

thnc25

Brighton, UK | 9-13 JUNE 2025

BRIGHTER TOGETHER

LuCySe4RE

A security education framework for R&E in Luxembourg

Cynthia Wagner & Denim Latić

Brighton, UK, Founders Room

12/06/2025

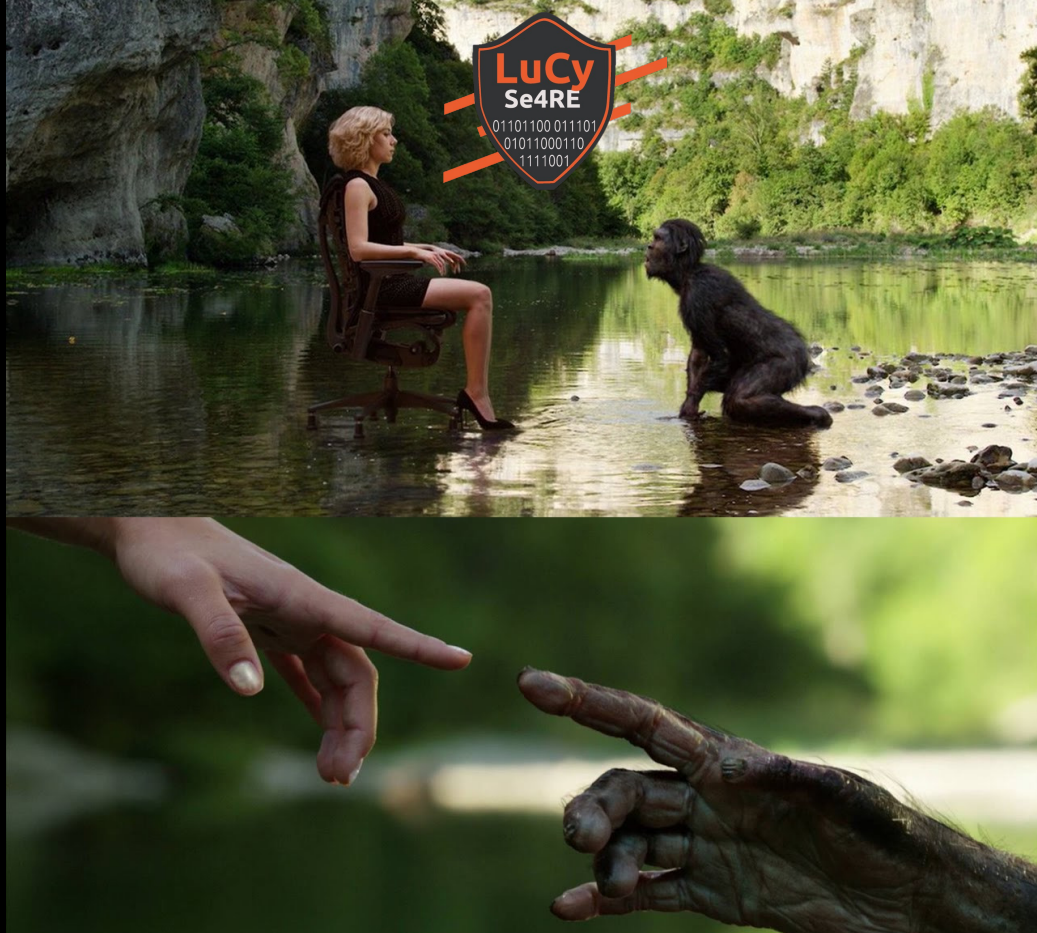


Co-funded by
the European Union



Let's talk about LuCy!

Lucy – 2014 by Luc Besson / EuropaCorp-Universal Pics.



Why LuCySe4RE?



