Hello LuCy, nice to meet you!

Cynthia Wagner & Denim Latić

Securing.What.Matters

<Prague.CZ><8-10 April 2025>

Co-funded by the European Union

Luxembourg **Cy**ber**Se**curity **4 R**esearch & **E**ducation Project

Why LuCySe4RE?

- A lot of small organisations shape our R&E community
  - No security monitoring
  - Lack of competences, interest and budget
- New EU directives show up quickly such as NIS2, CER …
- LuCy aims to improve overall cybersecurity maturity and awareness within R&E
- Respect our philosophy of using open-source

The lo

M tings

Me gs

Meeti

The long way to LuCySe4RE

Quantity

Retention

Alerting

Type of logs

24/7?

The LuCySe4RE framework objectives

assess the status quo of cybersecurity preparedness and improve it

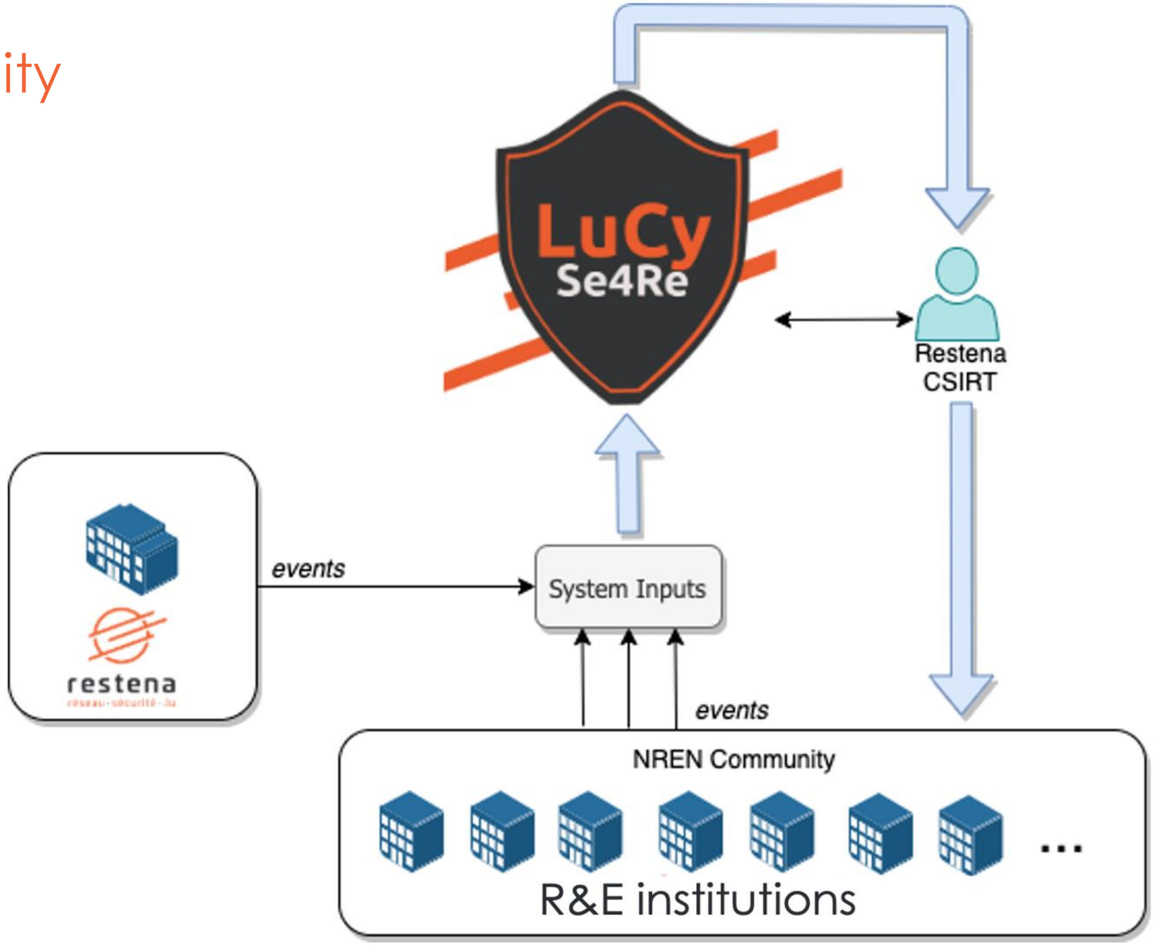
deploy innovative cybersecurity solutions and make it available to organisations in the Luxembourg R&E sector

teach and raise awareness of current cybersecurity threats, countermeasures, and usage of relevant tooling

low-cost project for NRENS and provide a service for R&E community without additional costs

