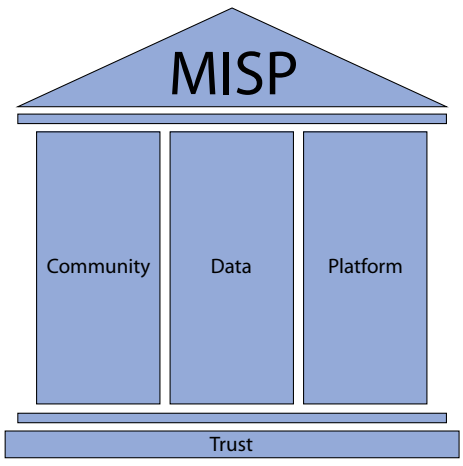
Malware Information Sharing Platform

What is MISP?

MISP – Malware Information Sharing Platform is a combination of a community of members, a knowledge base on malware, and a web-based platform. It is a practical and successful instantiation of the Smart Defence concept and is fully coherent with all current NATO Cyber Defence information sharing initiatives.



Initially built to support NATO Computer Incident Response Capability Technical Centre (NCIRC TC) missions, MISP allows sharing of technical characteristics of malware within a trusted community, without having to share information about the context of the incident.

It combines a searchable repository with a multidirectional information sharing mechanism. Where possible, MISP also provides automation mechanisms that enable the automatic import and export of data and the interfacing with other systems. The aim is to speed up the detection of incidents and the production of defence countermeasures, especially for malware that is not blocked by anti-virus protection, or that is part of sophisticated targeted intrusion attempts.

Why to use MISP?

1. NATO proven capability that can be used by the Nations

MISP is an everyday knowledge base and tool for Security Incident Investigators, Malware Analysts, and Incident Handlers. It is actively used by NCIRC since June 2012.

Malware experts will find in MISP the Indicators of Compromise (IOC) they need to correlate with their findings, and updates for detection systems. They will also find malware samples and a wide variety of technical information on malware, which will help them to get semi instant protection. MISP is an interactive platform that sends a notification each time something new is shared, provides automation for easy import and export of data, and integrates with cyber defence tools. MISP is a secure but easily reachable capability, accessible via the internet.

You should probably consider adopting MISP if part of your team's daily concerns is to know:

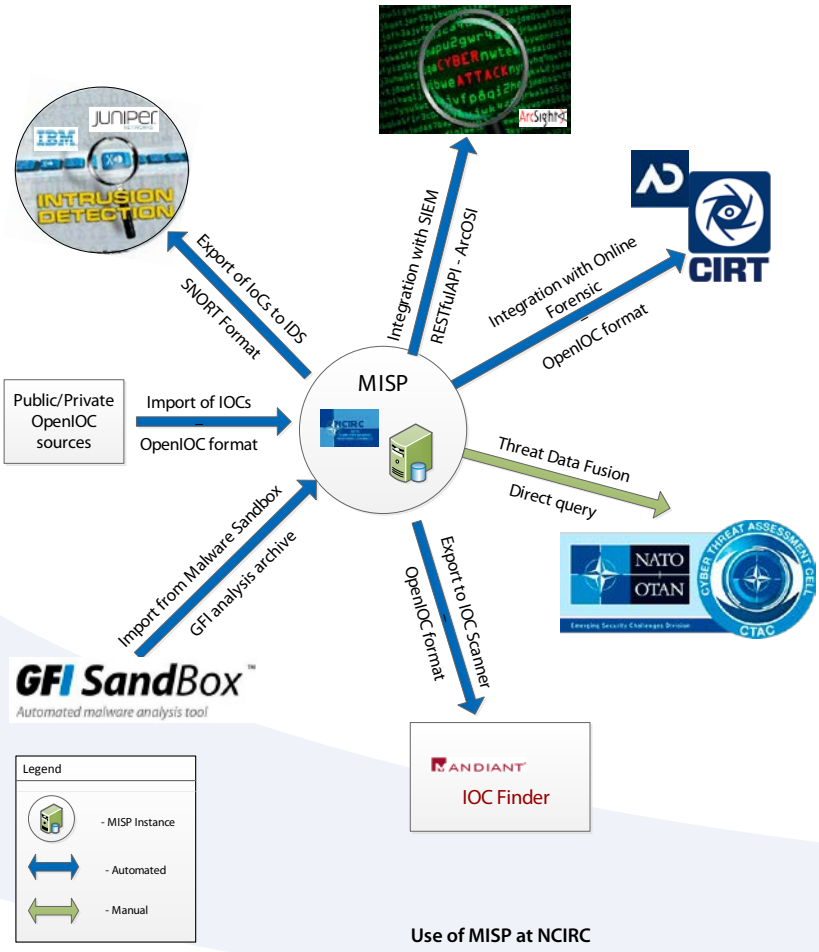
- whether you have seen a targeted malware in the past on your networks;
- whether any of your partners has seen it already;
- whether anybody else in the community has already performed an analysis of a malware;
- if a malware is part of an attack campaign or shares similarities with other malware we know;
- if the malware can possibly be attributed to a particular hostile entity as it has similarities with other malware generated by the same threat agent;
- the history of targeted malware-based attacks against the organization, and if there is a trend.

