



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

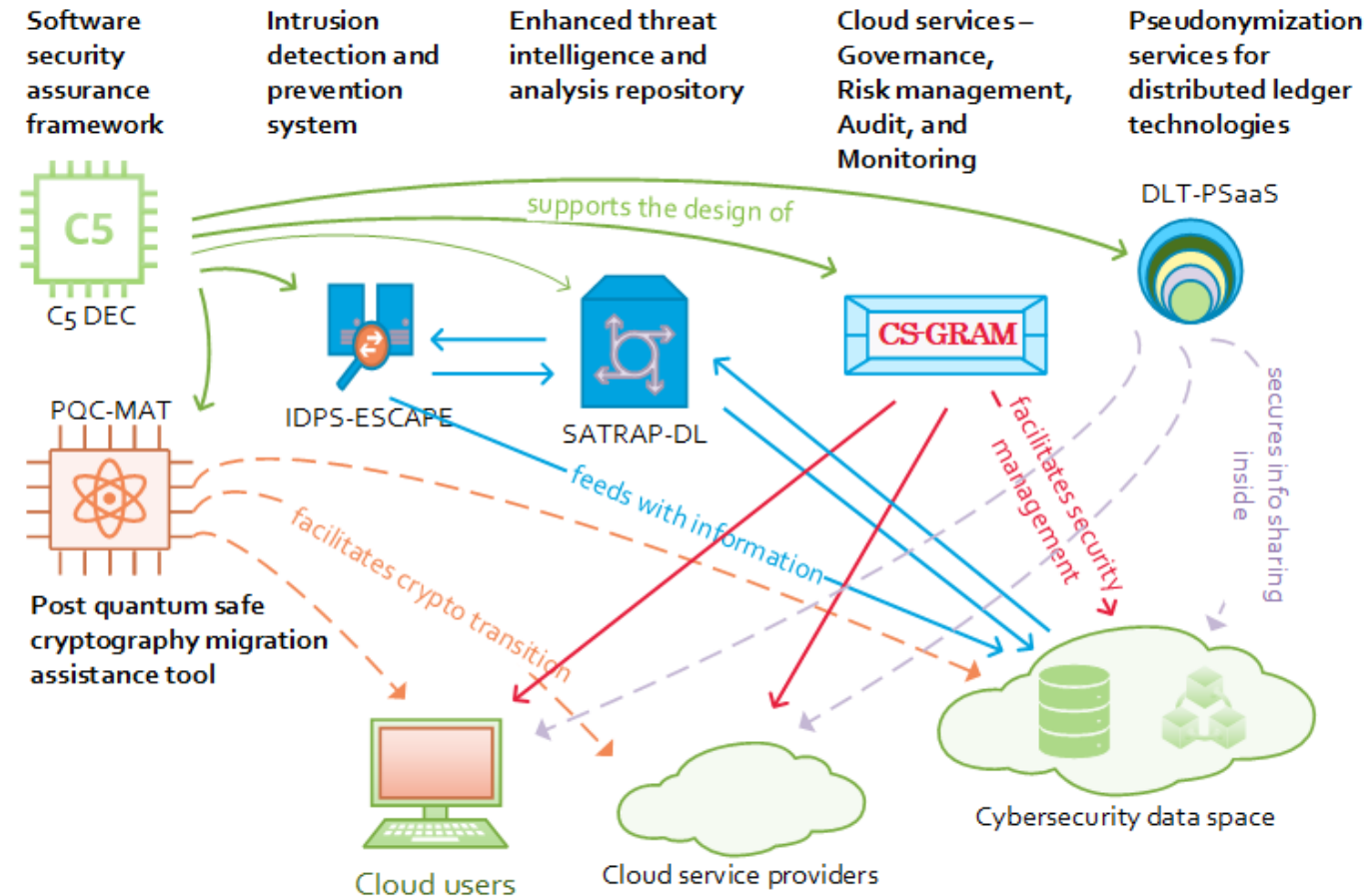
Itzel Vázquez Sandoval

<https://abstractionslab.com>

<https://www.itrust.lu>

2025-06-05

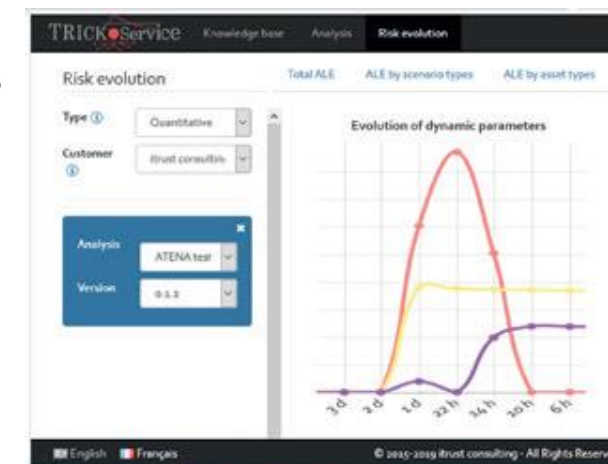
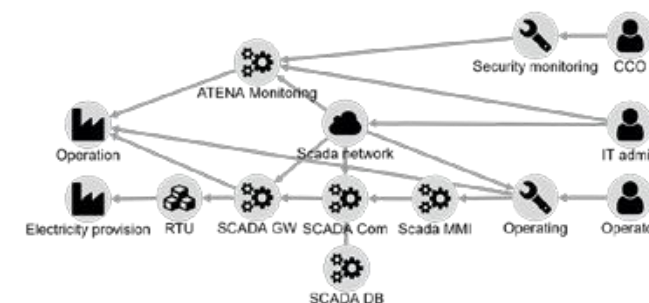
Cloud Cybersecurity Fortress of Open Resources and Tools for Resilience



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 Detection and Prevention Systems for Evading Supply Chain Attacks and Post-compromise Effects