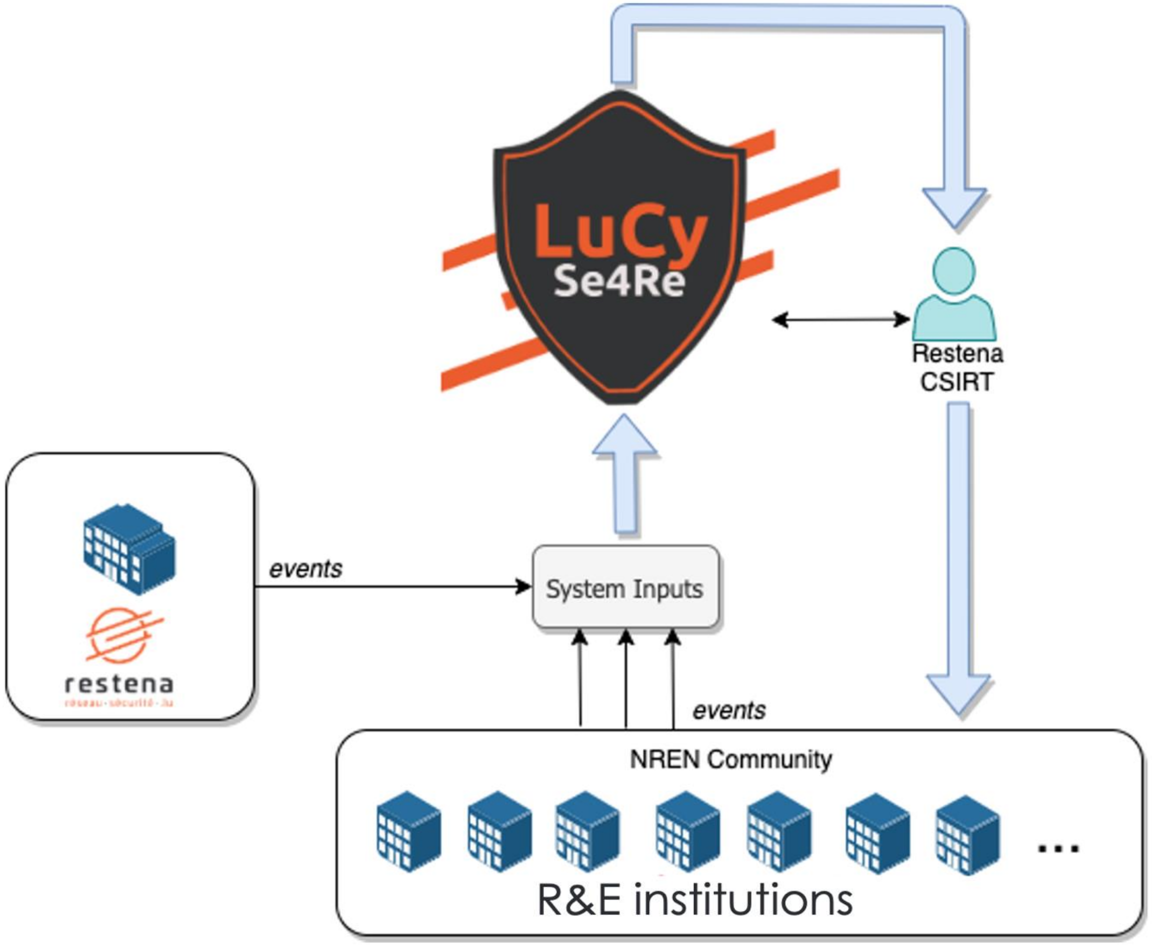
Let’s set the perimeter …

- Introduce a centralised solution for R&E community
  - Collect cybersecurity events
  - Threat detection
  - Monitoring, alerting and reporting
  - Incident response via CSIRT team
  - Access to dashboards for institutions
  - Dedicated Trainings
  - Cybersecurity awareness resources
  - Conferences
  - Security maturity assessment



