MISP

INTELLIGENCE SHARING

An introduction to information sharing

From observations to useful decisions with MISP

MISP Project / CIRCL

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

Reference: 3 November 2026

What you will be able to do

- Explain how observations become useful shared context.
- Distinguish data, interpretation and operational action.
- Choose an audience and an exchange method deliberately.
- Describe how feedback keeps information useful.

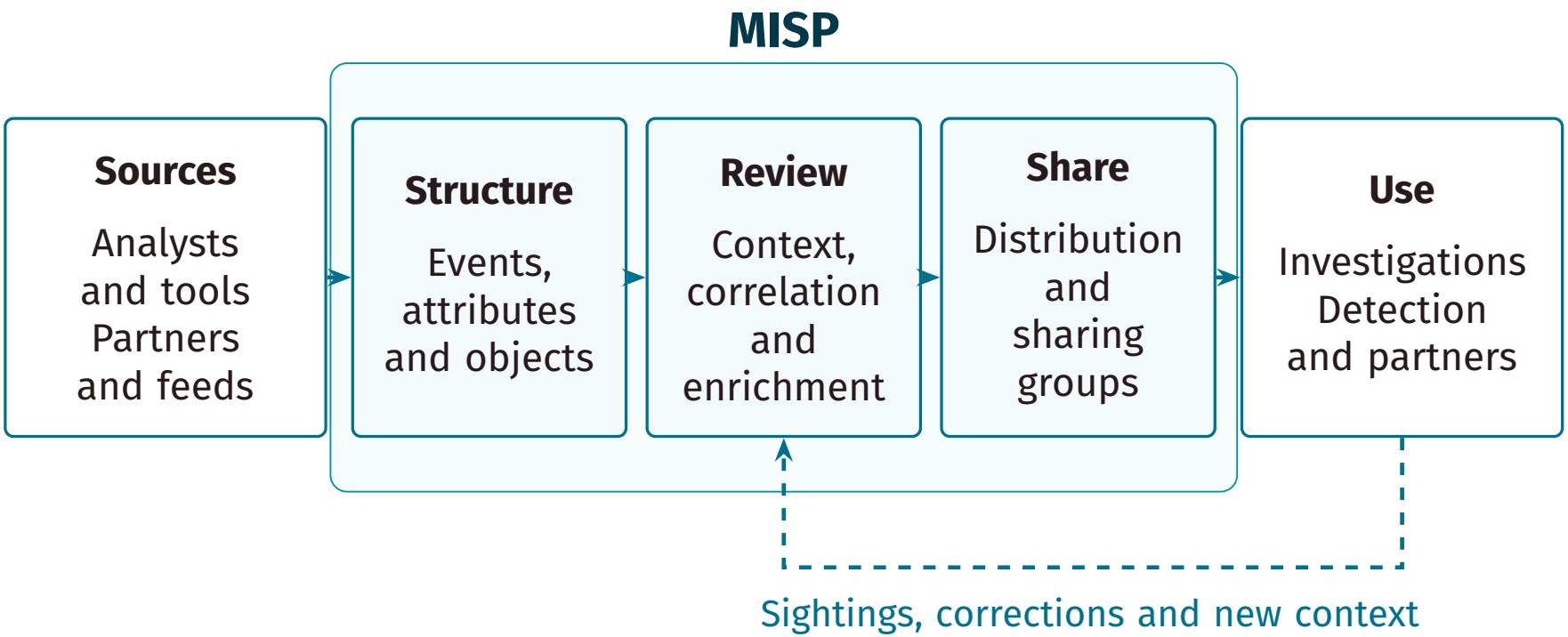
One case, two teams

- 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 reuse? What must they still establish?

