MISP

INTELLIGENCE SHARING

MISP Galaxy in 2.5

Explore the knowledge base, assess context, share carefully

CIRCL / MISP Project

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

Reference snapshot: 30 October 2026

Find context, assess evidence, make an assertion

- Explore the knowledge base beyond actor names.
- Choose the right cluster and attachment scope.
- Interpret relations and matrices carefully.
- Practise discovery, custom knowledge and contribution.

Explore the knowledge base

A large, reusable body of knowledge

- 136 Galaxy definitions and 136 cluster collections.
- 58,528 entries; 56,551 distinct cluster UUIDs.
- 79,372 listed directed relationship edges.

Start with the public catalogue

- Browse https://www.misp-galaxy.org/.
- Follow JSON and original-source references.
- Inspect collection scope, authors, version and status.

Choose a family that answers the question

- ATT&CK: observed techniques, software and activity groups.
- D3FEND and preventive measures: defensive context.
- DISARM: information-manipulation techniques and responses.
- Country, sector, detection and other domain knowledge.

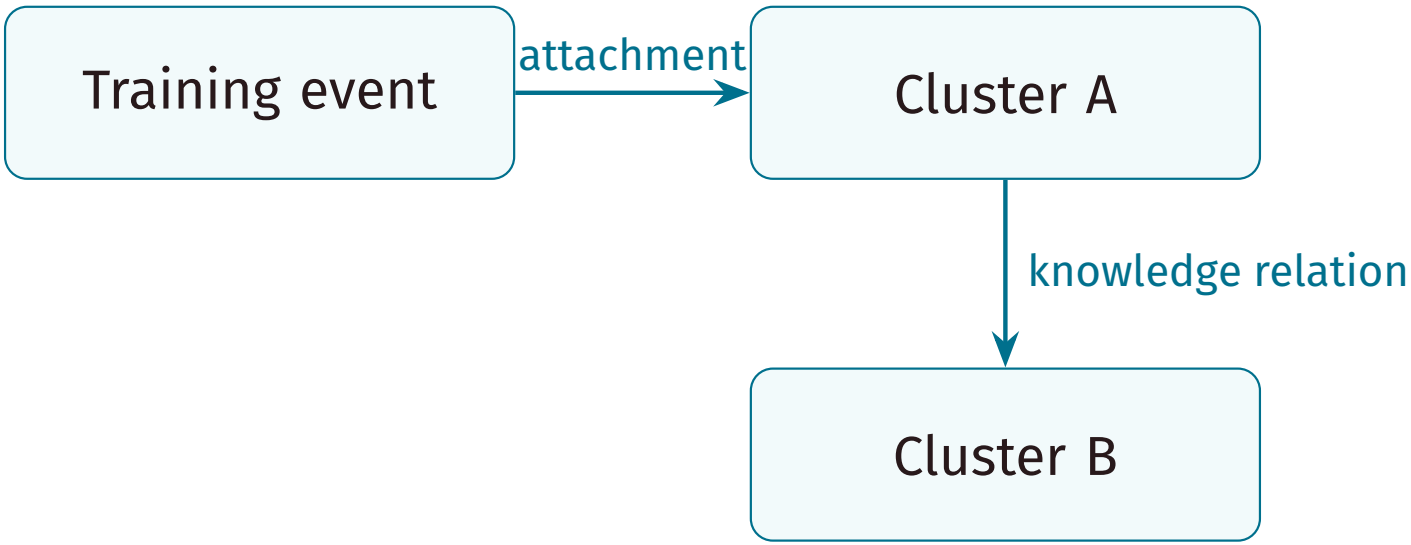
Galaxy, cluster and element

- Galaxy: the family and its presentation metadata.
- Cluster: one named concept with an individual UUID.
- Element: metadata such as synonyms, references or external IDs.

Context is different from incident data

- Taxonomy: classification vocabulary.
- MISP object: grouped typed attributes.
- Galaxy cluster: structured knowledge attached as context.

Three different links



An attachment does not create a cluster-to-cluster edge.

Search for identity, not just a familiar label

- Compare values, synonyms and external identifiers.
- Retain cluster UUID and collection provenance.
- Do not merge identities solely because names overlap.

