MISP

INTELLIGENCE SHARING

Sharing information with MISP

An introduction to useful, trusted collaboration

MISP Project / CIRCL

https://www.misp-project.org/

Reference: 3 November 2026

What you will be able to explain

- What MISP shares and why context matters.
- How to choose recipients and a useful response.
- How feedback improves shared information.

Start with a shared question

- Team A investigates a suspicious sign-in message.
- It records `login-support.example` and `192.0.2.25`.
- Team B has seen the same domain in another report.
- What can they learn together, and what remains uncertain?

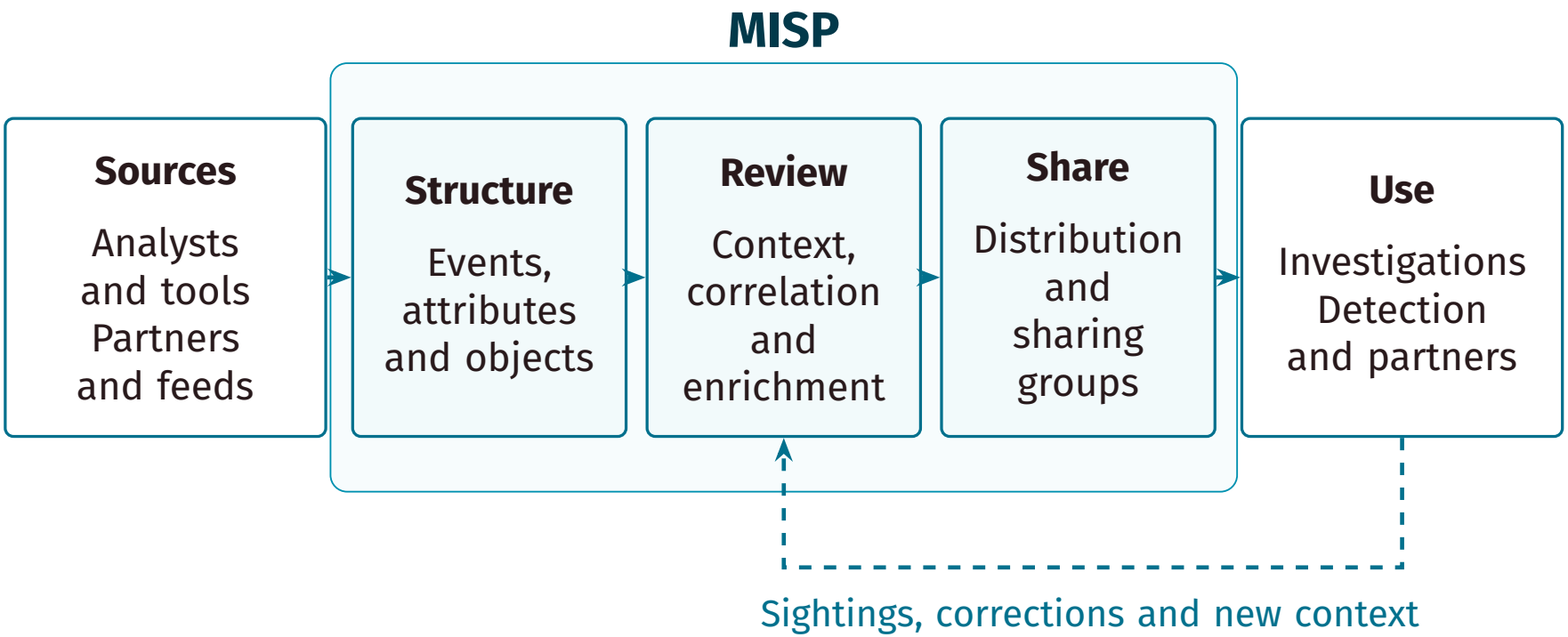
MISP makes observations reusable

- An open source platform for structured information sharing.
- A place to collect, connect and review threat information.
- A way for people and tools to collaborate across teams.
- A source of context for investigation, detection and response.

Keep the observation and its context together

- Event: the report or investigation context.
- Attribute: one typed observation, such as a domain.
- Object: related attributes grouped by a template.
- Tags and Galaxies: classification and structured context.

From observations to shared context



A correlation is a lead to investigate

- The same value can connect reports worth comparing.
- Check the source, timing and surrounding observations.
- Consider shared infrastructure, reuse and false positives.
- A match does not prove causation or attribution.

Choose the action before choosing the output

- Investigate: use the context to ask better questions.
- Detect or hunt: look for relevant observations in your data.
- Block: apply a reviewed policy with acceptable impact.

Choose who may receive the information

- Use distribution settings and sharing groups deliberately.
- Check the event, attributes and intended recipients.
- Use handling labels such as TLP alongside access controls.
- Review publication and exchange settings before sharing.

Quality improves through a feedback loop

- Record provenance, confidence and useful time context.
- Review warninglist hits and enrichment results.
- Add sightings, corrections and false-positive feedback.
- Reassess old information and update the intended use.

A sharing community needs a working agreement

- Agree on purpose, participants and expected contributions.
- Define handling, review and correction practices.
- Start with a small trusted group and useful information.
- Connect other communities when the policy supports it.