- Luxembourg Cybersecurity Services 4 Research & Education or LuCy in short
- 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

The long way to LuCySe4RE



The long way to LuCySe4RE

Quantity

Retention

Alerting

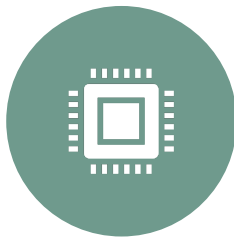
Type of
logs

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 LU R&E sector



teach and raise awareness of current cybersecurity threats, countermeasures, and relevant tools



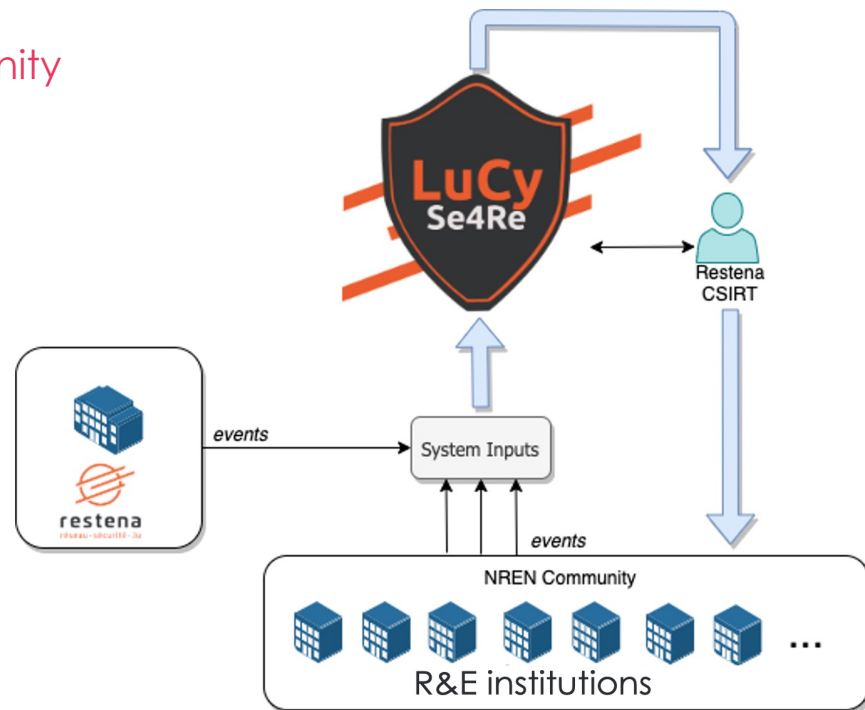
low-cost project for NRENS and provide a service for R&E community without additional costs

LuCySe4RE is protecting what matters

The technical perspective

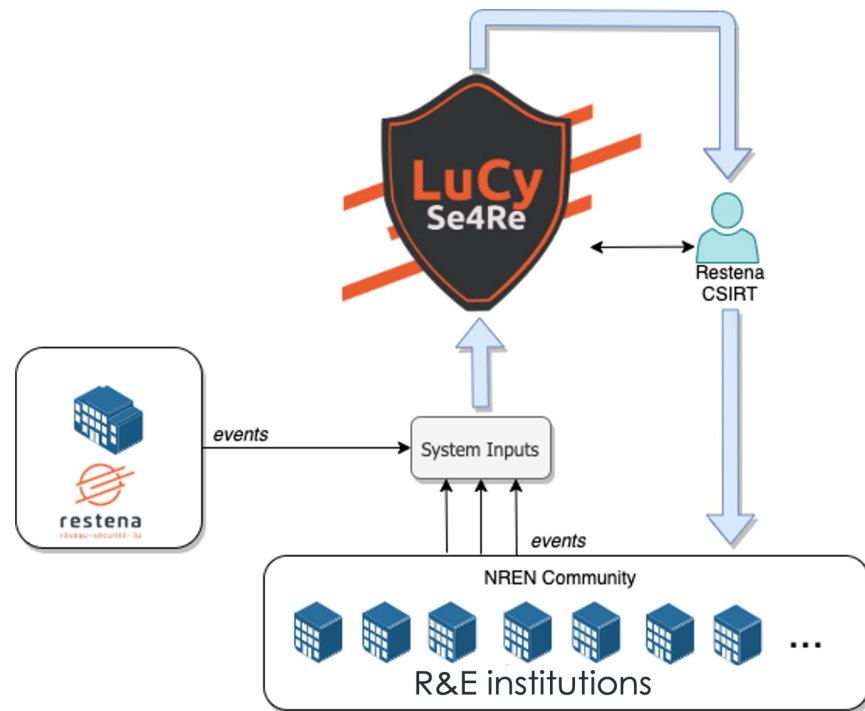
Let's set the perimeter ...

