Malware Information Sharing Platform MISP - A Threat Sharing Platform

Malware Information Sharing Platform MISP - A Threat Sharing Platform

↑ Back to Services

You can report incidents via our official contact including e-mail, phone or use the Anonymous reporting form.

Malware Information Sharing Platform (MISP) - A Threat Sharing Platform

Malware Information Sharing Platform (MISP) is developed as free software by a group of developers mainly from Belgian Defence and NATO / NCIRC (Computer Incident Response Capability).

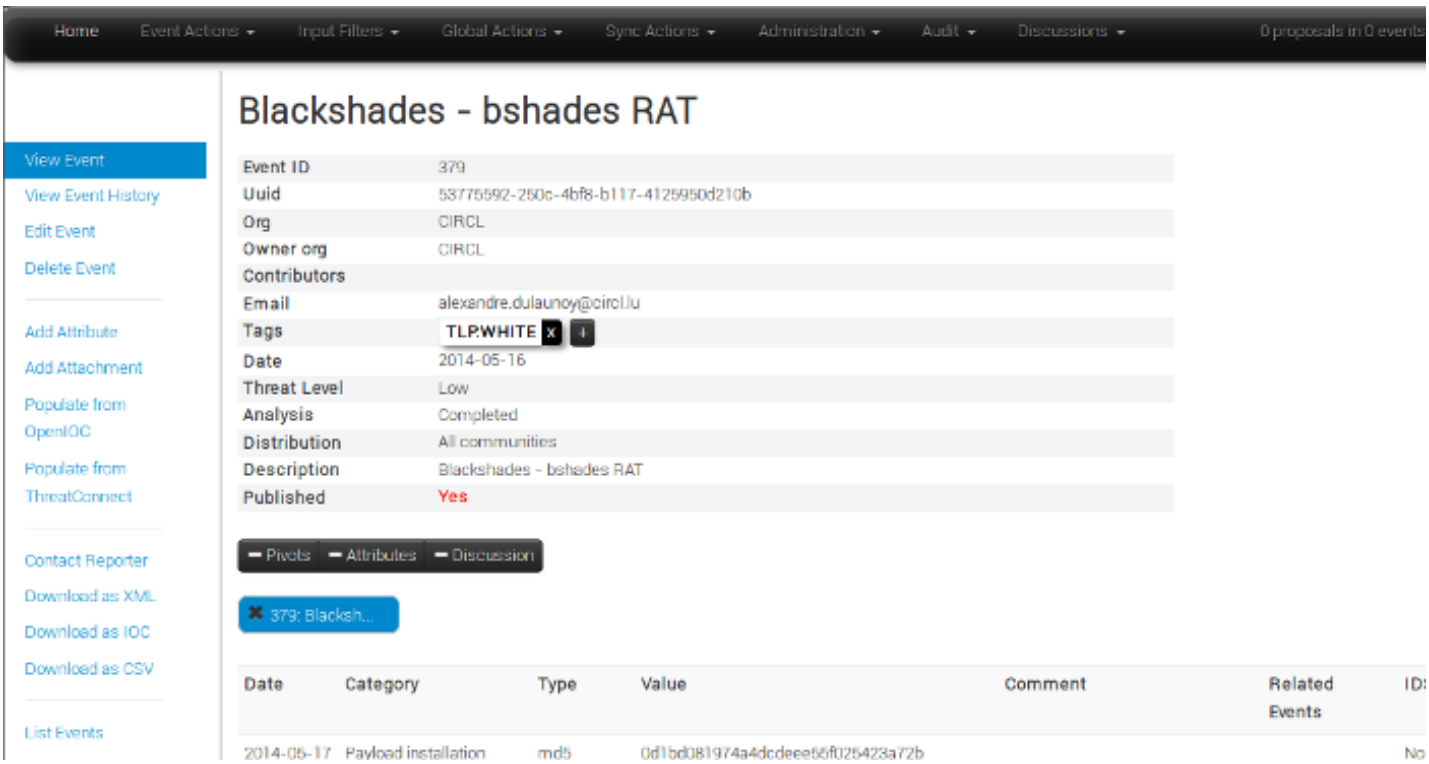
CIRCL operates several MISP instances (for different types of constituents) in order to improve automated detection and responsiveness to targeted and cybersecurity attacks in Luxembourg and outside. MISP acts as a platform for sharing threat indicators within private and public sectors.

