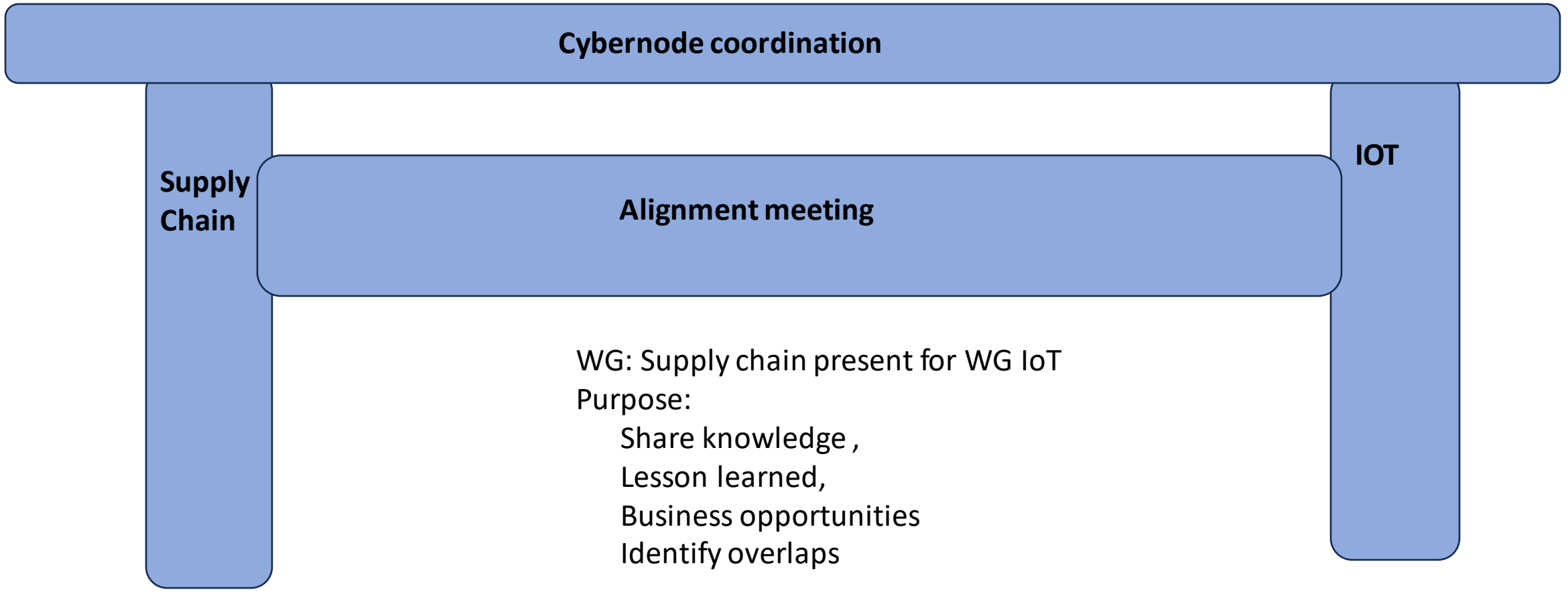
Secure supply chains/Open Source meets IOT security

Agenda (60 minutes)

- Premeeting
  - Presentation of WG: Software supply chain/open source
  - Challenges with WG
  - Opportunities with WG

- Public presentation CRA applied to IoT
  - Questions
- Post Meeting

hans@lammda.se



WG: Supply chain present for WG IoT

Purpose:

- Share knowledge ,
- Lesson learned,
- Business opportunities
- Identify overlaps

What is a IoT device ?

Examples of IoT devices are diverse and include smart thermostats, connected security cameras, wearable fitness trackers, smart home appliances (like refrigerators and lights), industrial sensors for manufacturing processes, and even autonomous vehicles. The Internet of Things has a wide range of applications across various industries, from healthcare and agriculture to transportation and smart cities, and it continues to grow and evolve as technology advances

IEC62443 ?
CRA ?
NIS2 ?

