



<https://sand5g-project.eu/>

Discover MISP

The Open Source Threat Intelligence and Sharing Platform



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.



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.



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



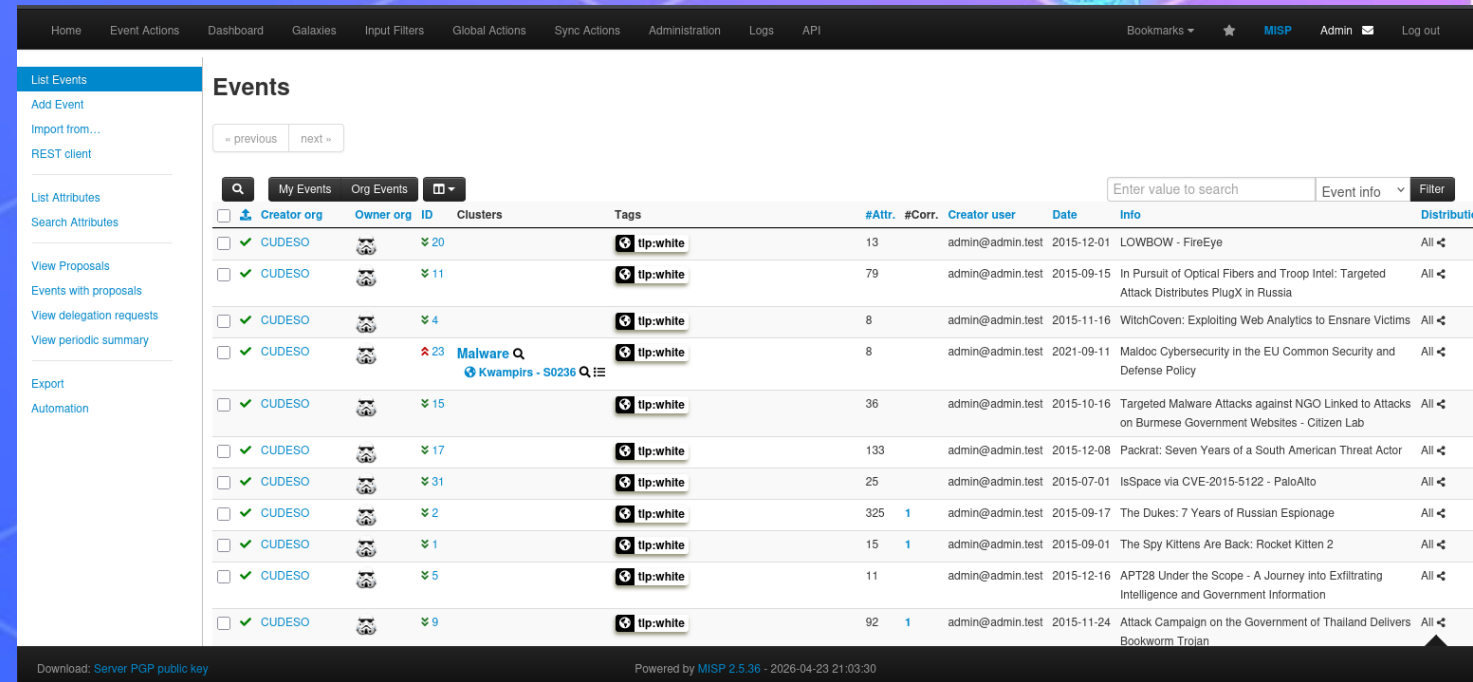
Key Components of the MISP Model

- **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.



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.