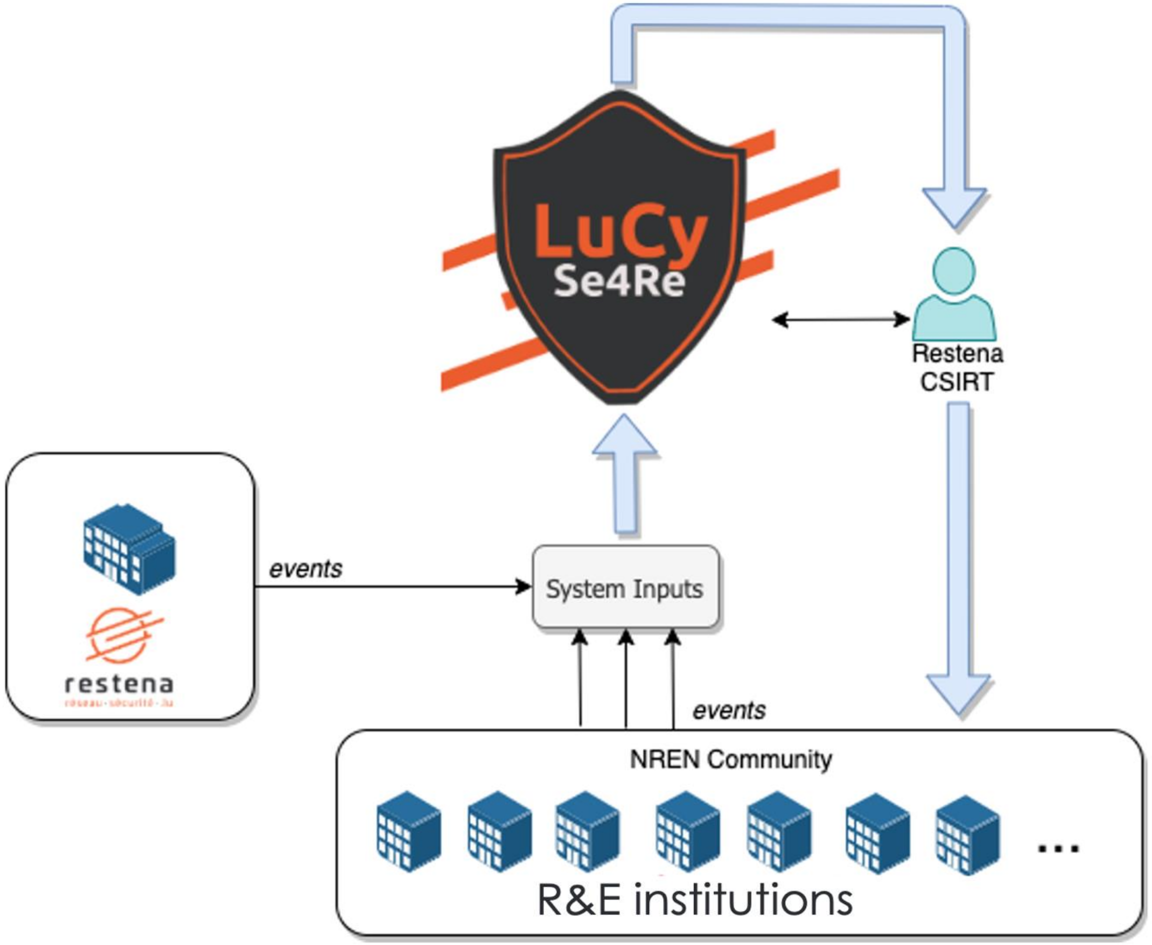
Community benefits

- Toolset adapted to R&E needs
- Better detection of sector specific threats
- Better preparedness due to community knowledge
- Compliance with new European directives
- Low costs for R&E institutions

