

Working group Secure supply chains/Open Source

Meeting 4: 2023-08-23

Agenda (30 minutes)

- Vision & Mission about this work group
- Previous meeting 3: 2023-06-14
- Problem: Open-source community versus CRA
- SBOM in CRA and OPENSSF
- Public, mirrored, rebuilt and modified packages
- Reduce dependency by rebuild (Hardening and Cost Per Dependency)
- Optional demo (8 minutes)
 - Generate tools from product SBOM
 - Hardening of lighttpd Alpine package
- Questions
- Post Meeting (52 minutes)

About our work group

About the group

Innovation depends on openness and cooperation, therefore the focus on open source in supply chains. Vulnerabilities such as Log4j and the escalation of cyber-attacks have sparked initiatives in both the US and Europe to improve security. The group will share knowledge and also analyze supply chain related topics on a global scale such as the EU Cyber Resilience Act (CRA) and OpenSSF.

Ongoing work

The <https://bomresolver.io> has been published by a member in Cybernode as open source. The resolver is an innovative solution that backtracks a software supply chain for the Alpine ecosystem. The <https://nosad.se> is a forum for Swedish authorities for sharing data and knowledge about open source. In addition to complete rebuild in isolation, the resolver is also capable of distributing revenues generated by providing compliance evidence. The goal is to have **continuous** and granular **funding** of open source projects in the software supply chain

Previous meeting 2023-06-14

- Swedish government website migrated to Kubernetes (<https://nosad.se>)
- Static content and large Kubernetes cluster for DDOS resilience
- Static content may sound simple but
 - Let us focus on SBOM and CRA
 - Serving of static content is still important for software distribution
 - DDOS attacks against update services may impact vulnerability handling
- <https://dl-cdn.alpinelinux.org/alpine/>
 - dl => Download
 - cdn => Content Delivery Network
- Supply chains currently limited to microservice, alpine, lighttpd and Kubernetes
- Important to work together with OpenSSF, KTH, other centers in ECCO etc

CRA PROBLEM

[Software to benefit businesses, innovators, public interest \(europa.eu\)](https://europa.eu)

“Open source offers great advantages in a domain where the EU can have a leading role. (CRA ????)

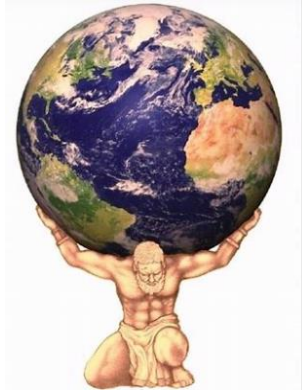


We are sorry.

Due to the EU Cyber Resilience Act
we can not deliver to the EU market.
The product is not available.

[EU cyber-resilience act \(europa.eu\)](https://europa.eu)

Funding Problem (openssl)



[Used widely on internet-facing devices](#)

[Om eSam - eSamverka](#)

Projektets bidragsgivare av källkod bör vara flera personer, [undvik enmansprojekt.](#)

[http://veridicalsystems.com/blog/\(2014\)](http://veridicalsystems.com/blog/(2014))

Hundreds of thousands of lines of very complex code, with every line of code you touch visible to the world, knowing that code is used by banks, firewalls, weapons systems, web sites, smart phones, industry, government, everywhere. Knowing that you'll be ignored and unappreciated until something goes wrong.

There should be at least a half dozen full time OpenSSL team members, not just one,

I'm getting old and weary and I'd like to retire someday.

The mystery is not that a few overworked volunteers missed this bug; the mystery is why it hasn't happened more often.

investment in OpenSSL would be a no-brainer.

Funding openssl 2023



Current sponsors 57



\$ 10



a month

Select

You'll receive any rewards listed in the \$10 monthly tier. Additionally, a Public Sponsor achievement will be added to your profile.

\$5 a month

Select

Thank you for sponsoring us. You can choose to have a badge on your profile showing your support or remain anonymous.

\$10 a month

Select

This is the same as the minimum tier but with a higher monthly amount for those who would like to contribute a little more.

\$20 a month

Select

This is the same as the minimum tier but with a higher monthly amount for those who would like to contribute a little more.

\$400 a month

Select

At this level you may be eligible to be a Bronze Sponsor. Please contact us for further information.

<https://www.openssl.org/support/acks.html>

<https://github.com/aapooksman/certmitm>

Links about CRA

[Update on the European Cyber Resilience Act - YouTube](#)

[2023.07 Members Meeting European Cyber Resilience Act \(hubspotusercontent-na1.net\)](#)