Private organizations in Luxembourg or accredited CERTs can request an access to their respective MISP platform.

What is MISP?

A platform for sharing, storing and correlating Indicators of Compromises of targeted attacks.

Malware Information Sharing Platform (MISP) allows organizations to share information about malware and their indicators. MISP users benefit from the collaborative knowledge about existing malware or threats. The aim of this trusted platform is to help improving the counter-measures used against targeted attacks and set-up preventive actions and detection.



CIRCL MISP - a trusted platform with multiple goals

The objective of the CIRCL Malware Information Sharing Platform is to:

- Facilitate the storage of technical and non-technical information about seen malware and attacks
- Create automatically relations between malware and their attributes
- Store data in a structured format (allowing automated use of the database to feed detection systems or forensic tools)
- Generate rules for Network Intrusion Detection System (NIDS) that can be imported on IDS systems (e.g. IP addresses, domain names, hashes of malicious files, pattern in memory)
- Share malware and threat attributes with other parties and trust-groups
- Improve malware detection and reversing to promote information exchange among organizations (e.g. avoiding duplicate works)

- Create a platform of trust - trusted information from trusted partners
- Store locally all information from other instances (ensuring confidentiality on queries)

How does MISP work?

Malware Information Sharing Platform is accessible from different interfaces like a web interface (for analysts or incident handlers) or via a ReST API (for systems pushing and pulling IOCs). The inherent goal of MISP is to be a robust platform that ensures a smooth operation from revealing, maturing and exploiting the threat information.

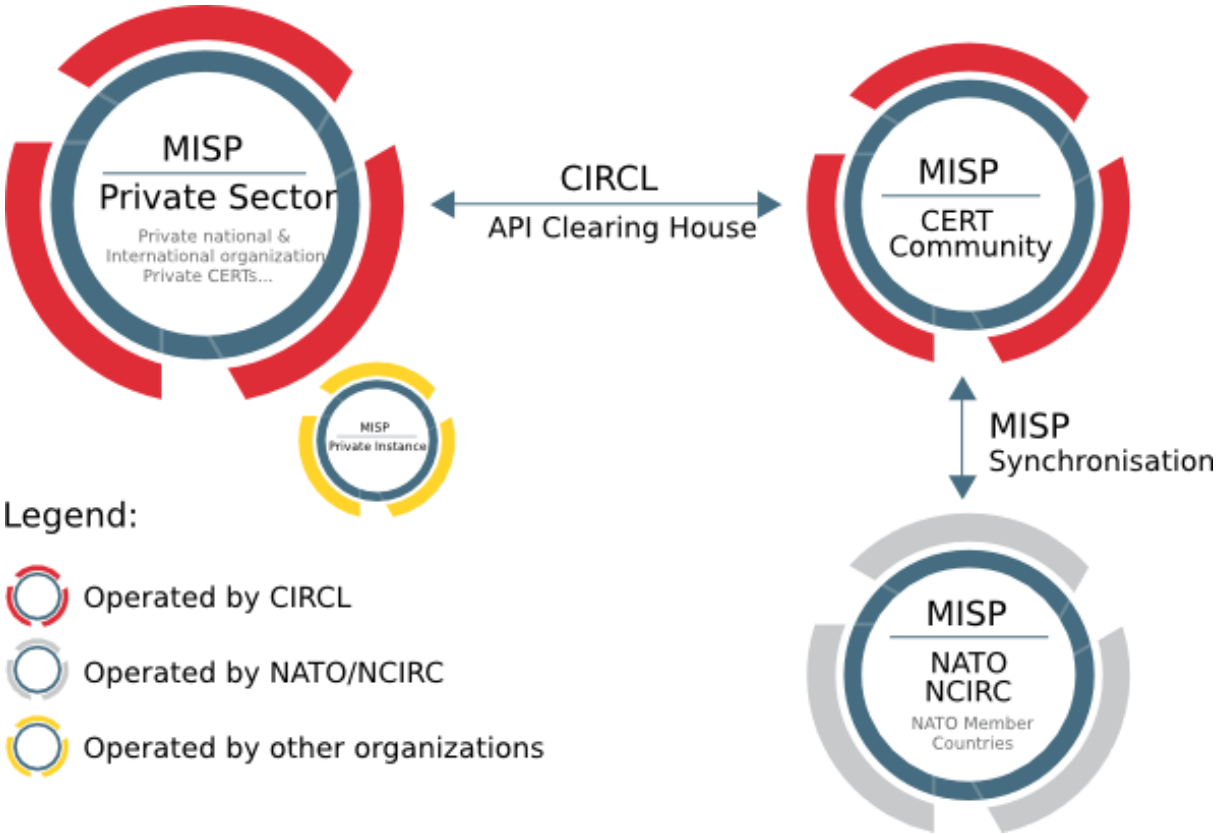
How to request access?