2. Smart Defence - Share to win

Benefits of joining MISP:

1. **Elimination of duplication of analytical work**: the same attacks are observed by different organizations and all of them spend time on performing the same analytical work. MISP will remove the need for a member of the community to analyze a malware that has been shared by another member.
2. **Faster threat detection**: all parties receive instant notification of a threat reported by one of them.
3. **Improving threat intelligence and attribution**: the centralized and shared malware information repository of MISP provides a more complete Threat Landscape View than from a single-organization perspective, and can give more indications towards concluding malware attributions.
4. **Enabling interoperability**: members can now share malware information in a 'normalized' format.
5. **Supporting automation** through various import and export features.

The key of its success is to **share** the technical part of the information of malware and **not share** the information about the context of the attack - technical information on a security incident taken out of its context is no longer sensitive. Also, it is this information which is actionable and can be used to improve the defence and detection mechanisms, and get tactical advantage on the attacking part. In one year of operation the MISP knowledge base already contains about 500 targeted attack related malware information entries.



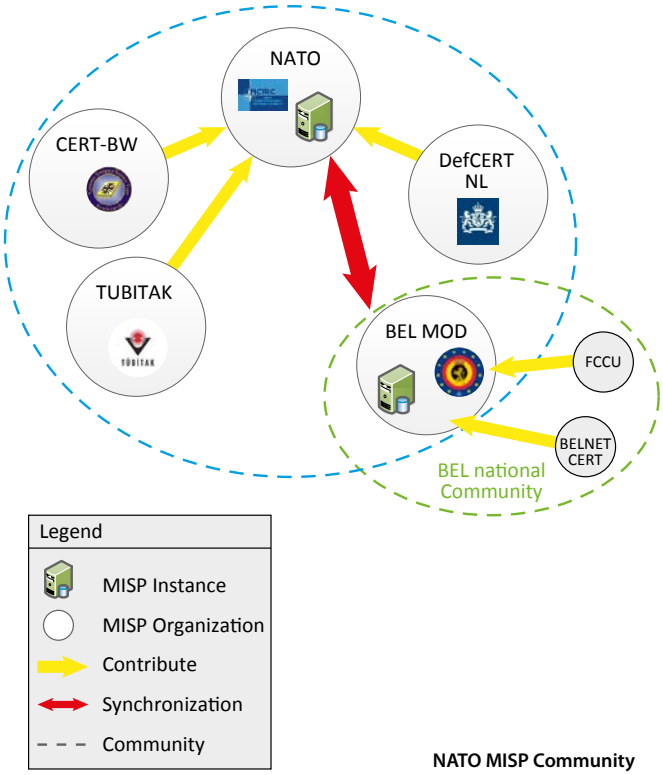
Use of MISP at NCIRC

The MISP Community

MISP works as a community where multiple instances of the platform hosted by different members can be interconnected, and it will synchronize the information between them.

Initial list of community members includes:

Organization
CCDCOE
CERTBw
CIRCL.LU
CZEMOD
Cyberint.ro
EISA
GOVCERT.LU
KAM.LT
MIL.be
NASK
NCIRC
NorCERT
TUBITAK
defCERTNL



NATO MISP Community

The Multinational Cyber Defence Capability Development (MN CD2) community is also currently investigating to what extent MISP could be a solution for the Information Sharing Work Package 1, and what could be the funding/subscription mechanism associated.

What is NCIRC TC?

NCIRC TC is the entity in the NATO Communications and Information (NCI) Agency responsible for providing Cyber Defence technical support to Cyber Defence Management Board (CDMB), NATO military and civilian bodies, as well as to the Allies. NCIRC TC is responsible for i.a. the development, implementation, maintenance and execution of NATO-wide technical and operational Cyber Defence services. In particular, this includes being:

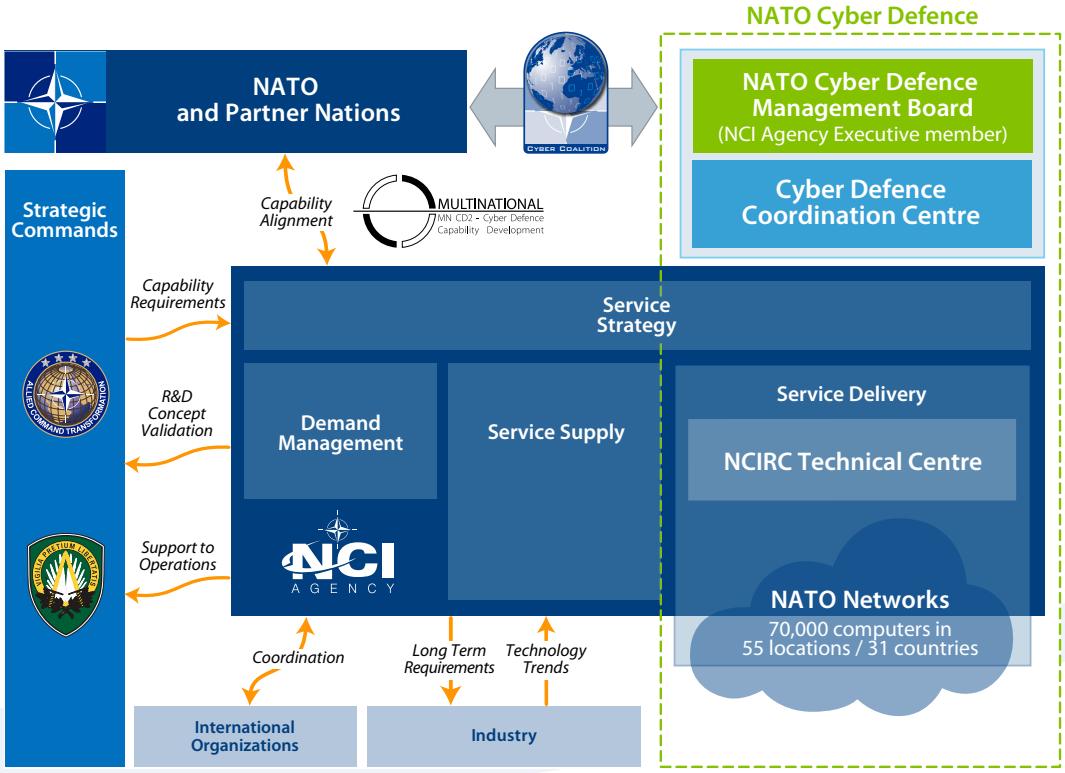
- responsible for providing NATO-wide COMPUSEC engineering services, including direction, support and advice;
- responsible for maintaining the highest level of COMPUSEC situational awareness, and for the early detection and resolution of security incidents affecting any constituent site;
- responsible for providing proactive COMPUSEC services, including assessment of threats, vulnerabilities and risks to NATO CIS, whilst also developing counter measures to address these risks.

About the NCI Agency

The NATO Communications and Information (NCI) Agency provides interoperable Communications and Information Systems and services connecting forces, NATO and Nations, where and when required.

The NCI Agency is the provider of NATO-wide IT services and state-of-the-art C4ISR capabilities, including Cyber and Missile Defence. In strengthening the Alliance, the Agency applies industry best practices and provides a full life-cycle approach: from analysis and concept development, through experimentation and Capability Development, to operations and maintenance for both missions and exercises.The NCI Agency is a key pillar of NATO Secretary General's Smart Defence and Connected Forces initiatives.

The Agency was established on 1 July 2012, as part of a broader NATO reform, through the merger of the NATO Consultation, Command and Control Agency (NC3A), the NATO Air Command and Control System Management Agency (NACMA), the NATO Communication and Information Systems Services Agency (NCSA – except Deployable CIS), the Active Layered Theatre Ballistic Missile Defence (ALTBMD) Programme Office and elements of NATO Headquarters Information and Communication Technology Service.



NCIRC TC, NCI Agency and the NATO Cyber Defence

3. Established Business Model

Who can join?

Membership of MISP is currently open to any cyber defence and governmental related constituent of the NATO Member Nations. Before an organization joins MISP it needs to be confirmed by either the point of contact listed in the MoU between the NATO CDMB and the NATO Member Nation or, for those cases for which there is no MoU between the nation and NATO CDMB, a representative of the Organization's National Representation at NATO. In any case, the membership request will be coordinated with the NCIRC Coordination Centre (NCIRC CC).

What are the costs?

MISP is a common funded capability that is offered to NATO Nations for evaluation purposes at no cost till the end of 2014. The exact business model to be applied for MISP can only be finalized once the NCI Agency CIS Security Services framework is in place.

How to join?

Joining instructions and Terms-of-Use have been developed to rule the usage of the platform and put in the necessary safe-guards to maintain trust within the community, and address the legal and the governance aspects as well as the controlling the information release. They can be obtained by sending an email request to MISPsupport@ncirc.nato.int.

For further information please contact NCI Agency POC:

Coordinator

Ms Agata Szydelko
Principal Account Manager Multinational and Organizations Demand Management
Tel: +32 2 707 84 41
e-mail: agata.szydelko@ncia.nato.int

NATO Communications and Information Agency
Agence OTAN d'information et de communication

Bâtiment Z
Avenue du Bourget 140
1110 Brussels
Belgium
www.ncia.nato.int