- 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

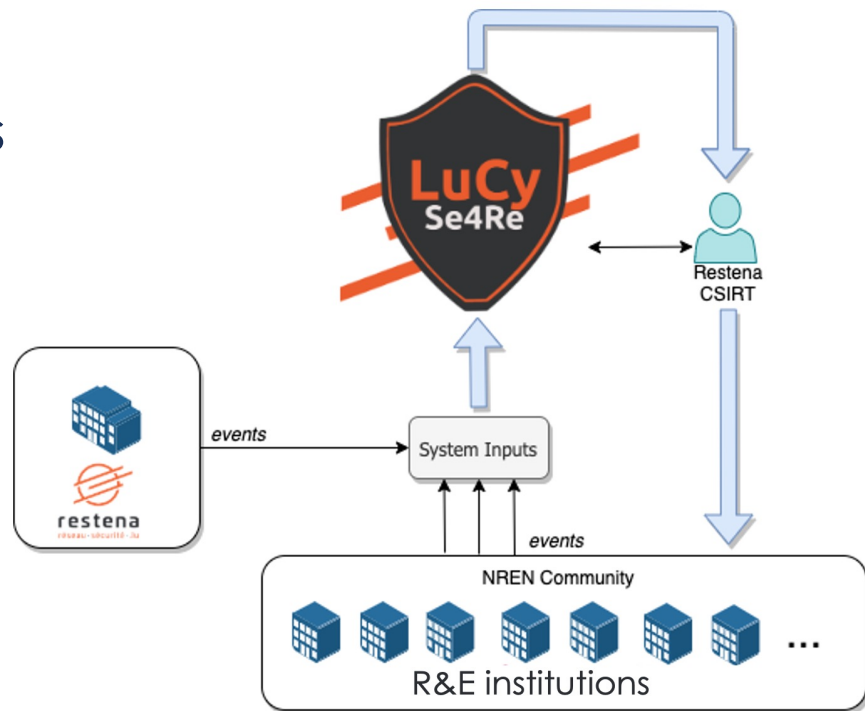
- Toolset adapted to R&E needs
- Better detection of sector specific threats
- Better preparedness due to community knowledge
- Compliance with new European directives
- Low costs for R&E institutions