Turn common obstacles into a first step

Obstacle	Useful first step
Limited time	Share a small, structured observation with its source.
Uncertainty	State what is known, unknown and open to correction.
Different tools	Agree on shared terms and use supported exchange formats.
Handling obligations	Review purpose, recipients and applicable policy with the responsible people.

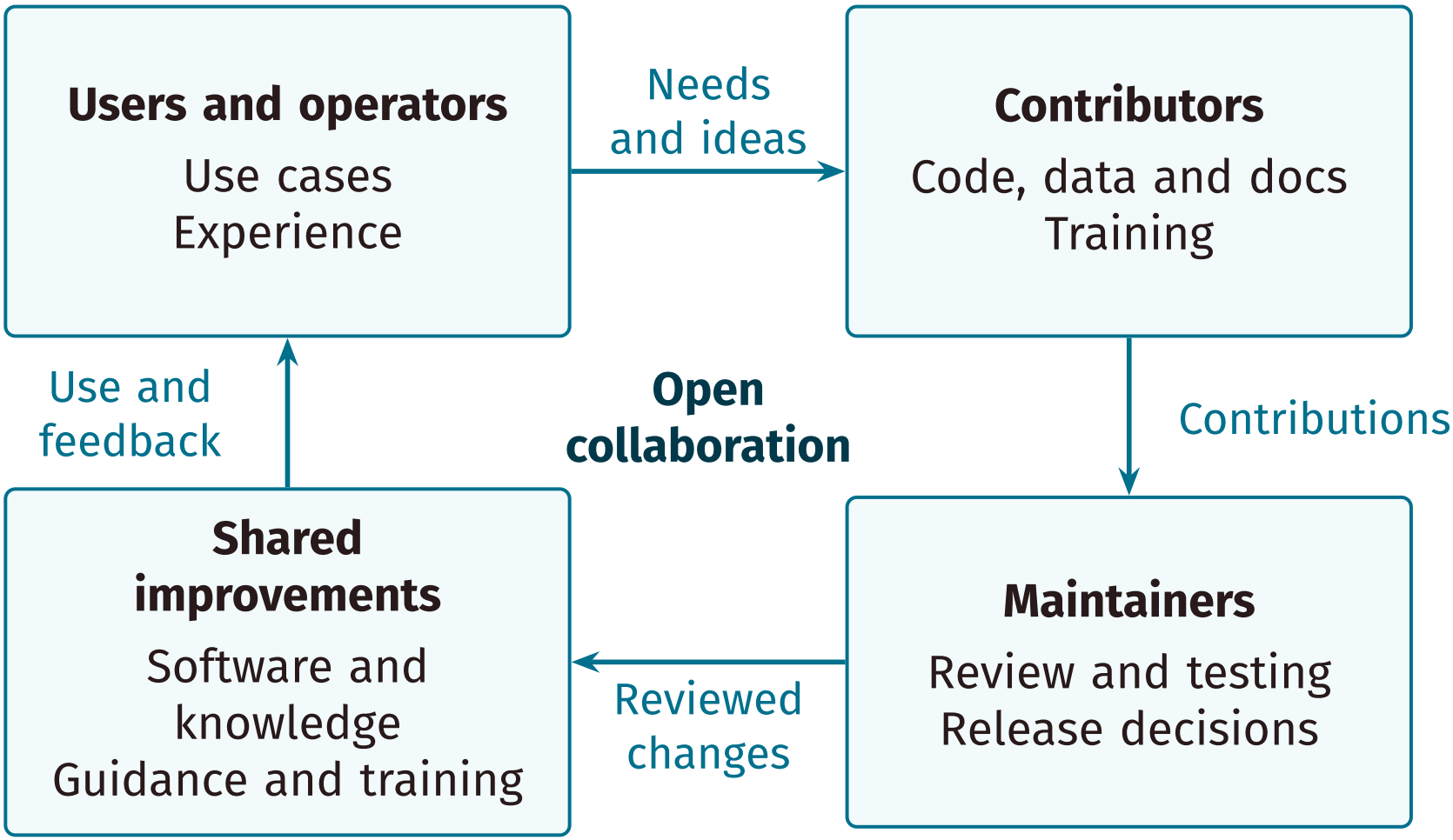
The project grew from a practical need

- Malware analysts wanted to avoid duplicated work.
- The early platform grew through practical user feedback.
- CIRCL and a wider community develop and improve MISP.
- Useful contributions include code, knowledge and training.

The MISP project is more than one application

Software	Knowledge	Standards	Communities
MISP platform REST API and PyMISP misp-modules	Taxonomies Galaxies Warninglists	Data formats Vocabularies Object templates	Trusted partners Shared practices Training and feedback

The community shapes MISP



A first exercise: explain a useful record

1. Draft a private, unpublished event for the synthetic report.
2. Add the domain and IP with source, time and uncertainty.
3. Explain a possible correlation and a suitable next action.
4. Review recipients and handling before any publication.

Continue with the task you need

- Everyday analysis: MISP usage and tagging.
- Richer context: objects, Galaxies and information quality.
- Integration: the REST API and PyMISP workshops.
- Community operation: administration and sharing practices.

Share useful context, then keep improving it

- Structure the observation and preserve its meaning.
- Choose the audience and action deliberately.
- Use feedback to improve quality and shared understanding.