If you work for an organization or an activity based in Luxembourg or an accredited CERT or a trusted security vendor/researcher, you can request access by contacting us. The registration and access requires the use of at least one PGP key per organization.

What are the rules?

The access is free-of-charge. The objective is to stimulate sharing practises among public and private actors. The access is mainly bound to distribution as described in the traffic light protocol.

How the information is shared among the MISP instances worldwide?



In MISP, there are 4 options regarding distributing events and their respective attributes:

- Your organisation only
- This community only
- Connected communities
- All communities

In the diagram above, you can see an overview of the MISP instances operated by CIRCL. As the distribution is inherent to the connectivity among the MISP instances, participant should keep in mind the overall connectivity to select the appropriate distribution category.

How can I access the MISP API?

When you connect to the MISP platform, there is a specific menu dedicated to automation and export. CIRCL developed a Python library to access MISP API called PyMISP. The API can be used to feed internal security devices (e.g. IDS, SIEM or alike) in order to improve detection. The PyMISP python library documentation is available.

Do I need to install MISP?

No. When you have access to the CIRCL MISP instance, you have an intuitive web interface to find and add threats and indicators. You can directly use the application without the need to install your own MISP instance. The API can be also used with a variety of other security devices if you need to integrate the threats and indicators in your infrastructure (SIEMs, IDS, A/V console, ⋯).

I had access to a CIRCL MISP platform but I lost my credentials

If you are part of an organization in MISP, you can ask your MISP organizational admin to reset your password. If not, you can contact CIRCL to reset the credentials.

I found a bug in MISP, what should I do?

If you have found a bug in MISP, we advise you to open an issue on the MISP GitHub issue page. If this is a security vulnerability that cannot be disclosed publicly, contact CIRCL.

About CIRCL

- Mission
- News
- RFC2350
- Team Members
- Contact

Services, Projects and Software

- Services
  - Dynamic Malware Analysis Platform
  - Malware Information Sharing and Threat Sharing Platform
- Projects
- Software

Publications and Presentations

- Publications
- Digital First Aid Kit
- Presentations

Public services

- Review and report malicious URLs
-
- BGP Ranking
- Common vulnerability exposure
- PGP key server
- Map of attacks against Luxembourg
- Free software

CIRCL is the CERT (Computer Emergency Response Team/Computer Security Incident Response Team) for the private sector, communes and non-governmental entities in Luxembourg.

PGP signature of this page and How to Verify Integrity of CIRCL Web Pages