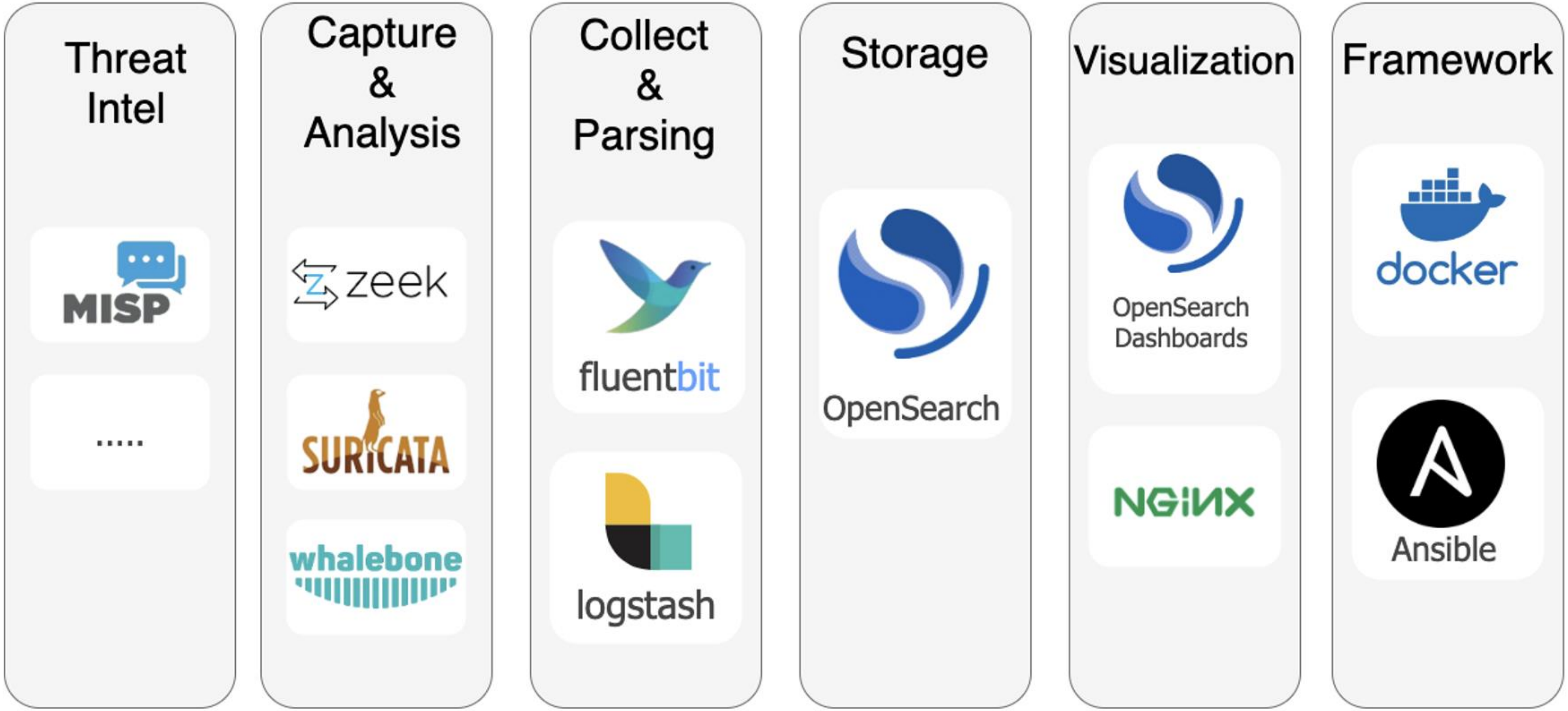


So who is LuCy?

- Based on open-source technologies only*
- Hardware has been reused and new hardware purchased
- On premises
- Establishing a SOC team



Current LuCySe4RE state of architecture



Threat Intel
- MISP
- .....

Capture & Analysis
- zeek
- SURICATA
- whalebone

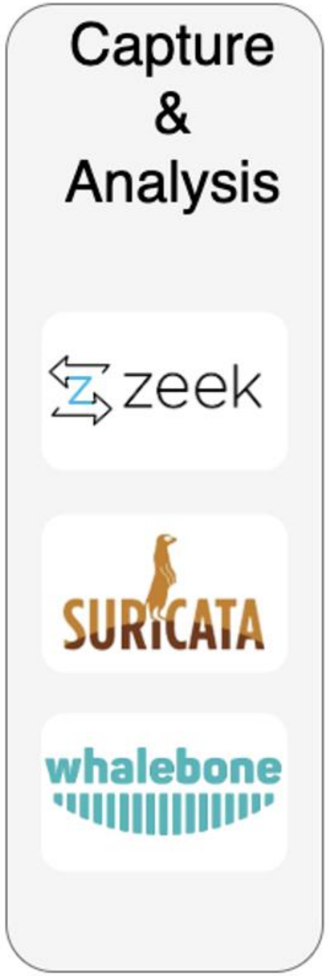
Collect & Parsing
- fluentbit
- logstash

