1

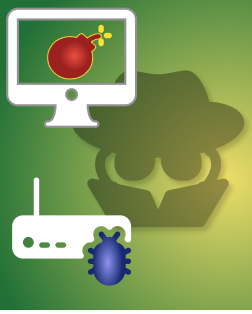
CRA

The problem

- The EU has seen a lot of disruption on the market caused by cybersecurity incidents
- We've seen it too - remember Coop closing stores?
- The costs are too high, the resilience is too low.
- The balance between users and suppliers is not where it should be - manufacturers need to take more responsibility for cybersecurity in software products

2

ENOUGH IS ENOUGH.



Governments around the world wants to shift the balance between software vendors and customers.

Vendors are told to focus on securing their customers and prioritise cyber security higher than new features.

OEJ@EDVINA.NET

3

CRA

Dependencies hurt

- Products are built on a lot of 3rd party software that can have security issues
- Our own software surely have security issues
- Tools we use may have security issues
- We need routines to handle them.

Security bugs in library code affecting many systems

Apache LOG4J™

OpenSSL Cryptography and SSL/TLS Toolkit

Supply chain attack - bad actor injecting code in build system.

solarwinds

4

CRA

Log4j/Log4shell

- Caused a lot of work
- 24/7 task groups
- Numerous manual routines (email, calls)
- Lack of inventory, lack of transparancy
- One incident with very high costs - TO FIND OUT IF SYSTEMS ARE AFFECTED, not only to fix the bug

Short summary

1 Shift responsibility to the manufacturer

EU thinks the customers need better protection for cyber security risks and puts the burden on the manufacturers.

Products needs to be secure by design and secure by default.

info@edvina.net

7

2 Free security updates.

The customer has the right to free security updates during a product's lifetime.

Manufacturers needs to keep users informed about vulnerabilities, exploits and necessary updates.

8

3 EU CE certification for all software

All software sold - standalone or embedded in hardware - will be required to certify for a new CE mark based on cyber security properties.

Customers needs to be able to make an informed choice.

4 Importers and distributors will be liable

Importers and distributors selling software or systems with embedded software on the EU common market will have to make sure products are CE certified.

They have the same responsibility as the manufacturer.

The proposed EU Cyber Resilience Act

5 Securing the software supply chain is mandatory

Software supply chain attacks are on the rise. Development companies needs to secure their software supply chains and work with vendors and Open Source projects to secure the full product from design to release.

The build, test and release process needs to be fully secured, verifiable and documented.

11

What time have we got?

Publication in the official journal
Q3 2024

Vulnerability handling processes

21 months after publication

Fully CE compliant certified products

36 months after publication

"Obligations concering actively exploited vulnerabilities and incidents having an impact on the security of products with digital elements".

12

CRA

What EU is saying:

Manufacturers needs to take security seriously throughout a product's life cycle.

The transition period of 24 months provides a clear direction for R&D investments.

Be transparent on cybersecurity aspects towards customers.

CRA

Which software?

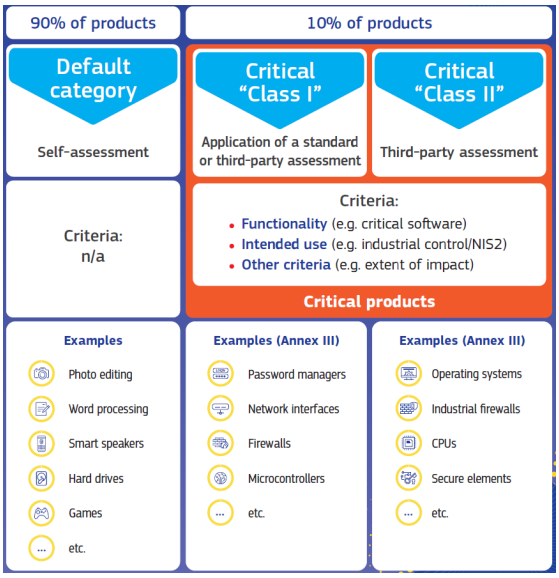
Everything from mobile applications to embedded systems.

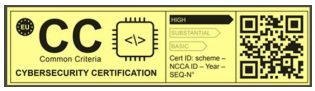
Excluding software-as-a-service with no local components (apps, systems)

Excluding those that have strict rules - like aviation, military, medical systems

CRA

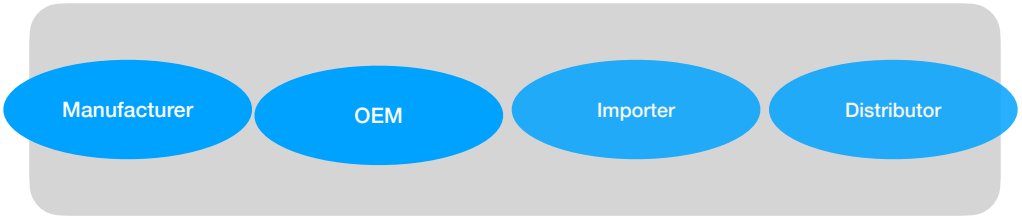
Classification





CRA

Who's responsible?



All are responsible.

CRA

Two phases

Phase one

Manage vulnerabilities

Report exploitable vulnerabilities

Inform customers

Phase one: 12/24 months after regulation. All products (old and new)

Phase two

Prioritise cyber security

Build secure products

Secure the supply chain

Phase two: 24/36 months after regulation. New and updated products.

Self-certification for some product categories, 3rd party certification for others

CE

17

CRA

CRA focus

18

CRA

Customer's insight

Transparency to customers.

SBOM & VEX

Documentation

Vulnerability process

Risk assessment

EU Declaration of conformance

19

CRA

Declaration of conformance

Transparency to customers.

