MISP

INTELLIGENCE SHARING

MISP best practices

Building sharing communities and useful intelligence

Team CIRCL

TLP:CLEAR

Reference: 3 November 2026

What you will practise

- Build a community around a shared operational need.
- Choose an audience and check the actual sharing path.
- Encode context that people and tools can use.
- Turn feedback into corrections and better exports.

Start with a decision, then choose the data

- **Incident response:** find related activity and coordinate help.
- **Proactive work:** compare research, sensors and public reports.
- **Advanced services:** support forensics and coordinated vulnerability handling.
- **Community services:** connect members facing similar threats.

CIRCL's experience: different communities, different needs

- Private-sector and CSIRT communities connect varied capabilities.
- Sector communities need specialised context and vocabularies.
- Cross-sector initiatives such as X-ISAC help bridge those groups.
- Exercise communities provide a place to rehearse collaboration.

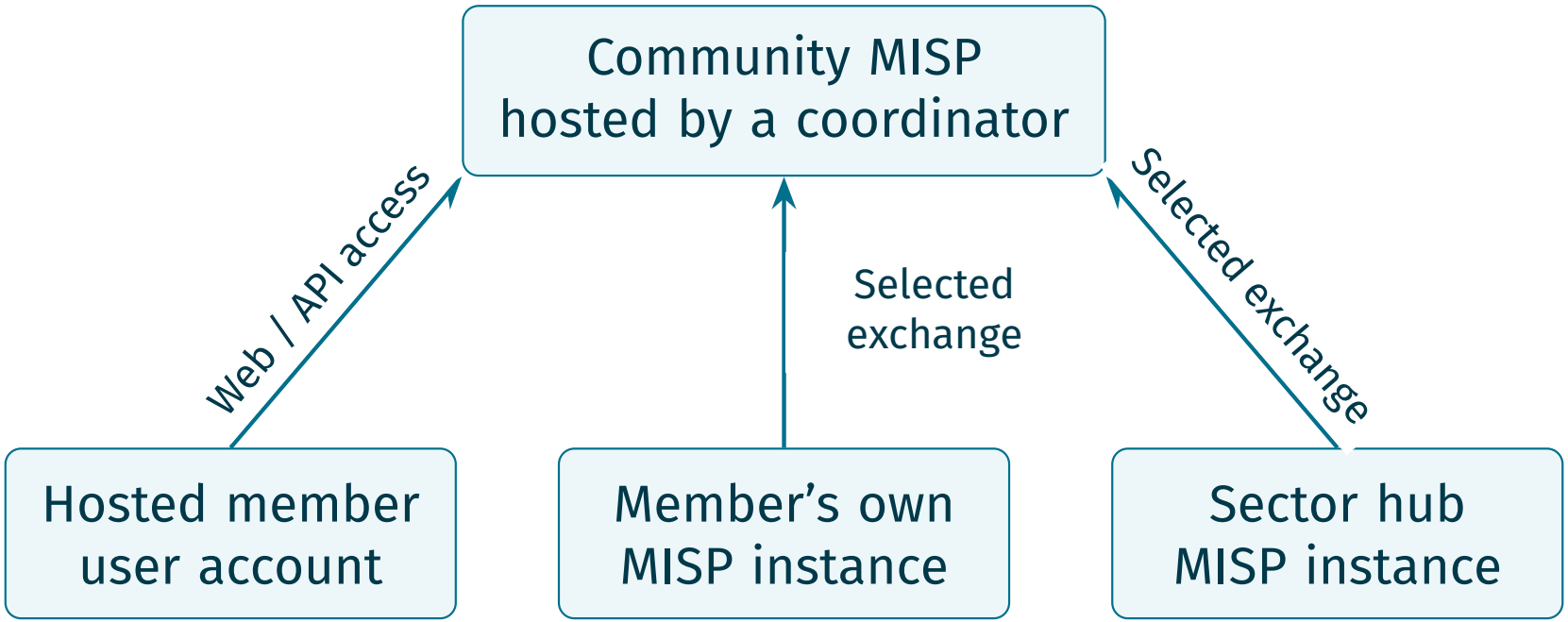
Cross-sector sharing needs a purpose

- Reused infrastructure or techniques can affect several sectors.
- Another community may already have analysis or a mitigation.
- Agree what can cross the boundary before an incident.
- Share the useful finding with its source and restrictions.