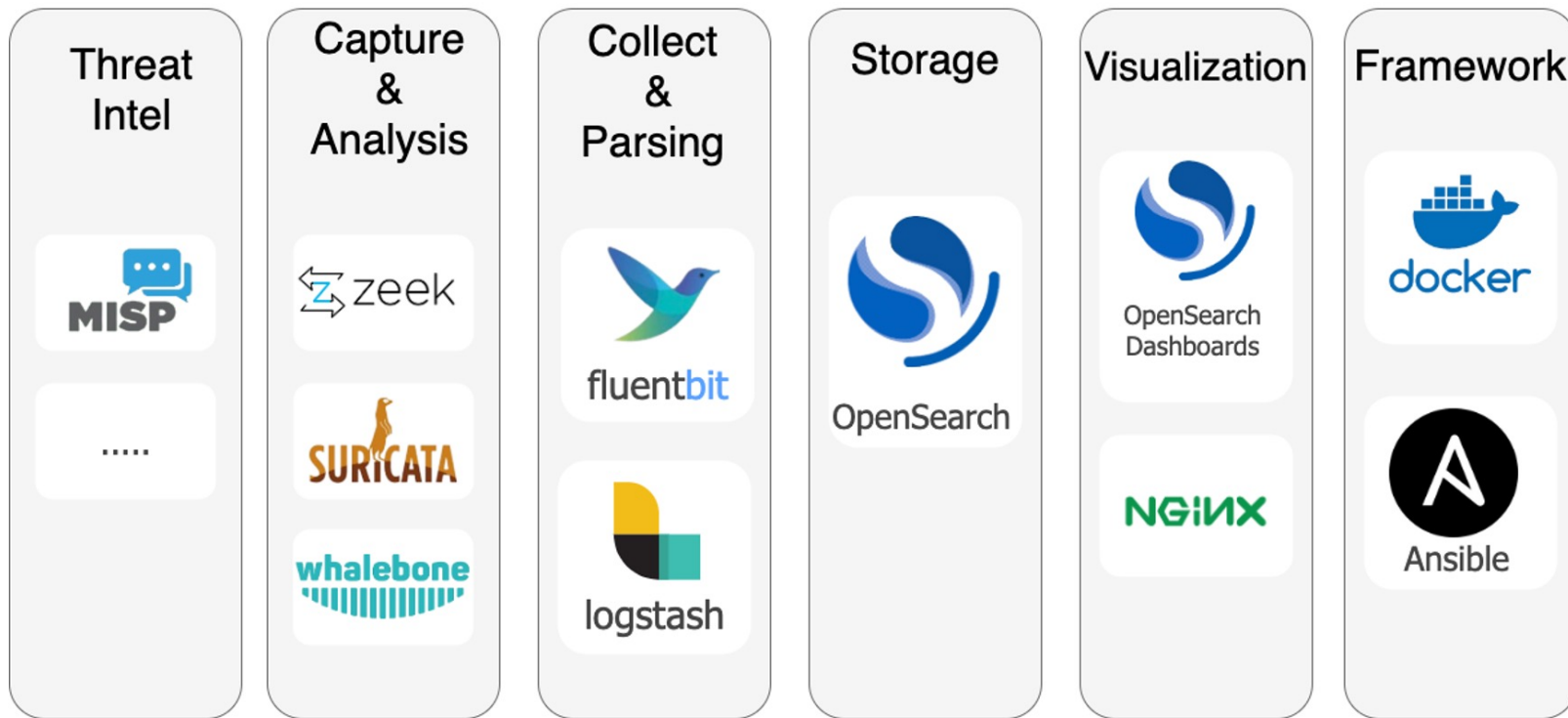
So what is LuCy?

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



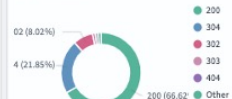


Current LuCySe4RE state of architecture



▲ Server

Select...



