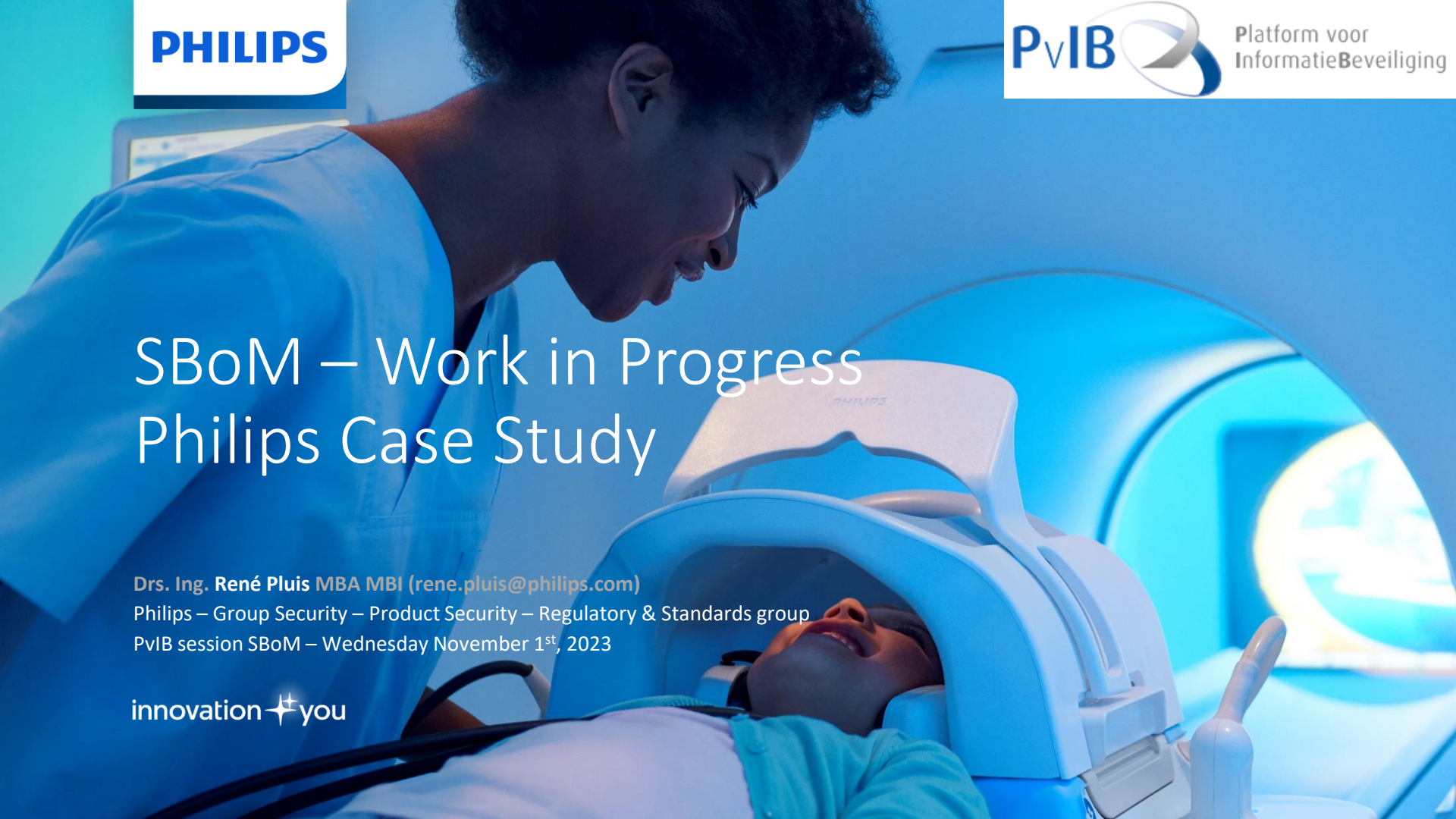


SBoM – Work in Progress
Philips Case Study

Drs. Ing. René Pluis MBA MBI (rene.pluis@philips.com)
Philips – Group Security – Product Security – Regulatory & Standards group
PvIB session SBoM – Wednesday November 1st, 2023

innovation you

1. Introduction to Philips & Healthcare

© Koninklijke Philips N.V.

Philips has reinvented itself many times

Founded on innovation and entrepreneurship

Expanding beyond lighting

Global expansion post-WWII

Diversified industrial conglomerate

Strategic portfolio choices sharpening focus

Our journey continues…

© Koninklijke Philips N.V.