Following the law text

Following any of compliant horisontal standards

Getting certified by a 3rd party

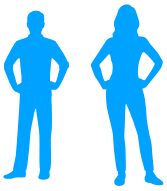
Manufacturing process documentation

Detailed description of product

Risk assessment

Vulnerability process

CE



Customers

20

CRA

Detailed requirements (in commission proposal)

1. Secure by design: → Product shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

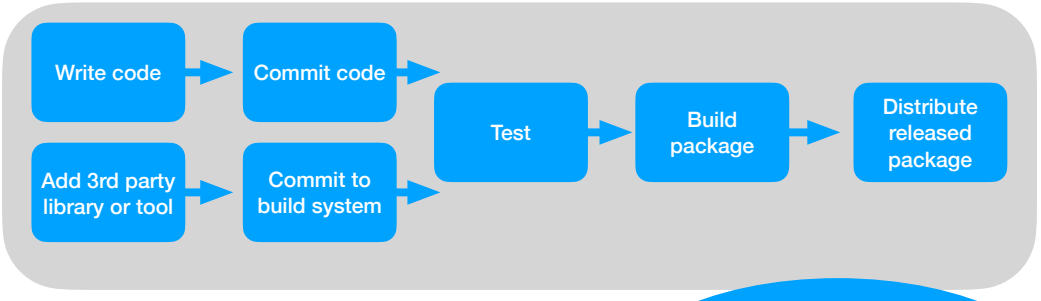
2. Delivered without any known vulnerabilities

3. High level of cybersecurity →

- 3a. Be delivered with a secure by default configuration
- 3b. Ensure protection from unauthorised access
- 3c. Protect confidentiality of stored, transmitted or otherwise processed data.
- 3d. Protect the integrity of stored, trqansmitted or otherwise processed data.
- 3e. Process only data that are adequate, relevant and limited to what is necessary.
- 3f. Protect the availability of essential functions (mitigate DoS attacks)
- 3g. minimise the negative impact of the device for other devices on the same network
- 3h. Be designed, developed and produced to limit attack surfaces
- 3i. Be designed, developed and produced to reduce the impact of an incident
- 3j. Provide security related information by recording and/or monitoring relevant internal activity
- 3k. Ensure that vulnerabilities can be addressed through security updates, including where applicable, through automatic updates

CRA

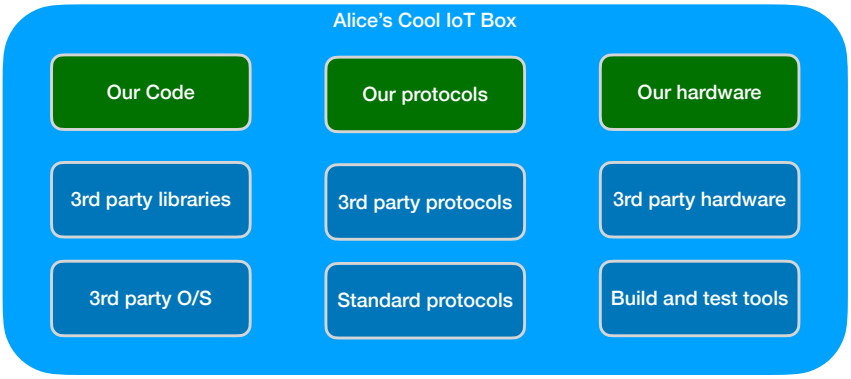
Software Supply chain security is critical



From idea to code to release and installation at customer site.

CRA

All products have many components



90%

Of the code in all software products is estimated to be based on Open Source

CRA

Ignoring CRA will be expensive

3. The non-compliance with the essential cybersecurity requirements laid down in Annex I and the obligations set out in Articles 10 and 11 shall be subject to administrative fines of up to 15 000 000 EUR or, if the offender is an undertaking, up to 2.5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher.

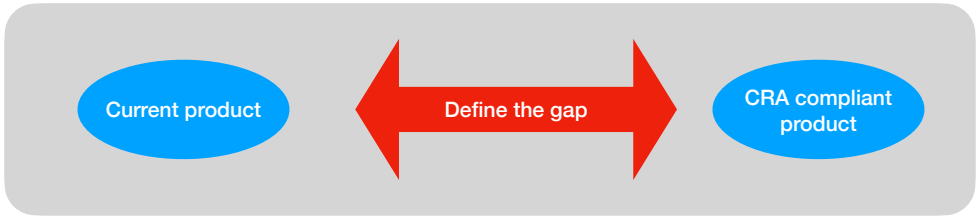
4. The non-compliance with any other obligations under this Regulation shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

5. The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5 000 000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Notice - “2.5% of total worldwide annual turnover” or 15 000 000 EUR

CRA

Short-term To Do list:



Is it possible to make current products compliant?

CRA
EUROPEAN UNION
CYBER
RESILIENCE ACT

Summary

- The new regulation will likely be in place **this year**
- In the first step, manufacturers will have to get **vulnerability handling** in place
- In the second step, products will have to have **security by design** - from creation to destruction
- **Supply chain attacks** are on the raise
- **Cost per dependency** will raise
- Many manufacturers will need a new way of communicating about security and risks with their customers. **Transparency** is required by law.

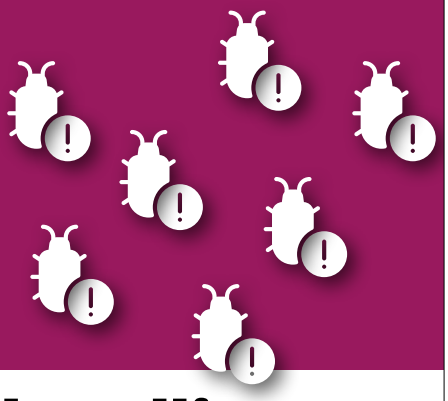
We're all in a hurry. You are likely already late to get your products and organisation in shape.

CRA

Reference

- https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

CRA
EUROPEAN UNION
CYBER
RESILIENCE ACT



Software Vulnerability handling with SBOM

oej 2024-05-21 v3.0

About me

- Open Source developer, consultant, IETF activist and much more
- Lives in Sollentuna, North of Stockholm, Sweden
- Owns the most beautiful dog in the universe
- **I'm lactose intolerant**

29

Buying food stuff.

(E) PASTA DE SÉMOLA DE TRIGO DURO Y PASTA DE SÉMOLA DE TRIGO DURO CON ESPINACAS. Ingredientes: pasta de sémola de **trigo** duro 50% (sémola de **trigo** duro, agua), pasta de sémola de **trigo** duro con espinacas deshidratadas 50% (sémola de **trigo** duro, agua, espinacas deshidratadas (0,9%)). **Puede contener trazas de soja** - Conservar en lugar fresco y seco. 100g PASTA • 1 LITRO de AGUA • 7g de SAL. Echar la sal en el agua hirviendo. Añadir la pasta. Revolver durante el primer minuto de cocción. Tiempo de cocción 6 min. Escurrirla sin eliminar toda el agua. Ver Lote y Consumir preferentemente antes de en alguno de los lados del paquete.
***Formas Especiales para Momentos Especiales.**

(S) PASTA AV DURUMVETE OCH PASTA AV DURUMVETE MED SPENAT. Ingredienser: pasta av **durumvete** 50% (**durumvete**, vatten), pasta av **durumvete** med torkad spenat 50% (**durumvete**, vatten, torkad spenat (0,9%)). **Kan innehålla spår av sojabönor.** Förvaras torrt och svalt. 100g PASTA - 1L. VATTEN - 7g SALT: Tillsätt salt i det kokande vattnet. Lägg i pastan och rör om. Låt koka i 6 minuter. Häll bort vattnet och servera. Konsumentkontakt: Barilla Sverige AB SE-682 82 Filipstad SE 020 - 75 80 81. ***Speciella Former för Speciella Tillfällen.**

