SAND5G

https://sand5g-project.eu/

Discover MISP

The Open Source Threat Intelligence and Sharing Platform

MISP Threat Sharing

This project has received funding from the DIGITAL EUROPE (DIGITAL) programme under Grant Agreement No 101127979

What is MISP

MISP Overview

MISP is an open-source platform supporting collection, analysis, and sharing of cyber threat intelligence for collaboration.

Importance of Information Sharing

Sharing threat intelligence reduces detection time and enhances response by breaking information silos across organizations.

Contextualized Threat Data

MISP enriches indicators by linking them to malware families, campaigns, and actors to create actionable intelligence.

Trusted Data Sharing

MISP allows participants to control what to share and with whom, respecting trust and legal constraints.

SAND5G

Why Information Sharing Matters

- Modern cyber attacks reuse infrastructure, tooling, and techniques.
- Organizations operating in isolation have limited visibility and delayed detection.
- Sharing threat intelligence enables early warning and faster response.
- Contextualized shared data improves confidence and reduces false positives.

SAND5G

MISP conceptual model

- Open-source, flexible, and hierarchical framework
- Designed for sharing, storing, and correlating cyber security indicators and threats
- Core components include structured events, attributes, and object
- Enables standardized threat analysis, automation, and collaborative intelligence sharing among organizations