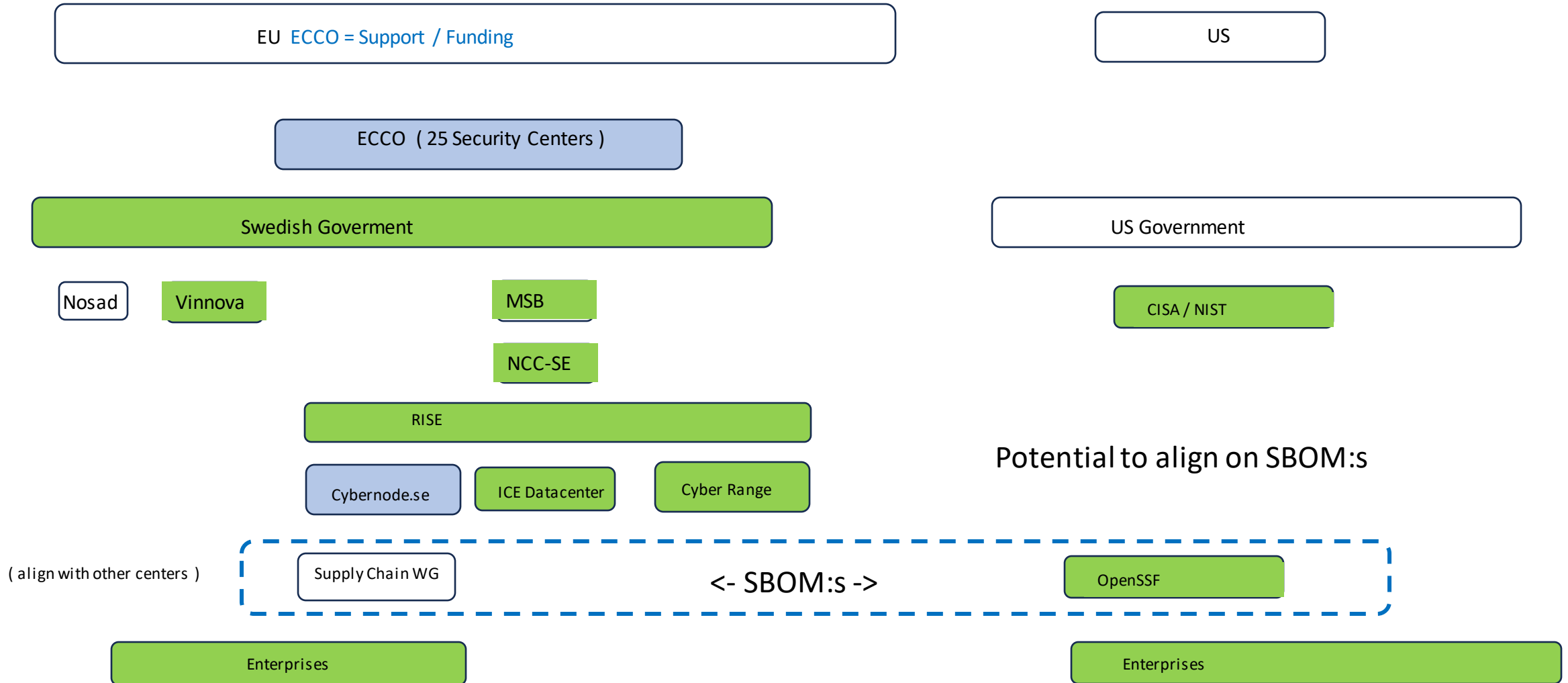
[Cyber Resilience Act | Shaping Europe's digital future \(europa.eu\)](#)

[EU cyber-resilience act \(europa.eu\)](#)

[Speeds and Feeds › Personal Musings of Steve Marquess \(veridicalsystems.com\)](#)

So the mystery is not that a few overworked volunteers missed this bug; the mystery is why it hasn't happened more often

Open Source and threats are global, US and EU strategies differs



(align with other centers)

Potential to align on SBOM:s

Article 37

In order to facilitate vulnerability analysis, manufacturers should identify, and document components contained in the products with digital elements, including by drawing up a software bill of materials.

Article 63

specify the format and elements of the software bill of materials
specify the EN 12 EN European cybersecurity certification schemes that can be used to demonstrate conformity

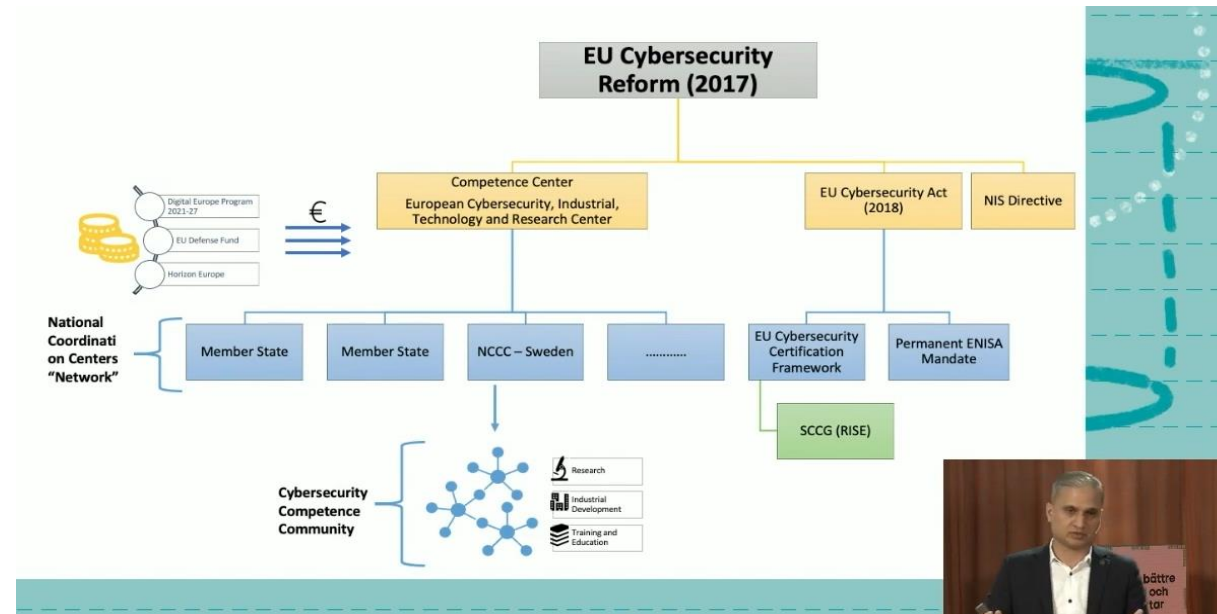
Section 2 of Annex 1

Manufacturers of the products with digital elements shall: (1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product.

[Cyber Resilience Act | Shaping Europe's digital future \(europa.eu\)](#)

[EU cyber-resilience act \(europa.eu\)](#)

List of software projects
US: SBOM
EU: Digital elements ?



[Opening swedish cybernode 2020](#)

[Implementing and delegated acts \(europa.eu\)](#)

[The European Cybersecurity Certification Group | Shaping Europe's digital future \(europa.eu\)](#)

GPT: "Is it possible to recreate an Alpine package using SBOM ?"



Default (GPT-3.5)

H is it possible to recreate a alpine package using a SBOM

Yes, it is possible to recreate an Alpine package (APK package) using a Software Bill of Materials (SBOM), but the process may involve multiple steps and considerations. Here's a general outline of how you might approach this:

1. Generate a Detailed SBOM:

Create a comprehensive Software Bill of Materials (SBOM) that includes information about all the dependencies, libraries, and components required by the package. This SBOM should provide details such as component names, versions, licenses, and any other relevant metadata.

2. Identify Build Requirements:

Review your SBOM to identify the specific build requirements for the package. This includes the necessary development libraries, headers, and tools that are needed to build the package from source.

3. Retrieve Source Code:

Obtain the source code for the package you want to recreate. You can usually find the source code associated with an Alpine package in the Alpine Linux Git repository or the upstream source repository.