Write a small community charter

- **Purpose:** priority questions, members and expected benefit.
- **People:** coordinators, contributors and escalation contacts.
- **Rules:** joining, leaving, handling and permitted use.
- **Service:** onboarding, feedback and incident support.
- **Review:** agree when to revisit scope and membership.

Three ways for members to participate



Choose according to capacity, ownership and handling needs.

Lead by example and lower the first barrier

- Publish a small, well-explained example for members to copy.
- Offer templates, pairing sessions and a named contact.
- Accept useful partial findings with uncertainty made explicit.
- Give credit and show how a contribution helped someone.

Participation is more than publishing events

- Analysis, enrichment and requests for assistance all add value.
- Sightings and false-positive reports improve existing work.
- Help consumers become confident contributors over time.
- Avoid volume quotas that reward duplicated or weak data.

Agree handling and privacy before sharing

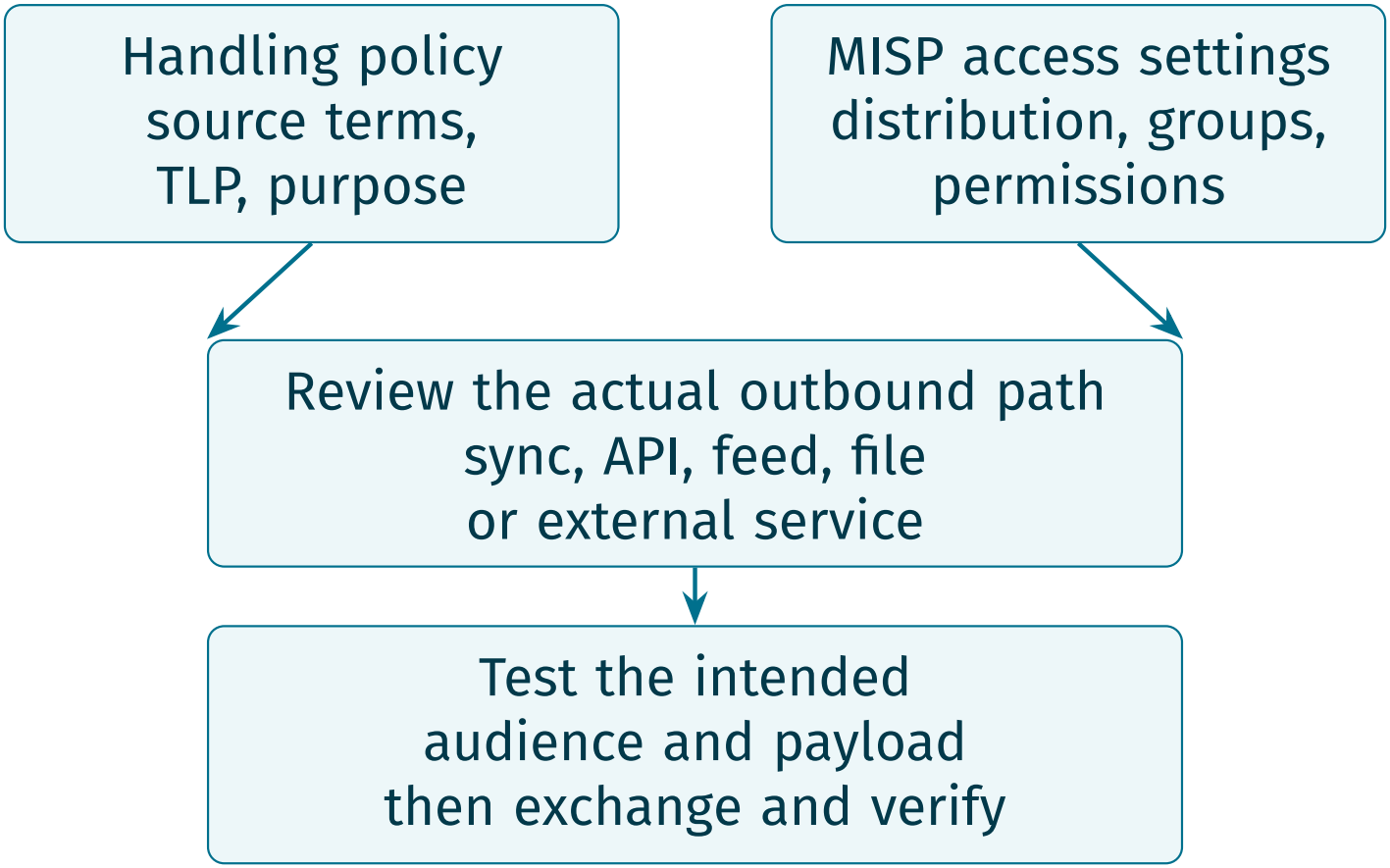
- Identify the purpose, recipients and permission to disclose.
- Minimise personal, victim and unrelated operational details.
- Agree retention, correction and incident escalation processes.
- Resolve legal and contractual questions with the responsible advisers.

