

**THE WORLD NEEDS
A FREE GLOBAL
VULNERABILITY
INTELLIGENCE
PLATFORM.**

**WANT TO
HELP?**

Update Feb '26

Olle E. Johansson, 2026-02 v2.1, oej@edvina.net



Vulnerability intelligence platforms are shaking

The NVD program is gone. More or less.

What is the EUVD?

Legislators adding pressure.

The CVE program is still around. But for how long?

Commercial vendors filling the void.

My SBOM check shows no issues!

What should we do?

My personal view

Towards a global federated vulnerability platform



Unfortunately, many things at the same time.

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

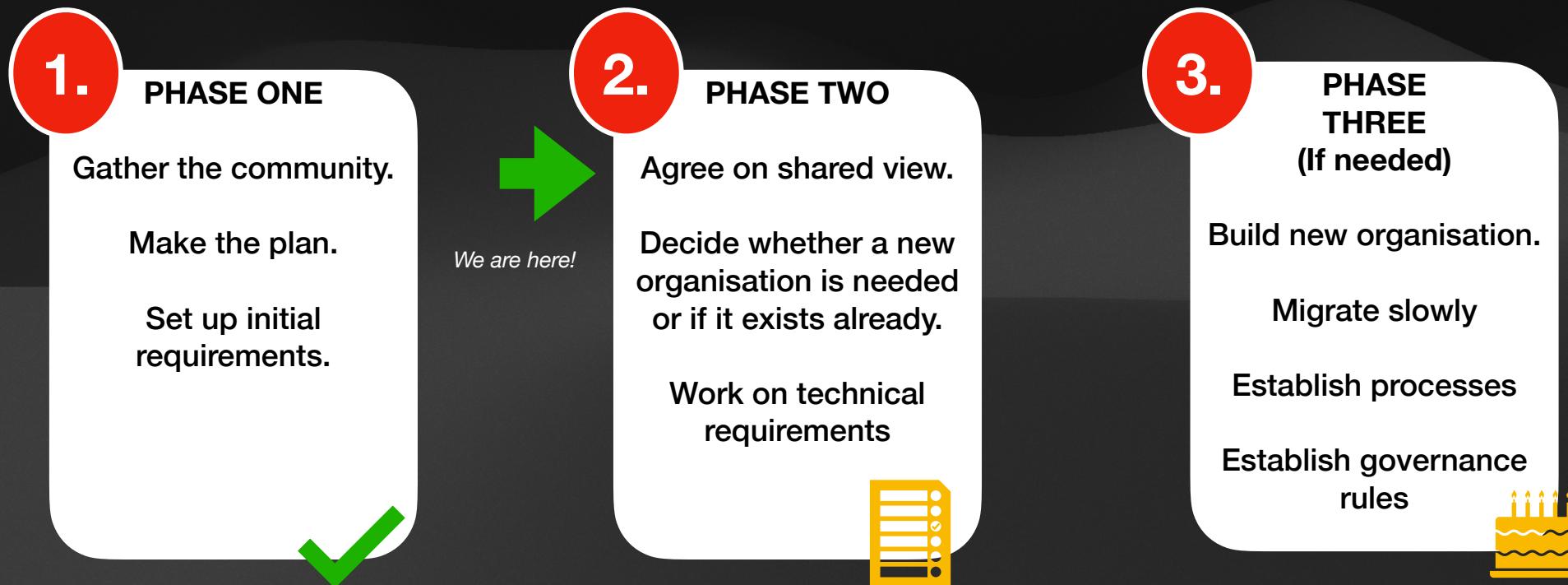
Short term

Work on a global solution and a migration path

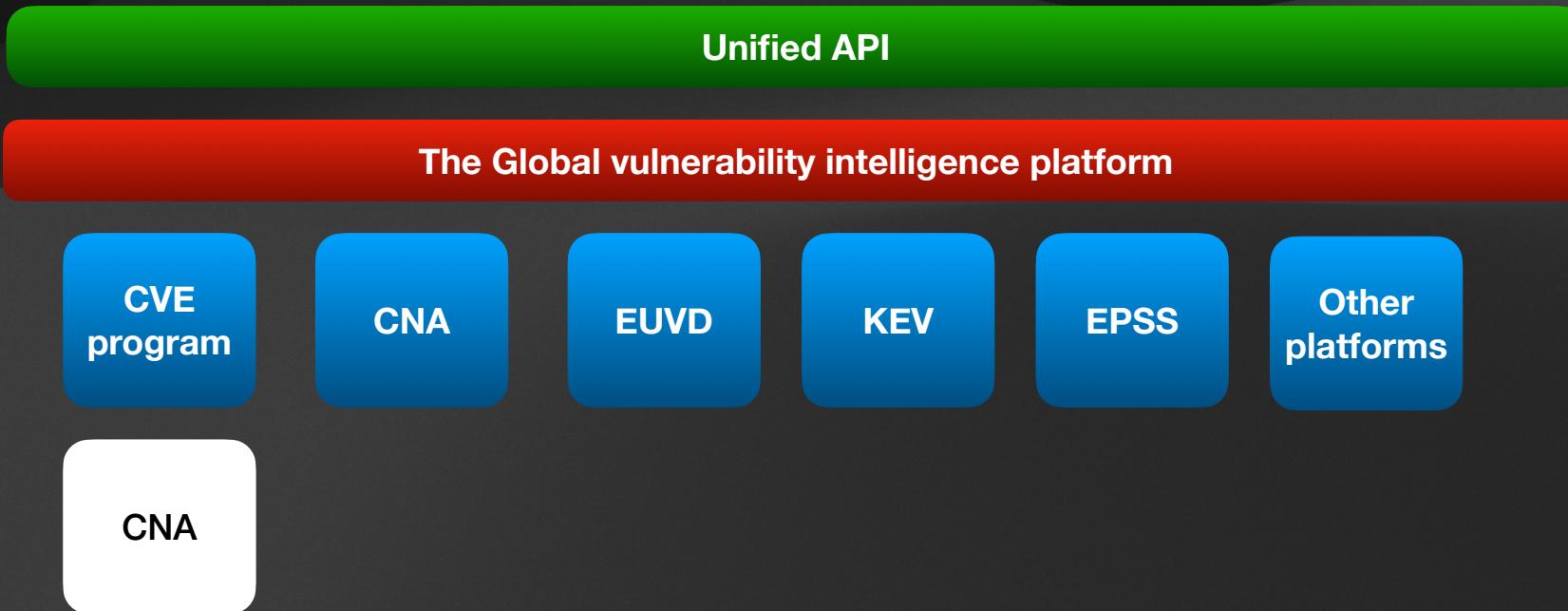
Long term



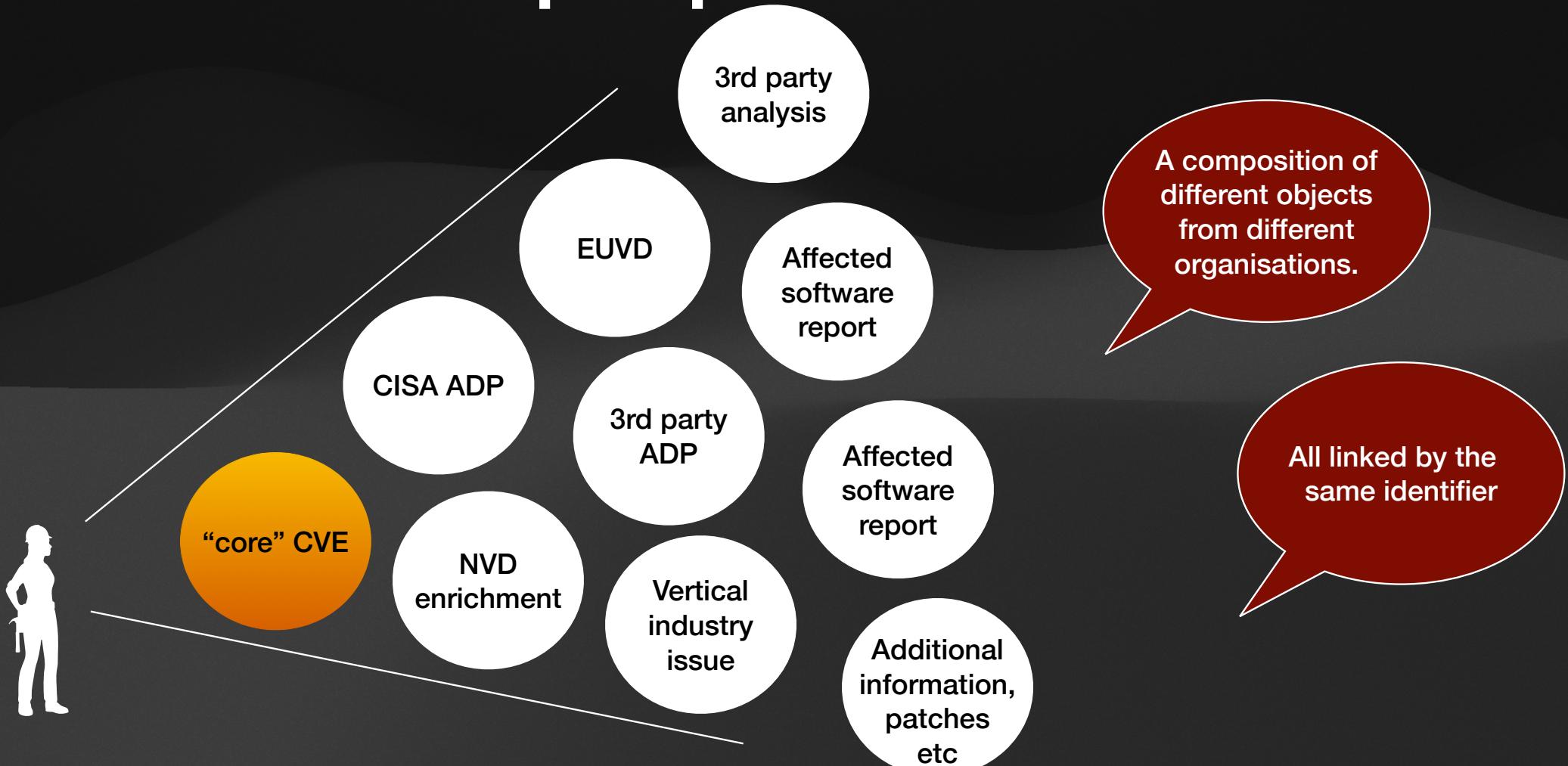
The GVIP project plan



A view of a potential solution



From the user perspective



Requirements for a new system