Decades of (medical) innovation

1905
First patent granted

1924
Introduction of Metalix X-ray tube

1927
Acquisition of X-ray firm C.H.F. Müller

1927
First Philips radio with Miniwatt valve

1939
Introduction of rotary electric shaver

1947
First 100kV electron microscope

1950
First Philips TV

1956
First Philips image intensifier with TV

1976
Sono Diagnost B ultrasound

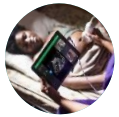
1979
Tomoscan whole-body CT scanner

1983
Gyroscan Nuclear Magnetic Resonance system

1989
Integris, Philips' first dedicated interventional system

2003
Philips Ambient Experience

2013
IQon Spectral CT computed tomography imaging system



2015
Philips Lumify portable ultrasound

2017
Azurion, Philips' next-generation image-guided therapy platform

2018
Philips IntelliSpace Portal

2019
Philips IntelliSite Pathology Solution

2020
Radiology Operations Command Center

2021
Spectral CT 7500

© Koninklijke Philips N.V.

Philips, a born innovator

For over 130 years, we have been improving people's lives with a steady flow of ground-breaking innovations

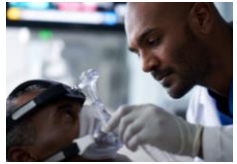
Products come and go ...
Technologies change ...

But Philips is still
about one thing:

Creating meaningful
innovation that improves
people’s lives

© Koninklijke Philips N.V.

We have a strong and focused portfolio driving innovative solutions that promote health and improve healthcare delivery

Diagnosis & Treatment			Connected Care			Personal Health
						
Diagnostic Imaging	**Ultrasound**	**Image Guided Therapy**	**Enterprise Informatics**	**Monitoring**	**Sleep & Respiratory Care**	**Personal Health**
Patient- and staff-centered solutions that simplify workflow and deliver more precise diagnosis and clear pathways with predictable outcomes Uniquely integrating best-in-class imaging with specialized devices to innovate procedures and improve lives			Patient care solutions, advanced analytics and patient and workflow optimization across all care settings Therapies to support patients in their chronic care needs			Products and services to support healthier lifestyles and disease prevention

© Koninklijke Philips N.V.

The future of digital health

Personalized
Care pathways and digital health solutions tailored to the individual

Connected
Healthcare delivered “anytime, anywhere” through a distributed, highly accessible network

Integrated
Care teams can make better informed decisions through 360-degree, longitudinal patient views

© Koninklijke Philips N.V.

2. Introduction SBoM (Software Bill of Materials)

© Koninklijke Philips N.V.

Software Bill of Materials – Why & When

Executive order 14028 – Improving the nations cybersecurity (12-May-2021)

- Office of Management and Budgets (OMB) memo is for software developed after 14-Sep-2022
- This memo mandates that U.S. federal agencies begin obtaining a self-attestation, attesting to conforming to the NIST guidance's as of 13-Jun-2023 (for critical SW)
- This is not a regulation (you can have 510(k) clearance, but can't sell to a US government customer)

Philips program: Executive Order impact

- NIST 800-218 (SSDF - Secure Software Development Framework) for self-attestation
- SBoM (topic for this presentation)

On 29-Dec-2022, U.S. President Biden signed the omnibus bill into law (JRQ121922), includes FDA provisions. For Cybersecurity: sec. 3305, based on the PATCH Act.

- As of 29-Mar-2023 provide the FDA in pre-market submissions a software bill of materials (SBoM)
- As of October 2023, FDA has 'right for refusal' if pre-market submission does not have an SBoM

Other regulations already in effect or will follow (FDA Draft Guidance on Cybersecurity Content of Pre-Market Submissions, Draft EU Cyber Resilience Act (CRA), IMDRF, China - Guidelines for Registration Review of Medical Device Cybersecurity, ..)

© Koninklijke Philips N.V.

AST – Application Security Testing (AST)

Core capabilities offer foundational testing functionality, with most organizations using one or more types, which include:

- **SAST** – Static AST analyzes an application's source, byte or binary code for security vulnerabilities, typically during the programming and/or testing phases of the software development life cycle (SDLC).
- **DAST** – Dynamic AST analyzes applications in their running (i.e., dynamic) state during testing or operational phases. DAST simulates attacks against an application (typically web-enabled applications, but, increasingly, application programming interfaces [APIs] as well), analyzes the application's reactions and, thus, determines whether it is vulnerable.
- **IAST** – Interactive AST instruments a running application (e.g., via the Java Virtual Machine [JVM] or the .NET Common Language Runtime [CLR]) and examines its operation to identify vulnerabilities. Most implementations are considered passive, in that they rely on other application testing to create activity. IAST tools then evaluate.
- **SCA** – Software Composition Analysis is used to identify open-source and, less frequently, commercial components in use in an application. From this, known security vulnerabilities, potential licensing concerns and operational risks can be identified.

Source: 2022 Gartner® Magic Quadrant™ for Application Security Testing
via: The 2020 Gartner Magic Quadrant for Application Security Testing – BMC Software | Blogs

© Koninklijke Philips N.V.

What is in it? Compare ….

