CyFORT
SUITE OF OPEN-SOURCE TOOLS

IDPS-ESCAPE, SATRAP-DL, C5-DEC, OpenTRICK

At Luxembourg GRC summit - GRC & open-source pitch session

Carlo Harpes
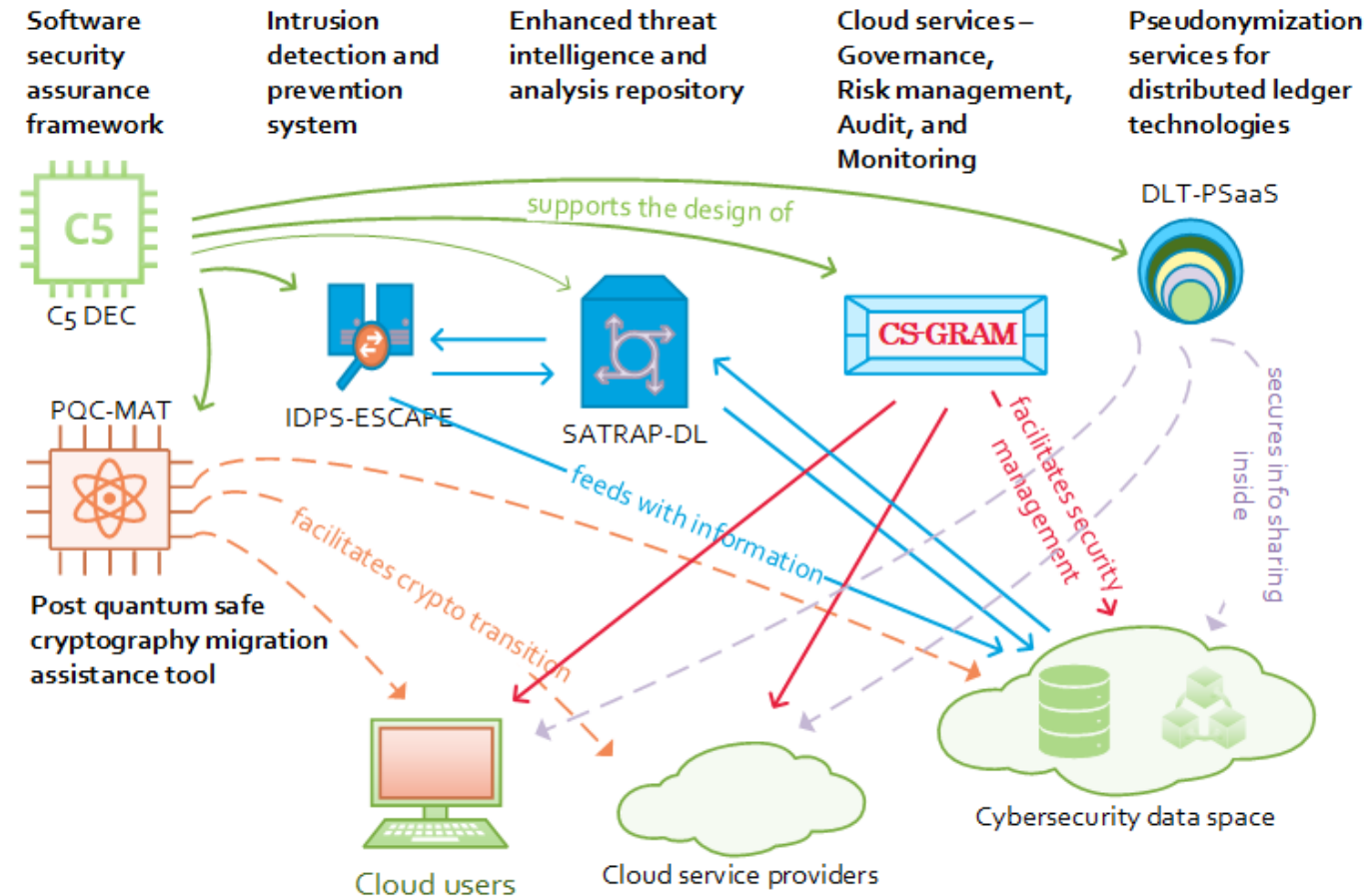
Arash Atashpendar

Itzel Vázquez Sandoval

https://abstractionslab.com
https://www.itrust.lu

2025-06-05

CyFORT

Cloud Cybersecurity Fortress of Open Resources and Tools for Resilience

Open Tool for Risk management of an ISMS based on a Central Knowledge base
https://github.com/itrust-consulting/OpenTRICK

- An open source Webapp (with multiple Excel-based I/O functions)