4. Configure Build Environment:

Set up a build environment that matches the Alpine Linux distribution version and architecture. This environment should include the necessary development tools and libraries identified in the SBOM.

5. Build the Package:

Use the retrieved source code and the build environment to compile and build the package. Follow the build instructions provided by the package's documentation or source repository. Ensure that you use the correct build options and parameters, including those that align with the SBOM.

Answer is yes from GPT
But
The devil is in the details



How do I verify the correctness of a SBOM



H how do I verify the correctness of a SBOM

Verifying the correctness of a Software Bill of Materials (SBOM) is a critical step to ensure that the information it contains is accurate and reliable. Here are some steps you can take to verify the correctness of an SBOM:

1. **Source of SBOM:**

Ensure that the SBOM comes from a trusted and reliable source. If you're generating the SBOM yourself, make sure you follow accurate procedures to gather dependency information. If you're receiving the SBOM from a third party, verify their credibility and reputation.

2. **Cross-Reference with Documentation:**

Cross-reference the SBOM with the project's official documentation, README files, and other relevant sources. Confirm that the listed components, versions, and licenses match the documented dependencies.

3. **Review Version Numbers:**

Check that the versions of components listed in the SBOM are consistent with the versions used in the project. Mismatched or outdated versions could lead to compatibility issues or security vulnerabilities.

4. **Compare with Build Configurations:**

Compare the SBOM with the project's build configuration files (e.g., package.json for Node.js, pom.xml for Maven). Verify that the dependencies listed in the SBOM match those specified in the build files.

5. **Use Dependency Analysis Tools:**

Utilize automated dependency analysis tools to cross-check the SBOM. Tools like dependency-check, WhiteSource, and FOSSA can help identify any known vulnerabilities associated with the listed components.

Why not close the loop ?

1. Create a complete SBOM from a binary package
2. Generate the BUILD tools from the complete SBOM
3. Feed the complete SBOM into to the generated tool
4. Compare the initial and generated package



SBOM presentation by Siemens

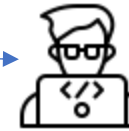
Ease of use in DEV/SEC/OPS

Security



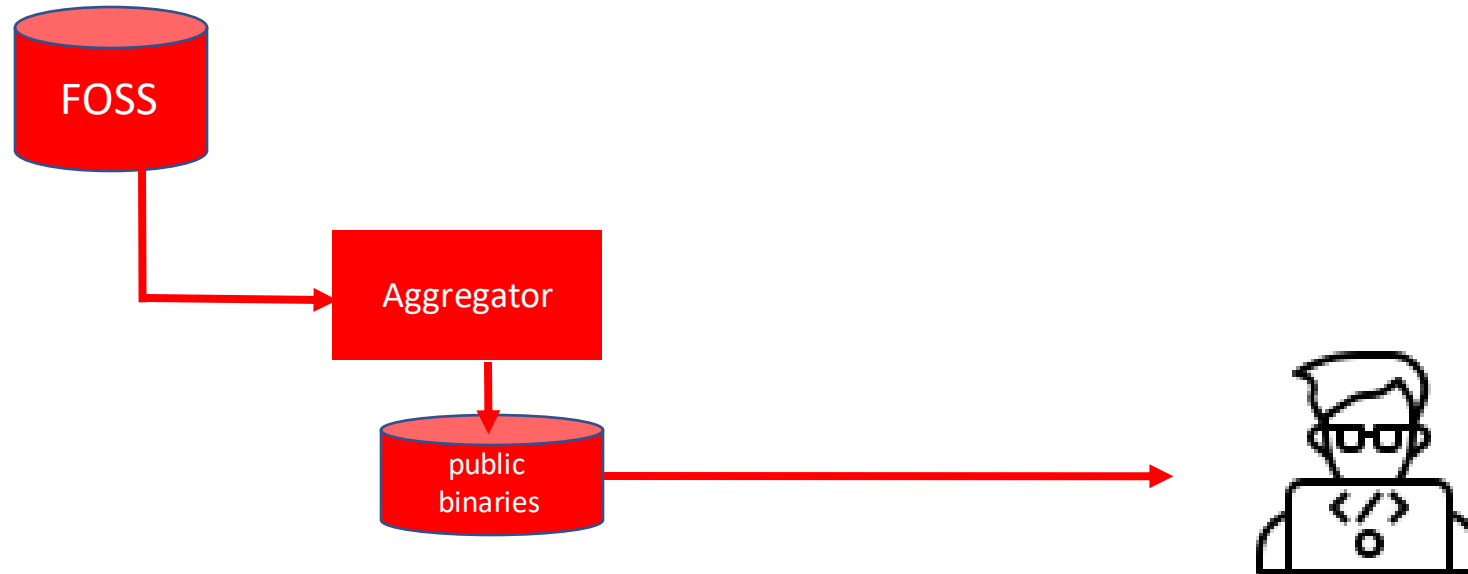
Keep way-of-working
Improve security

Developer



Repository	
Public binary packages	http://dl-cdn.alpinelinux.org/alpine
Mirror of public repository	https://services.lammda.se/alpine/public/
Isolated rebuild of packages	https://services.lammda.se/alpine/approved/
Customized packages	https://services.lammda.se/alpine/custom/