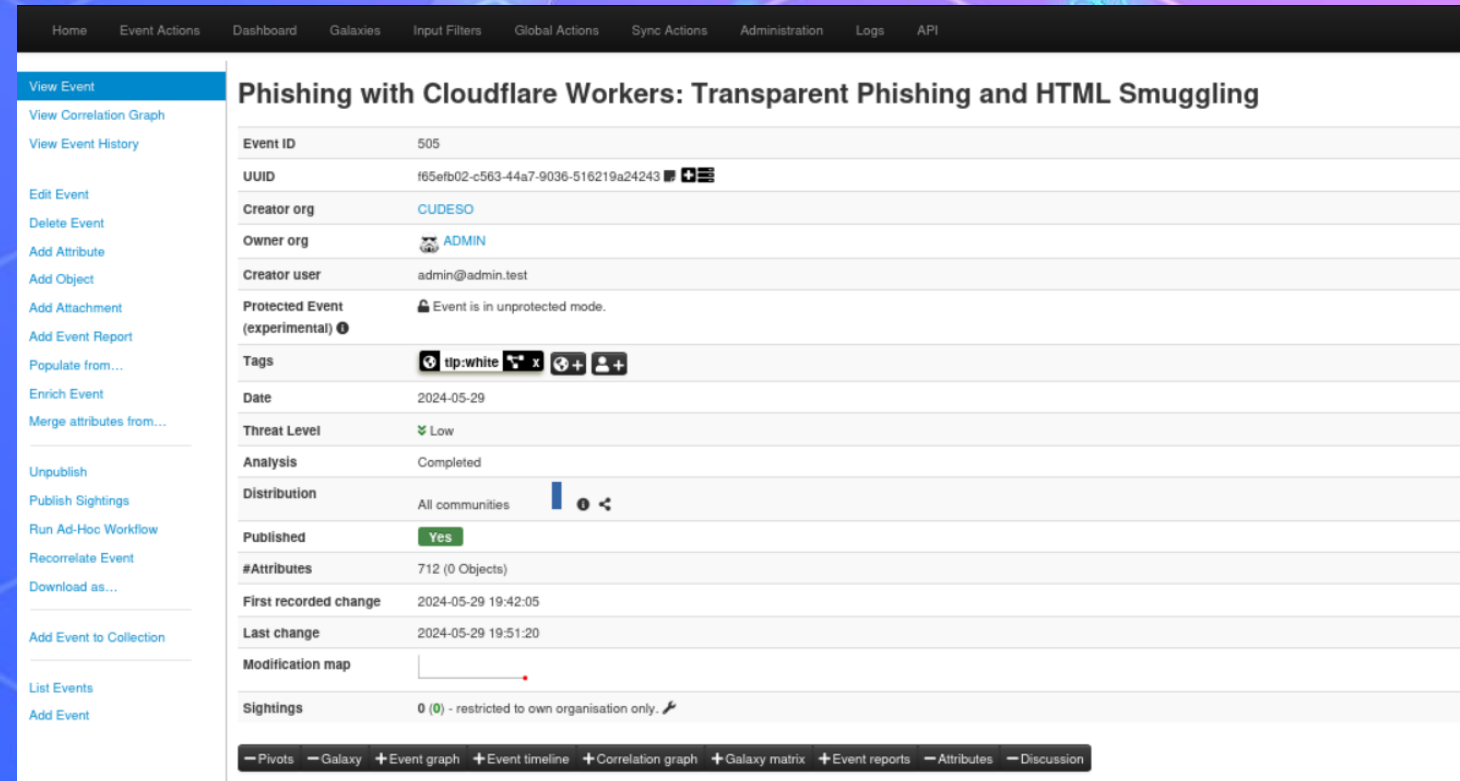


The screenshot displays the MISP web interface. The top navigation bar includes links for Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. On the right, there are links for Bookmarks, MISP, Admin, and Log out. The left sidebar contains a 'List Events' menu with options like 'Add Event', 'Import from...', 'REST client', 'List Attributes', 'Search Attributes', 'View Proposals', 'Events with proposals', 'View delegation requests', 'View periodic summary', 'Export', and 'Automation'. The main content area is titled 'Events' and features a table of event records. The table has columns for checkboxes, Creator org, Owner org, ID, Clusters, Tags, #Attr., #Corr., Creator user, Date, Info, and Distribution. The events listed are primarily from the 'CUDESCO' organization, with various tags like 'tip:white' and 'Malware Q'. The footer of the interface shows 'Download: Server GPG public key' and 'Powered by MISP 2.5.36 - 2026-04-23 21:03:30'.