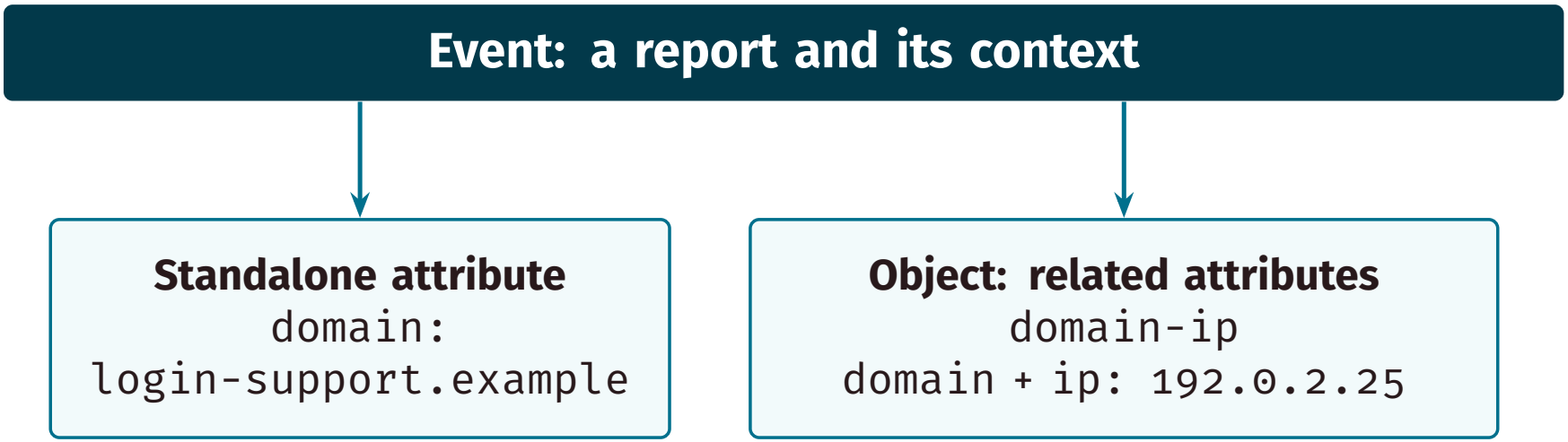
MISP supports people and tools

- An open source platform for structured information sharing.
- Collect observations from analysts, tools and partners.
- Connect and review records without losing their context.
- Provide useful inputs for investigation, detection and response.

From observations to shared context



A small model for a useful record



Tags and Galaxy clusters add context; sightings add observation feedback.

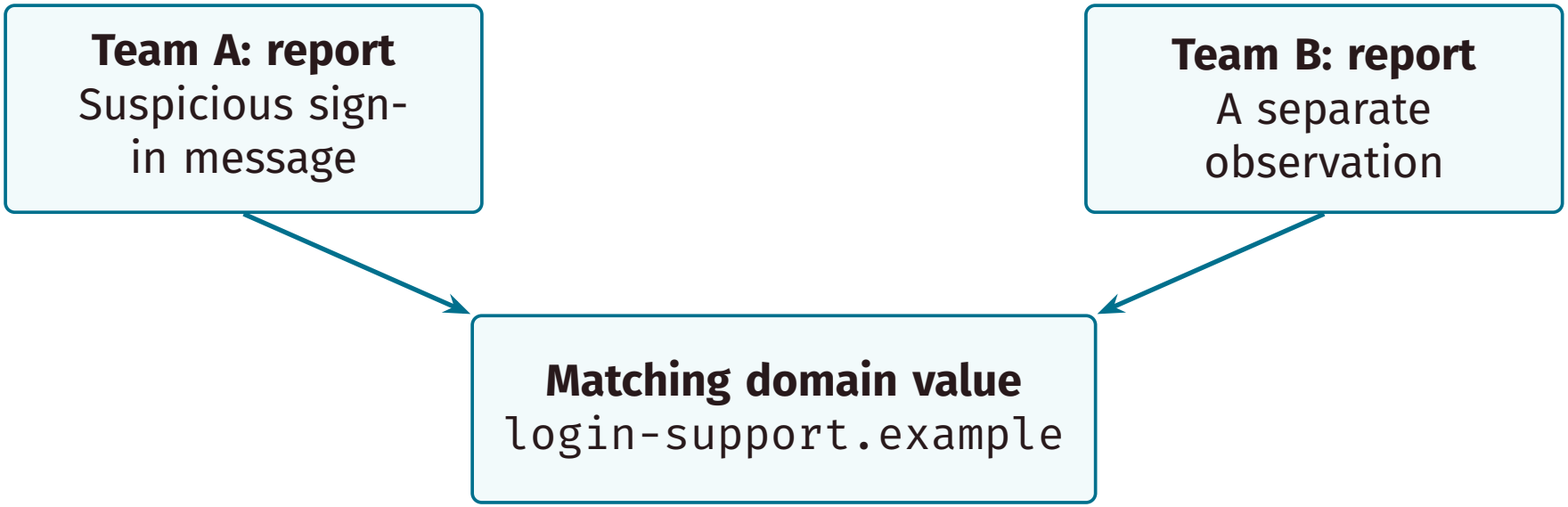
Describe the observation before acting on it

- Type: the form of a value, such as `domain` or `ip-dst`.
- Category: a broad contextual classification.
- Comment, source and time: what supports this observation?
- `to_ids`: eligibility under an export policy, not proof.