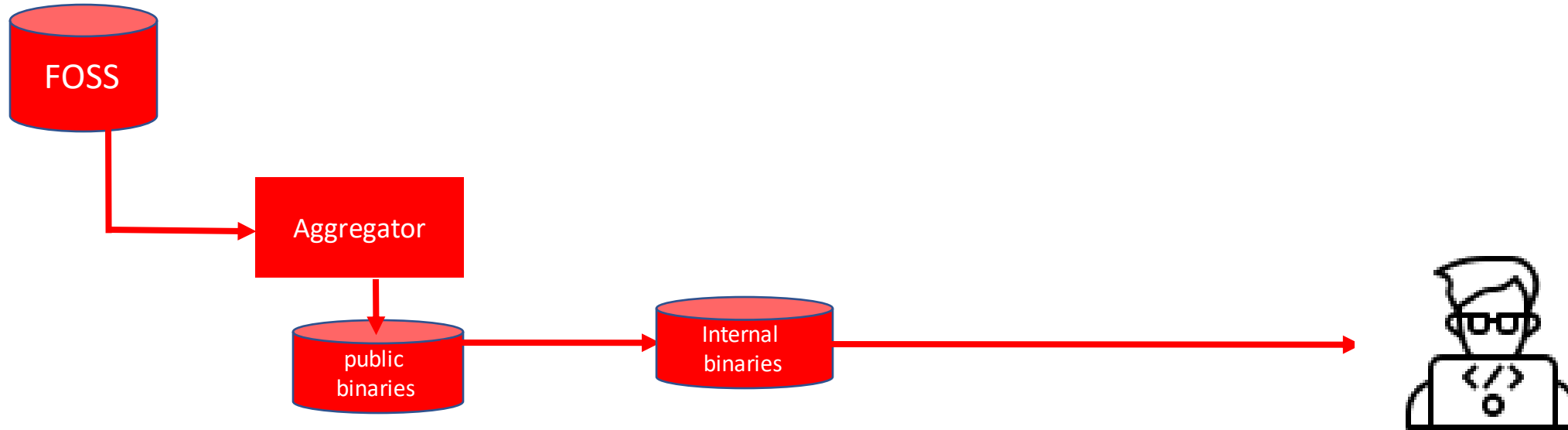
Direct download from Internet



Public binary packages

<http://dl-cdn.alpinelinux.org/alpine>

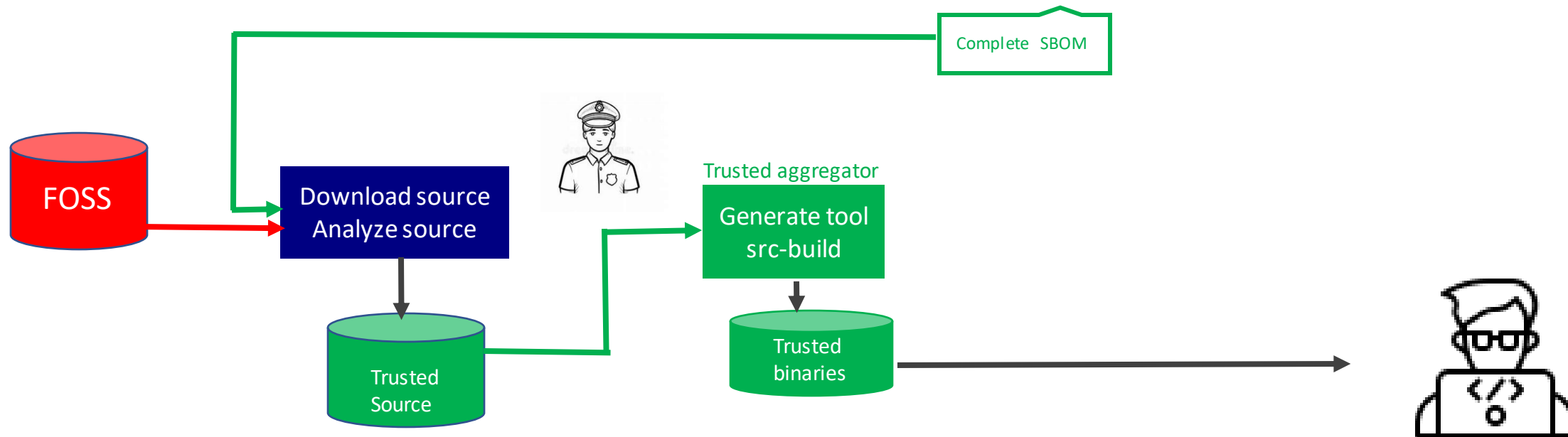
Mirror of public binaries



Mirror of public repository

<https://services.lammda.se/alpine/public/>

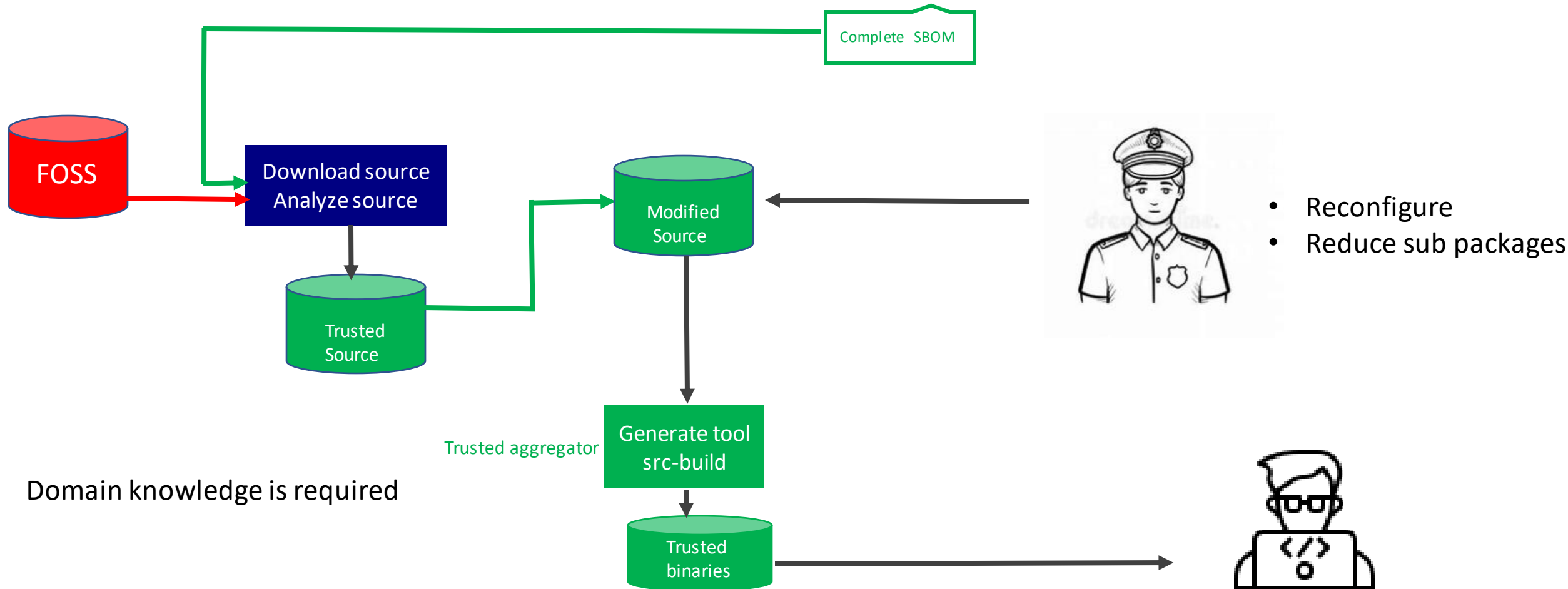
Build package from SBOM



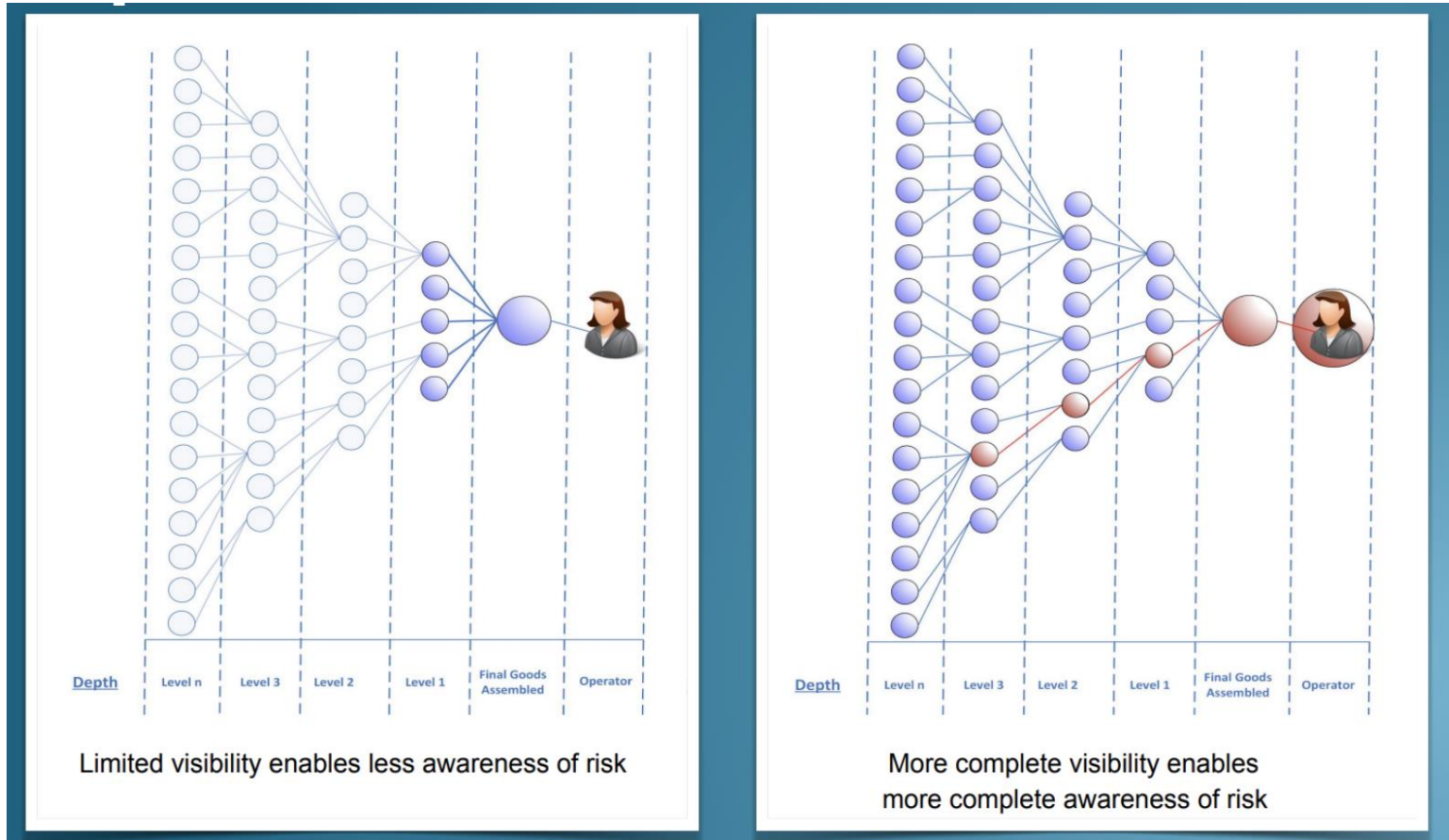
Isolated rebuild of packages

<https://services.lammda.se/alpine/approved/>

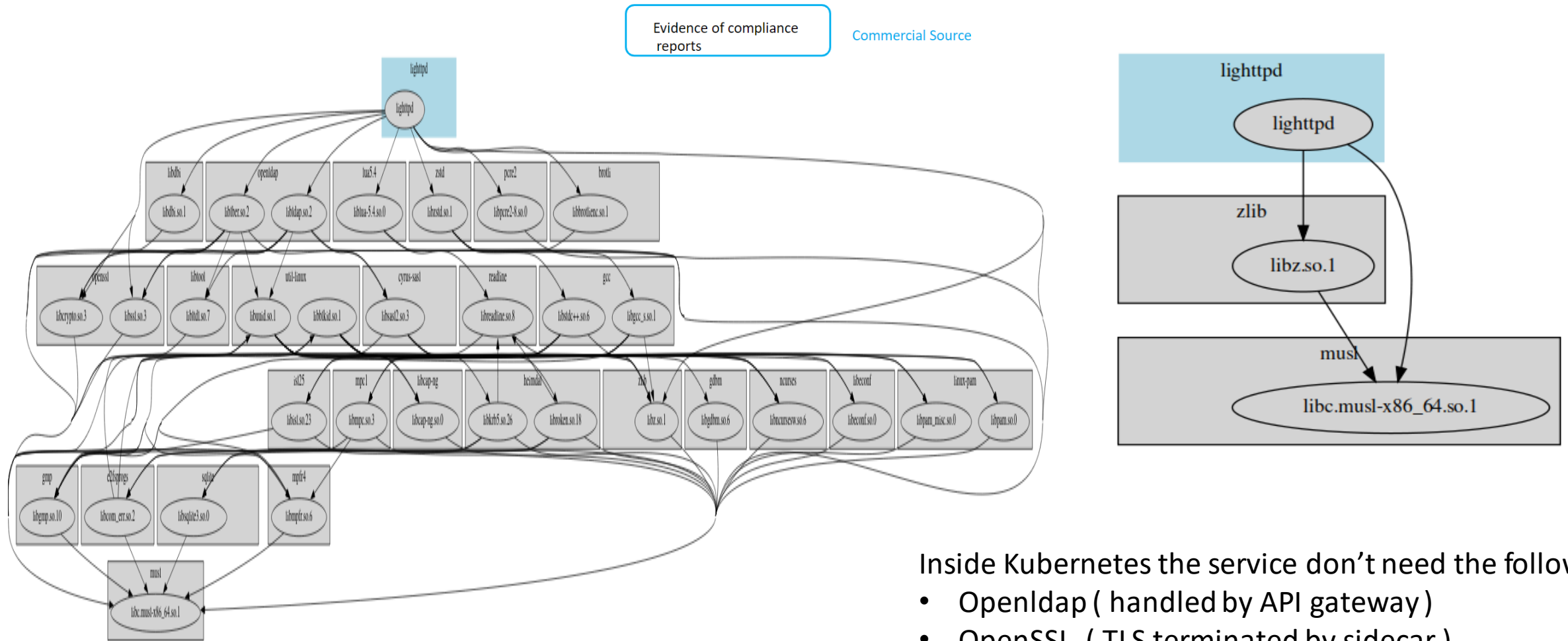