Use current TLP 2.0 markings

TLP:CLEAR	No TLP limit on onward sharing; other obligations still apply.
TLP:GREEN	Share within the relevant community, away from public channels.
TLP:AMBER	Need-to-know sharing within the recipient organisation and its clients.
TLP:AMBER+STRICT	Need-to-know sharing within the recipient organisation only.
TLP:RED	Individual recipients only; no further disclosure.

TLP communicates boundaries; configure access separately.

Align the policy, the audience and the path



A marking alone does not configure a MISP access rule.

Select distribution deliberately

- Start sensitive drafts with **Your organisation only**.
- Use a **sharing group** for an explicitly defined set of organisations.
- Review event, object and attribute distribution together.
- An attribute cannot widen its event's permitted audience.
- Test access with both an intended and an excluded recipient.

Sub-communities need maintained boundaries

- Use sharing groups where members can share one platform.
- Consider separate instances when governance or operations differ.
- Name an owner for membership and periodic access reviews.
- Review manual exports, feeds and disconnected transfers too.

Publication is not a privacy switch

- Saving a draft and publishing it are separate actions.
- Unpublished data can still be visible to authorised users and API clients.
- Publication can trigger notifications and configured exchange.
- Preview the destinations, then verify delivery and visibility.

Build a record another analyst can understand

- **Provenance:** source, collection method and original reference.
- **Meaning:** what happened, why it matters and what is uncertain.
- **Time:** observation window, time zone and review date.
- **Action:** suggested use, owner and feedback contact.

Use the data model to preserve relationships

- Group related findings in an event with a meaningful scope.
- Use typed attributes for individual values.
- Use object templates for related fields such as an email or file.
- Link objects and cite the evidence behind the relationship.