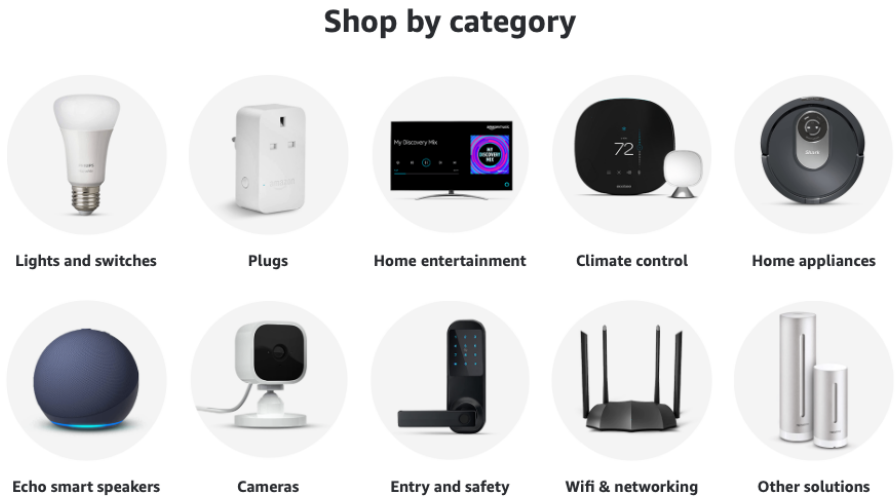
Having to read the small print. Always.

30

I also suffer from CURL allergy

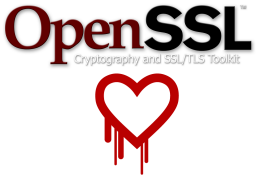
31

So how do I know if there's CURL inside?



32

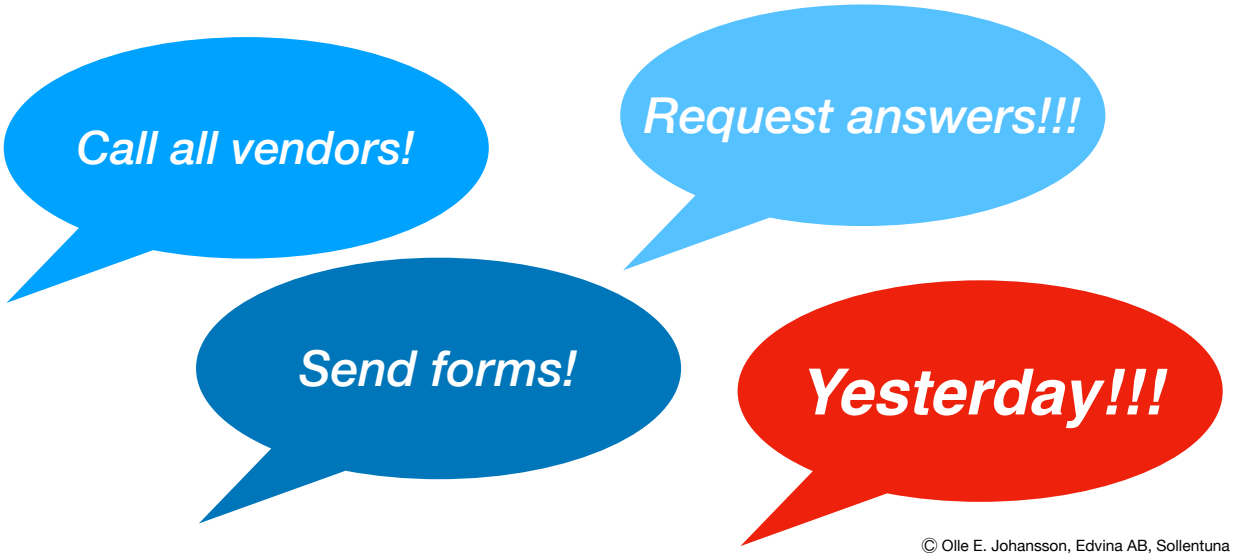
Bad things happen



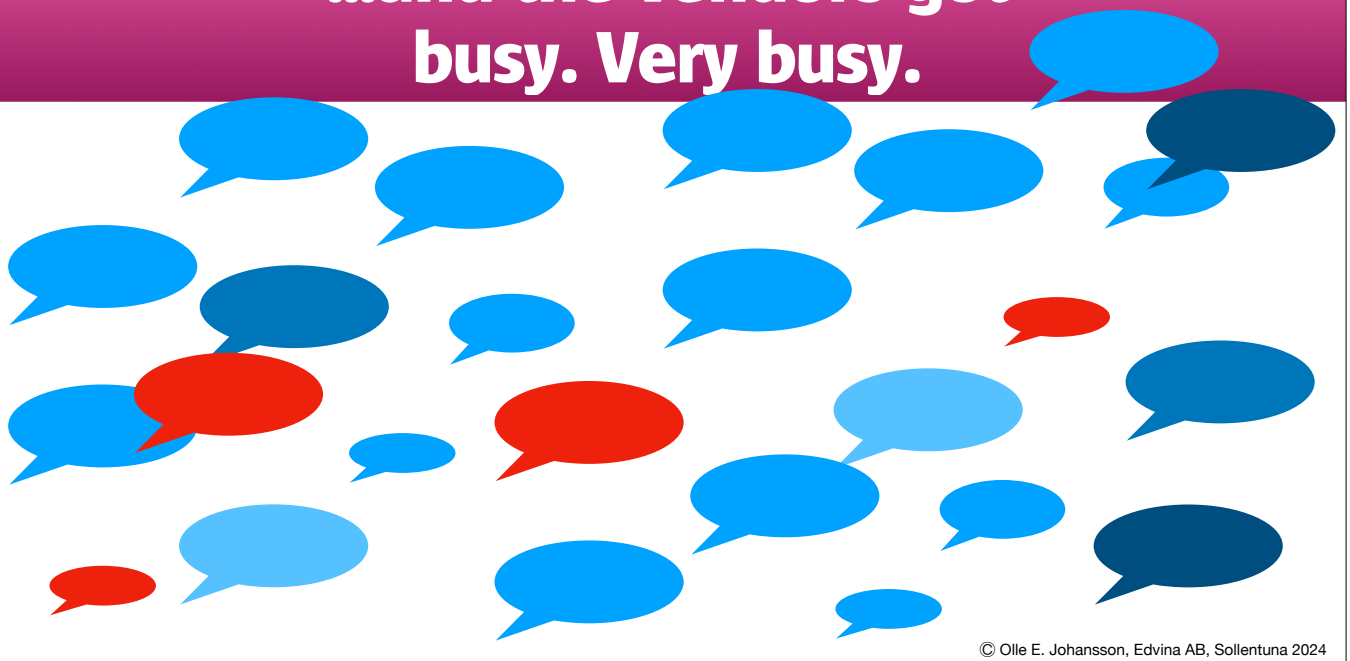
...and the customer becomes worried...