Hardening



Dependencies according to CISA



Hardening , reduce dependencies



- Inside Kubernetes the service don't need the following
- OpenIdap (handled by API gateway)
 - OpenSSL (TLS terminated by sidecar)

Rebuild, reduce dependencies

Original APKBUILD

```
build(){
  abuild-meson \
  -Db_lto=true \
  -Dwith_brotli=enabled \
  -Dwith_dbi=enabled \
  -Dwith_ldap=enabled \
  -Dwith_lua=true \
  -Dwith_openssl=true \
  -Dwith_pcre2=true \
  -Dwith_webdav_locks=enabled \
  -Dwith_webdav_props=enabled \
  -Dwith_zstd=enabled \
  . output
  meson compile -C output
}
```



Modified APKBUILD

```
build(){
  abuild-meson \
  -Db_lto=true \
  -Dwith_pcre2=true \
  . output
  meson compile -C output
}
```

Remove sub packages

Original APKBUILD

```
subpackages="  
  $pkgname-doc  
  $pkgname-dbg  
  $pkgname-openrc  
"
```

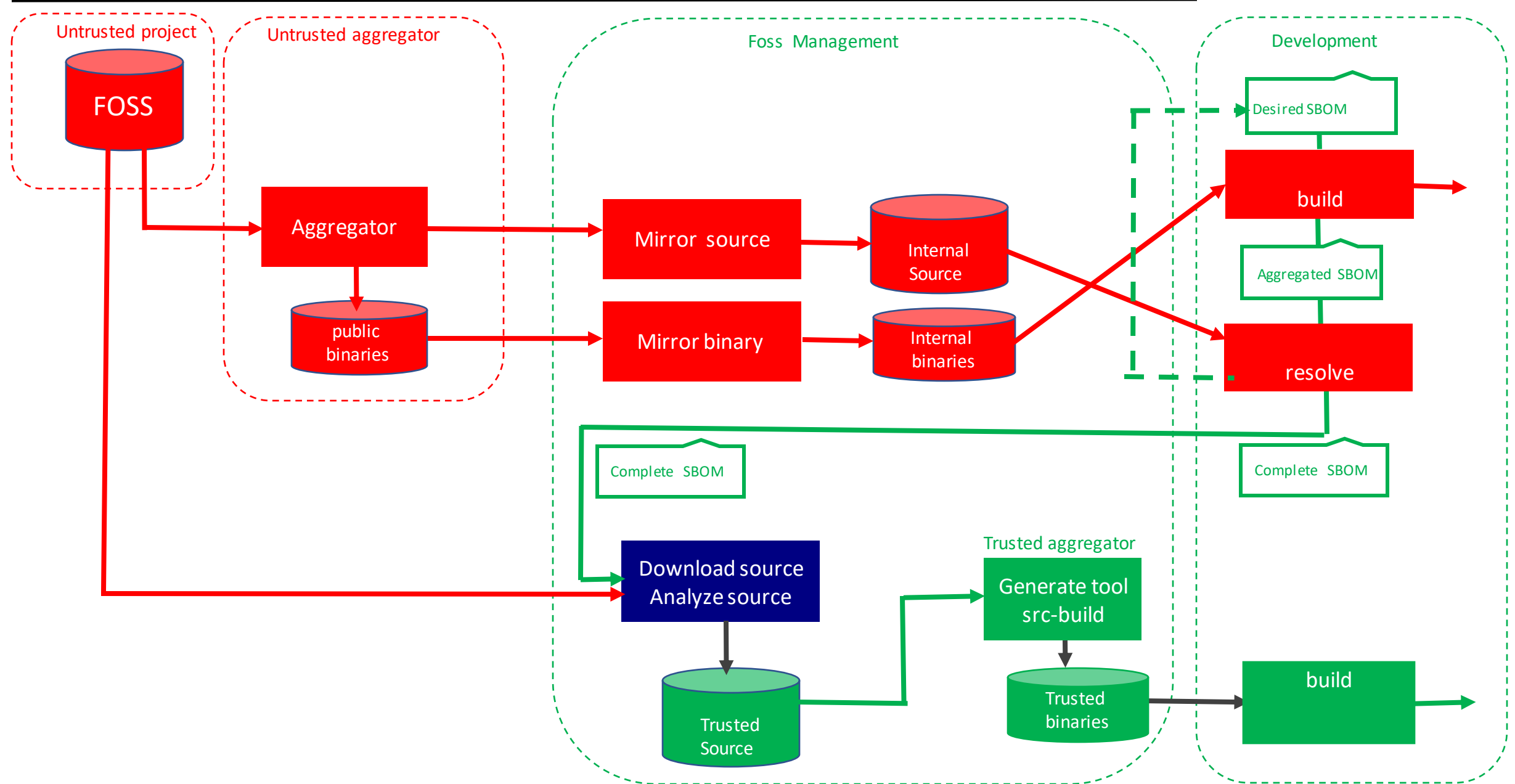


Modified APKBUILD

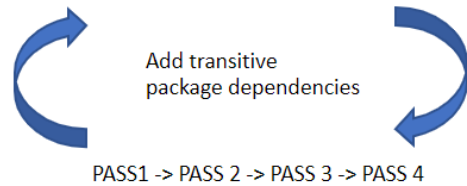
```
subpackages="  
  $pkgname-doc  
"
```