IOT

cybernode.se
Commissioned by NCC-SE

Supply Chain

- The big picture (eoj@edvina.net) (wide base)
- The innovative bomresolver.io (hans@lammda.se) (narrow edge)

About our work group

About the group (OpenSSF inspired , Olle from Edvina)

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 (bomresolver.io , Lamm Consulting)

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 ecosyste
The https://nosad.se is a forum for Swedish authorities for sharing data and knowledge about op 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

Presentations and source code

cybernode.se
Commissioned by NCC-SE

Bomresolver in the software supply chain context

- Serve static content required for software updates (NIS2 / CRA)
- Software bill of material (NIS2 / CRA)

Webbinar med Olle E Johansson från Edvina, om CRA och nya krav på programvara - YouTube

https://cybernode.se/app/uploads/2023/08/cybernode_2023_08_22.pdf
https://cybernode.se/app/uploads/2023/06/NOSAD-SBOM-cybernode_2023_06_14_public-1.pdf

https://bomresolver.io/events/
https://github.com/Nordix/bomres

https://services.lammda.se/nosad

CRA

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

EUROPEAN
COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

COOP and CRA proposal

cybernode.se
Commissioned by NCC-SE

Reasons for and objectives of the proposal

"Forcing a supermarket chain to close all its 500 shops across **Sweden**;"

Hackade Coop – kräver 600 miljoner

Coop på Stora Essingen håller fortsatt stängt. Foto: Ari Luostarinen

Coop har polisanmält it-attacken som tvingat majoriteten av kedjans butiker att hålla stängt under helgen. Samtidigt fortsätter arbetet med att starta om betalningssystemen, en butik i taget.

CRA article 10 and Open Source

cybernode.se
Commissioned by NCC-SE

Hobby and research is OK

In order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable.

Commercial support for your hobby project is not OK

In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for **technical support services**,

Linux and Kubernetes is not OK

by providing a **software platform** through which the manufacturer monetises other services,