Add classification and reusable knowledge

- Taxonomy tags provide shared classification terms.
- Galaxy clusters add structured knowledge and relationships.
- ATT&CK techniques can describe supported behaviour.
- Keep observation, assessment and uncertainty distinct.

A correlation asks a question



Compare sources, times and context.
A match does not establish a shared actor or campaign.

The same record can support different actions

- Investigate: compare reports and test a hypothesis.
- Detect or hunt: search for relevant observations.
- Block: use a reviewed policy and assess the impact.
- Record the decision and how it can be reconsidered.

Choose recipients using MISP controls

Distribution choice	Intended scope
Your organisation only	The owning organisation.
This community only	The local instance community.
Connected / all communities	Wider sharing subject to exchange rules.
Sharing group	An explicitly defined permitted audience.

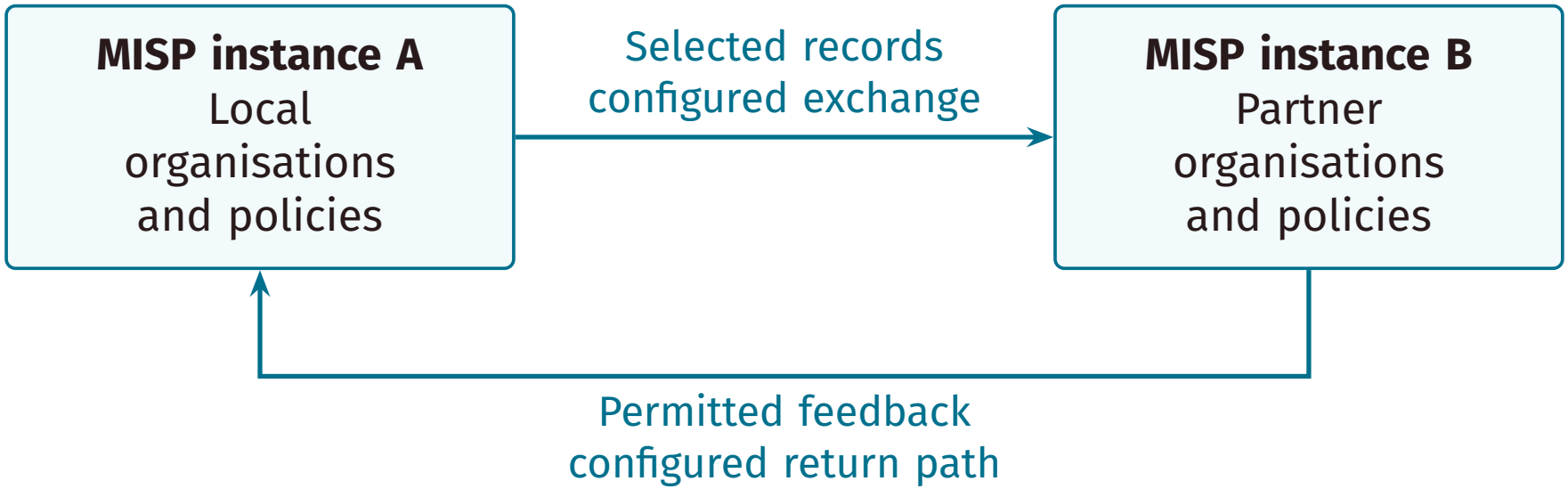
Handling labels and access controls do different jobs

- TLP 2.0 communicates handling expectations.
- Distribution and sharing groups control MISP visibility.
- Review sensitive details, purpose and recipient obligations.
- A label alone does not enforce the permitted audience.

Publication is a deliberate step

1. Review the record, source and intended use.
2. Check event and finer-grained distribution and tags.
3. Confirm the configured sync, feed or export destination.
4. Publish or exchange only under the agreed policy.

Instances exchange selected information



MISP instance C
No network exchange
in this example

No automatic global network.
Manual transfer also needs review.