Check whether the entry is current

- Read original references and collection version.
- Inspect revoked flags, deprecation metadata and historical descriptions.
- Check ATT&CK domain, platform and technique/sub-technique scope.

Apply context in MISP 2.5

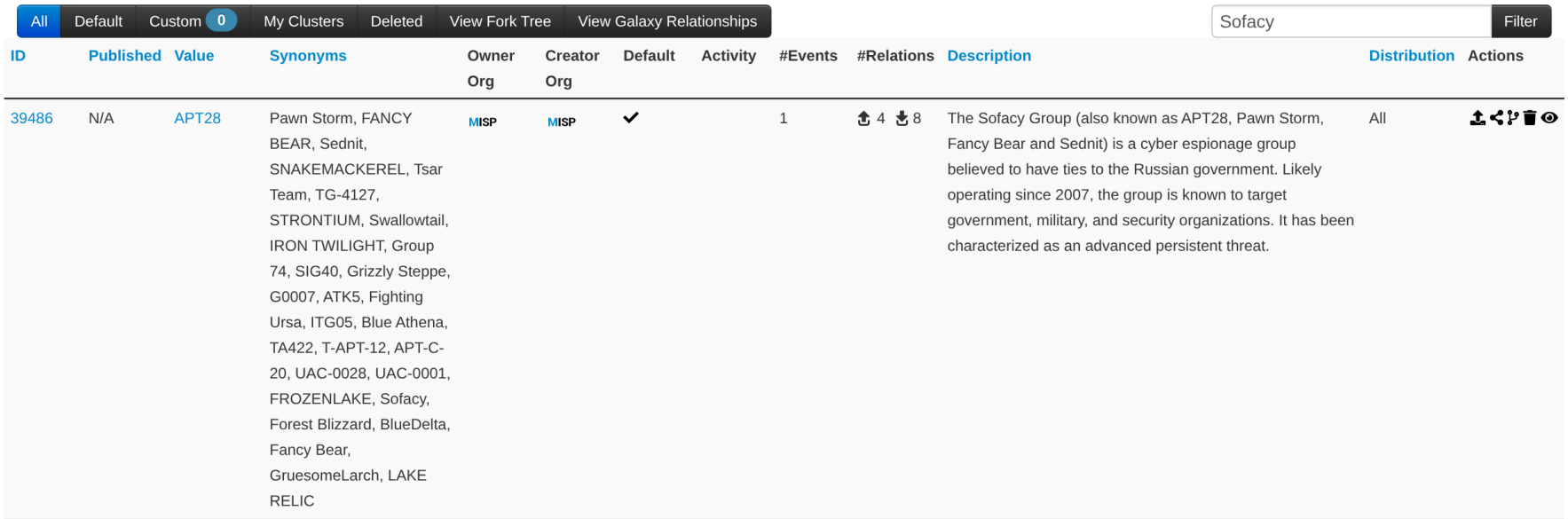
Choose the narrowest justified attachment

- Event scope describes the incident or report as a whole.
- Attribute scope can express a narrower observation.
- Verify the actual attachment after saving and exporting.

Use the installed cluster metadata

- Search and inspect the cluster before attaching it.
- MISP maintains a cluster-associated tag.
- Prefer UUID-backed identity over manually constructed labels.

Threat Actor: search for Sofacy



The APT28 result lists Sofacy as a synonym. Inspect the candidate.

MISP 2.5.50; synthetic lab, 1 November 2026.