Storage
- OpenSearch

Visualization
- OpenSearch Dashboards
- NGINX

Framework
- docker
- Ansible

Current LuCySe4RE state of architecture



Capture & Analysis

Capture & Analysis

Zeek: parsing of network traffic

Suricata: Online and Offline

- Online: live network

- Offline: PCAP files

Whalebone: secure DNS resolution

Current LuCySe4RE state of architecture

Collect
&
Parsing

fluentbit

logstash

Collect & Parsing

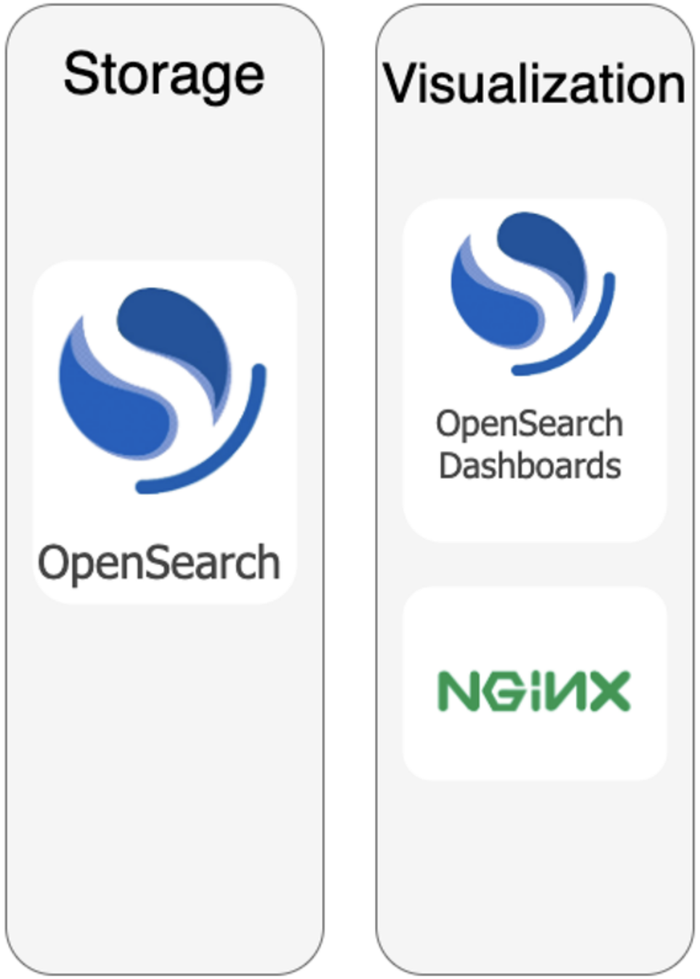
Fluentbit: Log collector

- Acquisition of logs per institution

Logstash: Parse & transform data

- Compatibility with Opensearch

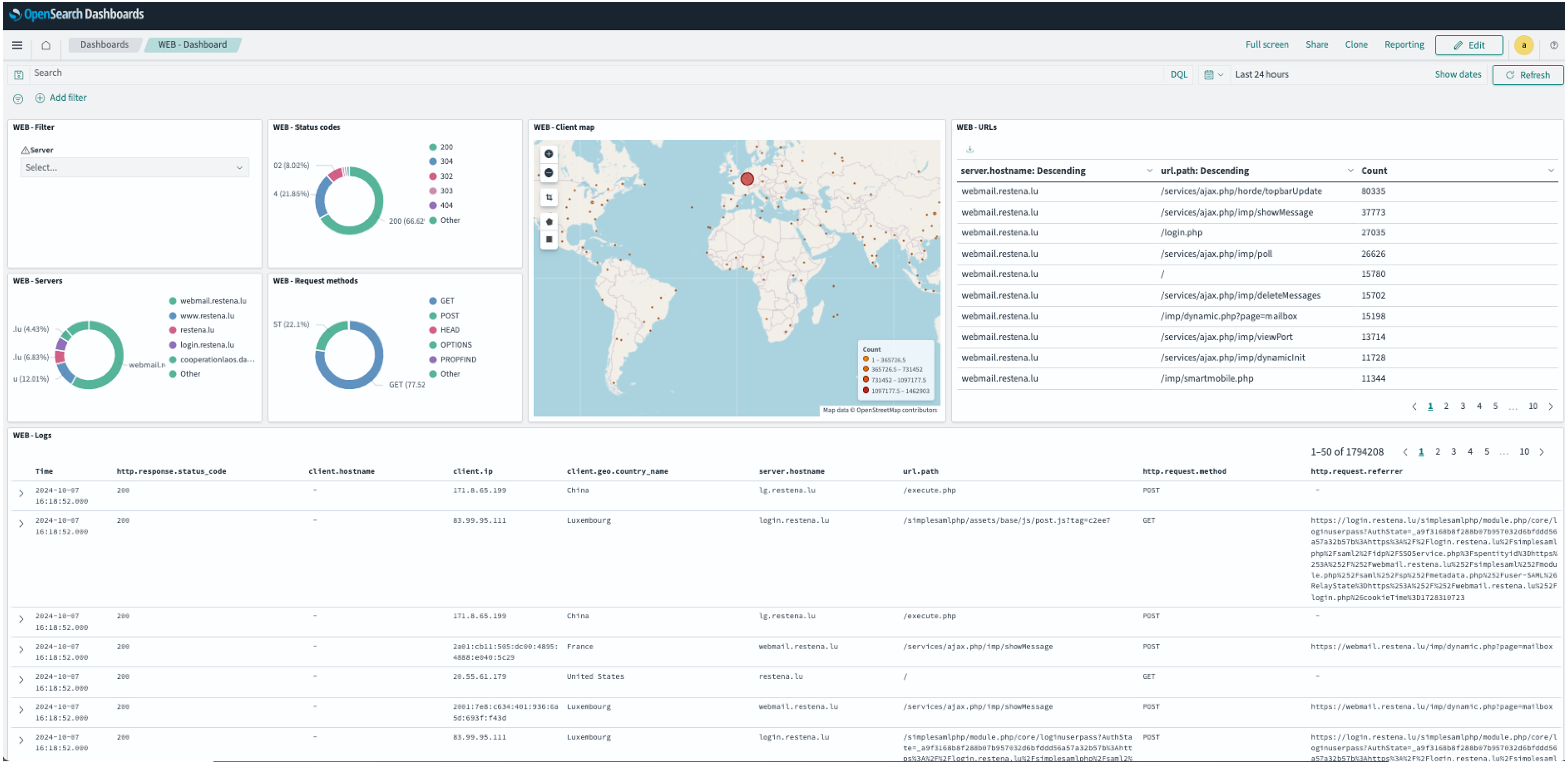
Current LuCySe4RE state of architecture



Storage & Visualization

Why OpenSearch?