	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution
☐	CUDESCO		20		tip:white	13		admin@admin.test	2015-12-01	LOWBOW - FireEye	All
☐	CUDESCO		11		tip:white	79		admin@admin.test	2015-09-15	In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia	All
☐	CUDESCO		4		tip:white	8		admin@admin.test	2015-11-16	WitchCoven: Exploiting Web Analytics to Ensnare Victims	All
☐	CUDESCO		23	Malware Q	tip:white	8		admin@admin.test	2021-09-11	Maldoc Cybersecurity in the EU Common Security and Defense Policy	All
☐	CUDESCO		15		tip:white	36		admin@admin.test	2015-10-16	Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites - Citizen Lab	All
☐	CUDESCO		17		tip:white	133		admin@admin.test	2015-12-08	Packrat: Seven Years of a South American Threat Actor	All
☐	CUDESCO		31		tip:white	25		admin@admin.test	2015-07-01	IsSpace via CVE-2015-5122 - PaloAlto	All
☐	CUDESCO		2		tip:white	325	1	admin@admin.test	2015-09-17	The Dukes: 7 Years of Russian Espionage	All
☐	CUDESCO		1		tip:white	15	1	admin@admin.test	2015-09-01	The Spy Kittens Are Back: Rocket Kitten 2	All
☐	CUDESCO		5		tip:white	11		admin@admin.test	2015-12-16	APT28 Under the Scope - A Journey into Exfiltrating Intelligence and Government Information	All
☐	CUDESCO		9		tip:white	92	1	admin@admin.test	2015-11-24	Attack Campaign on the Government of Thailand Delivers Bookworm Trojan	All

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.



The screenshot displays a security dashboard interface. The top navigation bar includes links for Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. A left sidebar lists various actions such as View Event, View Correlation Graph, View Event History, Edit Event, Delete Event, Add Attribute, Add Object, Add Attachment, Add Event Report, Populate from..., Enrich Event, Merge attributes from..., Unpublish, Publish Sightings, Run Ad-Hoc Workflow, Recorrelate Event, Download as..., Add Event to Collection, List Events, and Add Event. The main content area shows the details of a specific event titled "Phishing with Cloudflare Workers: Transparent Phishing and HTML Smuggling".

Field	Value
Event ID	505
UUID	f65efb02-c563-44a7-9036-516219a24243
Creator org	CUESO
Owner org	ADMIN
Creator user	admin@admin.test
Protected Event (experimental)	Event is in unprotected mode.
Tags	tip:white
Date	2024-05-29
Threat Level	Low
Analysis	Completed
Distribution	All communities
Published	Yes
#Attributes	712 (0 Objects)
First recorded change	2024-05-29 19:42:05
Last change	2024-05-29 19:51:20
Modification map	
Sightings	0 (0) - restricted to own organisation only.

At the bottom of the event details, there is a row of tabs: Pivots, Galaxy, Event graph, Event timeline, Correlation graph, Galaxy matrix, Event reports, Attributes, and Discussion. The "Event graph" tab is currently selected.

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.



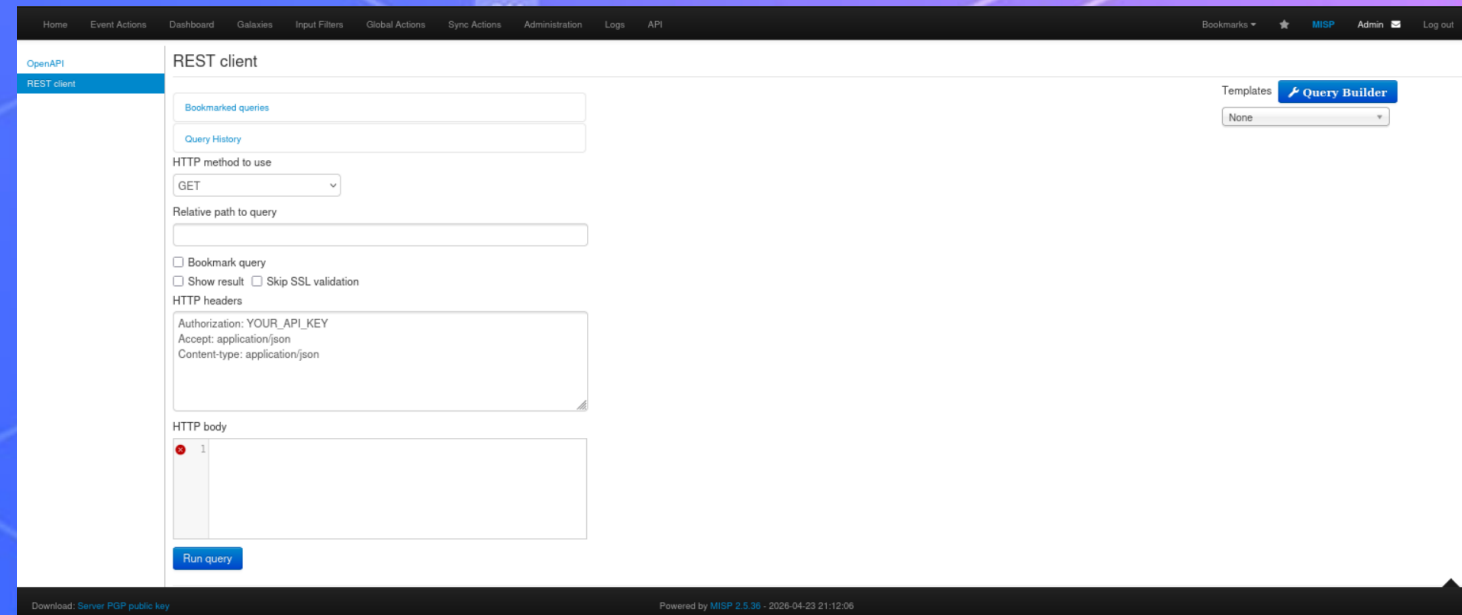
Information Sharing

- 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.

The screenshot displays the MISP web interface. On the left is a sidebar with navigation options like 'View Event', 'View Correlation Graph', and 'Edit Event'. The main panel shows details for 'Event 505: Phishing with Cloudflare Workers: Transparent Phishing and HTML Smuggling'. Key details include Event ID 505, UUID 165efb02-c563-44a7-9036-516219a24243, Creator org CUDES0, Owner org ADMIN, and Creator user admin@admin.test. The event is marked as 'Protected Event (experimental)' and 'Event is in unprotected mode'. It has tags 'tip:white' and a threat level of 'Low'. The distribution is set to 'All communities' and it is published. A diagram on the right illustrates the sharing model with nodes for 'This community', 'ADMIN', 'connected communities', and 'All communities', connected by arrows representing data flow.