CRA PROBLEM

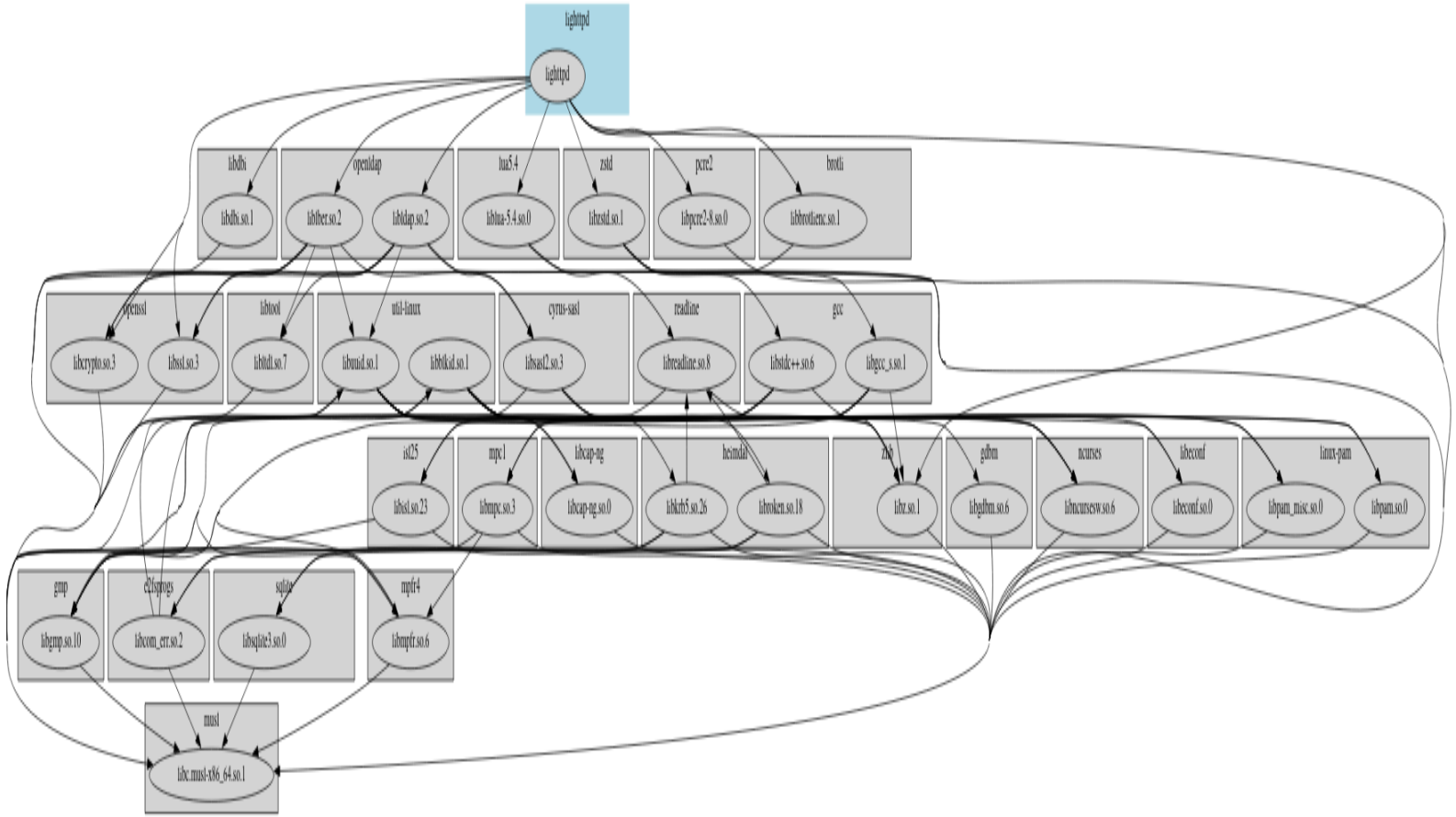
cybernode.se
Commissioned by NCC-SE

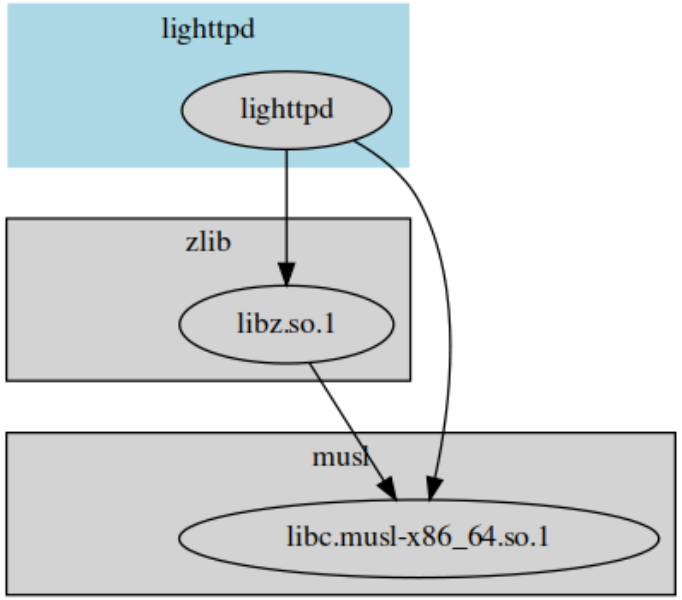
We are sorry.

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

CRA article 11 and hardening

CRA: comply with well-established Internet security standards (NIST).





NIST: "All the unneeded software, drivers, and services must be removed or disabled"

CRA article 34 Vulnerability database

Manufacturers should also consider disclosing fixed vulnerabilities to the European vulnerability database established under Directive [Directive XX/XXXX (NIS2)] and managed by ENISA or under any other publicly accessible vulnerability database.

