Best Practices in Threat Intelligence

MISP Project

Table of Contents

Introduction . . . 1
Best Practices . . . 2
  Improving Analysis . . . 2
  What To Share or What Counts As Valuable Information? . . . 3
  Expressing confidence in an analysis . . . 4
Authors and Contributors . . . 5
Glossary . . . 6

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

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

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 to and used by another group (e.g. a specific constituent, or a team within your organisation or a member of an ISAC, etc).

In the first case, MISP includes a mechanism to propose changes to the original creator, a mechanism we refer to as proposals. By using proposals, you can propose a change to the value or the context of an attribute (such as a typographic error 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 or discard it.

The advantages of using the proposal system include the lack of a need to create a new event as well as the process itself being very simple and fast. However, it assumes that the party providing the improvements is willing to lose control over the proposed data. This is pretty efficient for small changes but for more comprehensive changes, especially those that include non-attribute information such as galaxy clusters or objects, the event extension is more appropriate.

Apart from being more suitable for more comprehensive changes, the second scenario is also a great fit for the extended event functionality, allowing users wanting to provide additional information or an alternate view-point with the opportunity of creating a self-contained event (which can have its own custom distribution rules) that references the original analysis. This information can be shared back to the original author or kept within a limited distribution scope such as a specific sector, a trust group or as internal information for the organisation providing the additional information.

For more information about the extended 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.

Expressing confidence in an analysis

Expressing the confidence or the lack of in an analysis is critical step to help a partner or a third-party to check your hypotheses and conclusions.

Analysis or reports are often shared with technical details but often lack the overall confidence level associated.

Adding confidence or estimative probability have multiple advantages such as:

- Allowing receiving organisations to filter, classify and score the information in an automated way
- Information with low-confidence can still be shared and reach communities or organisations interested in such information without impacting organisations filtering out by confidence level
- Supporting counter and competitive analyses to validate hypotheses expressed in original reporting

Complement analysis with contrary evidences is also very welcome to ensure the original analysis and the hypotheses evaluated.

MISP taxonomies contain an exhaustive list of confidence levels including words of estimative probability or confidence in analytic judgment.

threat-intelligence.eu includes an overview of the methodologies and process to support threat intelligence.

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