SAND5G

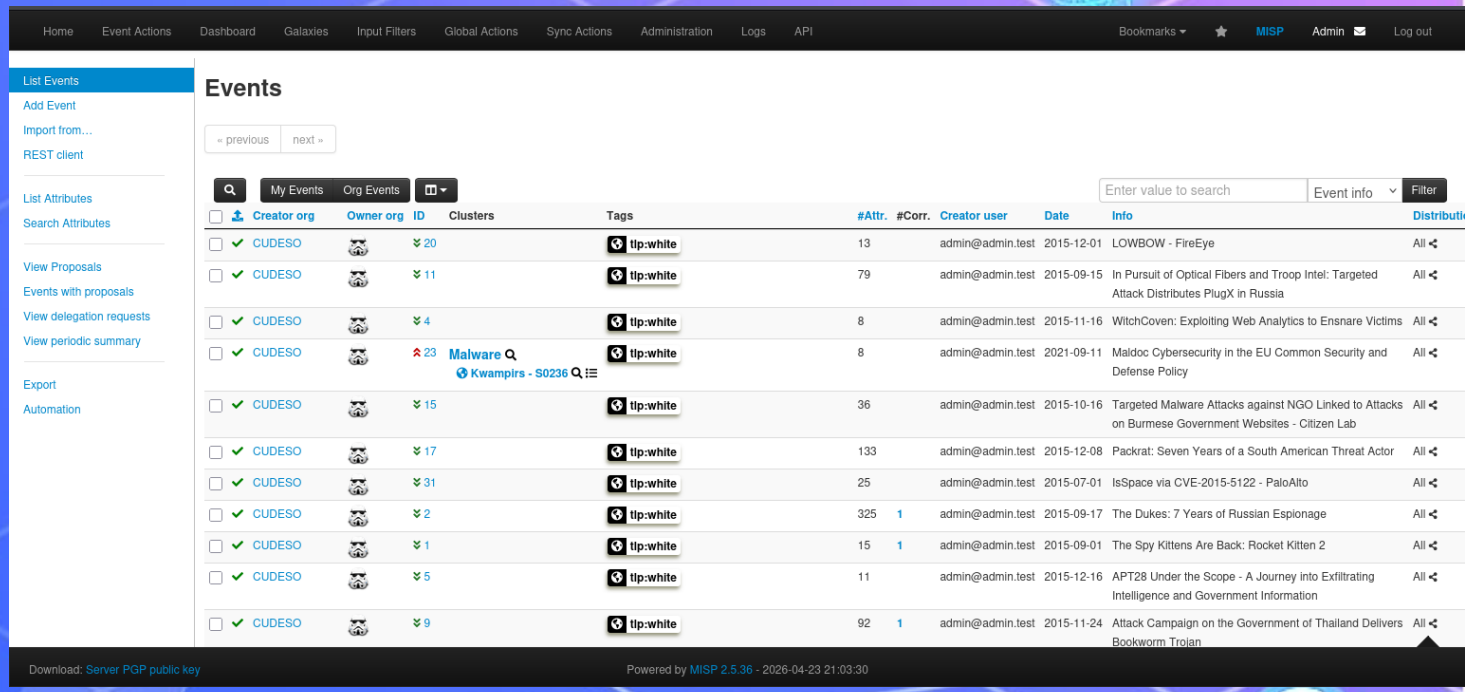
Key Components of the MISP Model

- **Event:** The top-level container for information sharing, representing a specific incident or threat scenario.
- **Attribute:** The fundamental unit of data (e.g., IP address, file hash) used to describe a threat within an event.
- **Object:** A structured set of attributes that form a complex concept (e.g., a file, a user, a process), allowing for more detailed context.
- **Correlation:** Automatic links created between events or attributes that share common elements.