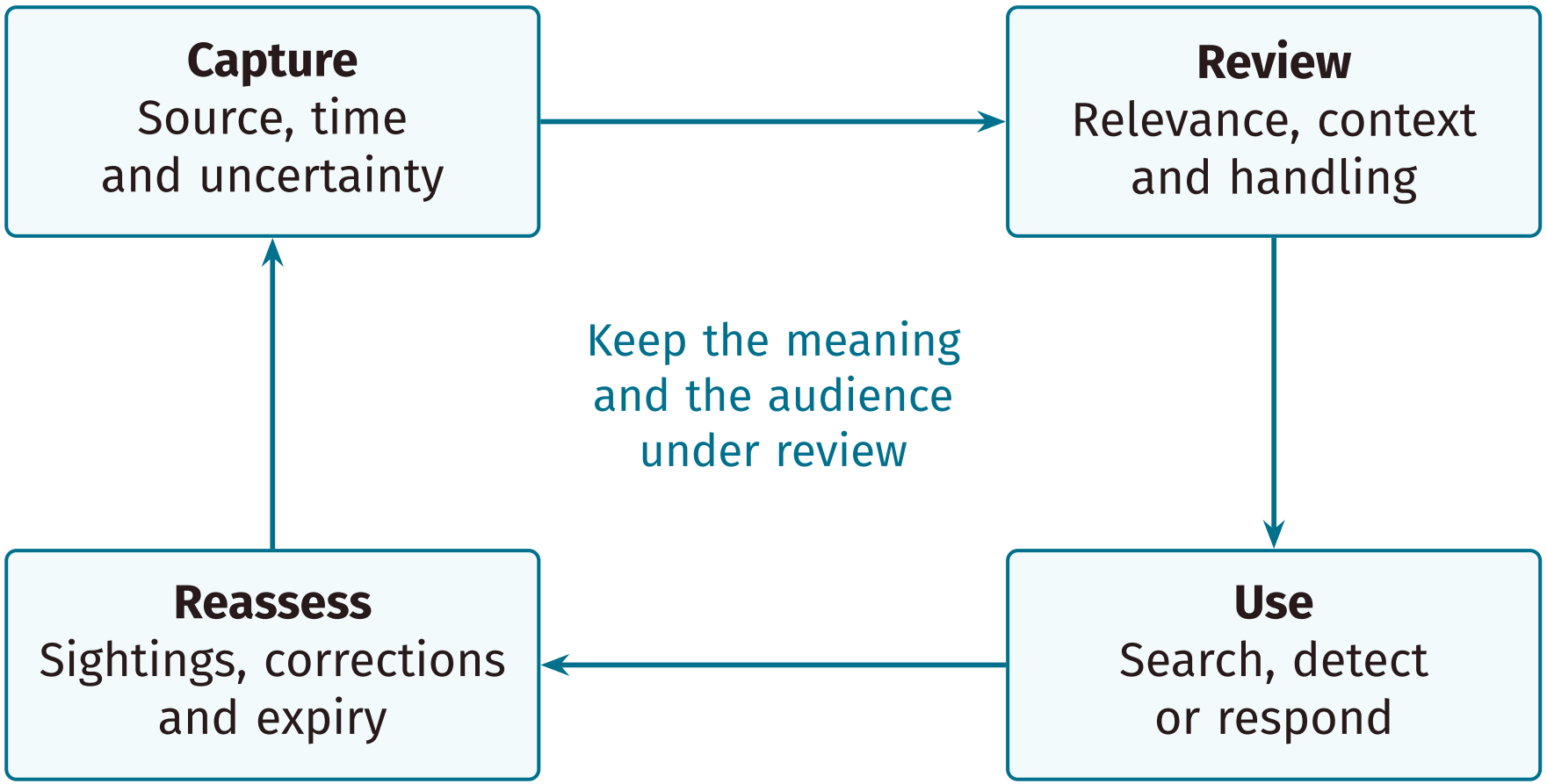
Choose the exchange method for the need

- Synchronisation: selected exchange between MISP instances.
- Feeds: fetch data from a configured provider.
- API and exports: integrate with a specific consumer.
- Manual transfer: review the file and destination too.

Collaborate while keeping responsibility clear

- Event ownership identifies who maintains the record.
- Proposals let others suggest attribute changes.
- Extended events can add another organisation’s context.
- Agree how corrections reach the responsible people.

