The path towards a

global vulnerability management *platform*

Olle E. Johansson, 2025-04 v1.2, oej@edvina.net

My starting point in 2023…

EU is leading software security legislation

…and base that on US funded systems

So I started thinking (in 2023)

- **1. Why doesn’t other parts of the world contribute funding?**
- **2. Why isn’t this lead by a a global organisation?**

- I started discussing this in many forums - OWASP SBOM Forum, Swedish security forums, OpenSSF and possibly more
- Did get much interest but very little energy. The system actually worked.

Olle E. Johansson, oej@edvina.net

Then bad things started to happen

Attackers could continue to work, but defenders where in the dark.

Feb 2024
NVD practically stopped adding metadata

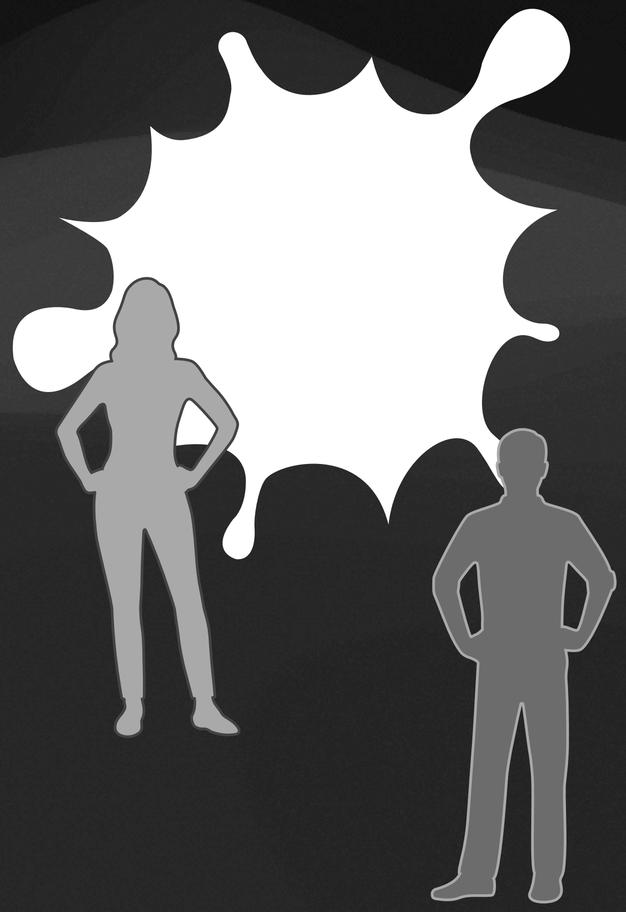
Suddenly, I got a lot of companions joining forces with me.

April 2025
CVE funding issues shook the world.

Olle E. Johansson, oej@edvina.net

Many stepped forward with good intentions

- Many groups took the chance to try to provide alternatives to the CVE program
- Even ENISA (EU) stepped forward (in my view clumsily)
- Focus was on technical solutions
- But they did not solve the trust problem nor the global issues
- Parts of the CVE board launched the CVE Foundation
- **I worked hard to push toward the need for a long term global solution with a large amount of trust, and including the existing CVE program and the CNAs in that work**



Olle E. Johansson, oej@edvina.net

But Why?

- Users needs to be able to verify if their platforms and products are safe and secure
- Many legislations require access to vulnerabilities (e.g. EU CRA, NIS2)
- The SBOMs need this to work

Olle E. Johansson, oej@edvina.net

What should we do?

My personal view

Towards a global federated vulnerability platform

Unfortunately, many things at the same time.

Short term

Help the CVE program and the CNAs in their work and start a dialogue about contributing.

Long term

Work on a global solution and a migration path

Olle E. Johansson, oej@edvina.net

The global platform

This won’t be a quick fix or an easy fix

Boring work, but required

Build a new organisation with global stakeholders from industry, community and governments

Olle E. Johansson, oej@edvina.net

The global platform

This won’t be a quick fix or an easy fix

Boring work, but required

Build a new organisation with global stakeholders from industry, community and governments

We love it.
Can we start now?
I have an idea! I have code.