CVE-2022-28321 Detail

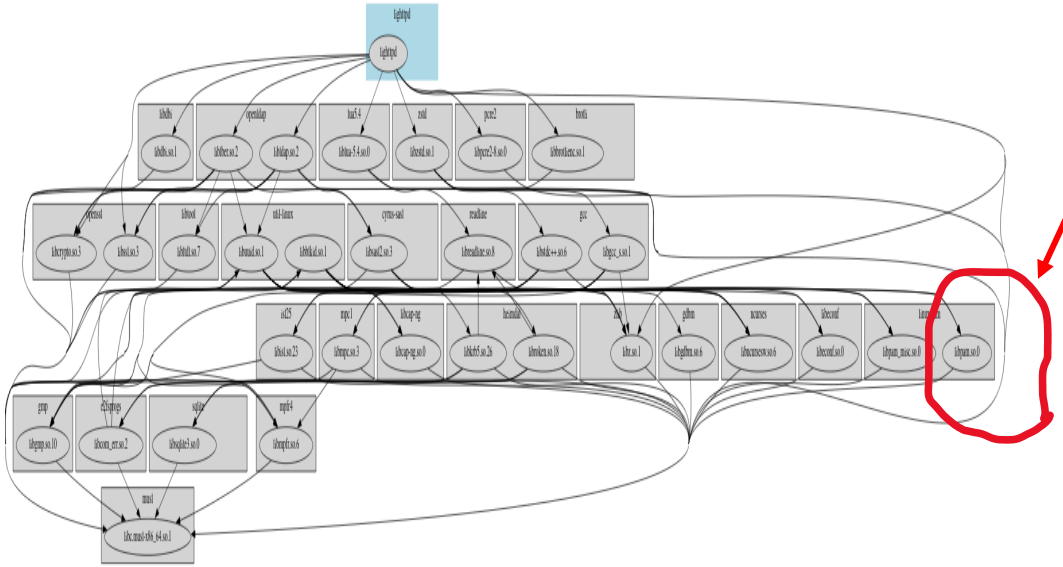
Description

The Linux-PAM package before 1.5.2-6.1 for openSUSE Tumbleweed allows authentication bypass for SSH logins. The pam_access.so module doesn't correctly restrict login if a user tries to connect from an IP address that is not resolvable via DNS. In such conditions, a user with denied access to a machine can still get access. NOTE: the relevance of this issue is largely limited to openSUSE Tumbleweed and openSUSE Factory; it does not affect Linux-PAM upstream.

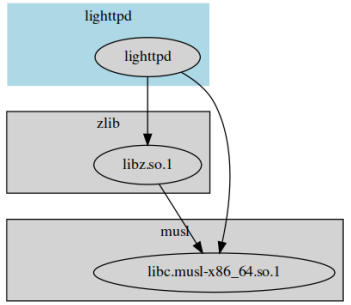
Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Hardening may generate false positive alerts