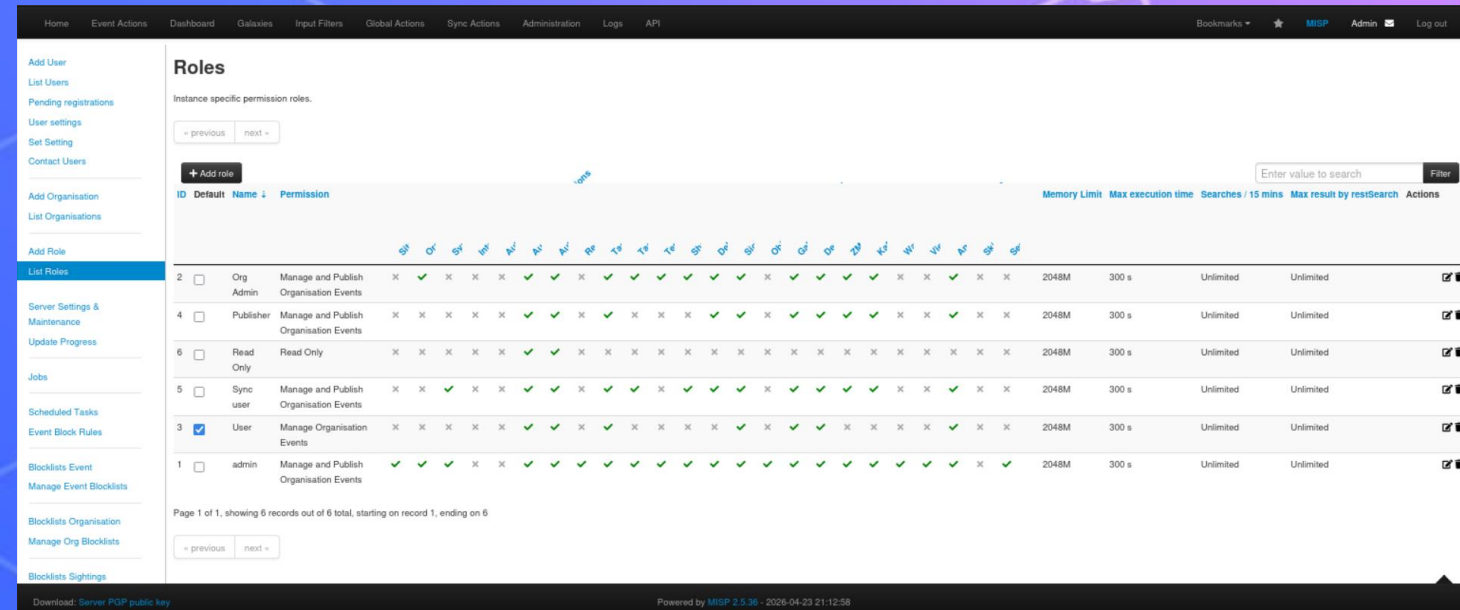
Integration & Automation

- 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.



The screenshot shows the 'Roles' management interface in MISP. The left sidebar contains navigation links for user and organization management. The main area displays a table of roles with columns for ID, Default status, Name, Permission, and various system metrics. The 'User' role (ID 3) is selected.

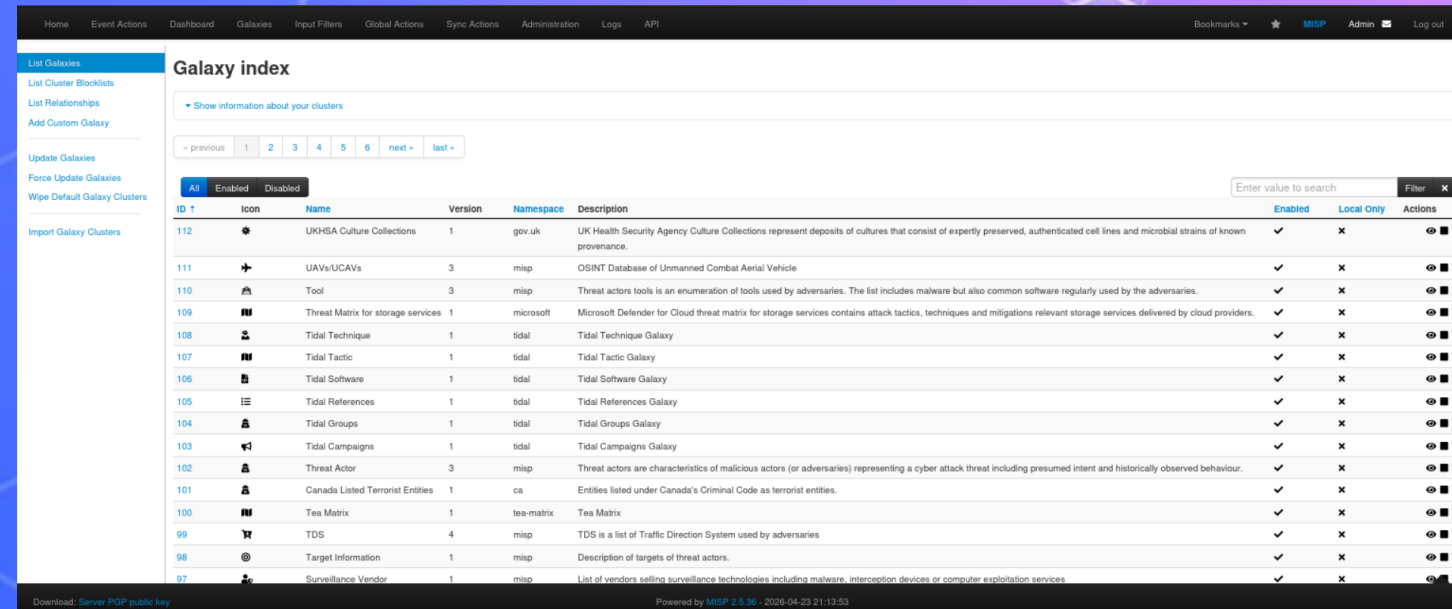
ID	Default	Name	Permission	Memory Limit	Max execution time	Searches / 15 mins	Max result by restSearch	Actions
2	☐	Org Admin	Manage and Publish Organisation Events	2048M	300 s	Unlimited	Unlimited	
4	☐	Publisher	Manage and Publish Organisation Events	2048M	300 s	Unlimited	Unlimited	
6	☐	Read Only	Read Only	2048M	300 s	Unlimited	Unlimited	
5	☐	Sync user	Manage and Publish Organisation Events	2048M	300 s	Unlimited	Unlimited	
3	☒	User	Manage Organisation Events	2048M	300 s	Unlimited	Unlimited	
1	☐	admin	Manage and Publish Organisation Events	2048M	300 s	Unlimited	Unlimited	