Quality is a cycle, not a checkbox



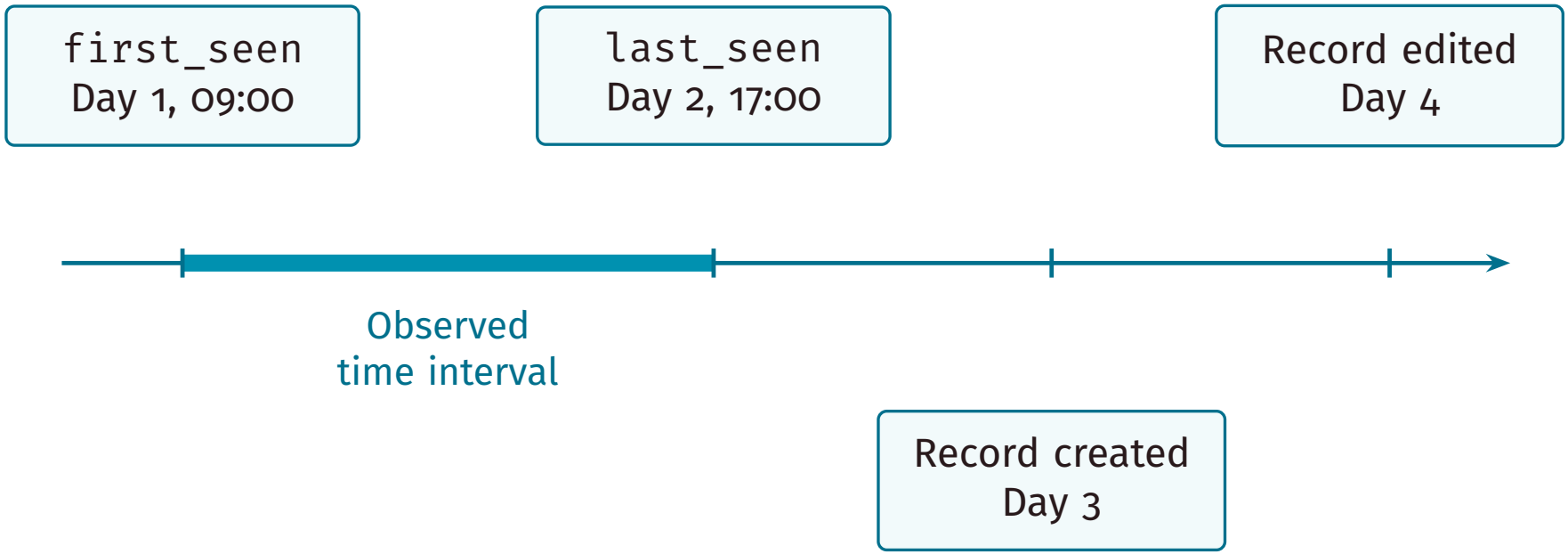
Use review aids without outsourcing judgment

- Warninglists flag potentially misleading values.
- Enrichment adds context from selected sources.
- Compare provenance and keep uncertainty visible.
- Check what an external module sends to its provider.

Sightings communicate different kinds of feedback

- Sighting: an observation of the data point.
- False positive: feedback about an unsuitable interpretation.
- Expiration: feedback that relevance has ended.
- Include the source and time; agree how feedback is used.

Observation time is different from record time



Fictional dates. An edit does not mean the activity happened again.

Age and decay support reassessment

- Different observations have different useful lifetimes.
- A decay model provides a review or filtering signal.
- Review the model, sightings and consumer policy.
- Keep historical context when an operational use expires.

Automate a reviewed decision

- Use the REST API and PyMISP for defined workflows.
- Filter for the consumer, purpose and audience.
- Test with synthetic data and inspect the output.
- Return feedback and handle failures explicitly.

A community needs a working agreement

- Agree purpose, participants and expected contributions.
- Define handling, correction and escalation practices.
- Start with a small trusted group and useful records.
- Revisit the agreement as people and use cases change.

Turn obstacles into a first contribution

Obstacle	A useful first step
Limited time	Share a small observation with a source.
Uncertainty	State what is known and open to correction.
Different tools	Agree vocabulary and supported formats.
Handling obligations	Review purpose and recipients with responsible people.