- for ISO/IEC 27001 compliant risk management with guidance from 27005

- to model dependencies (cf. DRAW)

- to document the level of **security/compliance** and estimate implementation **costs** for multiple referential (27002, 27701, GDRA, PIMS, tisax, ENISA, IEC…

- to assess the **frequency and impact** of standard or ILR/CSSF/privacy-specific attack scenarios applied to selected assets

- to estimate residual risks based on (pre-defined but configurable) **risk reduction factors**

- to prepare a **risk treatment plan** and a cost per phase summary table

- to export with one click reporting compliant for regulator ILR, CSSF based on a correspondence table for internal versus regulator-defined asset names and evaluation levels

- to generate a customer-specific full report of all information and graphs

- to compare evaluation of parameter over years or for different scopes

- can replace fixed value estimates with formula on parameters updated via API for dynamicity (e.g. to use an impact calculation based on the number of customers, or attack likelihood based on the current number of unpatched system).
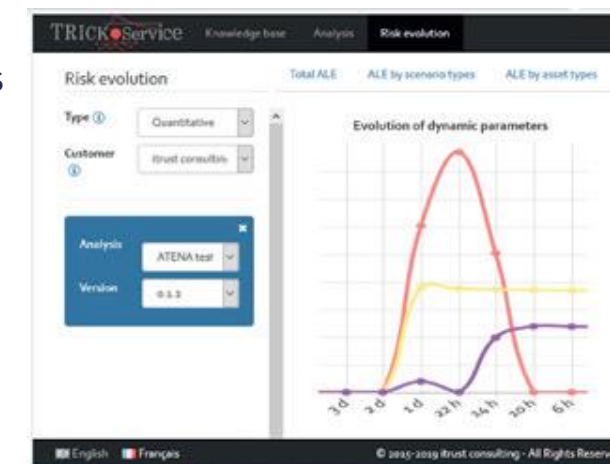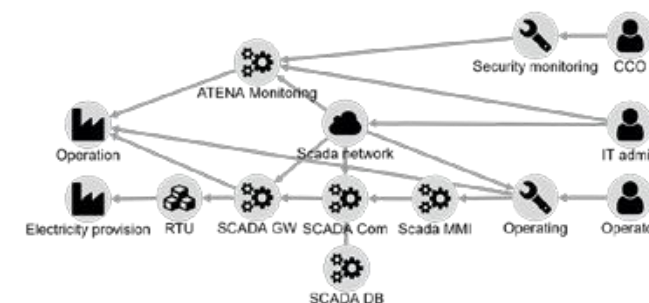
IDPS-ESCAPE

Intrusion **D**etection and **P**revention **S**ystems for **E**vading **S**upply **C**hain **A**ttacks and **P**ost-compromise **E**ffects