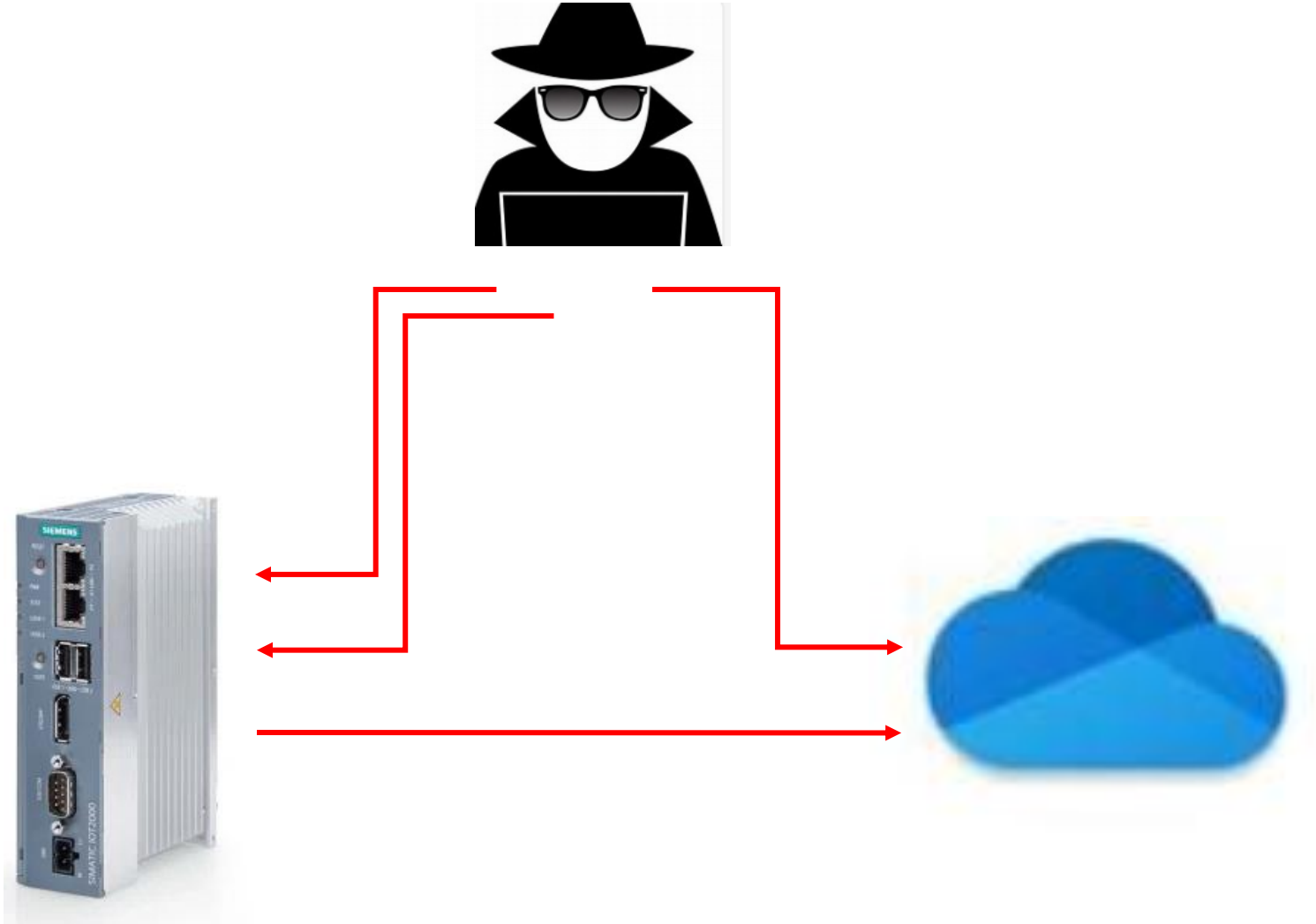


CRA includes NIS2

This Regulation, which applies to all connectable hardware and software products, also aims at facilitating the compliance of digital infrastructure providers with the supply chain requirements under the [Directive XXX/XXXX (NIS2)] by ensuring that the products with digital elements that they use for the provision of their services are developed in a secure manner and that they have access to timely security updates for such products

Attack scenario

- Direct attack against IoT device
- Direct attack against Cloud service
- Install malware/bot on IoT device
  - Control bot from darknet
  - Sell DDOS as service
  - Fire of DDOS attack



Record breaking DDOS attack !!!

cybernode.se
Commissioned by NCC-SE

Cloudflare mitigates record-breaking 71 million request-per-second DDoS attack

This was a weekend of record-breaking DDoS attacks. Over the weekend, Cloudflare detected and mitigated dozens of *hyper-volumetric* DDoS attacks. The majority of attacks peaked in the ballpark of 50-70 million requests per second (rps) with the largest exceeding **71 million rps.** This is the largest reported **HTTP DDoS** attack on record, more than 54% higher than the previous reported record of 46M rps in June 2022.
The attacks were HTTP/2-based and targeted websites **protected by Cloudflare**. They originated from over **30,000** IP addresses. Some of the attacked websites included a popular gaming provider, cryptocurrency companies, hosting providers, and cloud computing platforms. The attacks originated from numerous cloud providers, and we have been working with them to crack down on the botnet

Content Delivery Network

cybernode.se
Commissioned by NCC-SE

- 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 EVIDENCE of COMPLIANCE

cybernode.se
Commissioned by NCC-SE

This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council14 , including to provisions for the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of **demonstrating compliance** of processing operations by controllers and processors with that Regulation. Such operations could be embedded in a product with digital elements. Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679.

CRA article 6 and IEC62443

SS EN IEC 62443-4-1

Secure by design (SD)

Secure implementation (SI)
Security verification and validation testing (SVV)
Management of security-related issues (DM)
Security update management (SUM)
Security guidelines (SG)

CRA includes GDPR

This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council14 , including to provisions for the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance of processing operations by controllers and processors with that Regulation. Such operations could be embedded in a product with digital elements. Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679.

NIS2 and Lesson learned

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

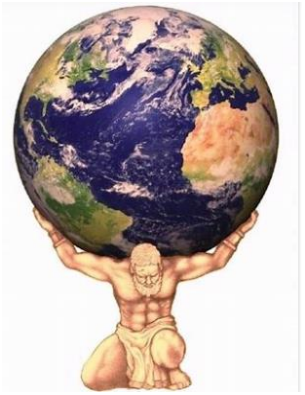
(Text with EEA relevance)

To exchange views on the policy on follow-up actions following large-scale cybersecurity incidents and crises on the basis of **lessons learned** of the CSIRTs network and EU-CyCLONe

In-depth reporting that draws **valuable lessons** from individual incidents and improves over time the cyber resilience o

Lesson learned Hearthbleed

cybernode.se
Commissioned by NCC-SE



Used widely on internet-facing devices

Om eSam - eSamverka

Projektets bidragsgivare av källkod bör vara flera personer, undvik enmansprojekt.

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.