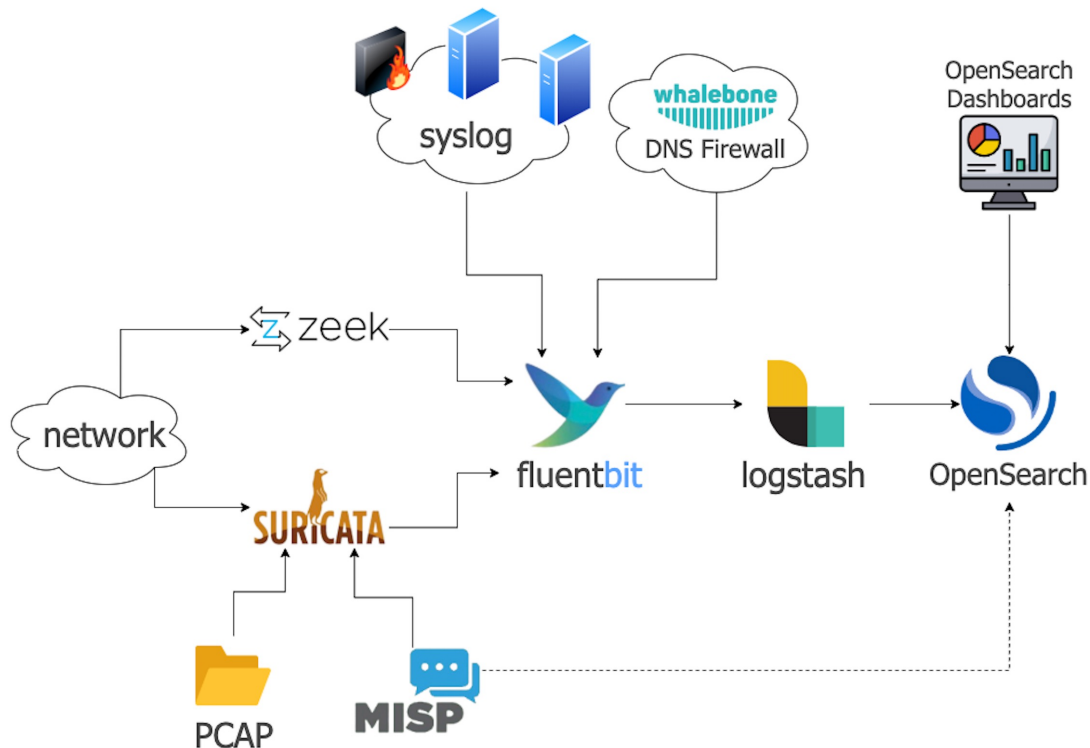
server.hostname: Descending	url.path: Descending	Count
webmail.restena.lu	/services/ajax.php/horde/topbarUpdate	80335
webmail.restena.lu	/services/ajax.php/imp/showMessage	37773
webmail.restena.lu	/login.php	27035
webmail.restena.lu	/services/ajax.php/imp/poll	26626
webmail.restena.lu	/	15780
webmail.restena.lu	/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

Time	http.response.status_code	client.hostname	client.ip	client.geo.country_name	server.hostname	url.path	http.request.method	1-50 of 1794208	< 1 2 3 4 5 ... 10 >
> 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	/s/mpleanlphp/assets/base/js/post.js?tag=c2ee7	GET	https://login.restena.lu/s/mpleanlphp/module.php/core/loginuserpass?AuthState=...a57a32b5763a4https3Aa2f2c2fLogin.restena.lu/s2f6tmpleanlphp62f5am1u2f2fdp2f2f350service.php3f5pentiyl030https253Aa252f262f2fwebma11.restena.lu/s252f5tmpleanlbu252fmodu1e.php252f5am1u252f2f62f2fmetadeta.php252fuser=5a4m1u2eRelayState30dhttps3Aa252f52f2fwebma11.restena.lu/s252fLogin.php26cookieTime1302f28310723	
> 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	-	2001:cb11:505:dc00:4895:4880:e949:5c29	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	-	2001:708:c634:401:936:16a:561e93f7430	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	/s/mpleanlphp/module.php/core/loginuserpass?AuthState=...a9f3160b6f280b76957a326b760d056a57a326b763a4https3Aa2f2c2fLogin.restena.lu/s252f6tmpleanlbu252fmodu1e.php252f5am1u252f2f62f2fmetadeta.php252fuser=5a4m1u2eRelayState30dhttps3Aa252f52f2fwebma11.restena.lu/s252fLogin.php26cookieTime1302f28310723	POST	https://login.restena.lu/s/mpleanlphp/module.php/core/loginuserpass?AuthState=...a9f3160b6f280b76957a326b760d056a57a326b763a4https3Aa2f2c2fLogin.restena.lu/s252f6tmpleanlbu252fmodu1e.php252f5am1u252f2f62f2fmetadeta.php252fuser=5a4m1u2eRelayState30dhttps3Aa252f52f2fwebma11.restena.lu/s252fLogin.php26cookieTime1302f28310723	