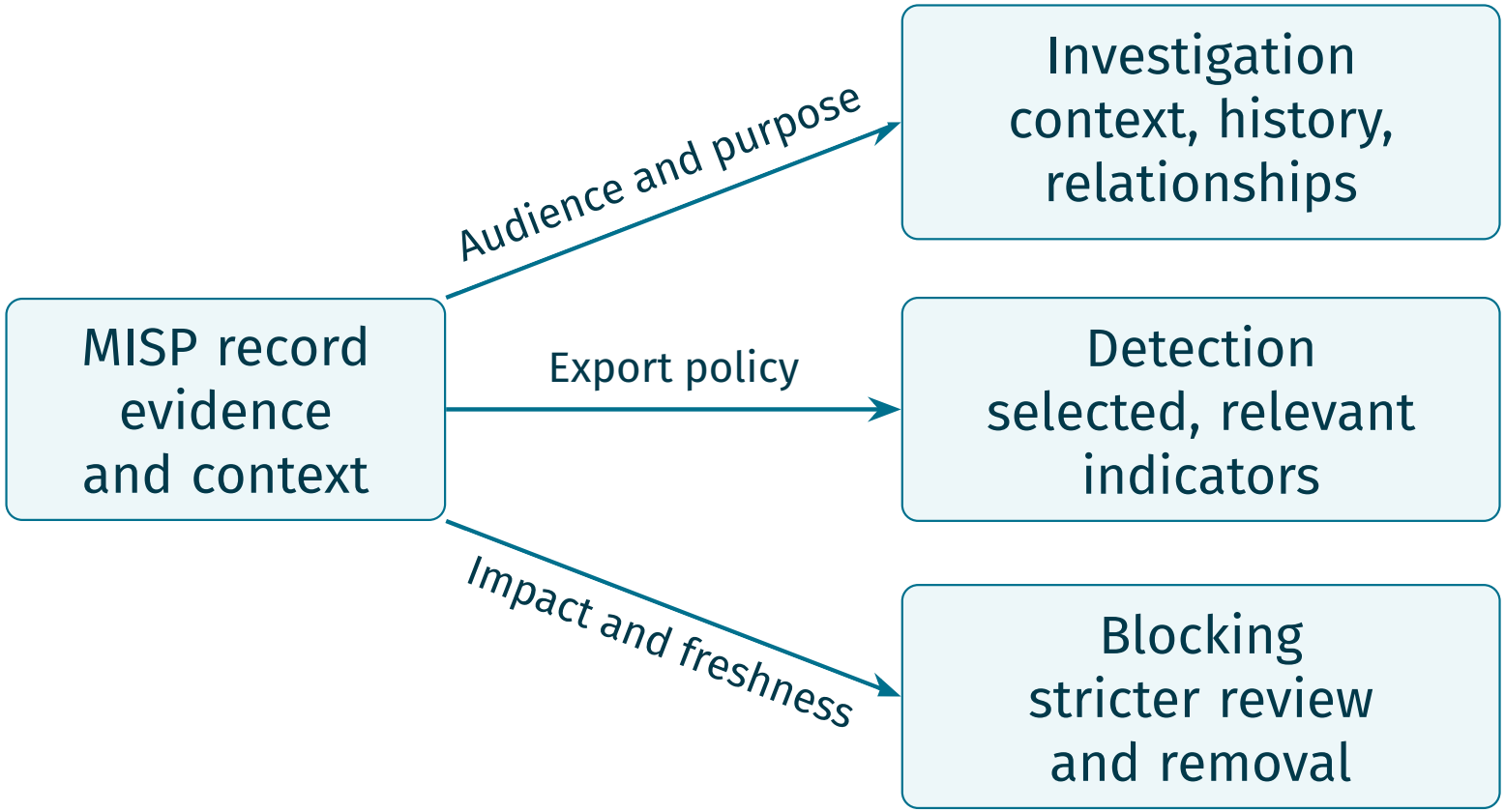
Choose a small, shared vocabulary

- Agree taxonomies for handling, confidence and analysis state.
- Define which tags apply to a whole event or individual attributes.
- Use galaxy clusters for evidence-backed malware, actors or techniques.
- Document local conventions; reuse upstream vocabularies first.

Enrichment has an outbound data flow

- Check what a module sends and which service receives it.
- Review source terms and handling before submitting a value or sample.
- Preserve the enrichment source, time and uncertainty.
- Review results before saving or propagating new claims.

One dataset, different decisions



Keep useful context; select action data for each consumer.

Treat `to_ids` as an input to export policy

- Enable it for attributes intended for detection use.
- Leave it off for contextual values such as a report's author.
- It does not grant access or establish maliciousness.
- Make export filters explicit; inspect what the consumer receives.

Handle false positives without losing the explanation

- A warninglist match prompts review of the value’s role.
- Shared hosting or a resolver may be relevant context.
- Exclude unsuitable values from action exports and explain why.
- Report the problem to the owner; agree who corrects it.