What

Who

When

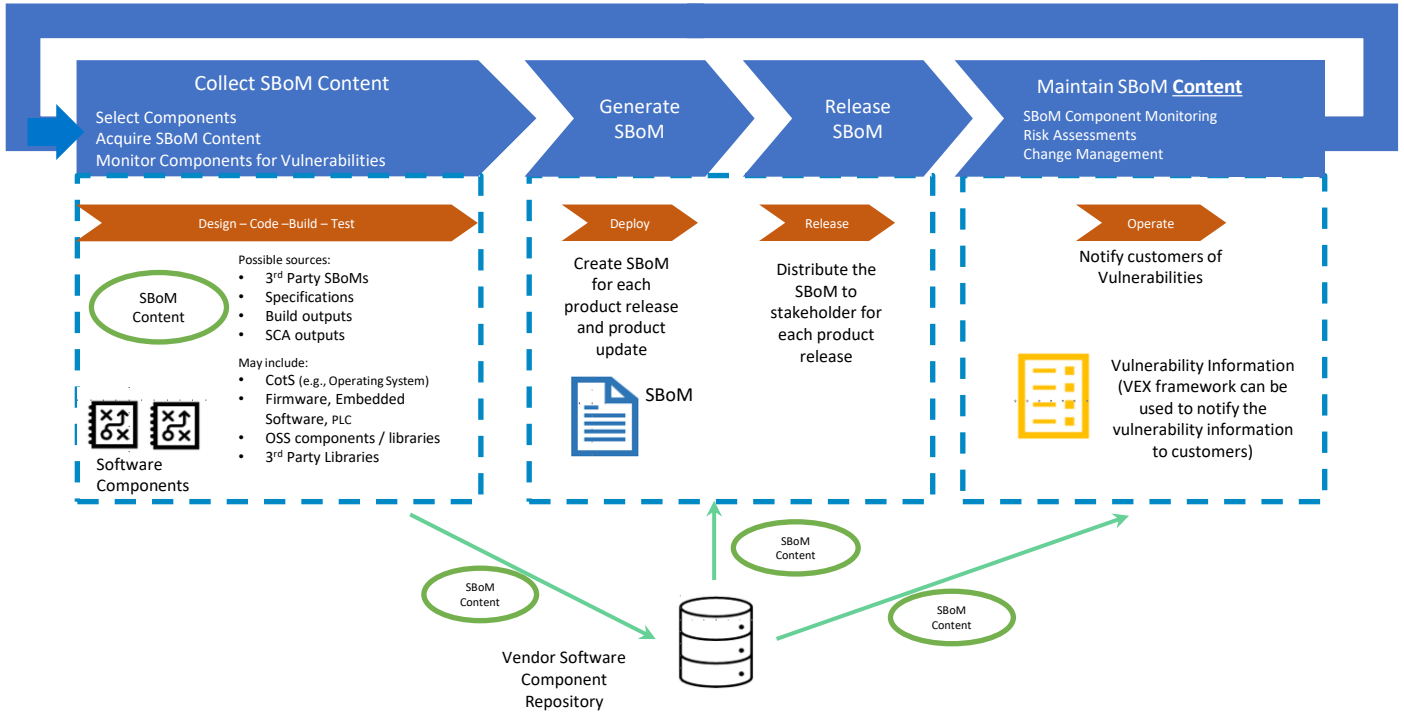
Best before?

May contain …..

SPDXVersion: SPDX-2.3DataLicense: CC0-1.0SPDXID: SPDXRef-DOCUMENT
DocumentName: Poky Core Image
MinimalDocumentNamespace: http://spdx.org/spdxdocs/core-image-minimal.spdx-64a9e982-8070-11ed-9975-9750774c5eb1
Creator: Organization: PhilipsCreator:
Tool: espdx.bbclassCreated: 2022-12-20T14:12:53Z#####
Package: core-image-minimal
PackageName: core-image-minimalSPDXID: SPDX
Ref-core-image-minimalPackageVersion: NOASSERTION
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: falsePackageHomePage: NOASSERTION
PackageSourceInfo: NOASSERTION
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageDescription: NOASSERTION
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-core-image-minimal#####
Package: aclPackageName: aclSPDXID: SPDXRef-acl-2.3.1
PackageVersion: 2.3.1PackageDownloadLocation:
https://download.savannah.gnu.org/releases/acl/acl-2.3.1.tar.gzFilesAnalyzed:
falsePackageHomePage: http://savannah.nongnu.org/projects/acl/PackageSourceInfo:
https://download.savannah.gnu.org/releases/acl/acl-2.3.1.tar.gzPackageLicenseConcluded: LGPL-2.1-or-later AND GPL-2.0-or-later
PackageLicenseDeclared: LGPL-2.1-or-later AND GPL-2.0-or-later

© Koninklijke Philips N.V.

