Best Practices in Threat Intelligence

MISP Project

Table of Contents

Introduction

This book objective is to compile the best practices in threat intelligence analysis with the support of the open source threat intelligence platform called MISP. The best practices described are from information sharing communities (ISAC or CSIRT) which are regularly using MISP to support their work and sharing practices.

Best Practices

Improving Analysis

Improvement of analysis can range from simple notification of a false-positive, a typographic error up to a complete competitive or counter analysis of the original analysis.

A common difficulty in threat intelligence is to improve existing analysis and how to do efficiently. One of the main question is to ask what will be the target audience of the improved analysis and the objective:

1. Informing the original analyst/author (e.g. a security vendor or a CSIRT) about a specific mistake or error which needs to be corrected.
2. Improving an existing analysis by performing a complementary analysis or review which will be shared and used by another group (e.g. a specific constituency, team within your organisation or member of an ISAC).

In the case number 1, MISP includes a mechanism to propose changes to the original creator. This mechanism is called proposal. By using proposal, you can propose a change in the value of an attribute (such as a typographic in an IP address, missing contextual information, type of the information, the category or the removal of an IDS flag). The proposal will be sent back to the original author who can decide to accept the proposal or discard it.

Adding proposal has some major advantages such as being very quick and there is no need to create a new event. But such approach works only if you are willing to lose control over the data. This is pretty efficient for small changes but if additional information such as galaxy or objects need to be added then the event extension is more appropriate.

In the case number 2, the extend event functionality is very handy. The extend event allow to create your own information into a self-contained event (which can have custom distribution rules) and reference the original analysis. The information can be shared back to the original author or kept in a limited scope such as a specific sector or trust group.

For more information about the extend event functionality in MISP, the blog post **Introducing The New Extended Events Feature in MISP** includes a lot of details.

What To Share or What Counts As Valuable Information?

Valuable information is a moving concept and highly depending of the goal of the users sharing and/or using the information. A valuable information can also evolve following the capabilities of an organisation.

Contribution comes in various shapes and sizes.

Information which are often distributed within sharing communities are the following:

- Analysis report of a specific threat (such as security vendor report, blog post) which can be open source intelligence or limited distribution
- Enhanced analysis of an existing report (such as data qualification, competitive or counter analysis)
- A post-mortem analysis of an incident
- Additional information about existing or known threats (such as adversary techniques, new malware samples or complementary discoveries)
- False-positive or false-negative reporting
- Asking for contribution or support from the community (such as "have you seen this threat?" or "do you have more samples?")

By having a look at the object templates or the MISP attribute types, this can help you to discover what it's actively shared within other communities. If a type or an object template is not matching your data model, you can easily create new ones.

When asking for the support of the community, using a specific taxonomy such as collaborative intelligence to express your needs might help everyone and improve automation.

Authors and Contributors

- Alexandre Dulaunoy
- Andras Iklody

Glossary

ISAC

Information Sharing and Analysis Center

MISP

MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing