Co-funded by
the European Union

LuCy
Se4RE
01101100 011101
01011000110
1111001



Hello LuCy nice to meet you!

A conclusion on a 3 year Open-Source cybersecurity project

Cynthia Wagner & Denim Latić

restena

Who is LuCy & who is Restena?

- **National Research & Education Network**
  - Small institution serving a large community (>150 institutions, >80k users)
- **Community**
  - From primary school up to the universities and public research centres and more
- **LuCySe4RE**
  - **Project to improve overall cybersecurity**
- **TLDR: Open-Source SIEM**

Why LuCy?



- R&E in Luxembourg → small institutions
- Lack of skills & budget
- New EU directives (NIS2 and many more)



LuCySe4RE: Step 1!



Restart: let's have baby steps, LuCy!

Quantity

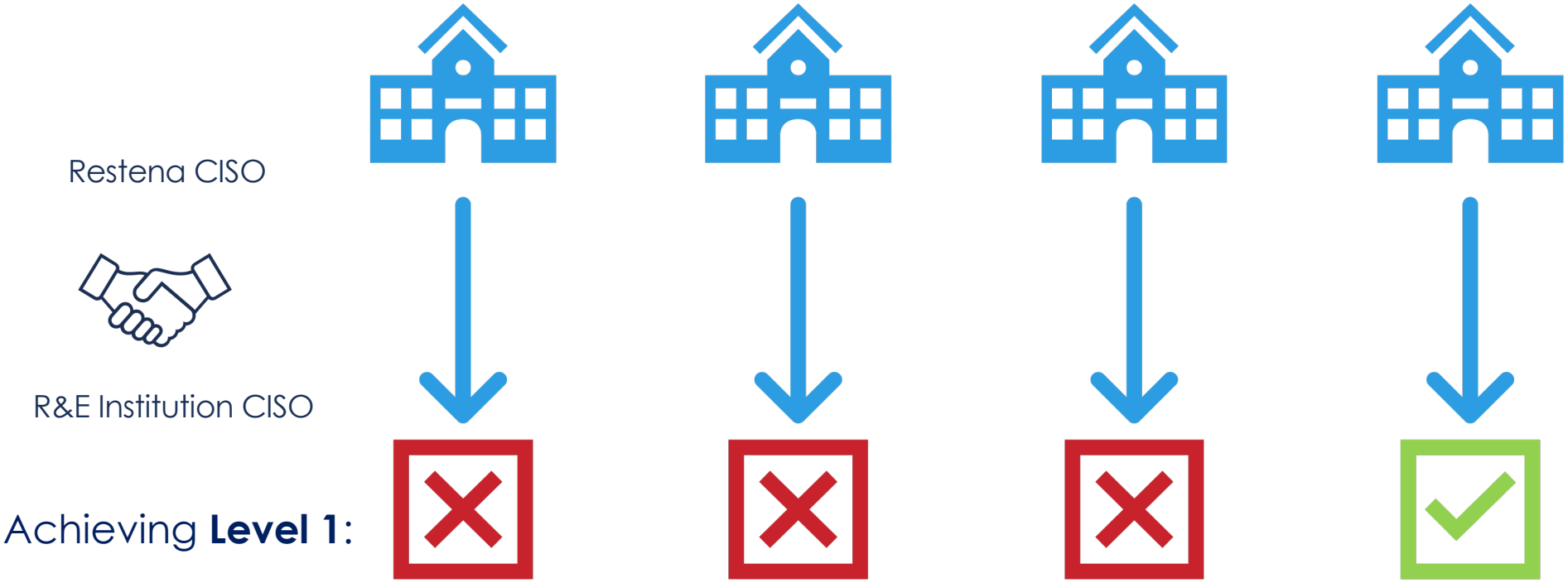
Retention

Alerting

Type of logs

24/7?

Assessing the R&E security maturity level





ISO27001:2022

Level	Description for GEANT* Security Baseline scheme
Baseline Level 1	Scope: minimum requirements for each organisation
Advanced Level 2	Scope: medium to large organisations or organisations that offer important services or providing access to research collaborations.
Expert Level 3	Scope: organisations processing sensitive and critical information or providing essential services and infrastructure

* https://security.geant.org/baseline/

Assessing the R&E security maturity level

- The requirements identified during the proposal are confirmed here
- A lot of effort has already been put in

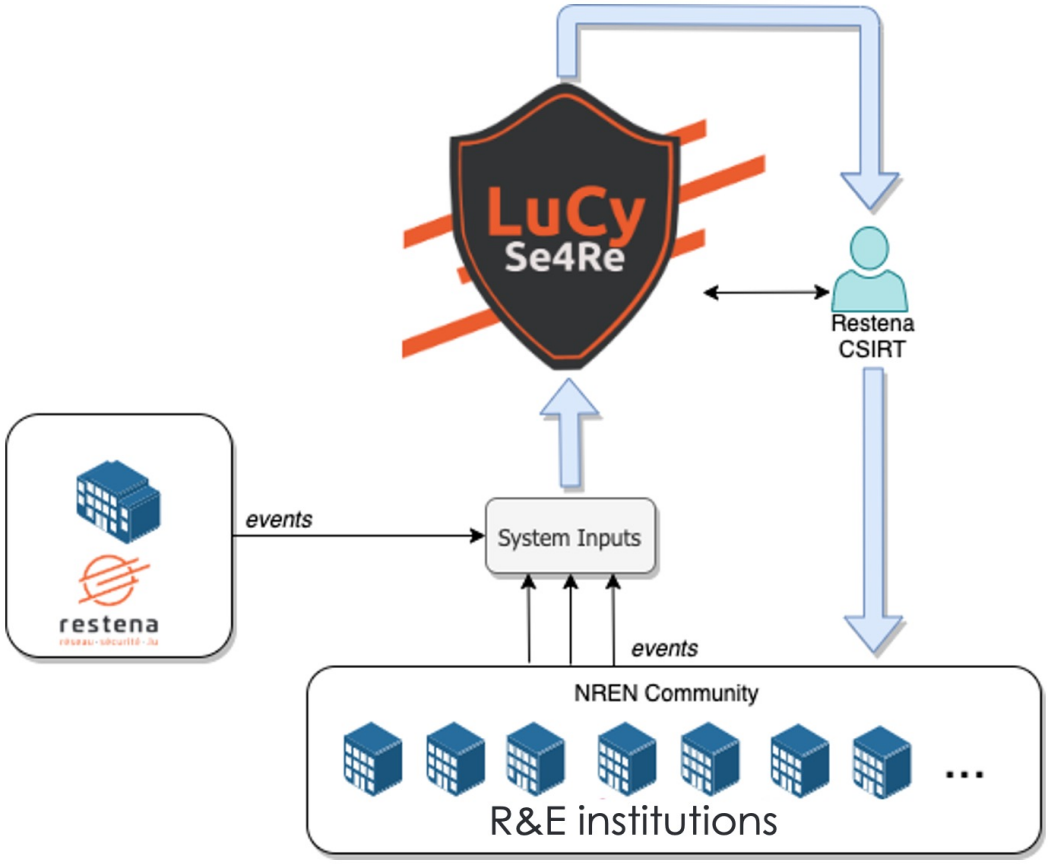
Risk Management | Regulatory and Privacy | Business Continuity Planning

- Some weak points taken from the security maturity assessment to highlight are:

Training & awareness | Incident Management | Vulnerability Management | Security Best Practices

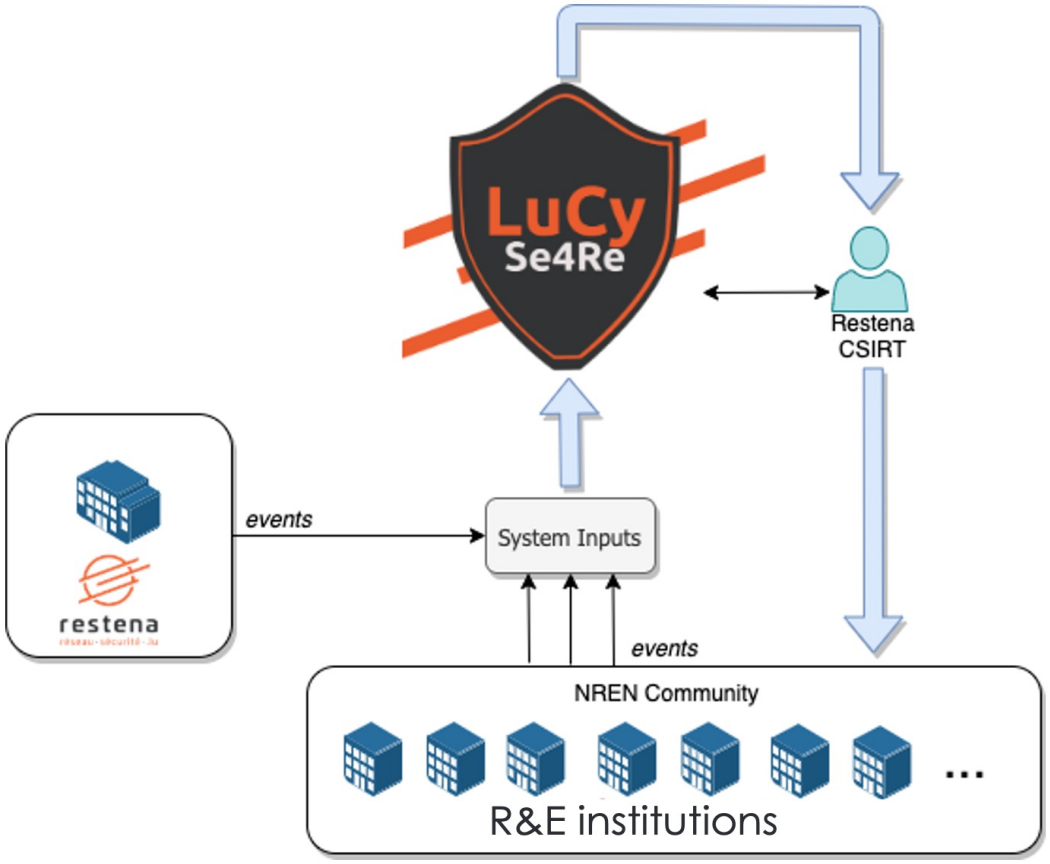
- So we're on track! Let's go!

