Mapping investigations and cases in MISP

E.205

CIRCL Computer Incident Response Center Luxembourg

MISP Project
https://www.misp-project.org/

March 23, 2022

Mapping investigations and cases in MISP
E.205
CIRCL Computer Incident Response Center Luxembourg
MISP Project
https://www.misp-project.org/
March 23, 2022

Objectives of this module

- Quick recap on MISP data model and the distribution levels
- Overview of the case to be structured and encoded
- Encoding technical data in MISP
  - Network indicators: `ip`,`domain`, `url`, ...
  - Files and binaries: non-malicious / malicious *payload*
  - Emails: `content`, `header`, `attachment`, ...
  - Web: URL, `cookies`, `x509`
  - Cryptographic materials: public / private key, `certificate`
  - Infrastructure and devices
  - Financial fraud: `bank-account`, `phone-number`, `btc`
  - Person: `name`, `online accounts`, `passport`, `visa`
  - Support tools and scripts: `yara`, detection/remediation scripts
  - Vulnerabilities: `cve`
  - External analysis: Reports, blogpost
  - -> (infection vector, ransome notes,)
- Adding relationships
- Adding timeliness

Objectives of this module
Quick recap on MISP data model and the distribution levels
Overview of the case to be structured and encoded
Encoding technical data in MISP
Network indicators: ip,domain, url, ...
Files and binaries: non-malicious / malicious payload
Emails: content, header, attachment, ...
Web: URL, cookies, x509
Cryptographic materials: public / private key, certificate
Infrastructure and devices
Financial fraud: bank-account, phone-number, btc
Person: name, online accounts, passport, visa
Support tools and scripts: yara, detection/remediation scripts
Vulnerabilities: cve
External analysis: Reports, blogpost
-> (infection vector, ransome notes,)
Adding relationships
Adding timeliness
Enrichments via module and correlation