Where in my network do I have the problem?

...and the customer went looking...



...and the vendors got busy. Very busy.

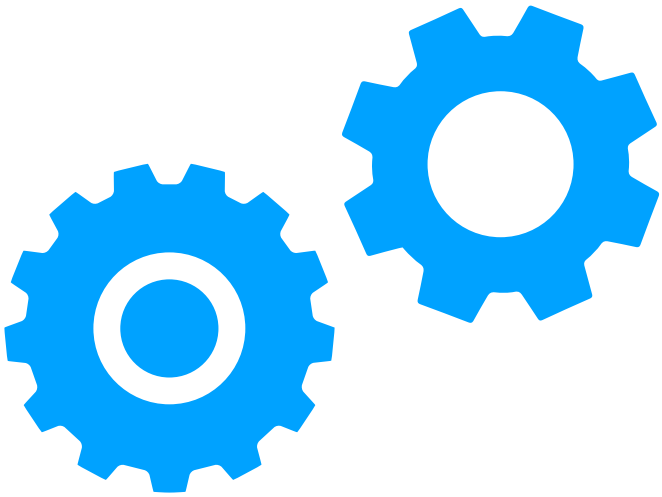


The problem

As a **customer** I want to be able to know **where** vulnerable components exist in my infrastructure.

As a **vendor** I want to know **where** vulnerable components exists in my products and build systems and fix them if needed.

Conclusion: We need to automate!



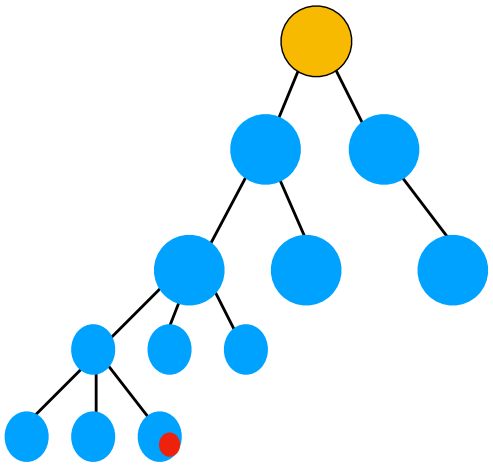
Tools are coming our way

Standardised data formats	Scanners of software	Scanners of containers
Vulnerability detection systems	3rd party assessment of Open Source	Commit signing solutions
Protocols are missing	Document management	Attestation creation, signing and management.

CRA

Critical tool: The SBOM

- **Software Bill of Materials**
- SBOM is a digitally signed file listing all components, their licenses, version and origin
- Used to track vulnerabilities
- Two main formats: SPDX, CycloneDX
- Many usages, not only vulnerability and license handling



CRA

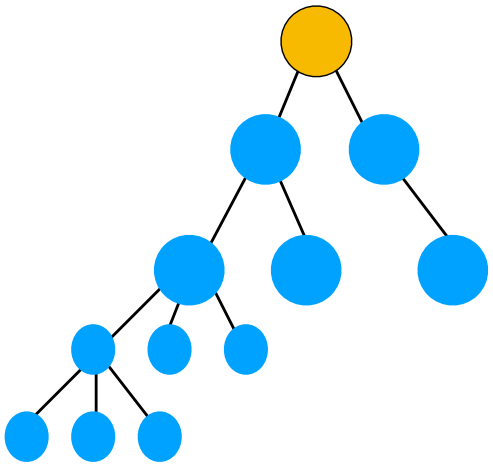
Types of SBOM (CISA)

DESIGN	SOURCE	BUILD	ANALYZED	DEPLOYED	RUNTIME
• SBOM of intented, planned software project or product with included components (some of which may not yet exist) for a new software artifact • Typically derived from design specification, RFC or initial concept.	• SBOM created directly from development environment • Source files, tools	• SBOM generated as part of the process of building the software • Source files, dependencies, build tools	• SBOM generated from analysis of artifacts • Executable, packages, containers, VMs	• SBOM generated from analysis of a system • Based on inventory of the system, using the configuration files and examination of execution	• SBOM generated through instrumenting the system running the software • Captures only the components present in the system, loaded and executing in memory as well as external calls or dynamically loaded components

SOURCE: https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf

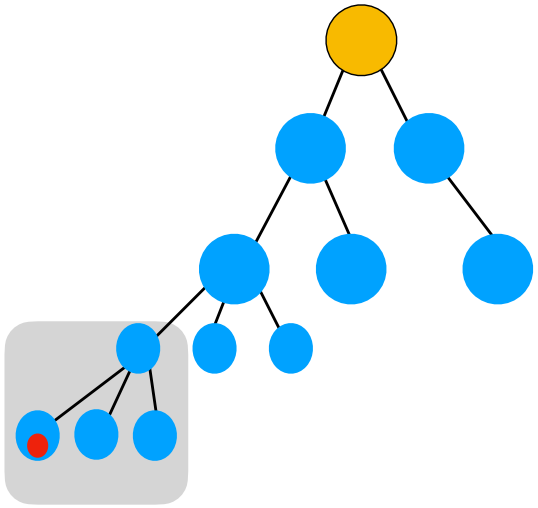
The external SBOM

- **The external SBOM is what you deliver downstream - to the users**
- This is something digitally signed
- It is **fixed for one specific version** of your software and changes only in the next release
- It includes all upstream SBOMs



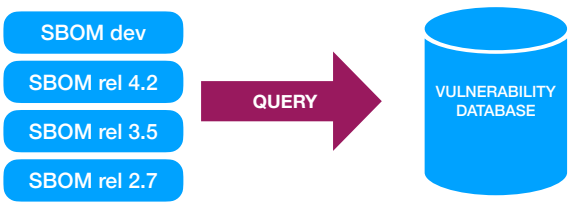
SBOM from upstream vendors

- How are you getting SBOMs from upstream?
- Do you want to expose them to customers? Do you have to?
- Who handles the vulnerabilities and how?
- Remember: Hardware modules often have firmware with dependencies.