- Cost of acquisition and maintenance
- No external cloud usage
- 100% control of the data
- Opensource!!



server.hostname: Descending	url.path: Descending	Count
webmail.restena.lu	/services/ajax.php/horde/topbarUpdate	80335
webmail.restena.lu	/services/ajax.php/imp/showMessage	37773
webmail.restena.lu	/login.php	27035
webmail.restena.lu	/services/ajax.php/imp/poll	26626
webmail.restena.lu	/	15780
webmail.restena.lu	/services/ajax.php/imp/deleteMessages	15702
webmail.restena.lu	/imp/dynamic.php?page=mailbox	15198
webmail.restena.lu	/services/ajax.php/imp/viewPort	13714
webmail.restena.lu	/services/ajax.php/imp/dynamicInit	11728
webmail.restena.lu	/imp/smartmobile.php	11344

‹ 1 2 3 4 5 … 10 ›

WEB - Logs

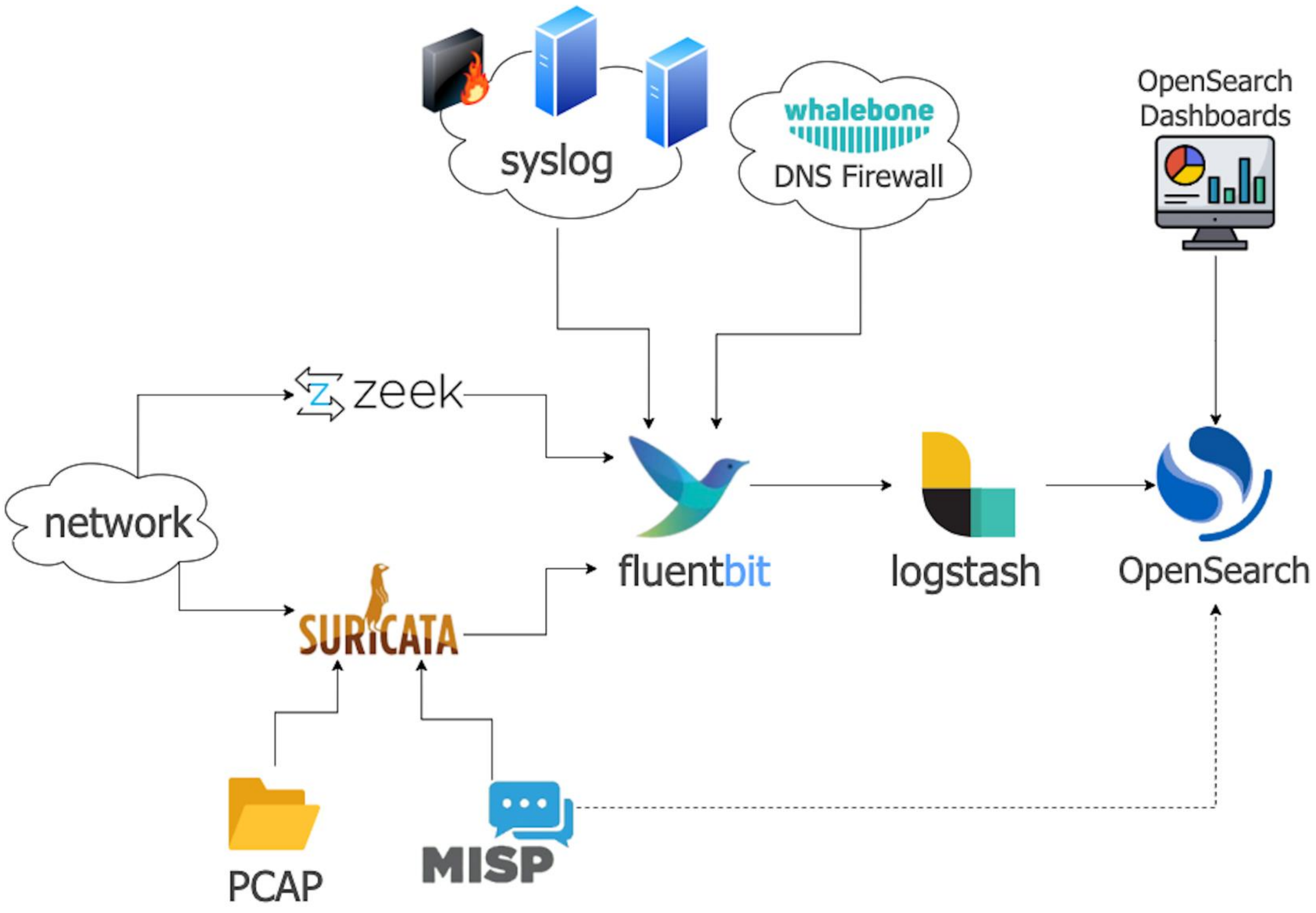
1–50 of 1794208 ‹ 1 2 3 4 5 … 10 ›

Time	http.response.status_code	client.hostname	client.ip	client.geo.country_name	server.hostname	url.path	http.request.method	http.request.referrer
2024-10-07 16:18:52.000	200	-	171.8.65.199	China	lg.restena.lu	/execute.php	POST	-
2024-10-07 16:18:52.000	200	-	83.99.95.111	Luxembourg	login.restena.lu	/simplesamlphp/assets/base/js/post.js?tag=c2ee7	GET	