- **Galaxy & Taxonomies:** Standardized frameworks for classifying threat actors and attack techniques, enhancing analysis.

SAND5G

Data Layer

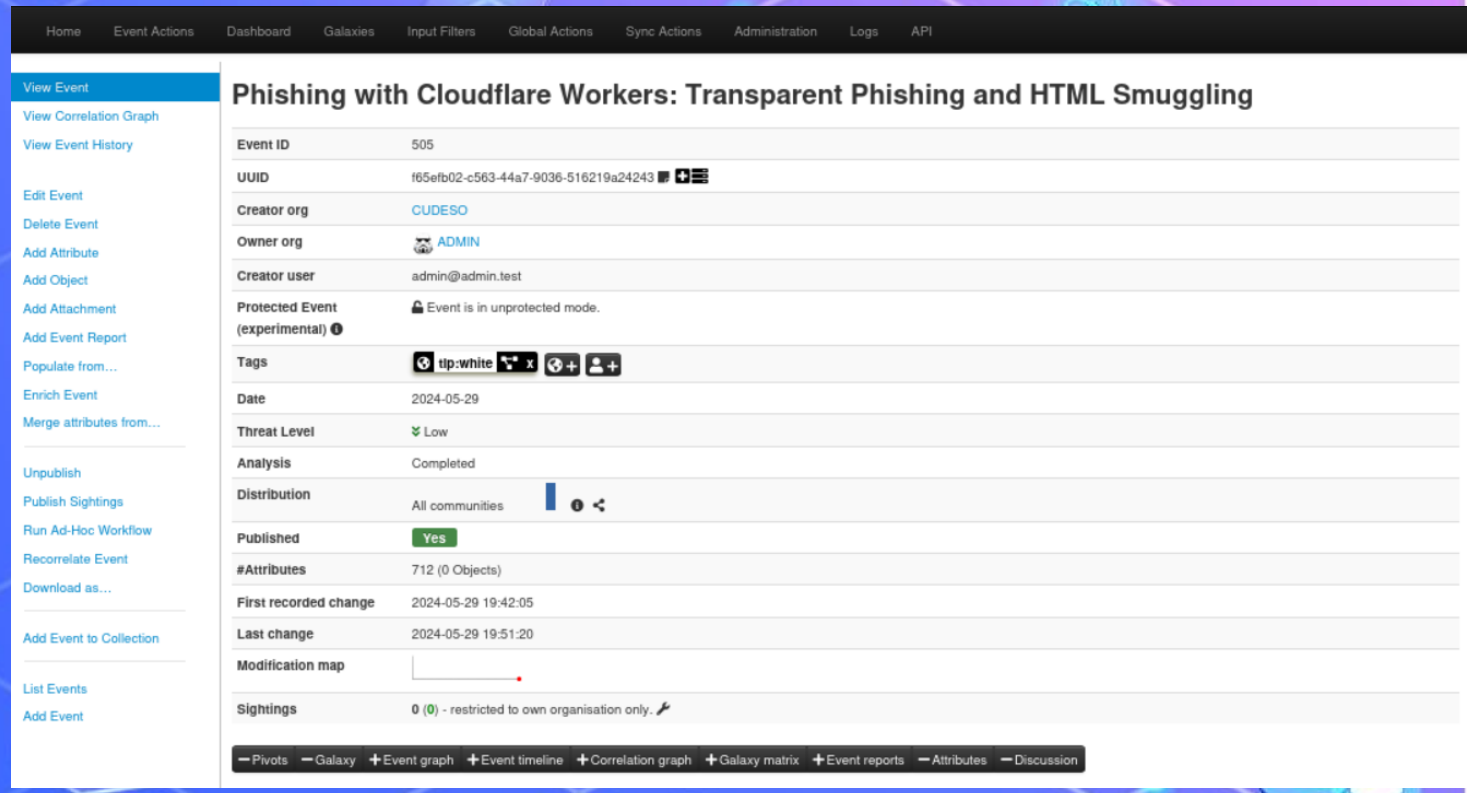
- The data layer represents the factual foundation of MISP.
  - It contains raw indicators such as IP addresses, domains, URLs, file hashes, and email artifacts.
  - Indicators are stored as attributes and logically grouped into objects.
  - Events provide a container for related indicators describing a specific incident or activity.