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

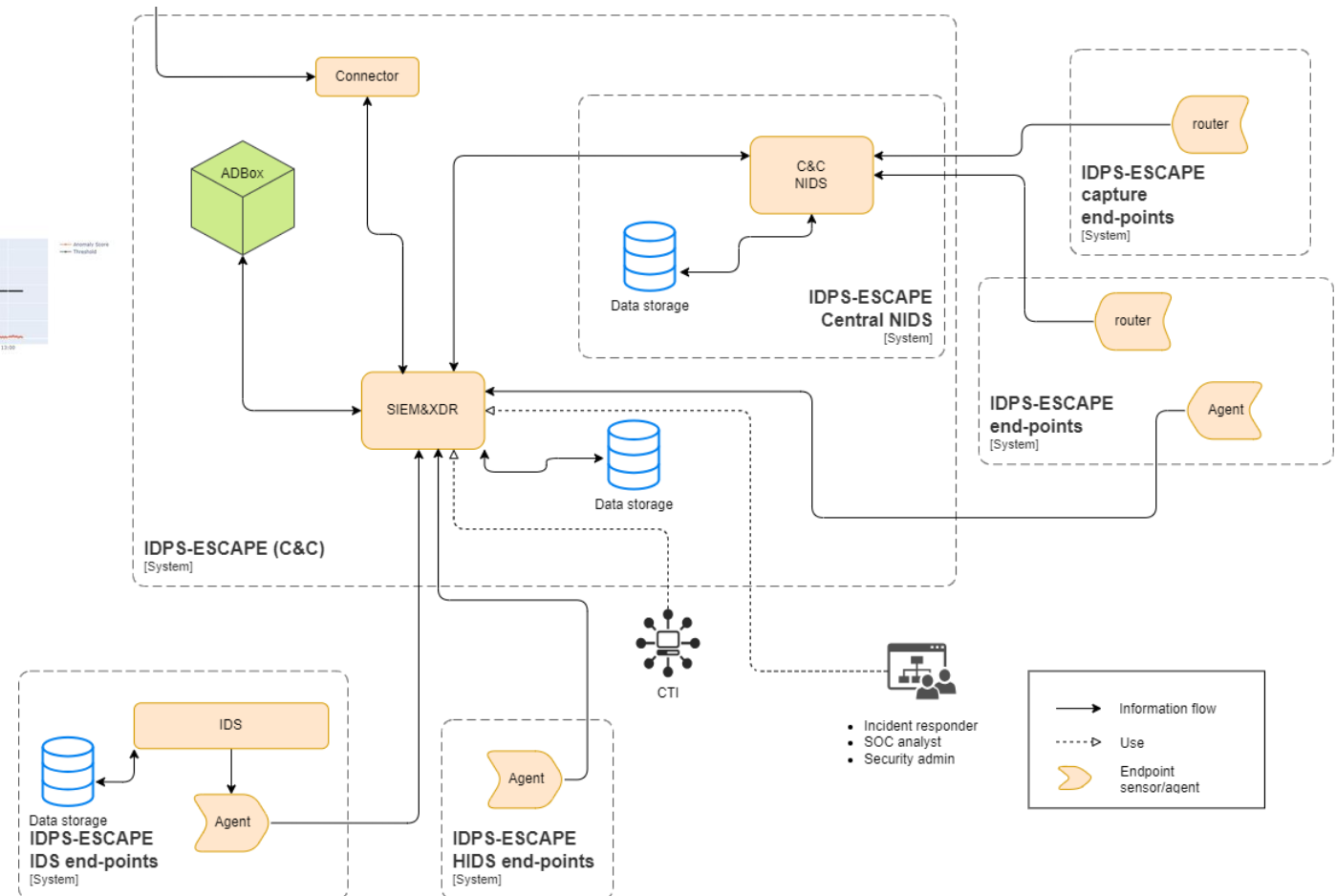
- Security monitoring, host & network intrusion detection and prevention
- **AI-powered anomaly detection**
- **Automated** security orchestration & **response** to cyber attacks
- Integrated with



wazuh.