Overview of Manufacturer Considerations (illustration from IMDRF)



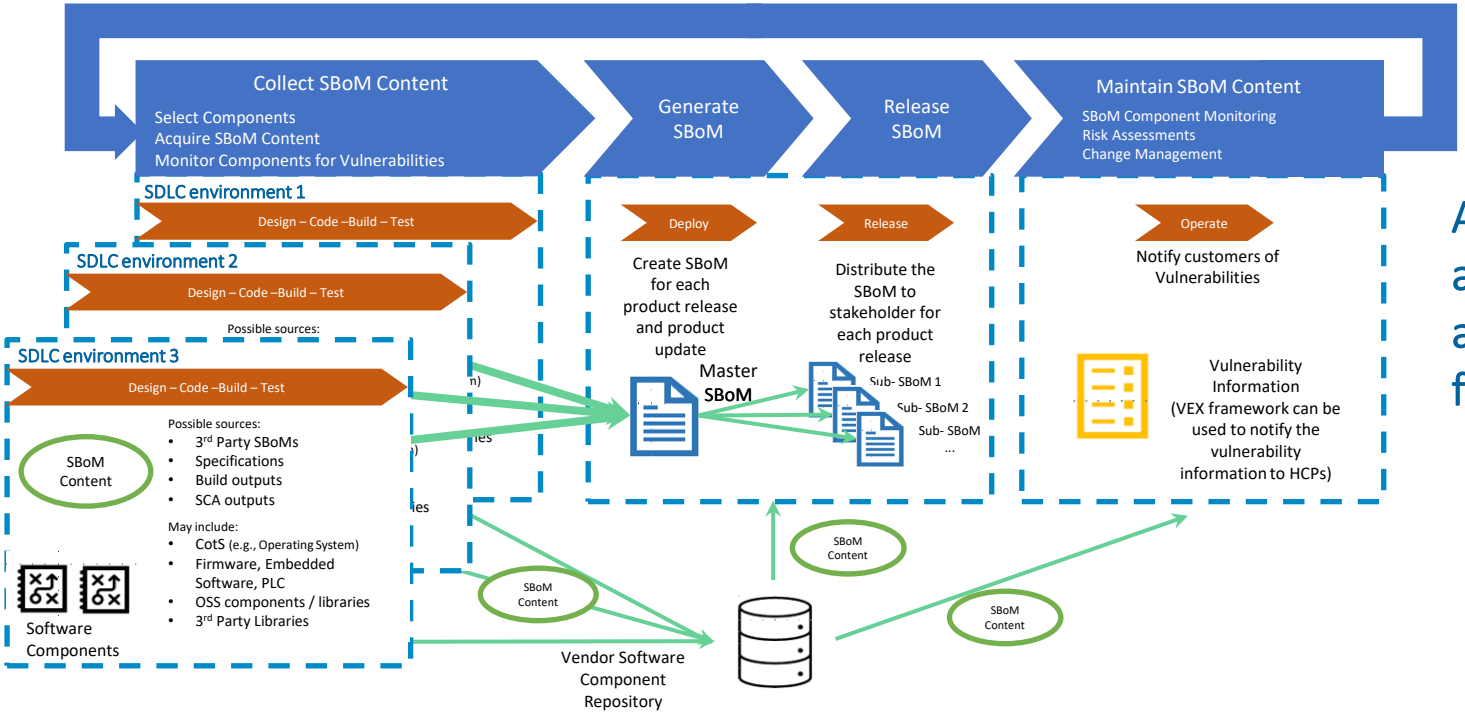
Straight forward SDLC with one development environment

IMDRF International Medical Device Regulators Forum

Source: https://www.imdrf.org/consultations/principles-and-practices-software-bill-materials-medical-device-cybersecurity

© Koninklijke Philips N.V.

Overview of Manufacturer Considerations (illustration from IMDRF)



Alternatives and variations are possible, for instance…

IMDRF International Medical Device Regulators Forum

Source: https://www.imdrf.org/consultations/principles-and-practices-software-bill-materials-medical-device-cybersecurity

© Koninklijke Philips N.V.

3. What makes up an SBoM?

© Koninklijke Philips N.V.

Format and structure SBoM files

An SBoM file is a ‘human readable’ and ‘computer parsable’ file, you should be able to open an SBoM file in for example notepad and see a structure according to some markup scheme (SPDX, CycloneDX, XML [future], …)

There is only ***one*** SBoM file per product which is available to buy. Per SBoM there is only ***one*** product.
(there can be several intermediate SBoMs saved during the CI/CD gates for audit purpose, but these are internal)

Once an SBoM is created, when the product is ready for release, it remains static. Every change in the product will result in a new version of that product and a new separately created SBoM for that product! An SBoM gets ***never*** updated! (It is allowed to correct content of an SBoM but only the meta-data if there is an error).

The use of cryptographic techniques (i.e., hashing for integrity, signing for non-repudiation, confidentiality(?), etc.) is still under discussion at the several standard setting and market specific groups and fora (e.g., CISA, H-ISAC, …).