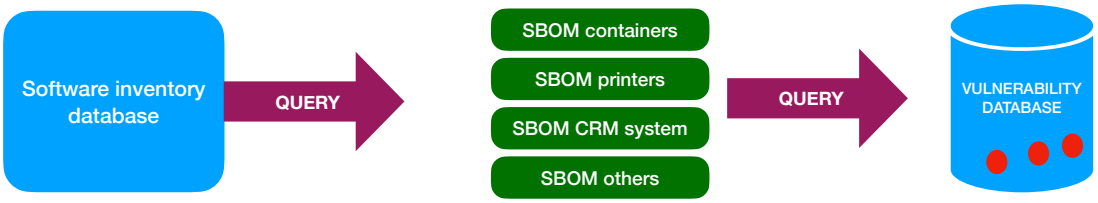
Finding vulnerabilities

- Check all your SBOMs with vulnerability database
- There are both commercial and open source systems for that.



SBOM: Customer control over installed base

- Get SBOMs for software, equipment and other assets with software
- Build an enterprise-wide SBOM database to check for vulnerabilities that can affect operations
- Extend SBOM with priority data - like “Internet facing”, “handling PIR data”, “Customer facing” etc to assist when prioritising which product to focus on when a problem arises.
- *Many enterprise customers will likely require SBOM, regardless of what the law says.*



Meet the SBOM

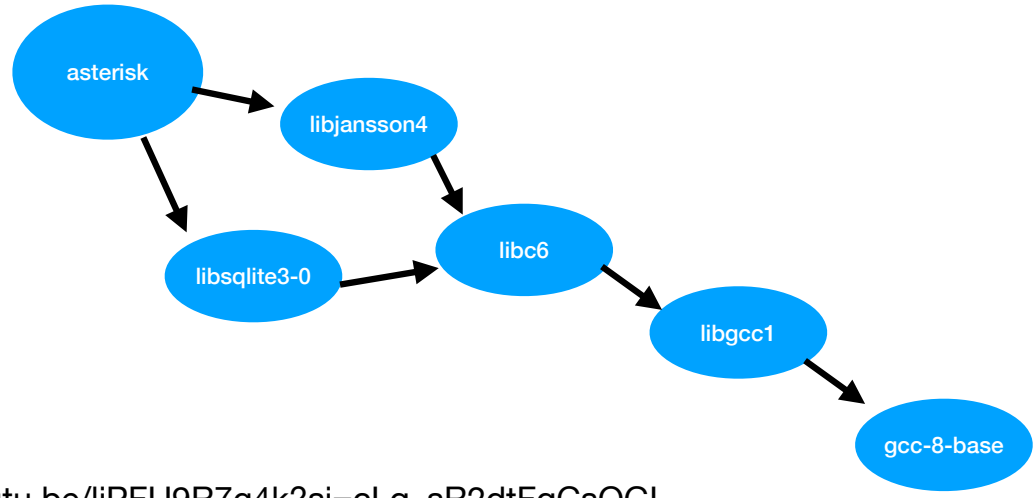
Installed packages in debian

```
$ sudo apt list --installed
Listing... Done
adduser/oldoldstable,now 3.118 all [installed]
apparmor/oldoldstable,now 2.13.2-10 amd64 [installed,automatic]
apt-dater-host/oldoldstable,now 1.0.1-1 all [installed]
apt-listchanges/oldoldstable,now 3.19 all [installed]
apt-utils/oldoldstable,oldoldstable-updates,now 1.8.2.3 amd64 [installed]
apt/oldoldstable,oldoldstable-updates,now 1.8.2.3 amd64 [installed]
asterisk-config/oldoldstable,now 1:16.28.0~dfsg-0+deb10u3 all [installed]
asterisk-core-sounds-en-g722/oldoldstable,now 1.6.1-1 all [installed]
asterisk-core-sounds-en-gsm/oldoldstable,now 1.6.1-1 all [installed]
asterisk-core-sounds-en-wav/oldoldstable,now 1.6.1-1 all [installed]
asterisk-core-sounds-en/oldoldstable,now 1.6.1-1 all [installed]
asterisk-modules/oldoldstable,now 1:16.28.0~dfsg-0+deb10u3 amd64 [installed,automatic]
asterisk-moh-opsound-wav/oldoldstable,now 2.03-1 all [installed]
asterisk-opus/oldoldstable,now 13.7+20171009-2 amd64 [installed]
asterisk/oldoldstable,now 1:16.28.0~dfsg-0+deb10u3 amd64 [installed]
base-files/oldoldstable,now 10.3+deb10u13 amd64 [installed]
```


What about dependencies?

```
 $ sudo apt-cache depends asterisk
asterisk
  Depends: adduser
 |Depends: asterisk-config
  Depends: <asterisk-config-custom>
  Depends: asterisk-core-sounds-en
  Depends: asterisk-modules
  Depends: lsb-base
  Depends: libc6
  Depends: libcap2
  Depends: libedit2
  Depends: libjansson4
  Depends: libpopt0
  Depends: libsqlite3-0
  Depends: libssl1.1
  Depends: libsystemd0
  Depends: liburiparser1
  Depends: libuuid1
  Depends: libxml2
  Depends: libxslt1.1
  Recommends: asterisk-moh-opsound-gsm
```

Let's check two dependencies



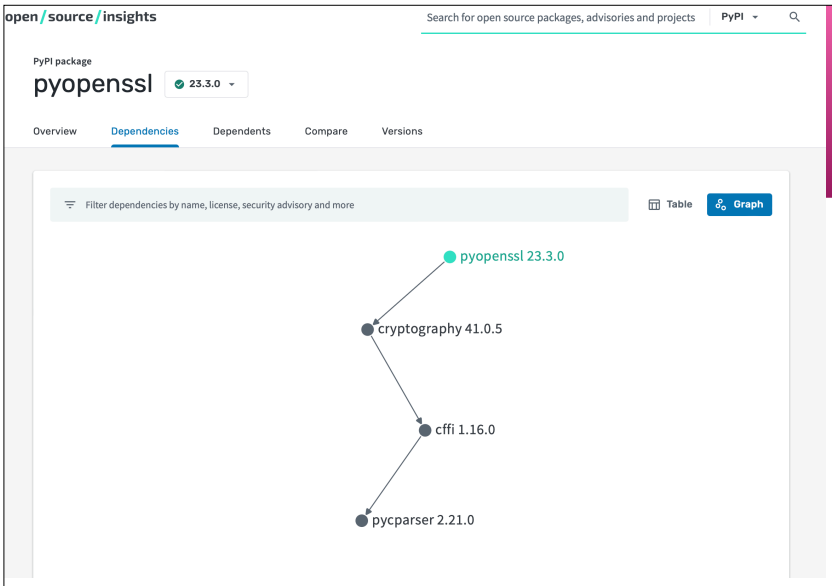
https://youtu.be/liPFU9R7g4k?si=cLq_sR2dtFqCsQGL