SAND5G

Context Layer

- The context layer explains what the data means and why it is relevant.
  - Taxonomies provide standardized classification of threats and information types.
  - Tags allow consistent labeling and filtering of intelligence.
  - Galaxies connect events to known threat actors, malware families, or campaigns.



Events, Objects and Usage Scenarios

Event and Object Structure

MISP organizes data into events that contain detailed objects representing attributes of security incidents.

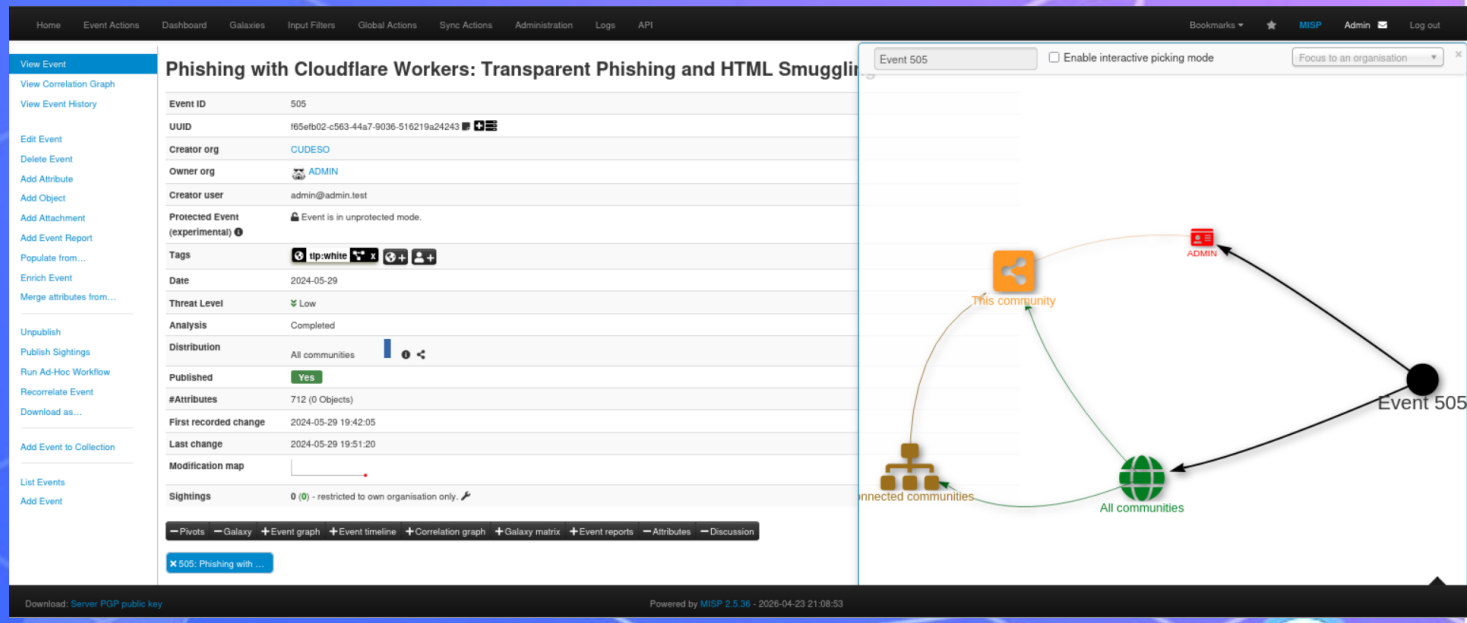
Operational Usage Scenarios

SOC analysts and responders use MISP daily to search, create, and enrich events for incident management.