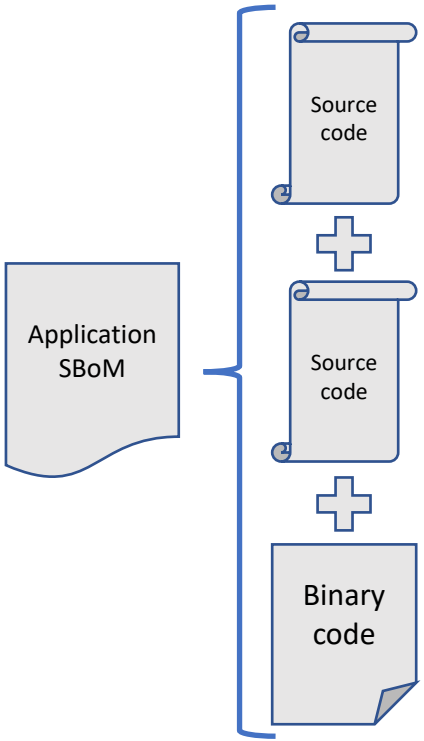
Uniquely naming an SBoM file is still not solved / widely accepted and remains under discussion.

There is no strong binding between product and associated SBoM, trust (but verify?)

© Koninklijke Philips N.V.

Application SBoM

Application



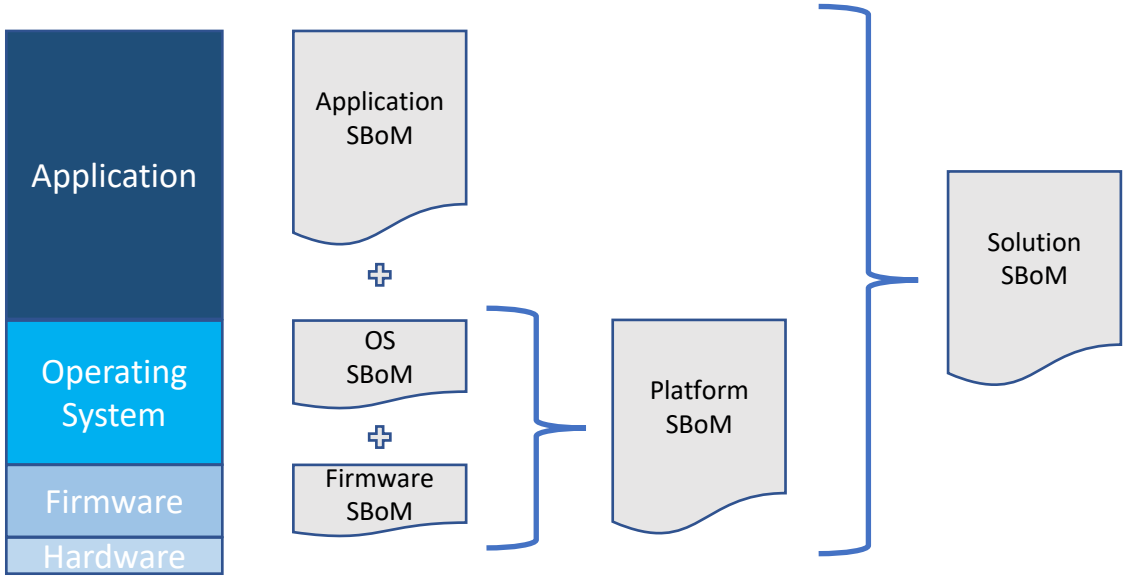
Own developed program statements

OSS program statements

3rd party binaries + SBoM

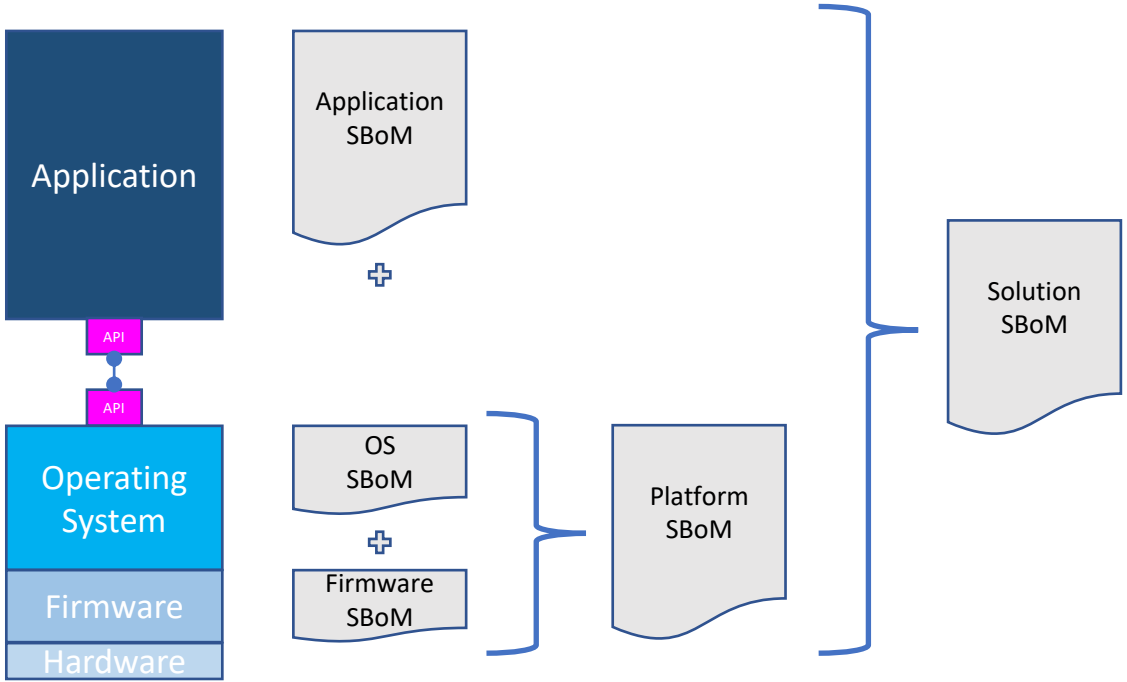
© Koninklijke Philips N.V.