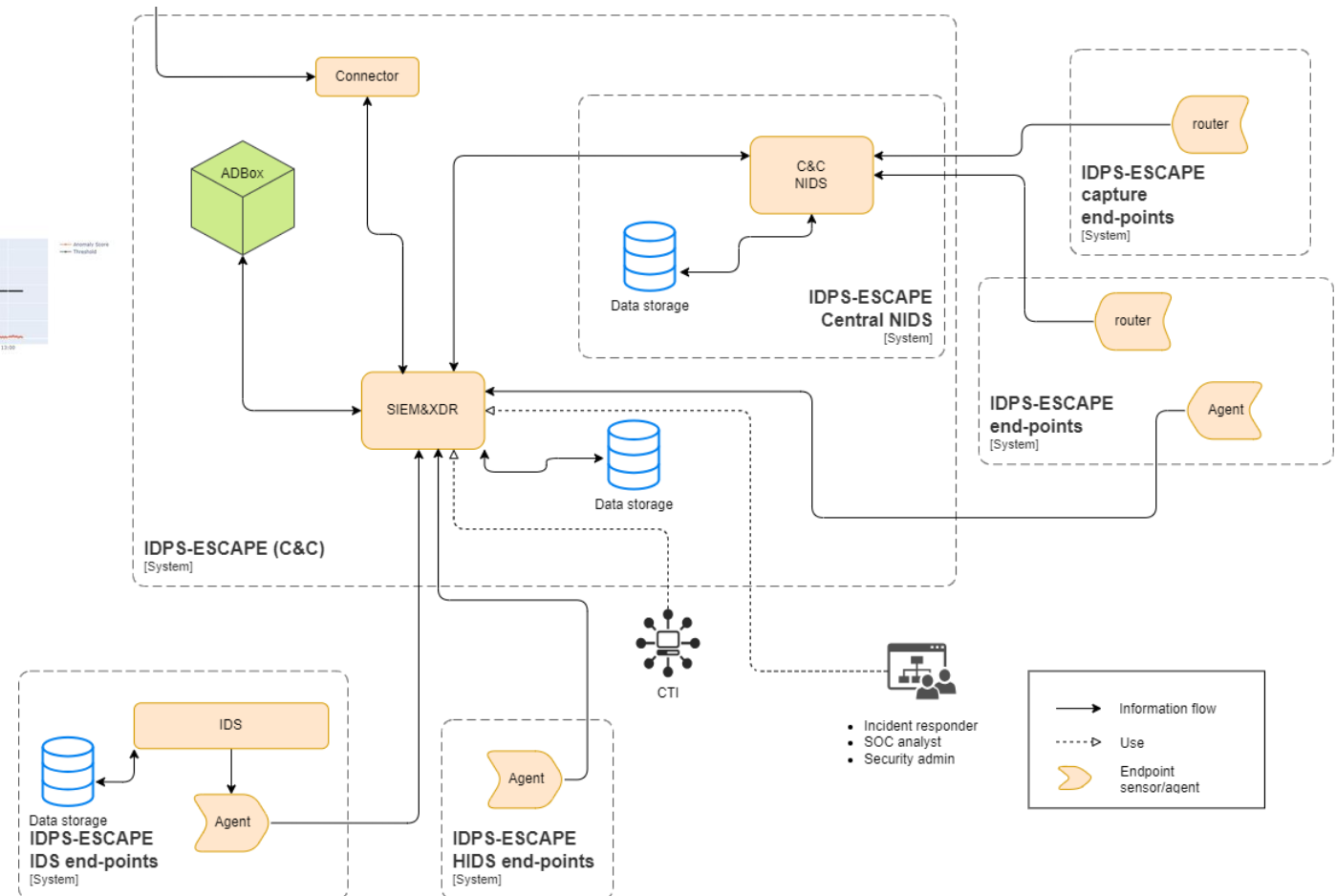https://github.com/AbstractionsLab/idps-escape

- Security monitoring, host & network intrusion detection and prevention

- **AI**-powered **anomaly detection**

- **Automated** security orchestration & **response** to cyber attacks
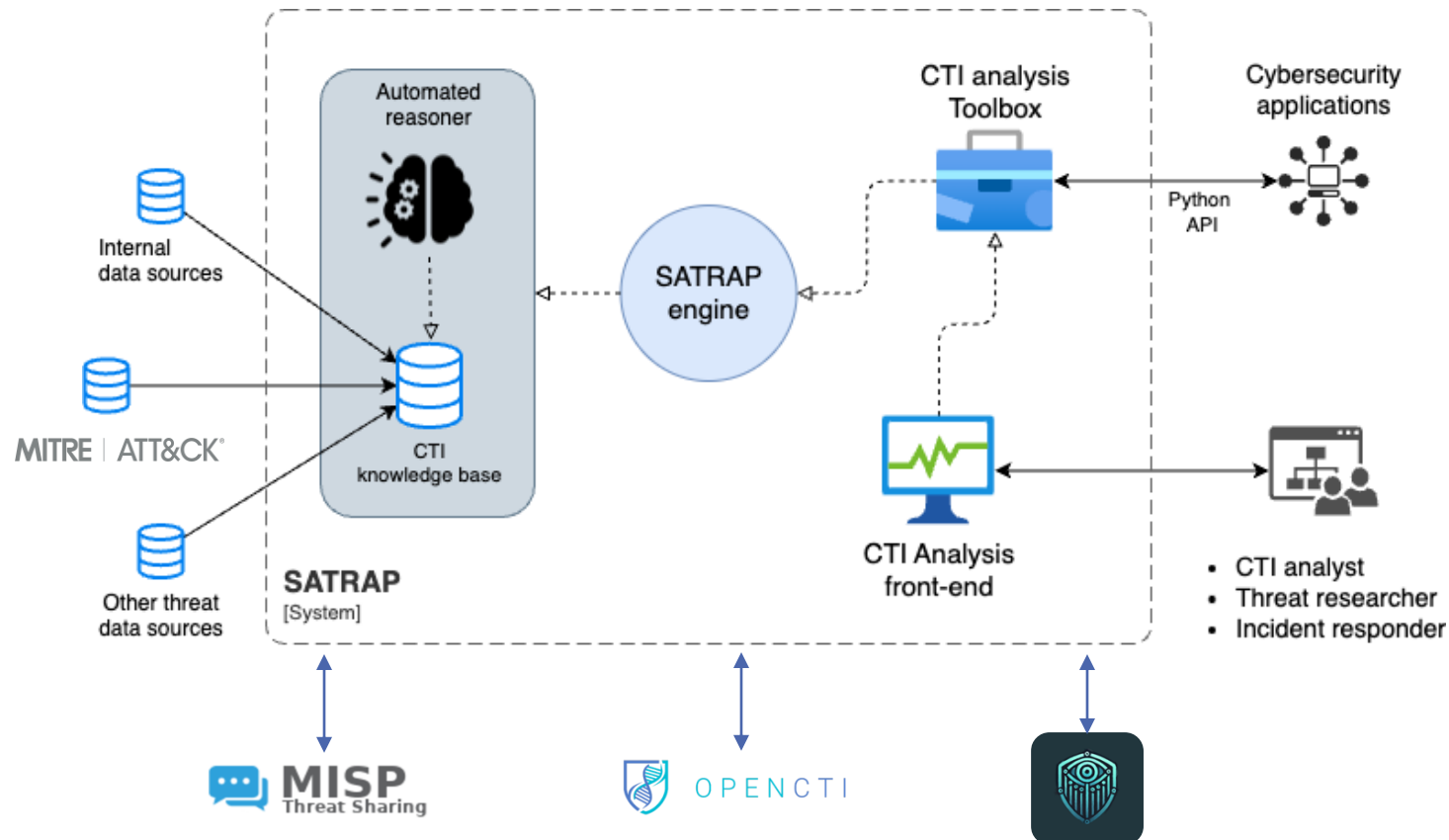
- Integrated with