SAND5G

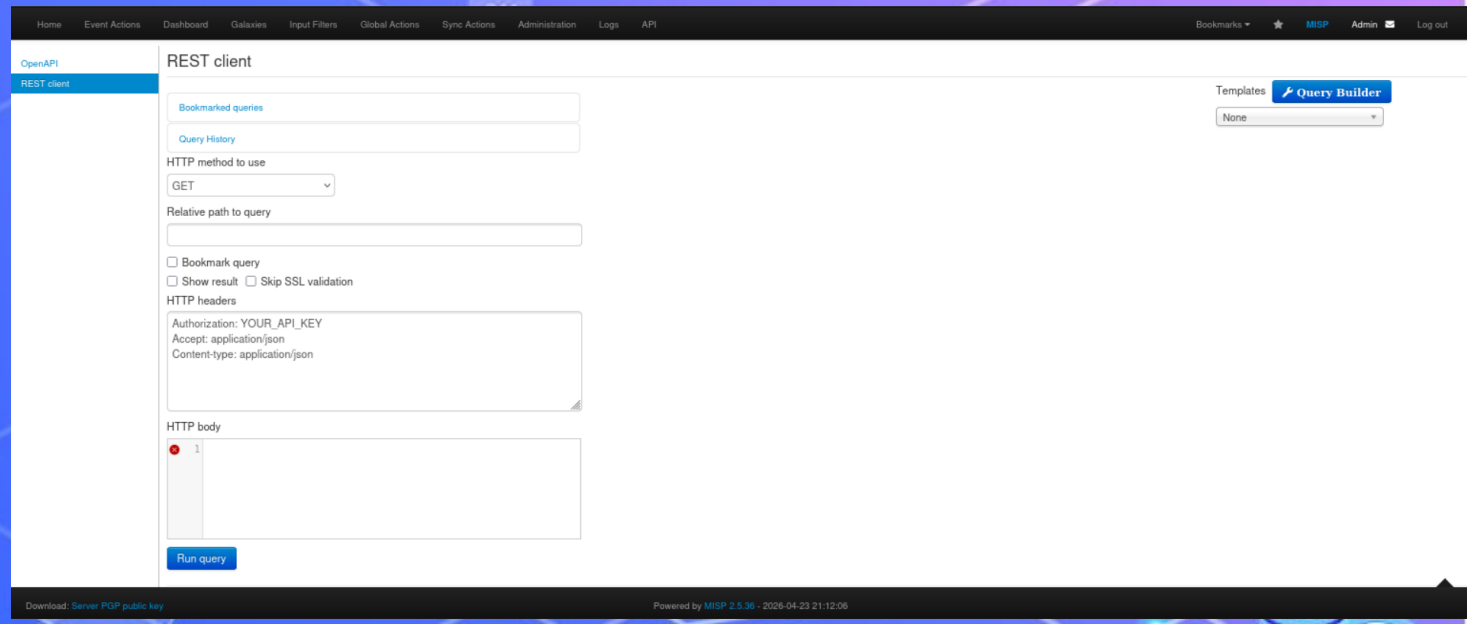
Information Sharing

- MISP is built around a trust-based sharing model between organizations.
  - Events can be shared selectively based on distribution levels and community memberships.
  - Synchronization mechanisms allow automated sharing between trusted MISP instances.
  - This model enables collaboration while maintaining data ownership and control.



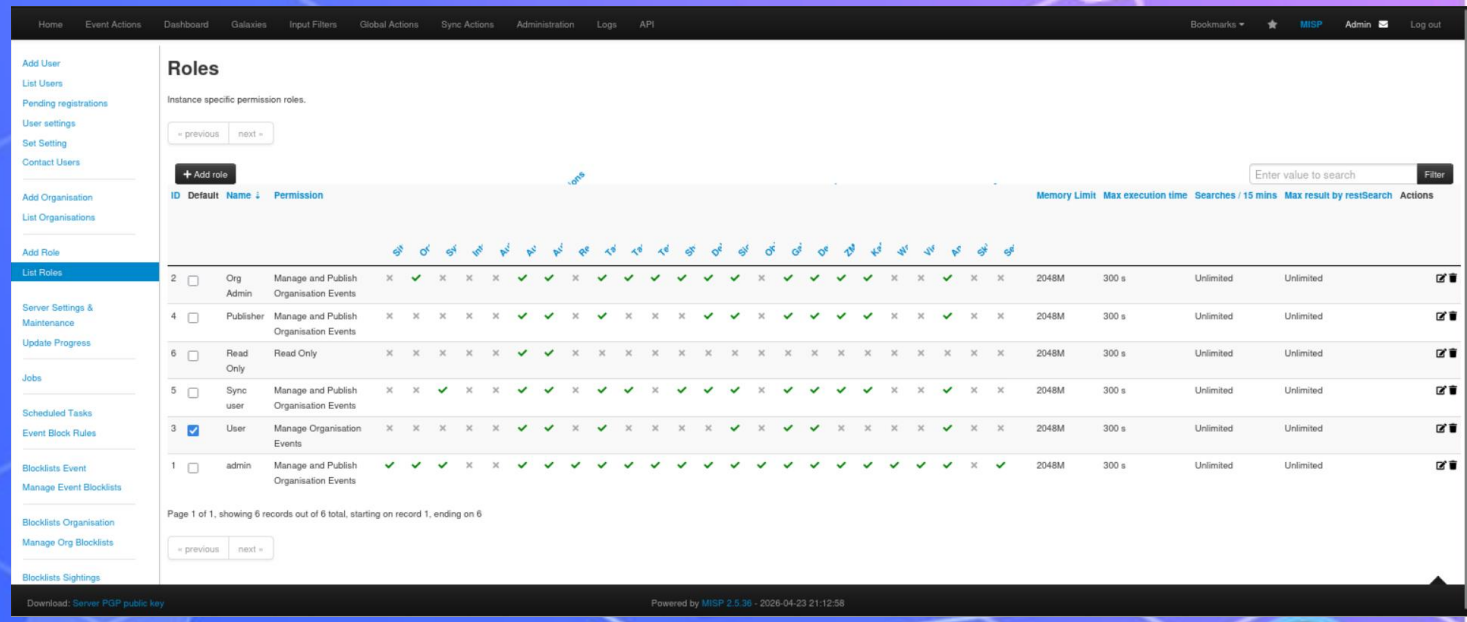
Integration & Automation

- MISP provides a REST API enabling full automation and system integration.
  - Threat data can be consumed by SIEM, SOAR, IDS, and malware analysis systems.
  - MISP supports feeds for importing open-source and commercial intelligence.
  - Automation improves scalability and reduces manual analyst workload.