Monolithic system



© Koninklijke Philips N.V.

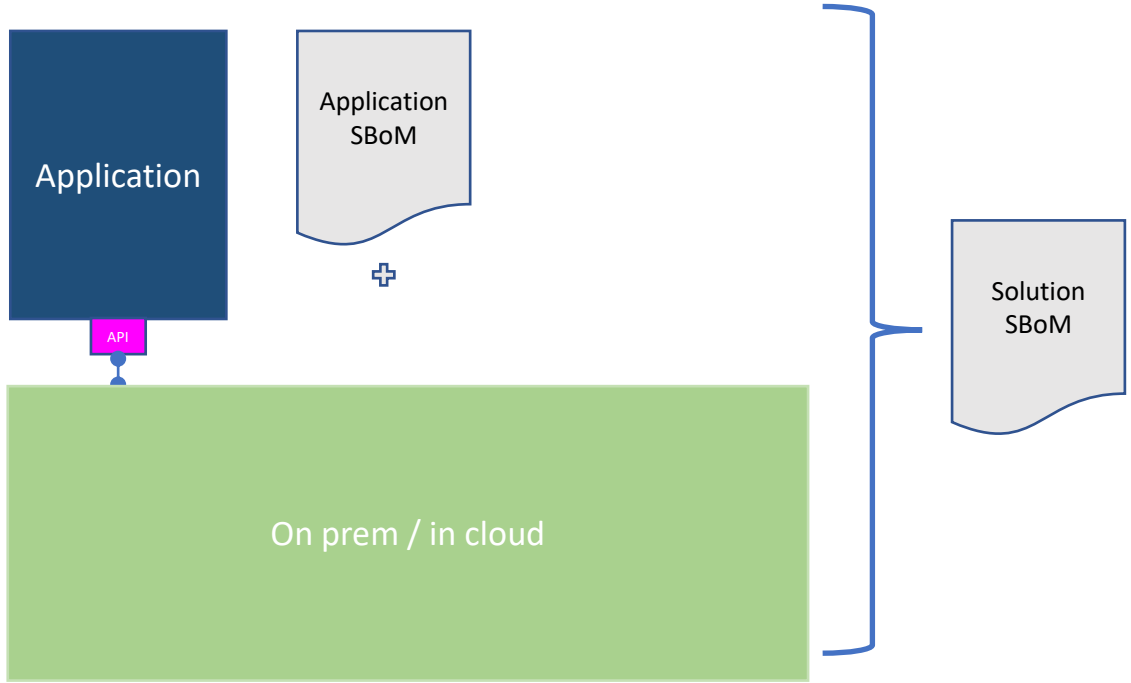
Application de-coupled from platform



(APIs are part of either the application code base or the OS code base)

© Koninklijke Philips N.V.