wazuh.

SURICATA®

MISP Threat Sharing

OPENCTI

Anomaly Scores and Prediction Over Time

— Anomaly Score
— Threshold

Connector

ADBox

C&C NIDS

Data storage

IDPS-ESCAPE Central NIDS [System]

router

IDPS-ESCAPE capture end-points [System]

SIEM&XDR

Data storage

IDPS-ESCAPE (C&C) [System]

router

Agent

IDPS-ESCAPE end-points [System]

IDS

Data storage
IDPS-ESCAPE IDS end-points [System]

Agent

Agent

IDPS-ESCAPE HIDS end-points [System]

CTI

- Incident responder
- SOC analyst
- Security admin

→ Information flow
⊳ Use
Endpoint sensor/agent

SATRAP-DL

Semi-**A**utomated **T**hreat **R**econnaissance and **A**nalysis **P**owered by **D**escription **L**ogics

https://github.com/AbstractionsLab/satrap-dl

Automated reasoning for cyber threat intelligence (CTI)

- **Automated CTI analysis** tasks such as deducing techniques and tools used by threat actors
- **Built-in rules** to derive **CTI knowledge** from existing data
- Textual and **visual explanations** of inferred **CTI knowledge**
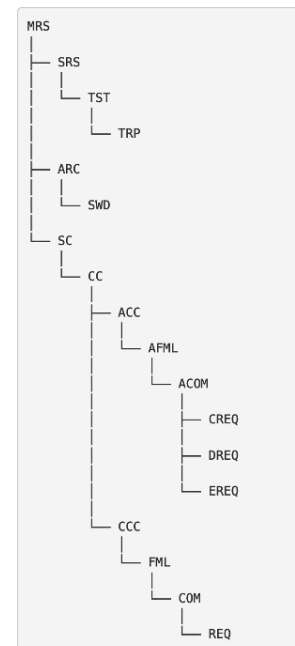- Powered by

C5-DEC

Common Criteria for Cybersecurity, Cryptography, Clouds – Design, Evaluation and Certification
https://github.com/AbstractionsLab/c5dec

- Build software using C5-DEC **method** and **tools**

- Generate documentation and technical reports while ensuring traceability

- Linkable system specifications and artifacts

- Features
  - Secure SW dev. life cycle
  - Common Criteria toolbox
  - Quantum-safe cryptography
  - Cyber-physical system security
  - Project management (HERMES)
  - AI-friendly (Markdown, YAML)

- Used on **IDPS-ESCAPE** and **SATRAP**

CONTACT

harpes@itrust.lu
arash@abstractionslab.lu
itzel@abstractionslab.lu

https://abstractionslab.com

Want to know more?

Meet us at BSidesLuxembourg 2025 on 19 June

GnuPG — Get our public keys for encrypted email from our website's team page

Signal — Contact us by email to request a Signal username

[matrix] — https://matrix.to/#/@<firstname>-alab:matrix.org

12 Rue du Château d'Eau
L-3364 Leudelange
Luxembourg