https://login.restena.lu/simplesamlphp/module.php/core/loginuserpass?AuthState=_a9f3168b8f288b07b957032d6bfddd56a57a32b57b%3Ahttps%3A%2F%2Flogin.restena.lu%2Fsimplesamlphp%2Fsaml2%2Fidp%2FSSOService.php%3Fspentityid%3Dhttps%253A%252F%252Fwebmail.restena.lu%252Fsimplesaml%252Fmodule.php%252Fsaml%252Fsp%252Fmetadata.php%252Fuser-SAML%26RelayState%3Dhttps%253A%252F%252Fwebmail.restena.lu%252Flogin.php%26cookieTime%3D1728310723
2024-10-07 16:18:52.000	200	-	171.8.65.199	China	lg.restena.lu	/execute.php	POST	-
2024-10-07 16:18:52.000	200	-	2a01:cb11:505:dc00:4895:4888:e040:5c29	France	webmail.restena.lu	/services/ajax.php/imp/showMessage	POST	https://webmail.restena.lu/imp/dynamic.php?page=mailbox
2024-10-07 16:18:52.000	200	-	20.55.61.179	United States	restena.lu	/	GET	-
2024-10-07 16:18:52.000	200	-	2001:7e8:c634:401:936:6a5d:693f:f43d	Luxembourg	webmail.restena.lu	/services/ajax.php/imp/showMessage	POST	https://webmail.restena.lu/imp/dynamic.php?page=mailbox
2024-10-07 16:18:52.000	200	-	83.99.95.111	Luxembourg	login.restena.lu	/simplesamlphp/module.php/core/loginuserpass?AuthState=_a9f3168b8f288b07b957032d6bfddd56a57a32b57b%3Ahttps%3A%2F%2Flogin.restena.lu%2Fsimplesamlphp%2Fsaml2%	POST	https://login.restena.lu/simplesamlphp/module.php/core/loginuserpass?AuthState=_a9f3168b8f288b07b957032d6bfddd56a57a32b57b%3Ahttps%3A%2F%2Flogin.restena.lu%2Fsimplesaml

LuCy data pipeline

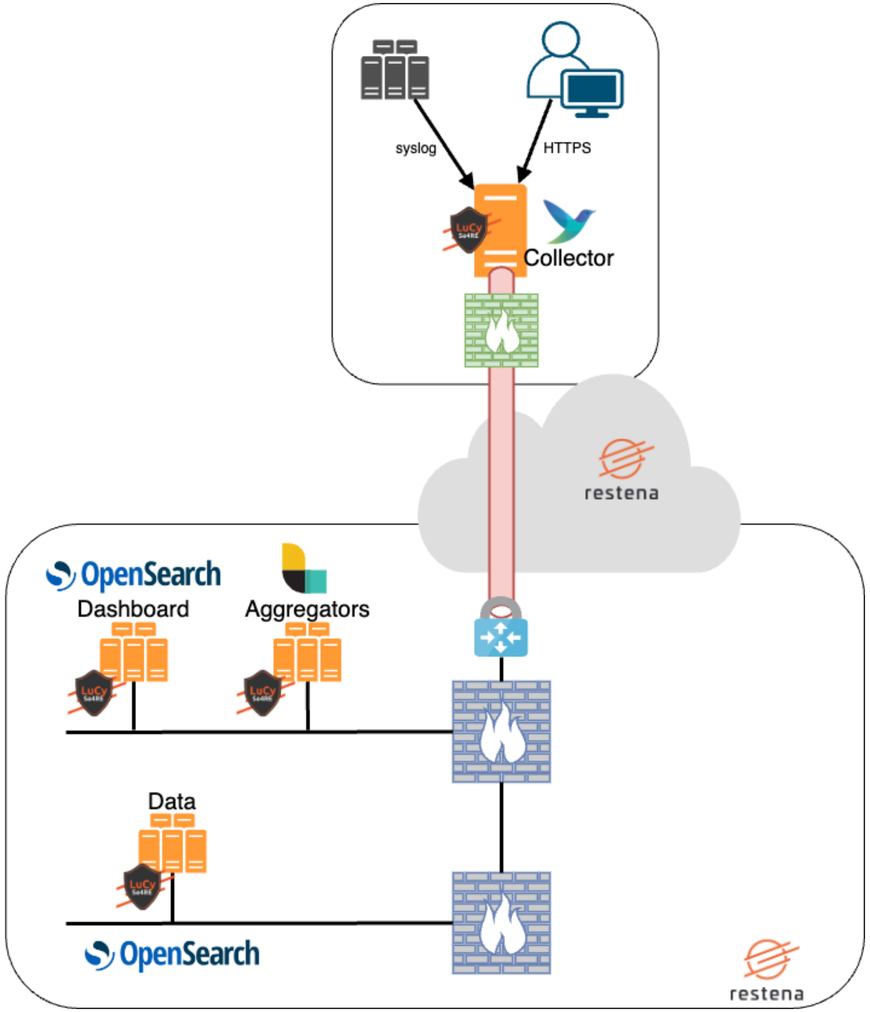
- Suricata offline and online
- Syslog from institutions