Page 1 of 1, showing 6 records out of 6 total, starting on record 1, ending on 6

Download: Server PGP public key | Powered by MISP 2.5.36 - 2026-04-23 21:12:58

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.



ID	Icon	Name	Version	Namespace	Description	Enabled	Local Only	Actions
112	🛡️	UKHSA Culture Collections	1	gov.uk	UK Health Security Agency Culture Collections represent deposits of cultures that consist of expertly preserved, authenticated cell lines and microbial strains of known provenance.	✓	✗	🔍 📄 🗑️
111	✈️	UAVs/UCAVs	3	misp	OSINT Database of Unmanned Combat Aerial Vehicle	✓	✗	🔍 📄 🗑️
110	🔧	Tool	3	misp	Threat actors tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.	✓	✗	🔍 📄 🗑️
109	☁️	Threat Matrix for storage services	1	microsoft	Microsoft Defender for Cloud threat matrix for storage services contains attack tactics, techniques and mitigations relevant storage services delivered by cloud providers.	✓	✗	🔍 📄 🗑️
108	🏗️	Tidal Technique	1	tidal	Tidal Technique Galaxy	✓	✗	🔍 📄 🗑️
107	🏗️	Tidal Tactic	1	tidal	Tidal Tactic Galaxy	✓	✗	🔍 📄 🗑️
106	🏗️	Tidal Software	1	tidal	Tidal Software Galaxy	✓	✗	🔍 📄 🗑️
105	📖	Tidal References	1	tidal	Tidal References Galaxy	✓	✗	🔍 📄 🗑️
104	👤	Tidal Groups	1	tidal	Tidal Groups Galaxy	✓	✗	🔍 📄 🗑️
103	📅	Tidal Campaigns	1	tidal	Tidal Campaigns Galaxy	✓	✗	🔍 📄 🗑️
102	👤	Threat Actor	3	misp	Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.	✓	✗	🔍 📄 🗑️
101	👤	Canada Listed Terrorist Entities	1	ca	Entities listed under Canada's Criminal Code as terrorist entities.	✓	✗	🔍 📄 🗑️
100	🏗️	Tea Matrix	1	tea-matrix	Tea Matrix	✓	✗	🔍 📄 🗑️
99	🚦	TDS	4	misp	TDS is a list of Traffic Direction System used by adversaries	✓	✗	🔍 📄 🗑️
98	👤	Target Information	1	misp	Description of targets of threat actors.	✓	✗	🔍 📄 🗑️
97	👤	Surveillance Vendor	1	misp	List of vendors selling surveillance technologies including malware, interception devices or computer exploitation services	✓	✗	🔍 📄 🗑️

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.

Add Widget

Basic widget showing some server statistics in regards to MISP.

Parameters

filter: A list of filters by organisation meta information (sector, type, nationality, id, uuid) to include. (dictionary, prepending values with ! uses them as a negation)

limit: Limits the number of displayed APIkeys. (-1 will list all) Default: -1

days: How many days back should the list go - for example, setting 7 will only show contributions in the past 7 days. (integer)

month: Who contributed most this month? (boolean)

previous_month: Who contributed most the previous, finished month? (boolean)

year: Which contributed most this year? (boolean)

start_date: The ISO 8601 date format at which to start

end_date: The ISO 8601 date format at which to end. (Leave empty for today)

Widget

API Activity

Width **Height**

2 2

Config

Submit **Cancel**

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.



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

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

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

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

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