ENFORCE project - cybercrime training

Improving the design of curriculum with practical information sharing

CIRCL
Computer Incident
Response Center
Luxembourg

MISP
Threat Sharing

Alexandre Dulaunoy *TLP:WHITE*

FIC 2020

Curriculum developed

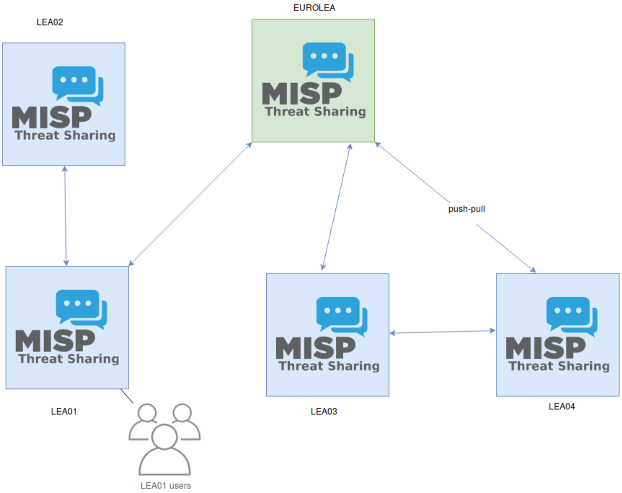
- E.100 MISP - Open Source **Threat Intelligence Platform Supporting Digital Forensic** and Incident Response
- E.200 Post Mortem Analysis Techniques of Fake Invoices Manipulated PDF documents
- E.201 **Digital Forensics** - An introduction into Post-mortem Digital Forensics
- E.202 **Network forensic** - Analysing black-hole monitoring dataset - How to better understand DDoS attacks from backscatter traffic, opportunistic network scanning and exploitation
- E.300 **Data mining** using AIL framework
- E.301 **Cryptography Workarounds** For Law Enforcement

Development process

- The development process is to bring together **forensic analysis, information sharing and information exchange**.
- The **law enforcement contribution is critical and helps us to improve open source software** such as MISP and the training materials at large for the LE community.
- **The sessions are interactive** and we work together on solving cases, discovering new findings and techniques on a real environment running on a Cyber Range platform (HNS).

Training setup to support information sharing

ENFORCE - Training / MISP overview



Practical outcomes of the ENFORCE project

- **Direct improvements into open source software** used by law enforcement
- The complete ENFORCE curriculum **will be open sourced** in May 2020
- **Ensuring the sustainability of the project** via contributors in various fields such as law enforcement

- Contact: info@circl.lu
- https://www.circl.lu/
- https://www.misp-project.org/
- https://github.com/MISP - https://twitter.com/MISPProject
- Don't hesitate to get in touch with us to access one of our sharing community or feedback to improve MISP.