Summary of requirements

The global vulnerability intelligence platform

FEDERATION

Many sources, one shared view.

GLOBAL

Stakeholders and funding from across the globe.

FREE

Vulnerabilities are a public good

INTEROPERABILITY

A shared set of open standards and open data formats

NAMING

The creator names his creation

GLOBAL IDENTIFIER

A globally unique shared namespace

TRUST

Users needs to be able to validate data correctness and origin

REPLICATION

Users need local access to the data

EXTENSABILITY

Attackers and risk continuously change.

<https://www.gvip-project.org/docs/requirements/>



Coming steps



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)

2.

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



3.

OPTIONAL

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

Summary of the proposed process

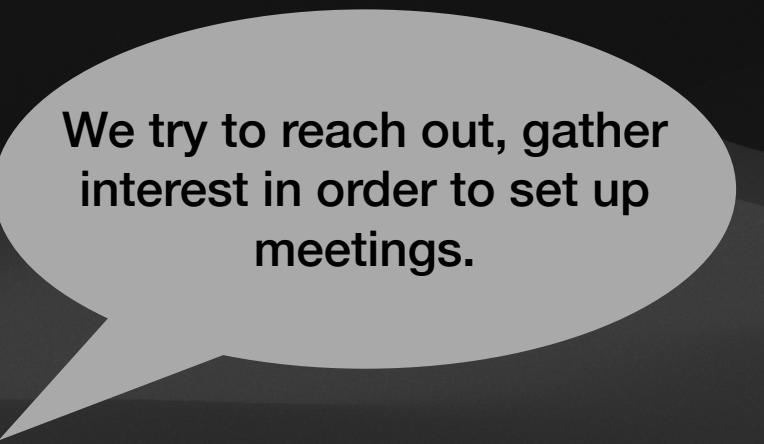
- 1: Reach an agreement on a working group - “interim board”
- that works on the next step of building an organisation
- 2: Organise a large amount of open workshops to gather input from stakeholders, try to form some level of baseline agreement on the way forward both on organisational and on technical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



Interested parties so far

Participating in the discussions

- OWASP Foundation
- OpenSSF
- Eclipse Foundation
- Erlang Ecosystem Foundation
- Apache Foundation
- Open Forum Europe
- The Sovereign Tech Resilience program
- aboutcode.org
- A large group of cybersecurity experts
- (These are the ones we have talked with. I guess there are many more)



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

The background features a dark navy blue gradient at the bottom transitioning to black at the top. Overlaid on this are several dark blue, wavy, horizontal lines of varying heights, creating a sense of depth and movement.

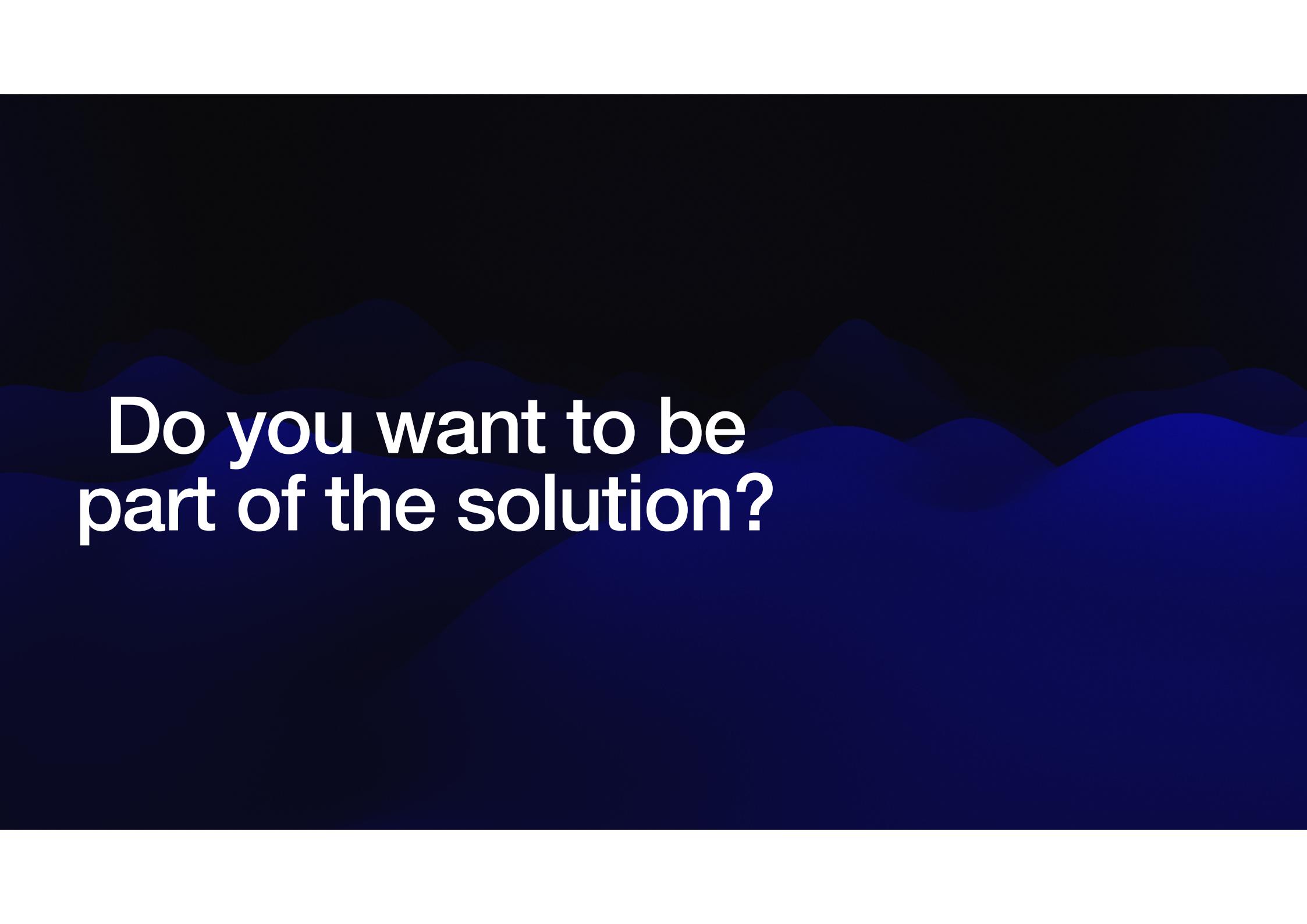
This will take time.



Patience, my friends, is a virtue



I think we can do this.



Do you want to be
part of the solution?

Points of contact



WWW.GVIP-PROJECT.ORG

- Web site: <https://www.gvip-project.org>
- LinkedIn, Mastodon
- Mailing list: cve@owasp.org
<https://groups.google.com/a/owasp.org/g/cve>
- OpenSSF Vulnerability disclosures working group
<https://github.com/ossf/wg-vulnerability-disclosures>
- Documents: github.com/gvip-project
- My email: **oej@edvina.net**

Q/A

oej@edvina.net