- (1/10) Installing brotli-libs (1.0.9-r14)
- (2/10) Installing libdbi (0.9.0-r4)
- (3/10) Installing gdbm (1.23-r1)
- (4/10) Installing libsasl (2.1.28-r4)
- (5/10) Installing libldap (2.6.5-r0)
- (6/10) Installing lua5.4-libs (5.4.6-r0)
- (7/10) Installing pcre2 (10.42-r1)
- (8/10) Installing zstd-libs (1.5.5-r4)
- (9/10) Installing lighttpd (1.4.71-r0)

- (1/2) Installing pcre2 (10.42-r1)
- (2/2) Installing lighttpd (1.4.71-r0)



Resolve process



Desired SBOM

```
# This is the reference image
#
alpine-base

lighttpd #S

# Pass 1

openssl
brotli
openldap
lua5.4
zstd

# Pass 2

ncurses
libtool
cyrus-sasl
util-linux

# Pass 3

heimdal

# Pass 4

e2fsprogs
```

Complete SBOM

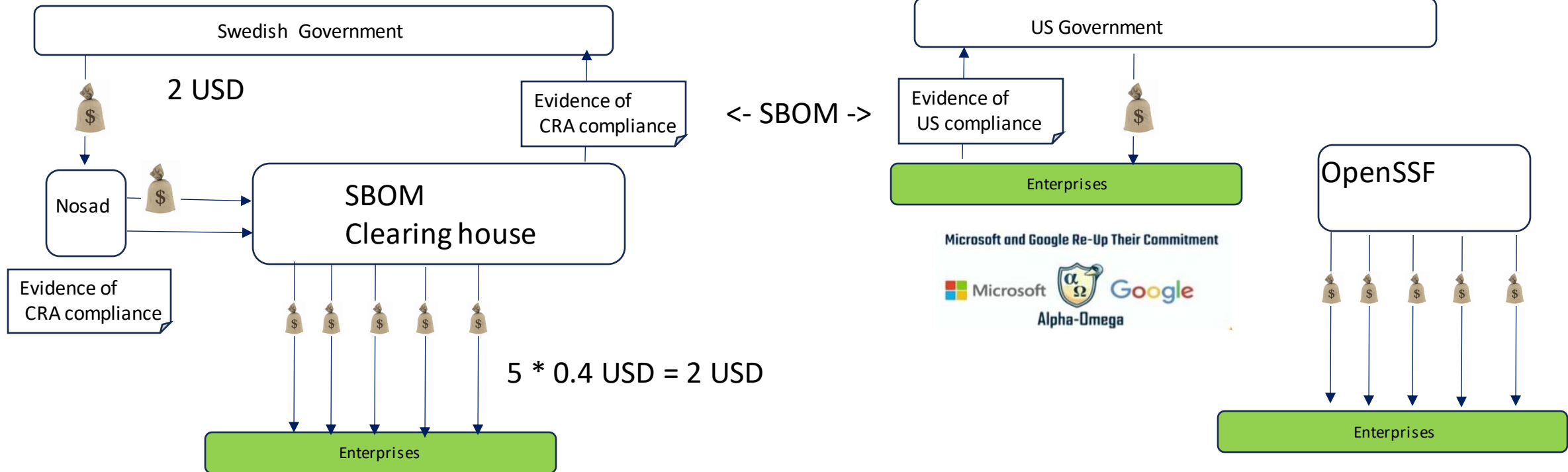
```
"resolver": {
  "status": false,
  "secondary": {
    "openssl": {
      "apk-tools": [
        "libcrypto.so.1.1",
        "libssl.so.1.1"
      ],
      "lighttpd": [
        "libcrypto.so.1.1",
        "libssl.so.1.1"
      ]
    },
    "brotli": {
      "lighttpd": [
        "libbrotlienc.so.1"
      ]
    },
    "openldap": {
      "lighttpd": [
        "liblber.so.2",
        "libldap.so.2"
      ]
    },
    "lua5.4": {
      "lighttpd": [
        "liblua-5.4.so.0"
      ]
    },
    "zstd": {
      "lighttpd": [
        "libzstd.so.1"
      ]
    }
  }
}
```