Package dependency lists

- Used in npm (javascript), python and other languages
- A list of top-level dependencies
- Every top level component have dependencies

```
24      "Topic :: Security",
25      "Topic :: Security :: Cryptography",
26    ]
27    dependencies = [
28      "appdirs ~= 1.4",
29      "cryptography >= 39",
30      "id >= 1.1.0",
31      "importlib_resources ~= 5.7; python_version < '3.11'",
32      "pydantic >= 2,< 3",
33      "pyjwt >= 2.1",
34      "pyOpenSSL >= 23.0.0",
35      "requests",
36      "securesystemslib",
37      "sigstore-protobuf-specs ~= 0.2.2",
38      "sigstore-rekor-types >= 0.0.11",
39      "tuf >= 2.1,< 4.0",
40    ]
41    requires-python = ">=3.8"
42
```

pyopenssl



I guess it depends on OpenSSL as well…

https://deps.dev/pypi/pyopenssl/23.3.0/dependencies/graph

CISA Minimum requirements on SBOM

- Supplier name
- SBOM Author
- SBOM Timestamp
- Component name
- Dependencies
- Component version
- Component identifiers

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

The name is important

Back to CURL

CURL from github.com
"The original"

CURL in XXX Linux Distro with local patches to improve stuff.

Curl in your Yocto Build

Microsoft CURL

Debian CURL Package

PHP CURL extension

CURL Package with backported fixes in Red Hat Enterprise

If an SBOM says CURL - what is it?

The CVE matching problem (debian)

PURL - package URL

https://github.com/package-url/purl-spec

- **PURL is critical** - a unique URL for the software used
  - *Just a name like “curl” or “nginx” is not enough*
- Will become an OWASP standard project included in the ECMA standardisation
- Part of CVE 5.1 json spec
- A way to specify the provenance of a component

https://github.com/package-url/purl-spec

CRA

SBOM quality

- **SBOM quality** is becoming an issue, as is CVE quality
- For automation, the **product identifiers** need to be exact
- **PURL is critical** - a unique URL for the software used
- Work is going on to build rating systems, quality checkers
- Will likely need manual work to adjust output from scanners

Suggested reading: https://edu.chainguard.dev/open-source/sbom/what-makes-a-good-sbom/

CRA

spdx

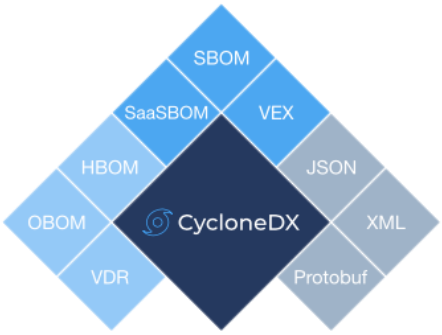
- The Software Package Data Exchange
- An open standard for communicating software bill of material information, including components, licenses, copyrights, and security references
- ISO/IEC 5962:2021
- A Linux Foundation project
- Standardised markers for open source licenses
- Used to scan and build SBOM

https://spdx.dev

CRA

CycloneDX

CycloneDX



OWASP CycloneDX is a full-stack Bill of Materials (BOM) standard that provides advanced supply chain capabilities for cyber risk reduction. The specification supports:

- **Software Bill of Materials (SBOM)**
- Software-as-a-Service Bill of Materials (SaaSBOM)
- Hardware Bill of Materials (HBOM)
- Operations Bill of Materials (OBOM)
- Vulnerability Disclosure Reports (VDR)
- Vulnerability Exploitability eXchange (VEX)
- Cryptography Bill of Materials (CBOM)
- Attestations

Strategic direction of the specification is managed by the CycloneDX Core Working Group, is backed by the OWASP Foundation, and is supported by the global information security community.

https://cyclonedx.org

CycloneDX SBOM overview

https://cyclonedx.org/specification/overview/

Using a scanner to create an SBOM

61

The truth

Your first SBOM produced by a scanner will stink.

62

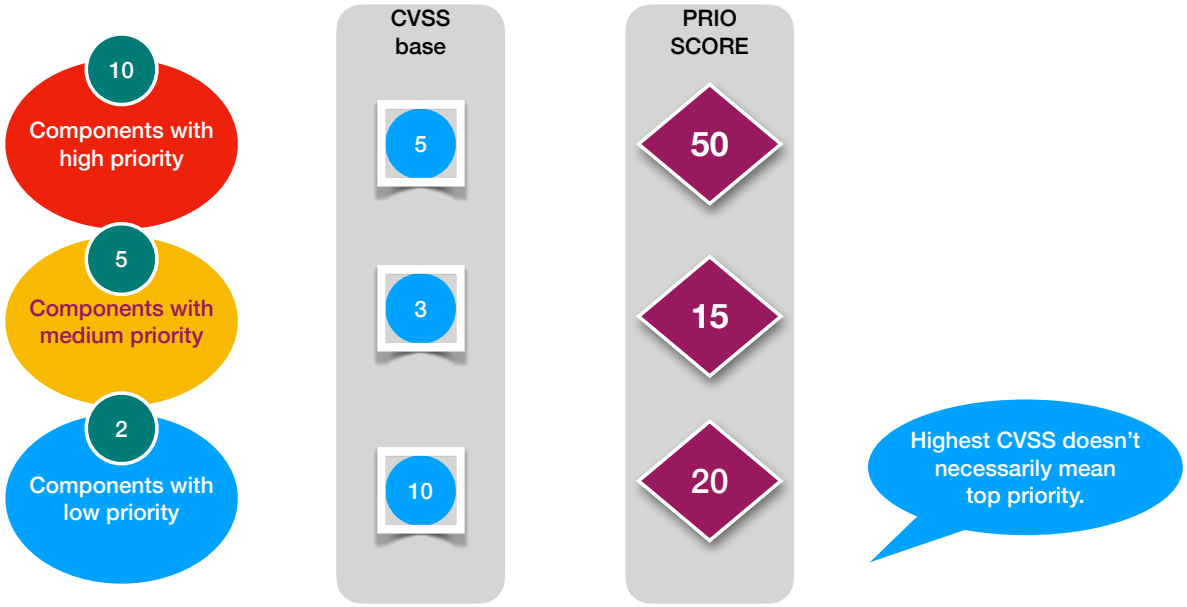
Scanners

- Typically use packaging lists to produce an SBOM
- Some are more advanced
- Many false positives and missing components

Where SBOM fails.