Application de-coupled from platform

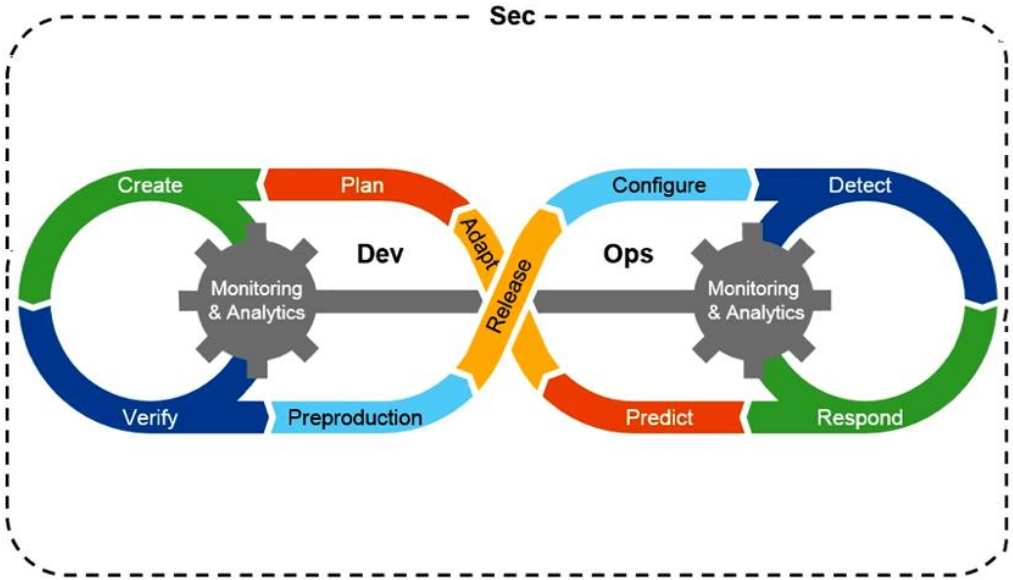


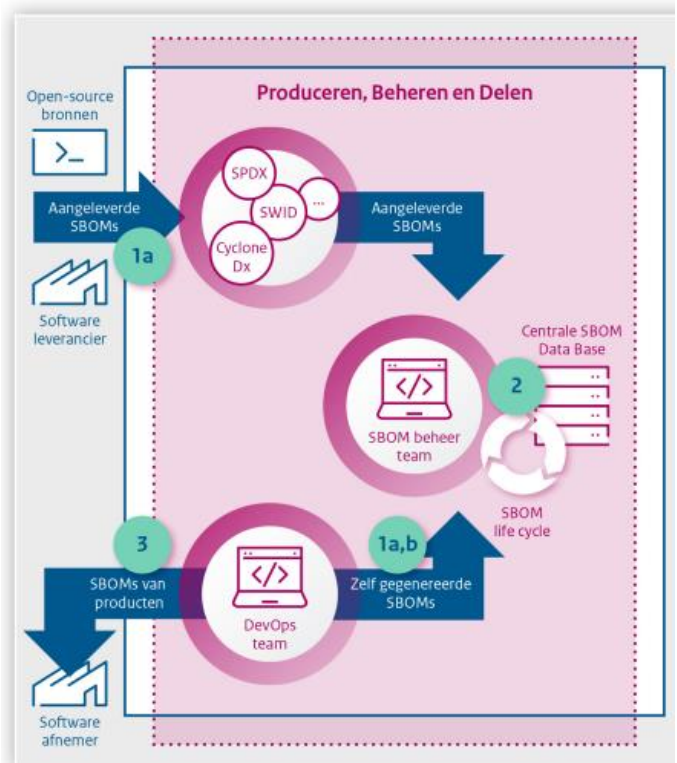
© Koninklijke Philips N.V.

3. Some experiences so far…

© Koninklijke Philips N.V.