Continuous and granular funding

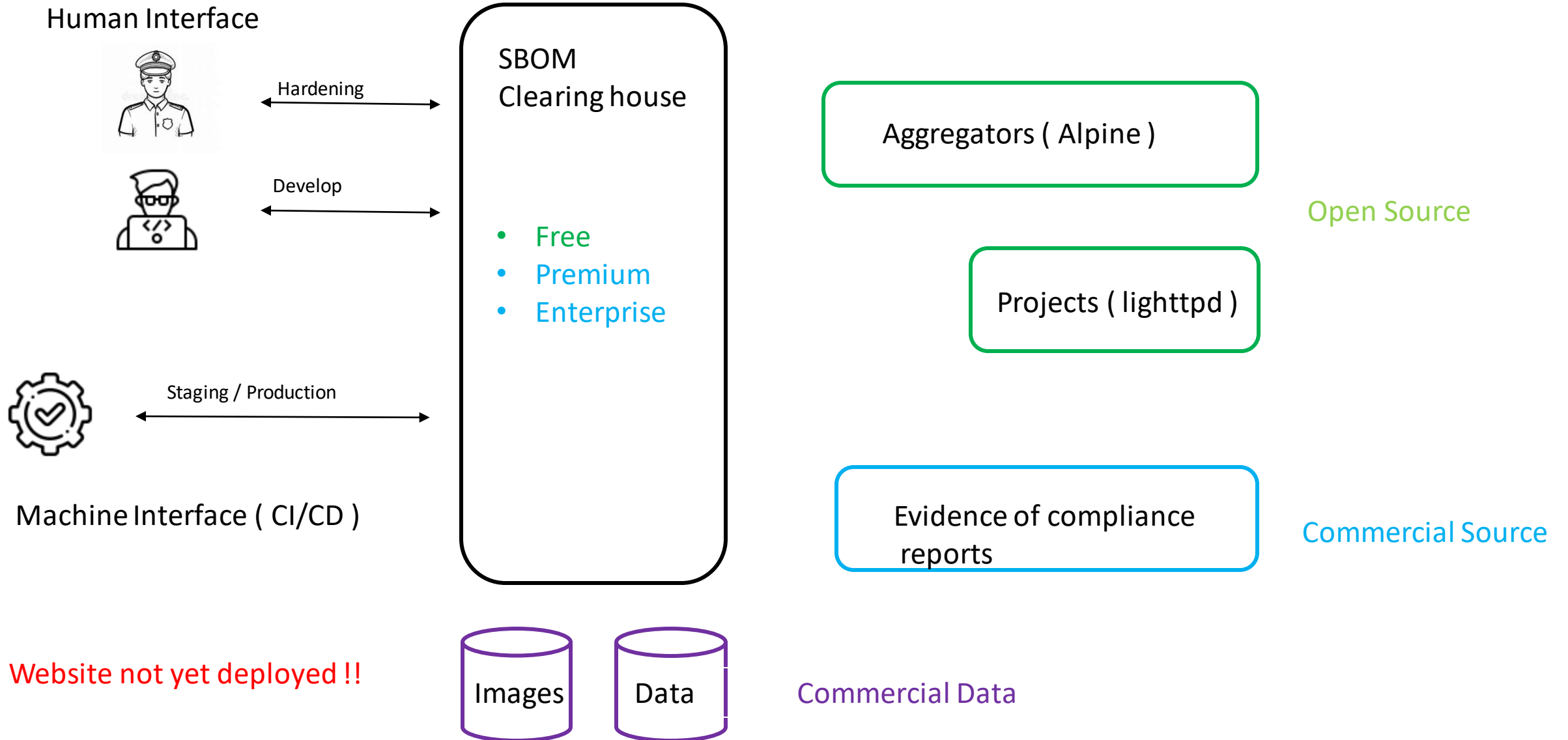
EU (CRA article 63 37, Section 2 , Annex 1)

US

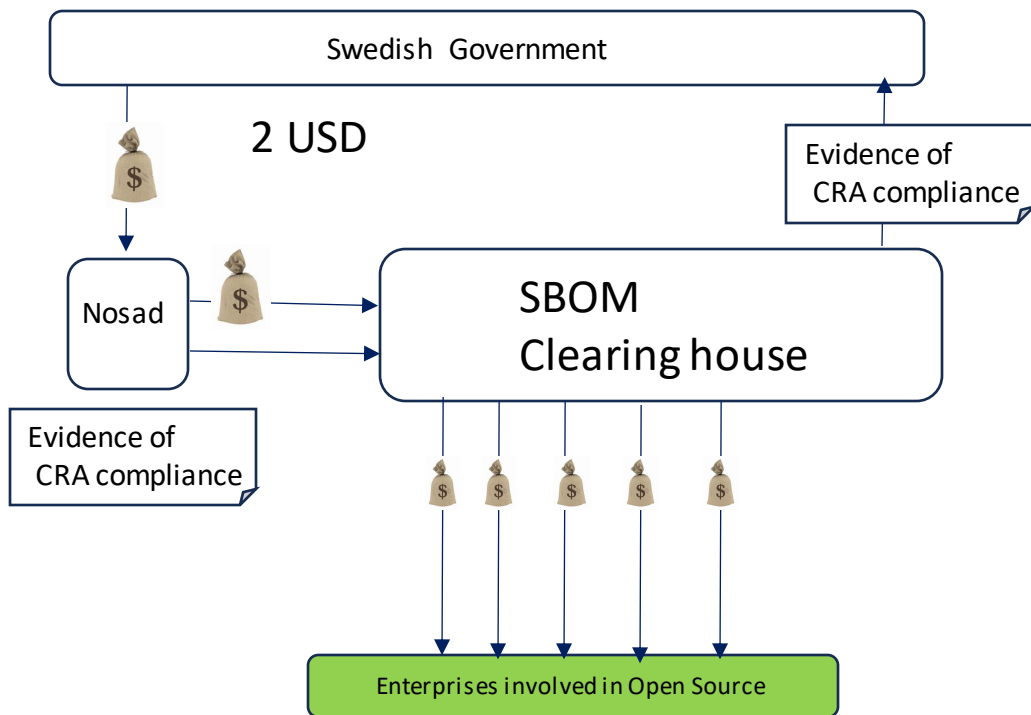
Executive Order 14028 of May 12, 2021



Open Source



CPD Cost Per Dependency



Invoice

Invoice id: 1023
 Invoice date: 2023-08-19 08:48
 Invoice due date: 2023-08-19 08:48

Service Provider

Name: SBOM Clearing House
 Street: Nybrogatan 34
 City: Stockholm
 State: Ostermalm
 Country: Sweden
 Post code: 114 43
 Vat/Tax number: Vat/556 76234

Client

Email: jonas@nosad.se

Detail

Name	Description	Units	Unit Price	Amount
lighttpd	1.4.71	1	2.0	2.0
musl	1.2.4	1	1.0	1.0
busybox	1.36.1	1	1.0	1.0
util-linux	2.38.1	1	1.0	1.0
openrc	0.48	1	1.0	1.0
bash	5.2.15	1	1.0	1.0
binutils	2.40	1	1.0	1.0
curl	8.2.1	1	1.0	1.0
gcc	12.2.0	1	1.0	1.0
gdbm	1.23	1	1.0	1.0
gmp	6.2.1	1	1.0	1.0
ifupdown-ng	0.12.1	1	1.0	1.0
isl25	0.25	1	1.0	1.0
openssl	3.1.2	1	1.0	1.0
libeconf	1.0.2	1	1.0	1.0
alpinelinux.org	3.18.2	1	1.0	1.0
Subtotal				17.00
Vat/Tax (9%)				1.53
Total				18.53

Optional Demo

1. Hardening of lighttpd by rebuild from source with BOMRESOLVER
2. Generate build tool for product SBOM

Post presentation

After the meeting the funding of openssl was discussed.

Source of contributions

- [Open Source Security Foundation - Wikipedia](#)
- [Home - Core Infrastructure Initiative](#)
- [Sponsor @openssl on GitHub Sponsors](#)

Other income

- Contracts
- Consulting