Administration

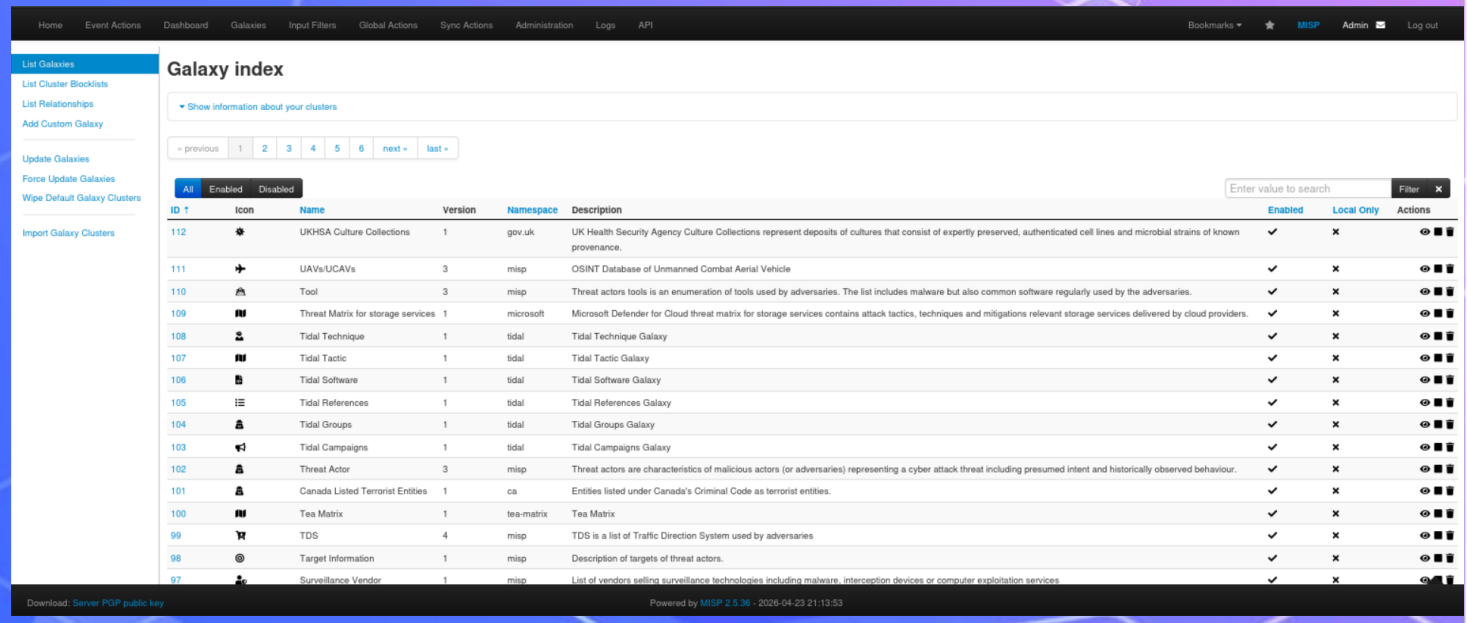
- Administrators manage users, roles, and organizational settings.
  - Role-based access control defines what users can view, create, or share.
  - Admins configure feeds, synchronization partners, and local policies.
  - Proper administration is essential for trust and data quality.



