

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, ransom notes,)
- Adding relationships
- Adding timeliness