Create a technical solution - standard APIs, data formats and replication support. A trusted platform.

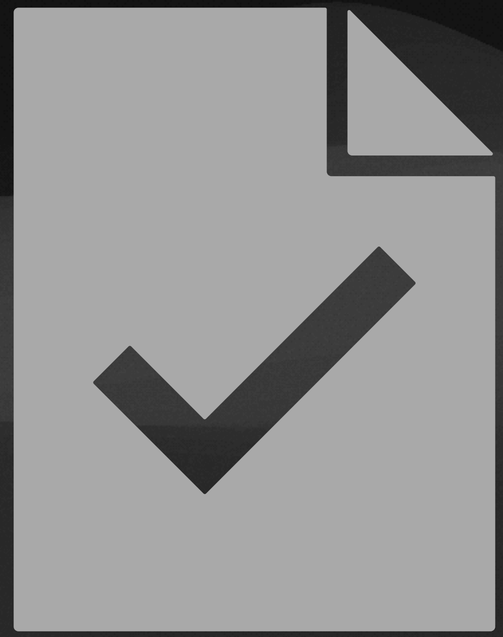
Stop it. Start with the boring parts, agree on requirements first, then start coding.

Olle E. Johansson, oej@edvina.net

Focus please!

…or I'll dismiss this class…

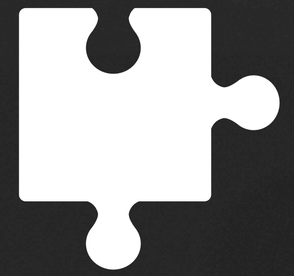
- We love discussing technology, code and stuff.
- We have to put that on hold while focusing on getting the organisation started - if we agree that we need that
- After that, start with requirements
- Then go back to the whiteboard and our code



Requirements for a new system

My suggested requirements
#1: FEDERATION

- **FEDERATION**: A global system needs to be operated by many actors, following the same rules and formats for managing vulnerability data. By using the same namespace, collisions in identifiers (CVE) will be avoided. The federation needs decentralisation.



Olle E. Johansson, oej@edvina.net

My suggested requirements
#2: GLOBAL

- **GLOBAL**: We need a multistake-holder organisation with global participation to manage the standards, the code of conduct, but maybe not the systems

Olle E. Johansson, oej@edvina.net

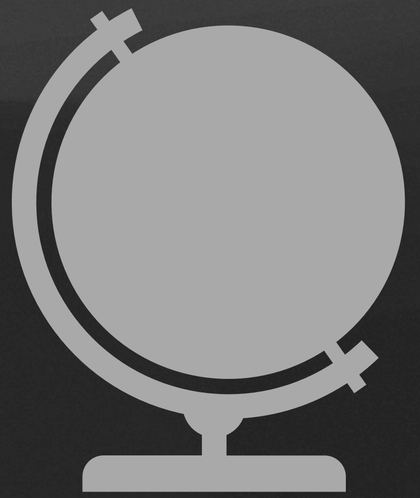
My suggested requirements
#3: FREE

- **FREE**: The data shall be freely accessible and replicable worldwide.
  No single jurisdiction owns this data. Everyone needs availability.

Olle E. Johansson, oej@edvina.net

My suggested requirements
#4: INTEROPERABILITY

- **INTEROPERABILITY**: The API for lookups needs to be standardised, as well as the data format and standards for replication of data.



Olle E. Johansson, oej@edvina.net

My suggested requirements
#5: NAMING

- **NAMING**: Vendors and creators (open source projects) need to be in control of their identifiers (DNS name) and the product names, no one else. The system may have a small managed namespace for software creators without a DNS name registration, which of course can’t guarantee any similarity with a natural name in order to avoid collisions.

Olle E. Johansson, oej@edvina.net

My suggested requirements
#6: GLOBAL NAMESPACE

- **GLOBAL NAMESPACE**: The identifier for a vulnerability needs to be globally unique

Olle E. Johansson, oej@edvina.net

My suggested requirements
#7: TRUST

- **TRUSTED and AUTHORITATIVE**: There needs to be a high level of trust in the system and the provided data, by using digital signatures and transparency systems to monitor the systems for invalid changes in data. This system should be authoritative for legislations and vertical standards world wide. All vulnerabilities must be independently verifiable.

Olle E. Johansson, oej@edvina.net

My suggested requirements
#8: REPLICATION

- **REPLICATION FRIENDLY**: The data needs to be replication friendly. One reason is that APIs can be used to track the content of SBOMs for a specific IP/Enterprise and having data locally (and off line) is much faster. In addition, local data offloads the traffic from the API endpoint.
- There should be no cost or other requirements put on availability for replication

Olle E. Johansson, oej@edvina.net

My suggested requirements
#9: EXTENSABILITY

- **EXTENSABILITY** with preserved integrity
- Data provided should not change, integrity should be protected
- Many providers should be able to provide additional data (like NVD, KEV and EUVD)
- Security researchers should be able to provide additional data (or corrections) like governmental organisations
- Users make a decision about whom to trust

Olle E. Johansson, oej@edvina.net

Coming steps

(my personal suggestions)

1. Gather around the round table

The first part, we have started

- 1. **Talk with everyone**, get organisations and individuals engaged
- 2. **Open Forums:** Set up a number of meetings to gather requirements and collect input on the process in order to be able move forward towards a more resilient solution to support global efforts related to cyber security. This process needs to have a **diverse set of parties** involved in order to build trust and confidence in a gradual buildup of a new platform.
- 3. The goal with the first part of this process is to agree on **governance** and **base requirements** similar to the requirements above, to agree on organisational rules (bylaws) and set up an interim board/work group to manage the process of forming the organisation (if needed)

Olle E. Johansson, oej@edvina.net

Part two: Gears in motion

Setting up an organisation

- 1. Organise a **series of workshops** to gather ideas and input from a worldwide community, creating a set of documents as input for further work in an organised way.
- 2. **Agree on requirements** on various parts of the technology solution
- 3. **Agree on a standards process** (using existing standard organisations wherever possible)
- 4. Start defining API’s, formats, naming

Olle E. Johansson, oej@edvina.net

Part three: Slow migration

Building trust and migrating

- Building trust takes time
- The CVE program needs to be part of this process and be part of the solution
- CNAs may either decide to work as before (with the CVE program) or contribute directly as part of the federation
- Other existing vulnerability databases, vendors and actors are of course invited to join the efforts

Olle E. Johansson, oej@edvina.net

Summary of the proposed process

OEJ's proposal

- 1: Reach an agreement on a working group - "interim board" - that works on the next step of building an organisation
- 2: Organise a large amount of open workshops to gather input from stakeholders, try to form some level of baseline agreement on the way forward both on organisational and on technical requirements
- 3: Create the new organisation (if needed) and start development of needed standards to build the solution
- 4. Live happily ever after :-)

Olle E. Johansson, oej@edvina.net

Interested parties so far

Participating in the discussions

- OWASP Foundation
- OpenSSF
- Eclipse Foundation
- Erlang Ecosystem Foundation
- A large group of cybersecurity experts

We try to reach out, gather interest in order to set up the first meetings.

- (These are the ones I have talked with. I guess there are many more)

Olle E. Johansson, oej@edvina.net

This will take time.

Patience, my friends, is a virtue

I think we can do this.

Do you want to be part of the solution?

Points of contact

- Mailing list: **cve@owasp.org**
- OpenSSF Vulnerability disclosures working group
  https://github.com/ossf/wg-vulnerability-disclosures
- My document:
  https://docs.google.com/document/d/1u6yPlCla7SO6YuHakjvmcGtcEmHdp-NANaqpTDTA7Q0/edit?usp=sharing
- Blogs:
  - https://openssf.org/blog/2025/04/23/vulnerability-enumeration-conundrum-an-open-source-perspective-on-cve-and-cwe/
  - https://owasp.org/blog/2025/04/17/owasp-global-vulnerability-intelligence.html
- My email: **oej@edvina.net**

Q/A

oej@edvina.net