Inspect the cluster identity and provenance

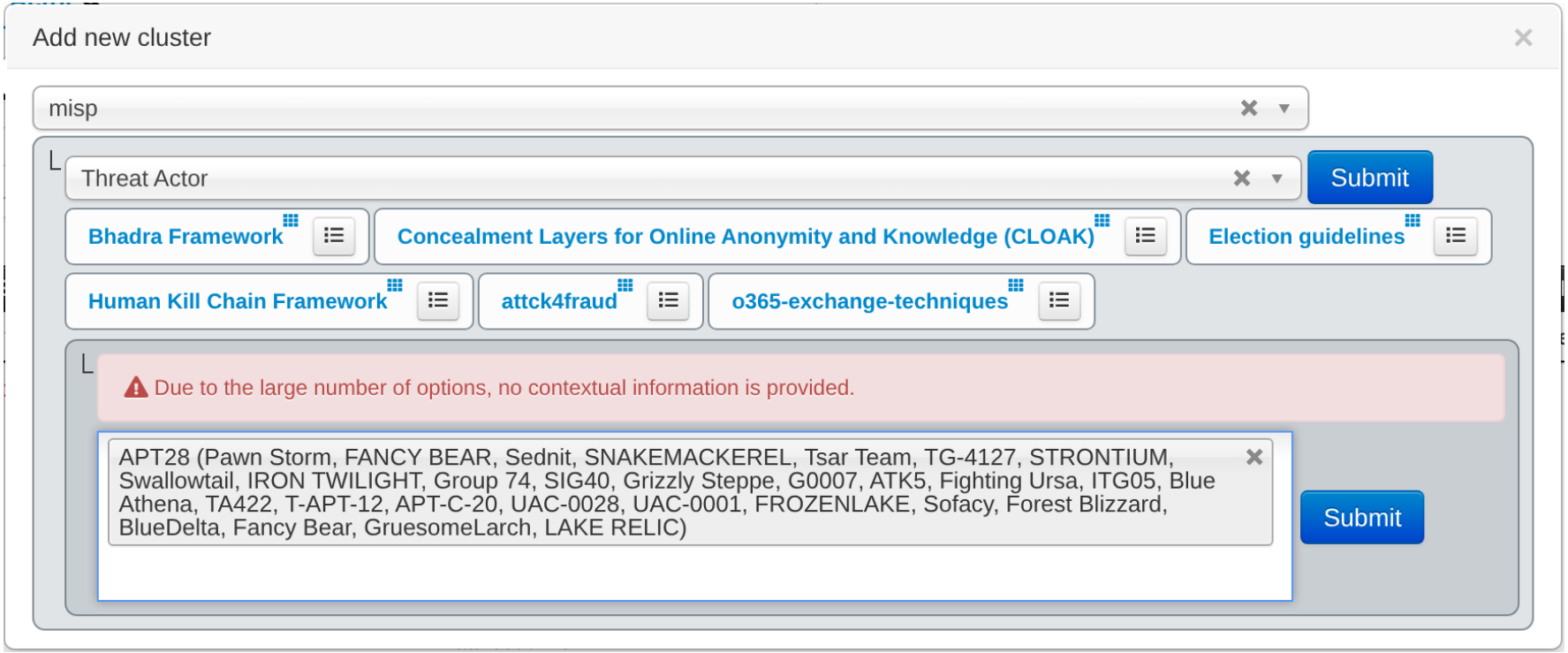
Threat Actor :: APT28

Cluster ID	39486
Name	APT28
Parent Galaxy	Threat Actor
Description	The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.
Default	Yes
Version	357
UUID	5b4ee3ea-eee3-4c8e-8323-85ae32658754
Collection UUID	7cdff317-a673-4474-84ec-4f1754947823
Source	MISP Project
Authors	Alexandre Dulaunoy, Florian Roth, Thomas Schreck, Timo Steffens, Various
Distribution	All communities
Owner Organisation	MISP
Creator Organisation	MISP
Connector tag	misp-galaxy:threat-actor="APT28"
Events	1 event
Attributes	1 attribute

Check the cluster UUID, collection, version and source.

MISP 2.5.50; synthetic lab, 1 November 2026.