LuCy data pipeline

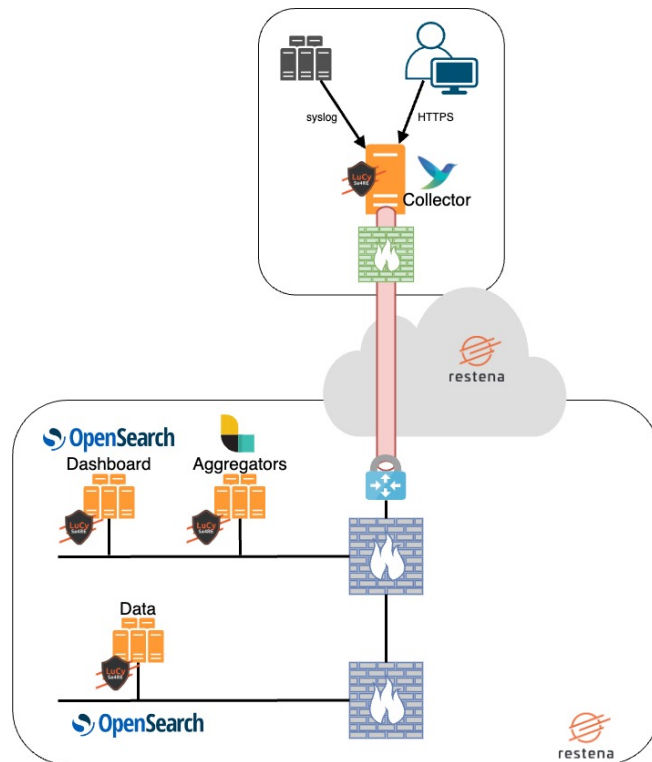
- Suricata offline and online
- Syslog from institutions
→ collection fluentbit
- Custom Opensearch Dashboards available to institutions
- Cooperation with DNS4EU for DNSFirewall






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



From LuCy to incident management



SOC initial
analysis

4 eyes
review

Action by
CSIRT

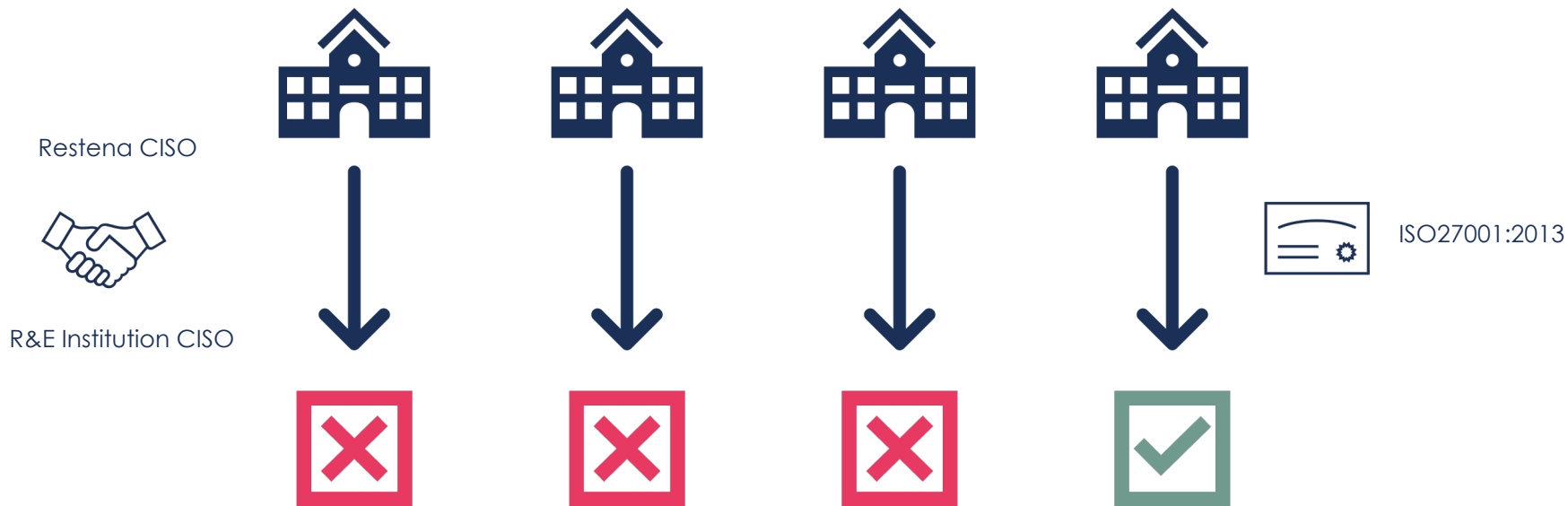
LuCySe4RE is protecting what matters

The governance perspective

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



✓ 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 are:

Training &
awareness

Incident
Management

Vulnerability
Management

Security
Best Practices

- A lot of effort has already been put in

Risk Management

Regulatory and
Privacy

Business
Continuity
Planning

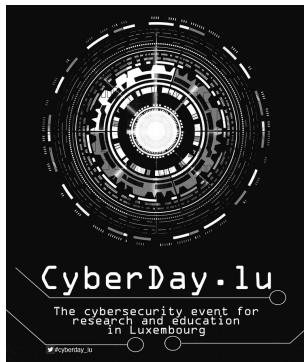
LuCySe4RE is protecting what matters

The human perspective



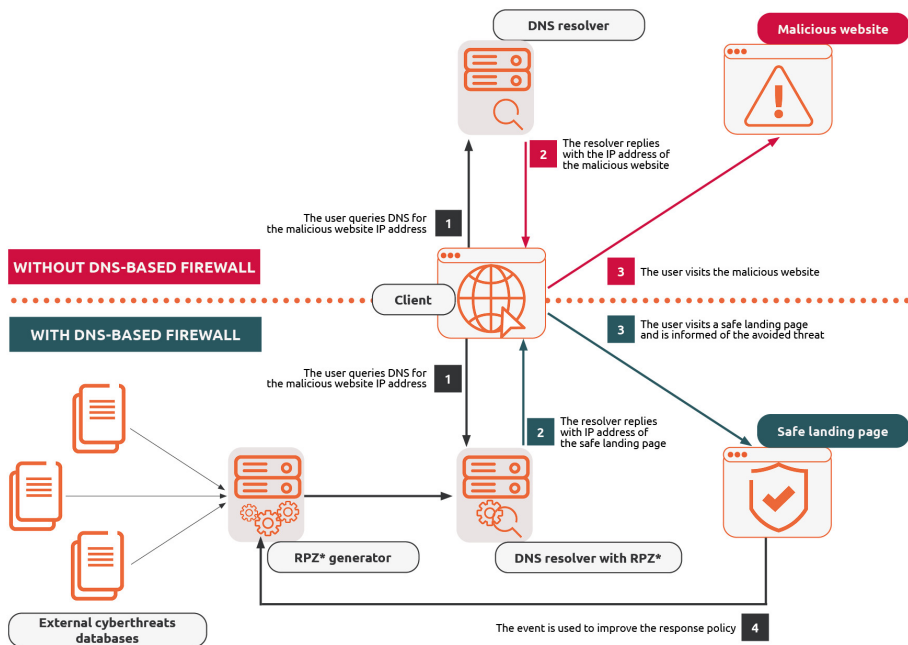
Awareness and education

- 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 (09 October 2025)
- BENELUX Security and Privacy Meeting (20-21 October 2025)
 - Dataprivacyday.lu (save the date: 28 January 2026)