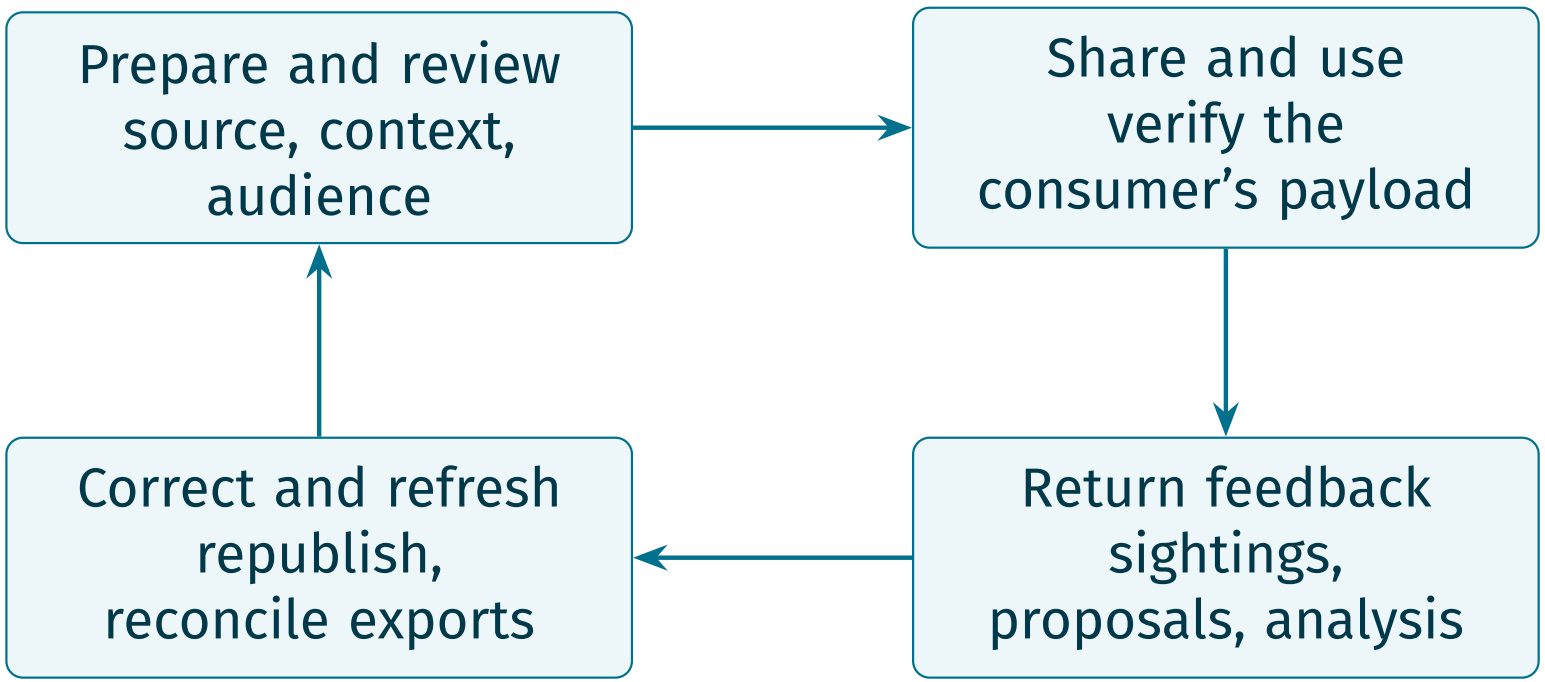
Age changes operational usefulness

- Record when the activity was observed, not just imported.
- Set review intervals appropriate to the data and the action.
- Use sightings and decay models to support reassessment.
- Remove stale action data from downstream tools as well.

Make feedback easy to act on

- **Sightings:** report an observation, false positive or expiration.
- **Proposals:** suggest attribute changes for the owner to review.
- **Extended events:** add separately owned analysis and context.
- **Analyst data:** record notes, opinions and relationships.

Close the loop after a correction



Assign an owner and a response expectation for each step.

Measure benefit and operational health

- How quickly do useful findings and corrections reach members?
- Which contributions led to a decision or a useful investigation?
- Are sync jobs, workers and consumer updates completing?
- Are false positives, stale exports and access issues resolved?

Demonstration: review a small phishing report

- Work in a lab, with organisation-only distribution initially.
- Create a fictional report containing `login.example.org`.
- Add provenance, observation time and a contextual email object.
- Inspect warninglist hits and decide which fields are detection candidates.

Exercise: check the audience and the consumer

1. Choose a lab sharing group and a compatible handling marking.
2. Check visibility with an included and an excluded lab account.
3. Preview a detection export; explain any missing values.
4. Submit a correction and verify the resulting lab export.

Before the next community contribution

1. Is the finding useful, sourced and clear about uncertainty?
2. Are the audience, handling and outbound paths appropriate?
3. Are contextual and actionable values distinguished?
4. Can recipients report a problem and receive the correction?

References for the operator and trainer

- Guidelines for setting up an information-sharing community
- Best Practices in Threat Intelligence
- MISP Book: usage, sharing, sightings and warninglists
- FIRST: TLP 2.0 definitions and usage guidance
- MISP compliance resources

Keep the community conversation going

- Share a small useful finding and ask for specific feedback.
- Bring one handling or integration question to the next meeting.
- CIRCL: info@circl.lu — https://www.circl.lu/
- MISP: https://www.misp-project.org/
- Contributions: https://github.com/MISP