  → collection fluentbit
- Custom Opensearch Dashboards available to institutions
- Cooperation with DNS4EU for DNSFirewall



LuCy pipeline with institutions

- VM template provided by Restena
- VPN tunnel to send logs & dashboard view
- Permissions handled on OpenSearch
- Retention period depends on institution



Awareness and education

- Awareness-raising and prevention material
  - Best practices and posters

- Training courses
  - A collaboration with the Luxembourg Digital Learning Hub
- A wide variety of topics as for example:
  - Incident management, Ansible, DNS Security, IPv6 (no comment pls)

- Conferences
  - Cyberday.lu (save the date: 09 October 2025)
  - Dataprivacyday.lu (save the date: 28 January 2026)

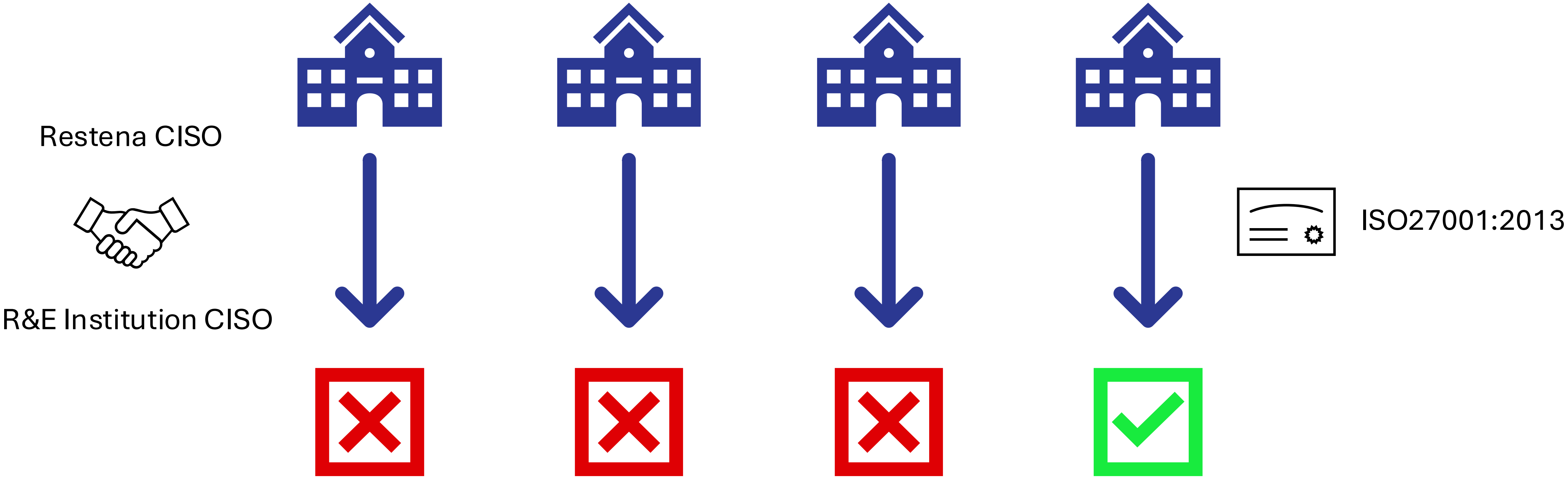
Assessing the R&E security maturity level

- Have a KPI for the impact of LuCySe4RE on overall security within R&E community

- Provide maturity level of R&E institution
  - Where are the flaws
  - Good argument for motivating management to invest in security

- Pre & Post implementation assessment
  - The security assessment for the PRE-implementation phase has been realised

Assessing the R&E security maturity level



Restena CISO

R&E Institution CISO

ISO27001:2013

Assessing the R&E security maturity level

- Digging deeper into the security maturity assessment results
  - The requirements identified during the proposal are confirmed here
  - Some weak points taken from the security maturity assessment to highlight here are:
    - Training and awareness
    - Incident Management
    - Vulnerability management
    - Internal security best practices
  - A lot of effort has already been put in
    - Risk Management
    - Regulatory and privacy
    - Business continuity planning

Closing words

☑ LuCySe4RE is ongoing work

LuCySe4RE is an open-source platform with an elaborated R&E focussed education framework

In-house RESTENA integration

Paves the way to comply with new European directives:

Critical Entities’Resilience (CER)

Network And information System Security 2 Act (NIS 2)

Thank you and see you next time LuCy!

Securing.What.Matters

<Prague.CZ><8-10 April 2025>

Cynthia Wagner & Denim Latić

Co-funded by the European Union