Protecting the most vulnerable

DNS FIREWALL Schematic diagram



• DNS Firewall solution

- Aimed to protect users from accessing malicious websites

→ Increase of overall IT security

→ Released as a new service for R&E

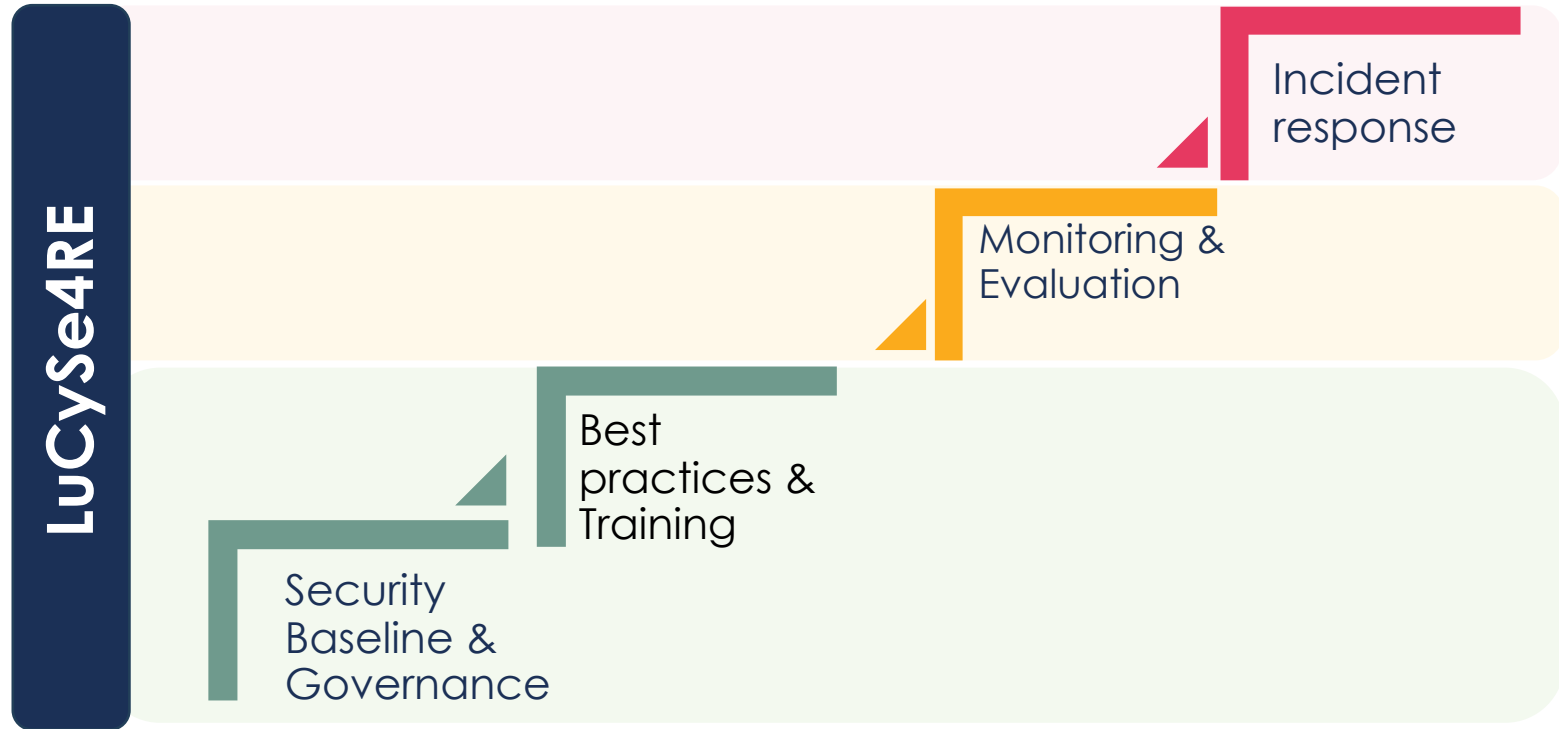
- Adding the feature of content filtering for high-schools

→ Since June 3rd protection in place

LuCySe4RE is protecting what matters

The wrap-up

Wrapping up – Prepare for the worst? We're on the way!





Closing words



LuCySe4RE is still developing and ongoing work



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



In-house RESTENA integration – no cloud solution
Supplier Independance



Paves the way to comply with new
European directives:

Critical Entities' Resilience (CER)
Network and information System Security 2 (NIS 2)

Thank you

Any questions?

admin@restena.lu



Co-funded by
the European Union