SAND5G

Taxonomies, Galaxies & Objects

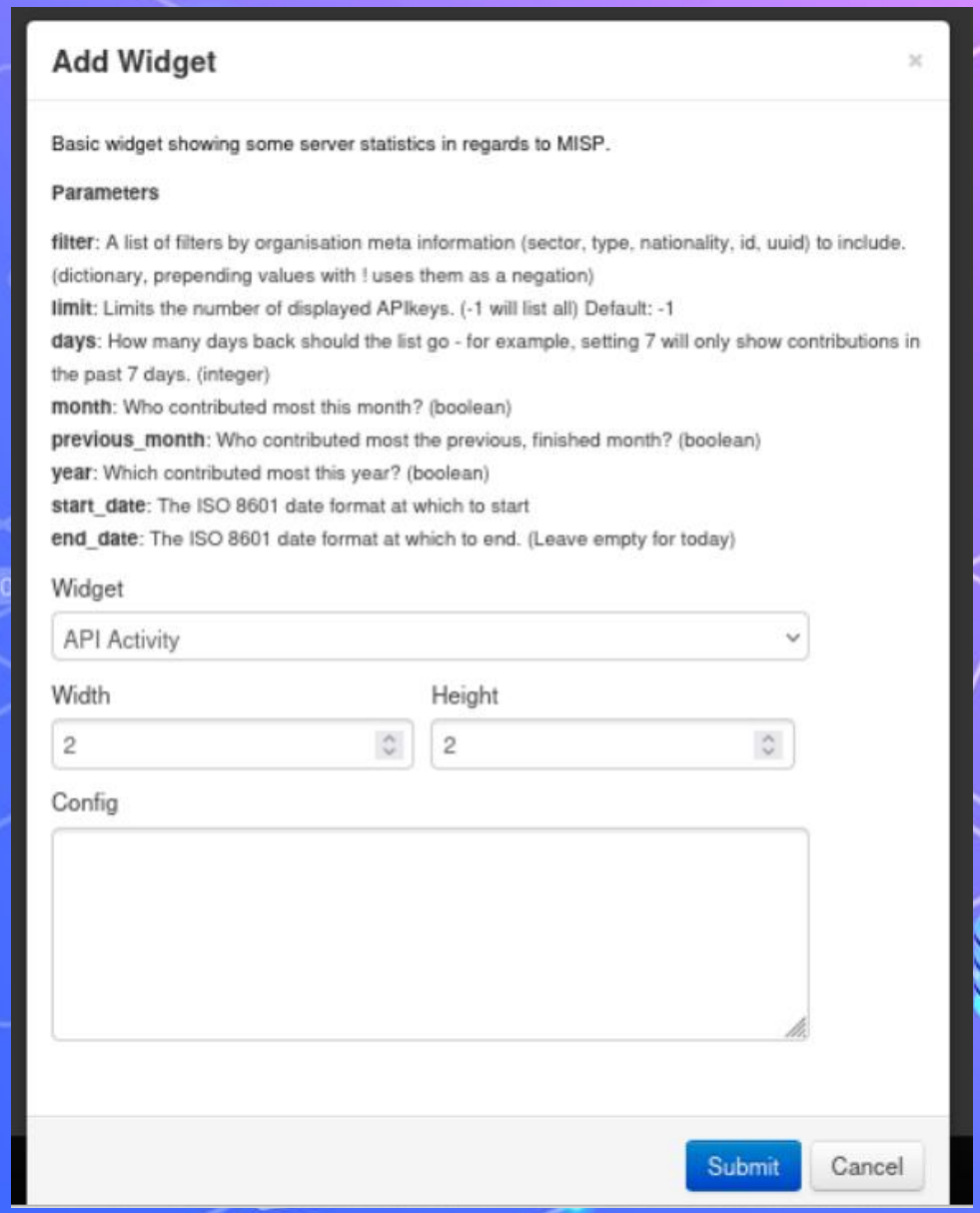
- Taxonomies ensure consistent classification across organizations.
  - Galaxies add strategic and threat intelligence context.
  - Object templates standardize data structures for common data types.
  - Together, these features improve correlation, search, and automated processing.



SAND5G

Dashboard

- The dashboard provides a high-level overview of activity within MISP.
  - It displays statistics, trends, and tag distributions.
  - Dashboards support operational awareness and management reporting.
  - Widgets can be customized based on user needs.