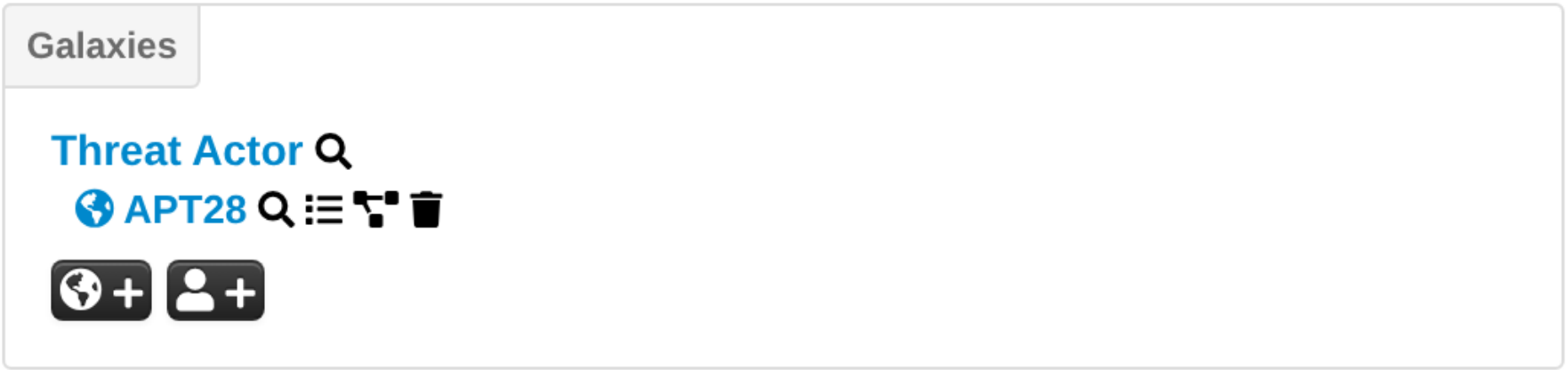
Attach the reviewed actor at event scope



Event Galaxies: Add new cluster → misp → Threat Actor.

MISP 2.5.50; synthetic lab, 1 November 2026.

Verify the saved event attachment



- APT28 appears under the event's Threat Actor Galaxy.
- Confirm UUID and scope in the saved event/export.
- An actor attachment records an assertion requiring evidence.

MISP 2.5.50; synthetic lab, 1 November 2026.

Keep visibility boundaries separate

- Event visibility controls incident access.
- Custom-cluster distribution controls knowledge access.
- Local attachment controls the association scope.
- Publication and sync settings control eligible sharing.

Matrix highlights are observations, not coverage

- Galaxy ordering defines matrix tabs and columns.
- Cluster kill-chain metadata places entries in that layout.
- A highlight does not establish detection or prevention efficacy.

Read graph edges as sourced assertions

- Inspect direction, relationship type and references.
- Review confidence or handling tags where supplied.
- Do not infer causality merely from a graph path.

Custom clusters and forks are supported

- Create permitted custom knowledge with explicit ownership.
- Fork a default cluster for local analysis.
- Record provenance, distribution and publication intent.

Updating files is different from updating the catalogue

- Select and update the intended Git revision.
- Import/update the MISP database through the operator workflow.
- Review changed knowledge and custom forks before sharing.

Explore, validate and contribute

Explore a pinned checkout offline

```
python3 examples/explore.py /tmp/misp-galaxy-lab --stats
python3 examples/explore.py /tmp/misp-galaxy-lab \
  --search T1059 \
  --collection mitre-enterprise-attack-attack-pattern \
  --limit 3
```

Repository structure: family versus collection

```
galaxies/training-knowledge.json
  type, namespace, name, uuid, version, description

clusters/training-knowledge.json
  type, name, uuid, version, source, authors, category
  values: [individual cluster entries]
```

An individual cluster can reference another

```
{
  "value": "Training observation A",
  "uuid": "<individual cluster UUID>",
  "meta": {"synonyms": ["Workshop A"]},
  "related": [{
    "dest-uuid": "<cluster B UUID>",
    "type": "related-to", "tags": []
  }]
}
```

Validate more than JSON syntax

- Check both repository schemas.
- Check identities, matching types and relationship targets.
- Exercise negative cases and inspect original sources.

Workshop: find, assess, attach

- Find a technique by external identifier and read its evidence.
- Compare a synonym search and a domain-specific collection.
- Attach to a disposable event; compare attribute and local scope.
- Inspect matrix/export results and remove training data.

Contribute at the correct source

- Manual collection: edit JSON with evidence and provenance.
- Generated collection: inspect the generator and upstream source.
- Preserve identities and update relevant versions.

Follow the current upstream validation workflow

```
./jq_all_the_things.sh
# Review and commit intended normalised changes.
./validate_all.sh
```

Make knowledge reusable and reviewable

- State source, identity, meaning and uncertainty.
- Keep attachment scope separate from knowledge distribution.
- Include reproducible examples and validation limits.
- Use the README for pinned references and workshop commands.