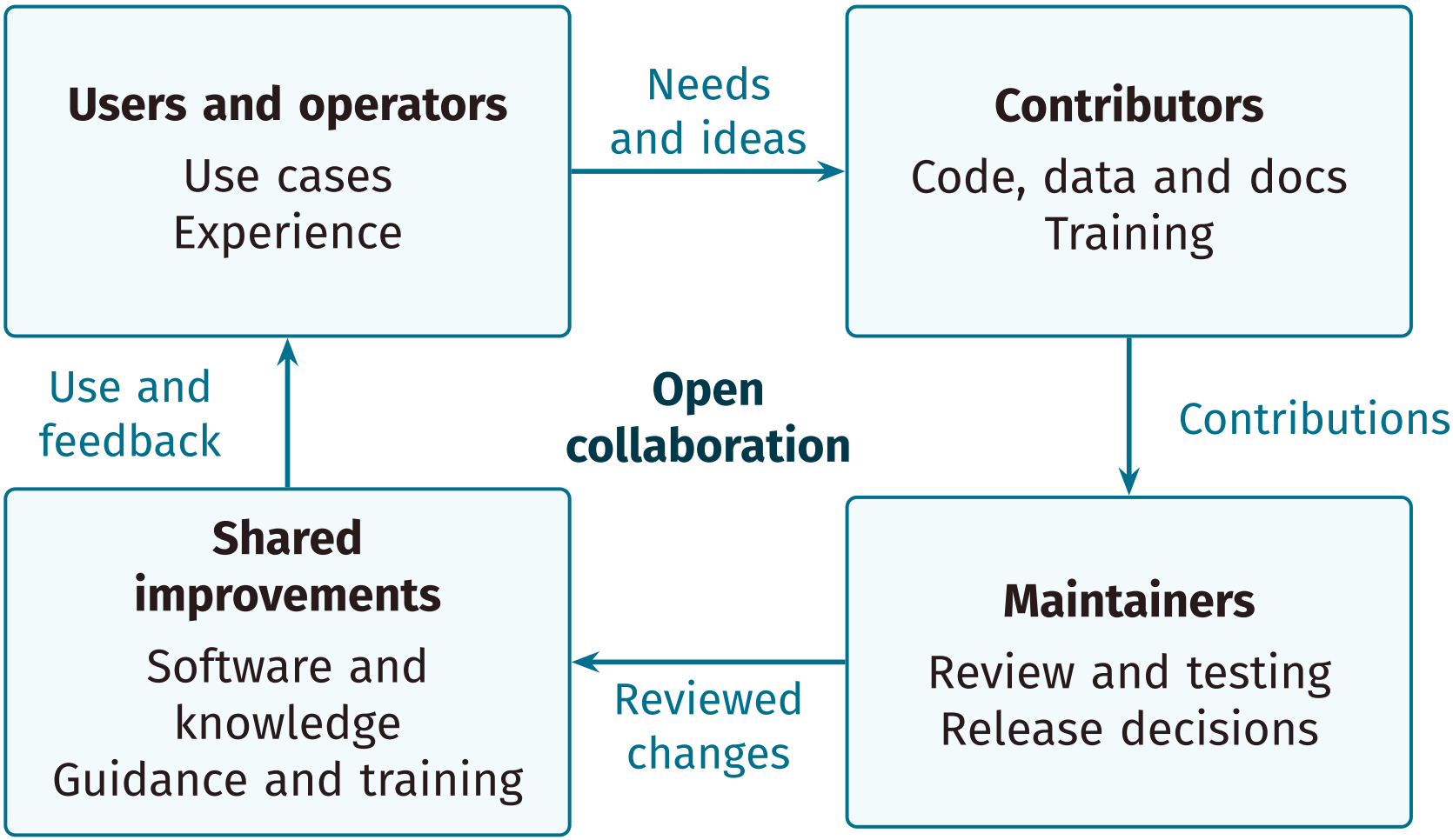
The project grew from a practical need

- In 2012, malware analysts wanted to avoid duplicate work.
- Christophe Vandeplas's early platform work became MISP.
- CIRCL and a wider community develop and improve it.
- Contributions include code, shared knowledge and training.

The MISP project has four complementary parts

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 improves the project



Exercise: make the case useful to Team B

1. Draft an event with the synthetic domain and IP.
2. Explain the source, time, relationship and uncertainty.
3. Choose a limited audience and a justified next action.
4. Describe how a correction would reach Team B.

Debrief: explain the decisions

- The matching domain is a lead, not attribution.
- An object groups a relationship that the source supports.
- Handling labels and visibility settings both need review.
- A hunt may be justified before any blocking decision.
- A correction needs an owner and a return path.

Continue with the task you need

- Everyday analysis: MISP usage, tagging and objects.
- Context and quality: Galaxies and indicator decay.
- Integration: REST API, PyMISP and feeds.
- Community operation: administration and sharing practices.

Share context, choose deliberately, keep improving

- Structure observations without losing their meaning.
- Choose recipients and action under an agreed policy.
- Use feedback to correct and reassess information.
- Contribute practices and knowledge as well as software.