D4 Project

Open and collaborative network monitoring

Team CIRCL
https://www.d4-project.org/

20190207

Alexandre Dulaunoy - Sami Mokaddem

Problem statement

- CSIRTs (or private organisations) build their **own honeypot, honeynet or blackhole monitoring network**.
- Designing, managing and operating such infrastructure is a tedious and resource intensive task.
- **Automatic sharing** between monitoring networks from different organisations is missing.
- Sensors and processing are often seen as blackbox or difficult to audit.

Objective

- Based on our experience with MISP[1] where sharing played an important role, we transpose the model in D4 project.
- Keeping the protocol and code base **simple and minimal**.
- Allowing every organisation to **control and audit their own sensor network**.
- Extending D4 or **encapsulating legacy monitoring protocols** must be as simple as possible.
- Ensuring that the sensor server has **no control on the sensor** (unidirectional streaming).

[1] https://github.com/MISP/MISP