OPENCTI

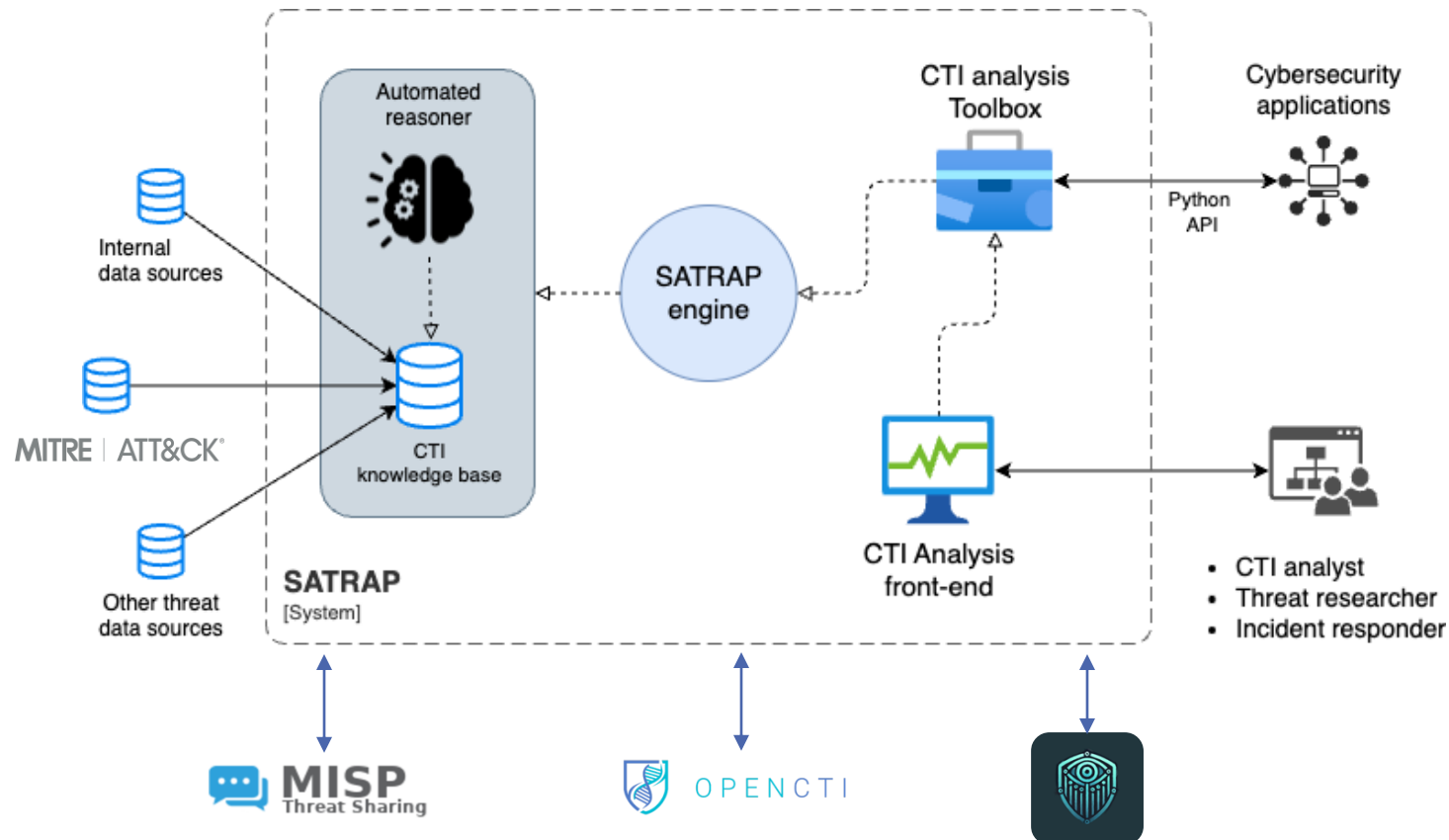


SATRAP-DL



Semi-Automated Threat Reconnaisance and Analysis Powered by Description Logics

<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

TypeDB

C5-DEC

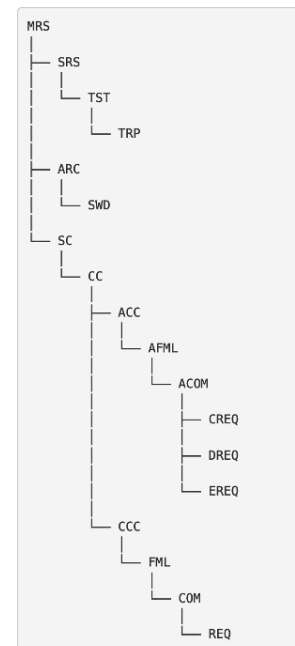


Common Criteria for Cybersecurity, Cryptography, Clouds – Design, Evaluation and Certification

<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

Tree Structure:



Published Documents:

- ACC
- ACOM
- AFML
- ARC
- CC
- CCC
- COM
- CREQ
- DREQ
- EREQ
- FHL
- MRS
- REQ
- SC
- SRS
- SWD
- TRP
- TST

Item Traceability:

General information	
Name of the company	itrust Abstractions Lab
Project title	CyFORT
Type	Report (REP)
Reference	3COM
Version	1.0
State	Final
Owner	Arash
Authors	Arash
Application date	03/07/2024
Classification	Confidential

Defect category	Defect description
0 = flawless	1 = insignificant defect
2 = minor defect	3 = major defect
4 = critical defect	

Parent links	Value
test-date	2025-03-29
test	ANT
defect-category	2 = minor defect
passed-steps	5
failed-steps	2
not-executed-steps	0
release-version	0.1
verification-method	LR

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



Get our public keys for encrypted email from our website's [team page](#)



Contact us by email to request a [Signal username](#)



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



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