- COMPLETENESS - missing components
- OVER DELIVERY - a lot of artefacts that will never have a CVE filed (i.e. /etc/hosts or docs in /usr/share)
- DEPTH - Doesn’t track dependencies
- OPEN SOURCE LICENSES
- NAMING OF COMPONENTS - which is the worse. Some add multiple guesses of CPEs just in hope that one of them will work

Managing vulnerabilities



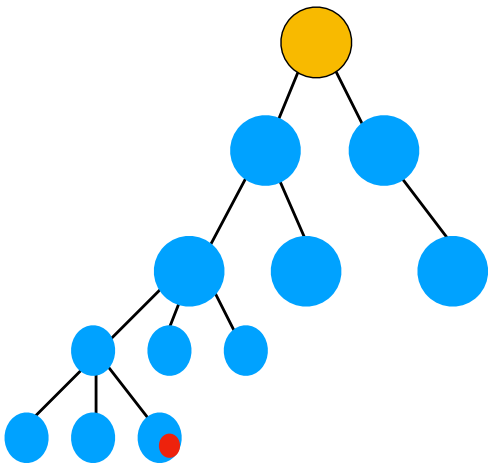
65

VEX

66

CRA

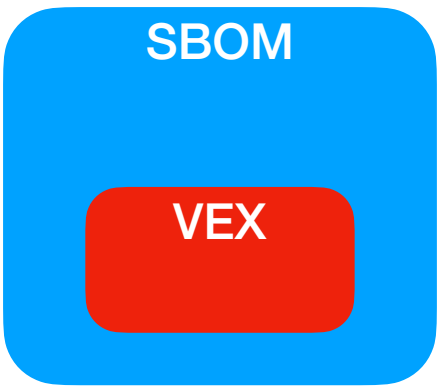
Telling the world how you handle a vulnerability: VEX



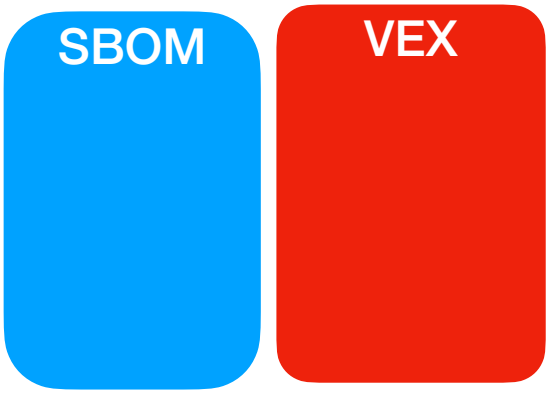
- An SBOM is a list of all ingredients in a software, all components
- This is compared with the NVD, national vulnerabilities database
- A list of known vulnerabilities will be highlighted for your software
- For each of these, you need to create a VEX entry, indicating how you handle this issue
- This will avoid a lot of questions to support…

CRA

VEX is related to your SBOM



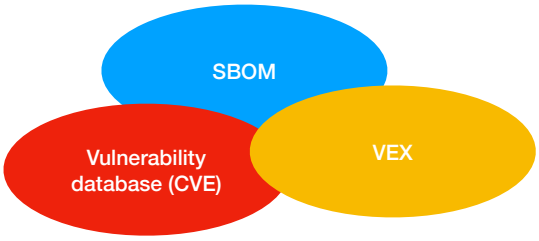
VEX included in SBOM



VEX as separately linked document.

CRA

VEX - vulnerability exploitability exchange



Known, affected

Known, not affected

Under investigation

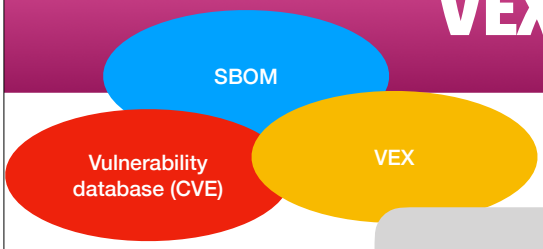
Fixed

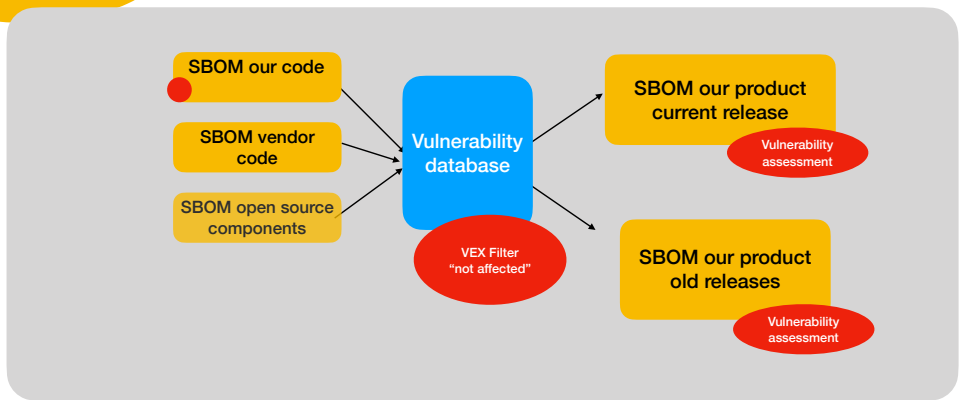
Documenting your assessment internally and externally.