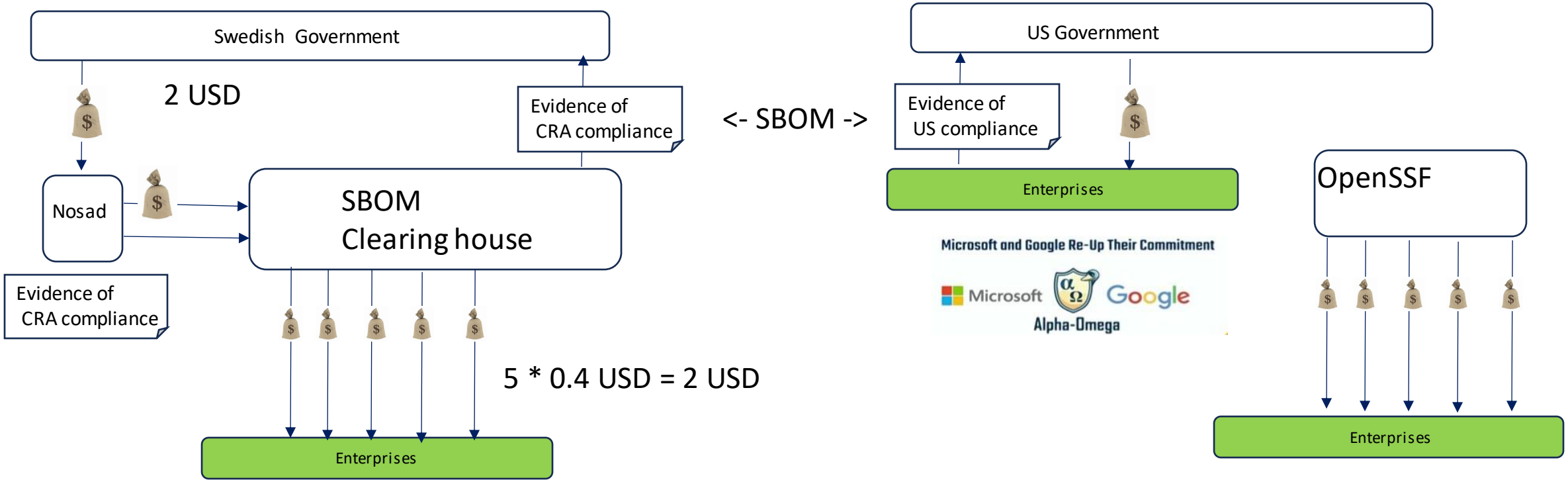
Continuous and granular funding

cybernode.se
Commissioned by NCC-SE

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

US

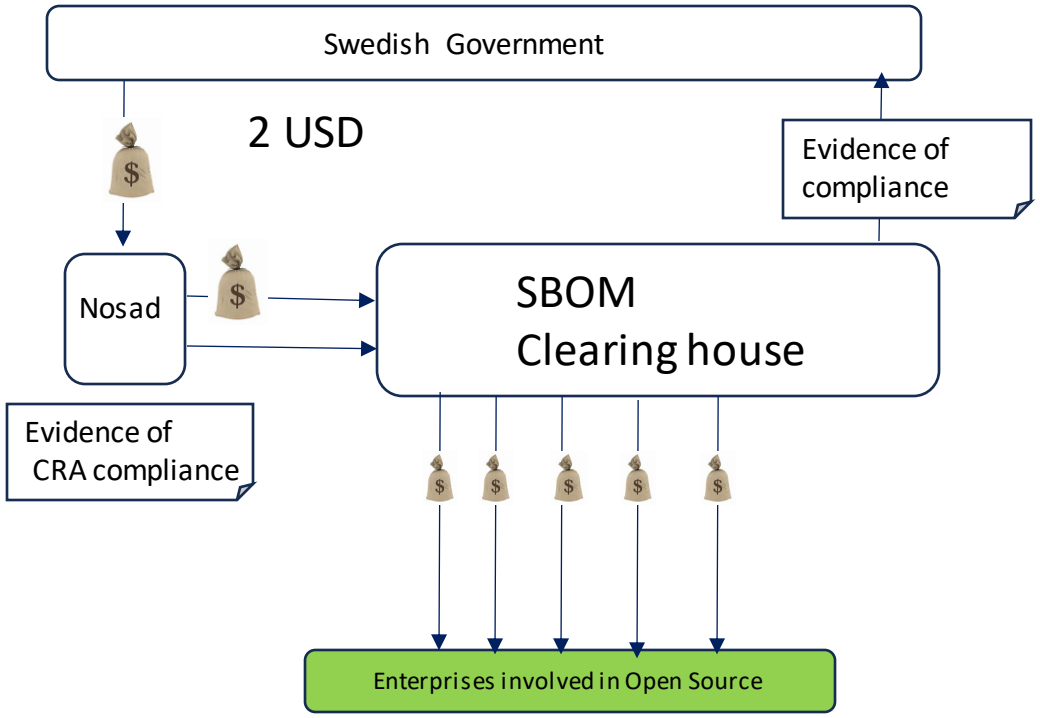
Executive Order 14028 of May 12, 2021



Open Source

CPD Cost Per Dependency

cybernode.se
Commissioned by NCC-SE



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

Security is the tax honest people pay