Knowledge Validation

Quiz Structure

The quiz contains five multiple-choice questions with four options each, focusing on key MISP concepts.

Answer Explanations

Correct answers include justifications; incorrect options address common misconceptions for better understanding.

Learning Reinforcement

Reviewing answers helps learners grasp principles and aids instructors in assessing participant understanding.

Practical Application

Learners are encouraged to revisit key slides and reflect on applying MISP in their organizational context.

SAND5G

Question and answers – Q1

Question 1 – Purpose of MISP

What is the primary goal of MISP?

A. To automatically block malicious traffic on the network

B. To collect, correlate, enrich, and share threat intelligence

C. To replace SIEM and IDS platforms

D. To perform vulnerability scanning across assets

✅ Correct answer: B

✅ Why B is correct

MISP is designed to handle threat intelligence lifecycle activities, including:

- Collecting indicators
- Correlating related data
- Enriching indicators with context
- Sharing intelligence with trusted partners
- This matches MISP's core mission.

❌ Why the others are wrong

A: Blocking traffic is the role of firewalls or IDS/IPS, not MISP

C: MISP complements SIEM/IDS; it does not replace them

D: Vulnerability scanning is outside MISP's scope

SAND5G

Question and answers – Q2

Question 2 – Data Layer

Which of the following best describes what is stored in the data layer of MISP?

A. Dashboards and statistics

B. Threat actor profiles and campaigns

C. Raw indicators grouped as attributes and objects

D. User permissions and roles

✅ Correct answer: C

✅ Why C is correct

The data layer contains factual information, such as:

- IP addresses
- Domains
- File hashes
- URLs
- Email artifacts

These are stored as attributes and grouped into objects within events.

❌ Why the others are wrong

A: Dashboards visualize data, they don't store indicators

B: Threat actor profiles belong to the context layer (galaxies)

D: User roles belong to administration, not the data layer

SAND5G

Question and answers – Q3

Question 3 – Context Layer

What is the main purpose of the context layer in MISP?

A. To store unverified indicators

B. To block malicious activity

C. To add meaning and classification to indicators

D. To export data to third-party tools

✅ Correct answer: C

✅ Why C is correct

The context layer answers “what does this data mean?” using:

- Taxonomies
- Tags
- Galaxies
- Confidence and sightings

This allows analysts to properly interpret indicators instead of treating them as isolated data.

❌ Why the others are wrong

A: Raw indicators are part of the data layer

B: Blocking actions are performed by security controls, not MISP

D: Exporting data is a function, not the purpose of context

SAND5G

Question and answers – Q4

Question 4 – Objects in MISP

Why are objects used in MISP?

A. To replace indicators

B. To delete duplicate events

C. To logically group related attributes

D. To visually decorate events

✅ Correct answer: C

✅ Why C is correct

Objects allow analysts to structure related attributes, for example:

- An email object with sender, subject, attachment hash
- A file object with filename and hash values

This improves:

- Data quality
- Correlation accuracy
- Automation

❌ Why the others are wrong

A: Objects do not replace indicators; they organize them

B: Deduplication is handled through correlation, not objects

D: Objects serve a functional purpose, not visual design

SAND5G

Question and answers – Q5

Question 5 – Information Sharing

Which statement best reflects how information sharing works in MISP?

A. All data is shared publicly by default

B. Sharing is based on trust and controlled distribution

C. Only administrators can see shared events

D. Data sharing is anonymous and uncontrolled

✅ Correct answer: B

✅ Why B is correct

MISP is built around trust-based sharing, where:

- Organizations define sharing communities
- Distribution levels control visibility
- Data ownership is preserved

This allows collaboration without losing control over intelligence.

❌ Why the others are wrong

A: Sharing is never public by default

C: Visibility depends on roles and distribution, not admin status only

D: Sharing is controlled, audited, and role-based

SAND5G