https://cyclonedx.org/capabilities/vex/

CRA

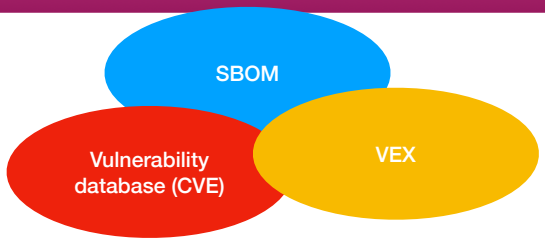
VEX - as a filter

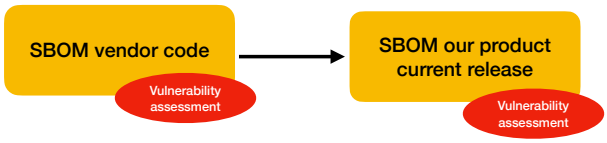




CRA

VEX - needs assessment

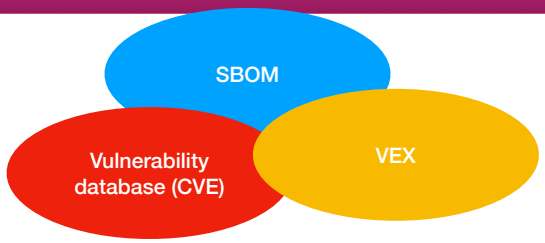




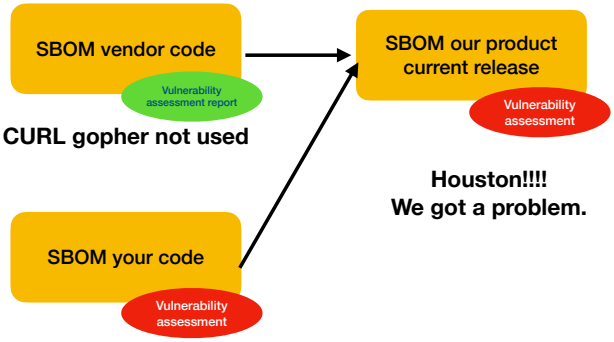
Do you trust your vendor's assessment?

CRA

VEX - complexity



CURL vulnerability in gopher protocol usage.



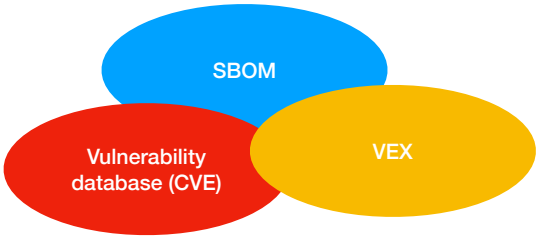
CURL gopher not used

Houston!!!!
We got a problem.

CURL gopher used

CRA

VEX - standards



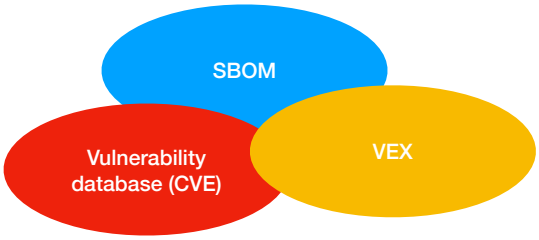
CycloneDX
https://cyclonedx.org/

OpenVex
https://github.com/openvex/spec/blob/main/OPENVEX-SPEC.md

https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf

CRA

VEX - online updates



- VEX updates needs to be available online
- Customers needs to be able to check the current status regurlarly
- Standard APIs for this will likely evolve

FUN?

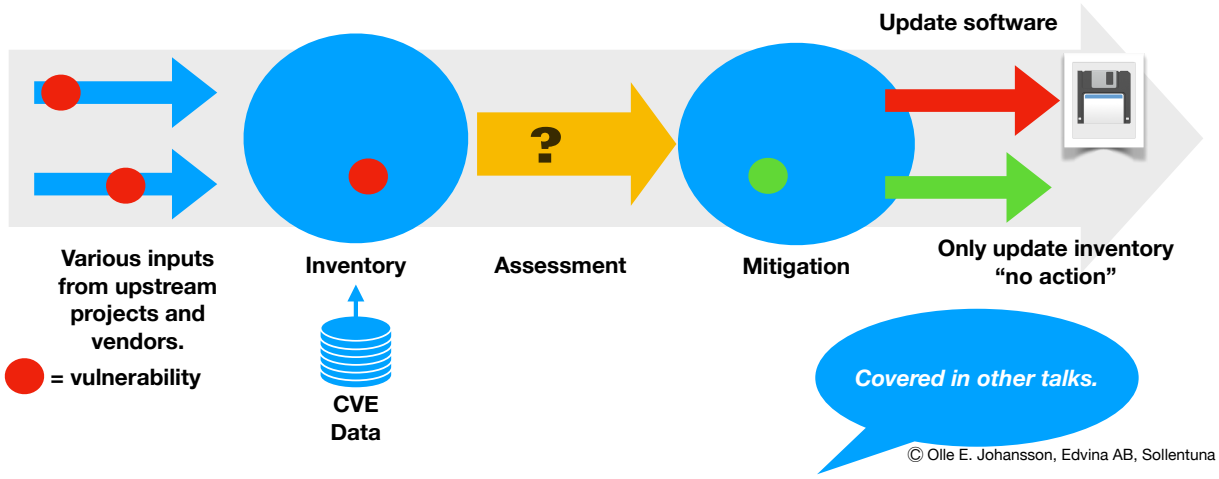
Conclusions

$PROFIT

SBOM is handiwork

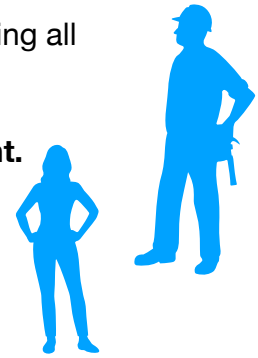
- No scanner will give you a proper SBOM for your product
- The team will have to work with SBOMs in the CI/CD process and make sure the output is correct and useful
- Run multiple scanners - compare with your “baseline” SBOM and monitor changes
- The baseline SBOM for your product is what you use for vulnerability checking
- Don’t forget the BUILD system SBOM

SBOM is at the core of a process



SBOMs are not done yet

- There are cases where the SBOM won't help you today and we're working on it in OWASP CycloneDX and the OWASP SBOM Forum
- It doesn't mean it won't help, but don't rely on it finding all your issues
- **Personal product knowledge still is very important.**



SBOMs are fun

- There are many issues to handle here both internally and externally.
- **It's a new tool that will help us manage our software in a better way, with more automation**
- **Using it correctly, it will lead to more secure software for our customers.**
- **Personally, I like exploring new areas of Technology. For me, it's fun.**

SBOMs are profitable

- Automation lowers cost of management
- Having control of dependencies means lower risk and better planning
- Properly managed and put in production, you will save yourselves from severe CRA fines
- And your customers will be more secure!

Working together

- We need to work together to form the best current practise
- We need to share tools, toolchains end experiences
- We need to work together to asses and mitigate vulnerabilities
- **We need to keep our customers secure while keeping costs under control**

CRA

Thank you! Some pointers

- Slides from various presentations: https://slideshare.net/oej
- Recordings of Dataföreningens lunch seminars: https://www.youtube.com/@securitydinosaur
- Working group for software supply chain security in Cybernode.se: https://cybernode.se/temagrupp-sakra-leveranskedjor-for-programvara-2/
- Nordic Software Security Summit 2024: https://www.dfkompetens.se/utbildning/nordic-software-security-summit-2024/
  - *Contact me directly for speaking opportunities*