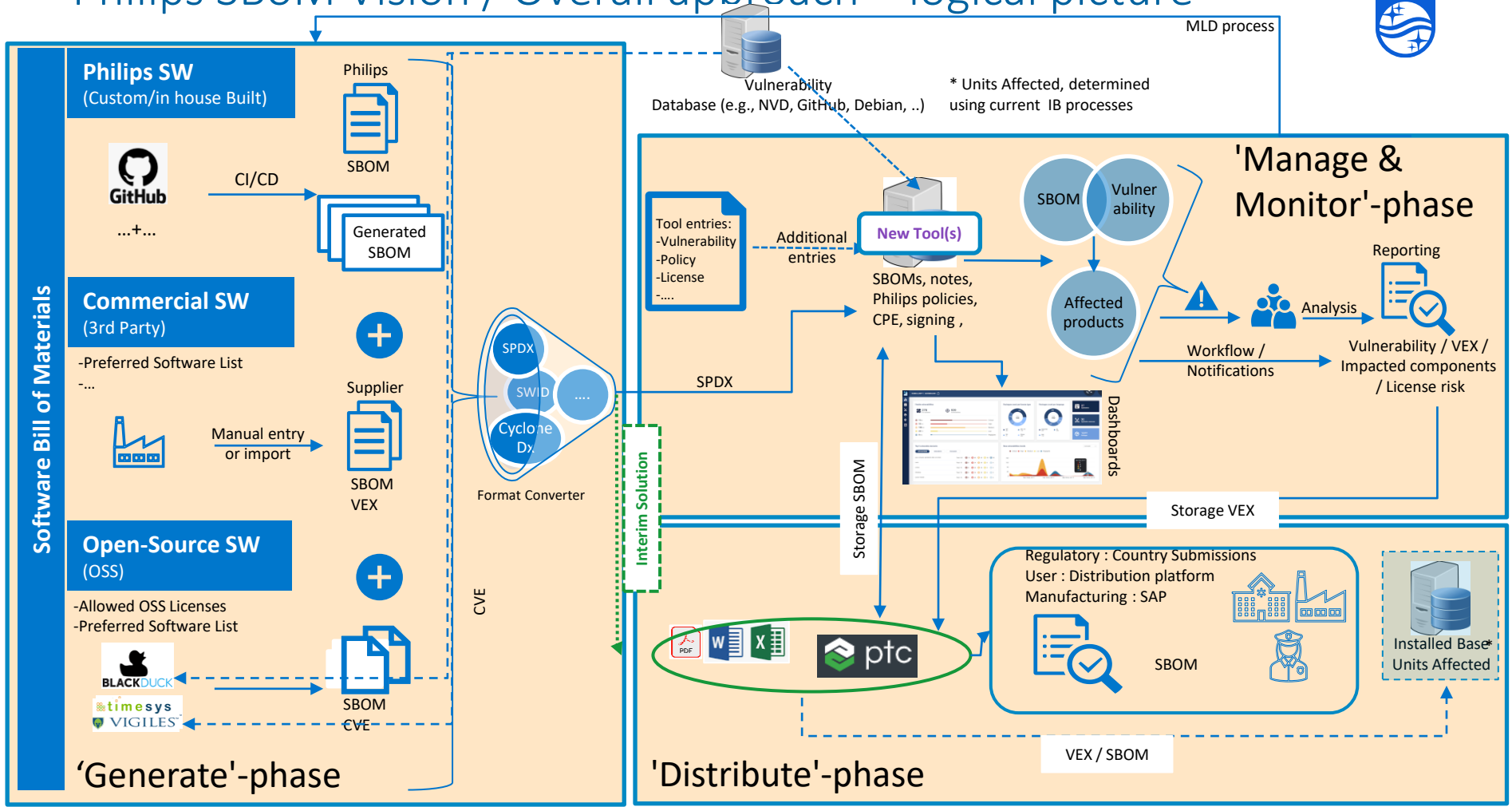
Life cycle DevSecOps – SBoM





© Koninklijke Philips N.V.

Philips SBoM Vision / Overall approach – logical picture



Implementation details…

Philips has roughly 20 business units, each with multiple products

‘Generate’ – phase

- Different environment need different SBoM generation tools
- Import from 3rd party suppliers impose challenges regarding existence, format and content SBoMs / VEX
- OSS relatively well supported but competition going on
- Standardization of formats not done yet (FDA / CISA / H-ISAC / IMDRF / …)

‘Manage & Monitor’ – phase

- How to import from different sources (SBoMs, vulnerability analysis, licenses, export restrictions, whitelists, …)
- How to incorporate feedback from M&M to generate process in different BU’s QMS processes
- How to address queries like ‘which SBoM contains …’, ‘how many versions of same library’, …
- Asset management / installed base (what to do with ‘end of support’ solutions still in production?)

‘Distribute’ – phase

- What if BU does not use designed publication process
- Who has access to what exactly and when?

© Koninklijke Philips N.V.

5. Some difficult questions…

© Koninklijke Philips N.V.

Difficult questions (devil is in the details)…

Are all the developing SBoM standards (SPDX, CycloneDX, …) interchangeable?

When to create what kind off an SBoM?

- See: https://www.cisa.gov/sbom section Types of Software Bill of Materials (SBOM)

What goes into an SBoM and what not?

- → YES: Information about the software components which is in the software packages themselves
- → YES: Meta-data about SBoM file creation itself
- → NO: Vulnerability information (VEX, VRF, CSAF, …) but accompanies SBoM
- → NO: Additional valuable information from commercial processes (End of Sales, country of origin, product version, etc.)

When getting an SBoM from a 3rd party accompanying the binaries….

- How do you verify if it is indeed from that 3rd party and not a roque party?
- How do you the integrity of the content of the SBoM (Hashing – how, what, …)
- How do you verify if content SBoM is matching binaries… and vice versa?

© Koninklijke Philips N.V.

Difficult questions (devil is in the details)… (part deux)

If you use cloud-based software / functions (SaaS, Functions as a Service, …)

- How do you get the correct SBoM for the instance of the application you invoke?
  - Cloud Service Provider provides answer about yes / no vulnerable (and how to verify that)?
  - Full stack collection of all SBoMs in cloud environment?

What and how about sharing vulnerabilities found based on the SBoM information?

- Which format?
  - VEX is not (yet) a standard, no defined content, no defined scheme (there are self proclaimed standards…)
  - CSAF – Common Security Advisory Framework is an OASIS standard since a while

- How to integrate into existing enterprise processes like
  - CVD – Coordinated Vulnerability Disclosure
  - PSIRT – Product Security Incident Response Team
  - RFP – can a potential future customer receive a full working SBoM?

© Koninklijke Philips N.V.

5. Conclusion

© Koninklijke Philips N.V.

THE question you should be able to answer:

Customer:

**“I heard about this new vulnerability in the news.
Are your products in my environment vulnerable for this?”**

Customer should not be interested (from a business point of view) in:

- SBoM contents
- VEX contents

The only thing a customer should be interested in is

**“Am I at risk, and if so,
what can you / I do to protect myself against this risk?”**

© Koninklijke Philips N.V.


PHILIPS