NEWSLETTER
Empowering SOCs Through Innovation

Is the Malware Information Sharing Platform Like a Good Neighbour?

In cybersecurity, trust is a necessity. Not blind trust, but structured, informed and responsible cooperation. Within the INTERCEPT Threat Sharing Platform, the Malware Information Sharing Platform - MISP - plays exactly that role. If the digital world were a neighbourhood, MISP would be the neighbour who keeps watch, shares what they see and helps others act before a small signal turns into a serious incident.

From Isolated Incidents to Shared Awareness

Cyber threats move at machine speed. A phishing campaign launched in one country can reach organizations across Europe within minutes. A newly discovered vulnerability can be exploited before many teams even become aware of it. In such an environment, working in isolation is no longer sustainable.

MISP, a globally recognized open-source threat intelligence platform, enables the structured exchange of security information between trusted participants. Instead of fragmented alerts or informal exchanges, threat data is shared in a standardized, machine-readable format. This includes indicators of compromise such as malicious IP addresses, domains and file hashes, as well as contextual information about attacker techniques, vulnerabilities and malware behaviour.

Because the data is structured, it can be automatically processed and correlated by security tools. This reduces manual effort and accelerates detection and response.

When One Detection Protects Many

Take a simple example: a company in Slovenia detects an attempted brute-force attack targeting its servers, originating from an IP address located in Africa. The attack may involve repeated login attempts, phishing components or even coordinated DDoS techniques. The company's Security Operations Center identifies the malicious activity, blocks it and analyzes the associated indicators.

Instead of stopping there, the relevant threat intelligence - such as the source IP addresses, attack patterns, timestamps and technical characteristics - is shared through the Threat Sharing Platform built on MISP.

All connected partners are immediately notified. They can proactively check their own systems for similar activity and implement preventive measures, such as blackholing the malicious IP addresses, applying targeted firewall rules or adjusting detection mechanisms.

This approach significantly reduces the time required to secure systems. More importantly, it prevents the same threat actor or infrastructure from successfully targeting other organizations within the network. A single detection becomes collective protection.

MISP at the Core of the INTERCEPT Threat Sharing Platform

Within INTERCEPT, MISP serves as the backbone of the Threat Sharing Platform. The project builds on this trusted and widely adopted technology and enhances it to support cross-organizational and cross-border collaboration, particularly between Security Operations Centers.

The aim is to make cooperation efficient without compromising data protection, confidentiality or regulatory compliance. Organizations retain control over what they share, how it is shared and with whom. At the same time, they benefit from access to a broader intelligence ecosystem.

Automation and intelligent correlation mechanisms help ensure that the platform delivers relevant and actionable insights rather than overwhelming users with raw data. The focus is on operational value - enabling faster decisions and more coordinated responses.

Built on Operational Expertise

The INTERCEPT partners bring substantial hands-on experience in operating Security Operations Centers and managing incidents across IT and OT environments, including critical infrastructures and industrial systems.

One of the partners, SI-CERT, already uses MISP in national-level operations, contributing valuable practical knowledge to the platform's development. This ensures that the solution is aligned with real operational workflows and the realities of incident response.

By strengthening monitoring, investigation and information-sharing capabilities, the platform enhances resilience across networks, servers and industrial environments.

Stronger Together

Cyber threats do not respect borders, sectors or organization size. However, access to timely and high-quality threat intelligence has traditionally been uneven. Larger organizations often have dedicated resources, while smaller entities may struggle to obtain actionable insights.

Through structured, trusted and secure intelligence sharing based on MISP, the INTERCEPT Threat Sharing Platform helps close that gap. Detection times are shortened, response is coordinated and defensive measures are strengthened collectively.

In this sense, MISP truly acts like a good neighbour. It does not replace internal security controls, but it ensures that no organization has to face evolving threats entirely alone.

Follow INTERCEPT journey on Digital media platforms

- WEBSITE
- LINKEDIN
- YOUTUBE
- X

Follow INTERCEPT

www.interceptcybersecurity.eu

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project funded under Grant Agreement No. 101190460 is supported by the European Cybersecurity Competence Centre.