What is LuCy?



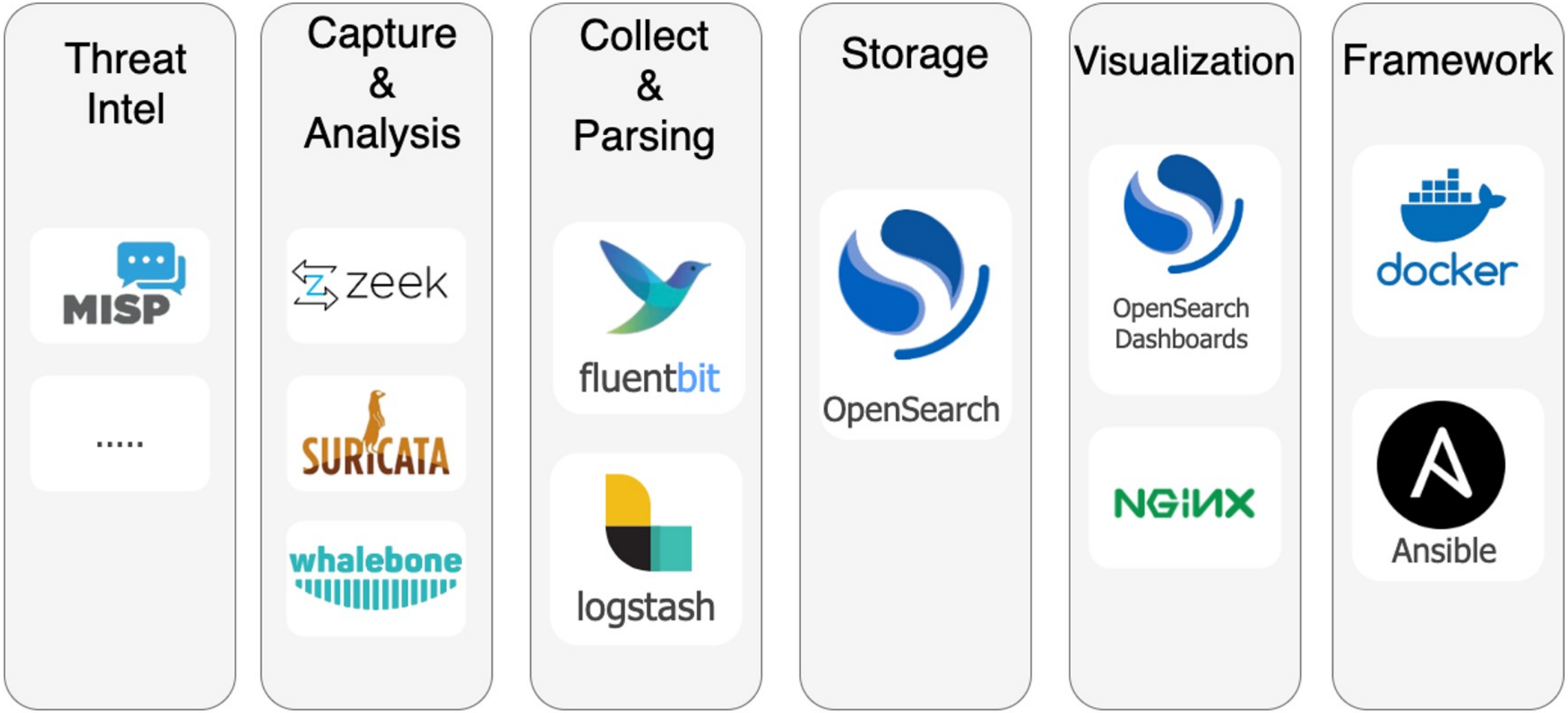
- Open Source technologies*
- New & reused hardware
- On-premises
- Centralised security solution for R&E

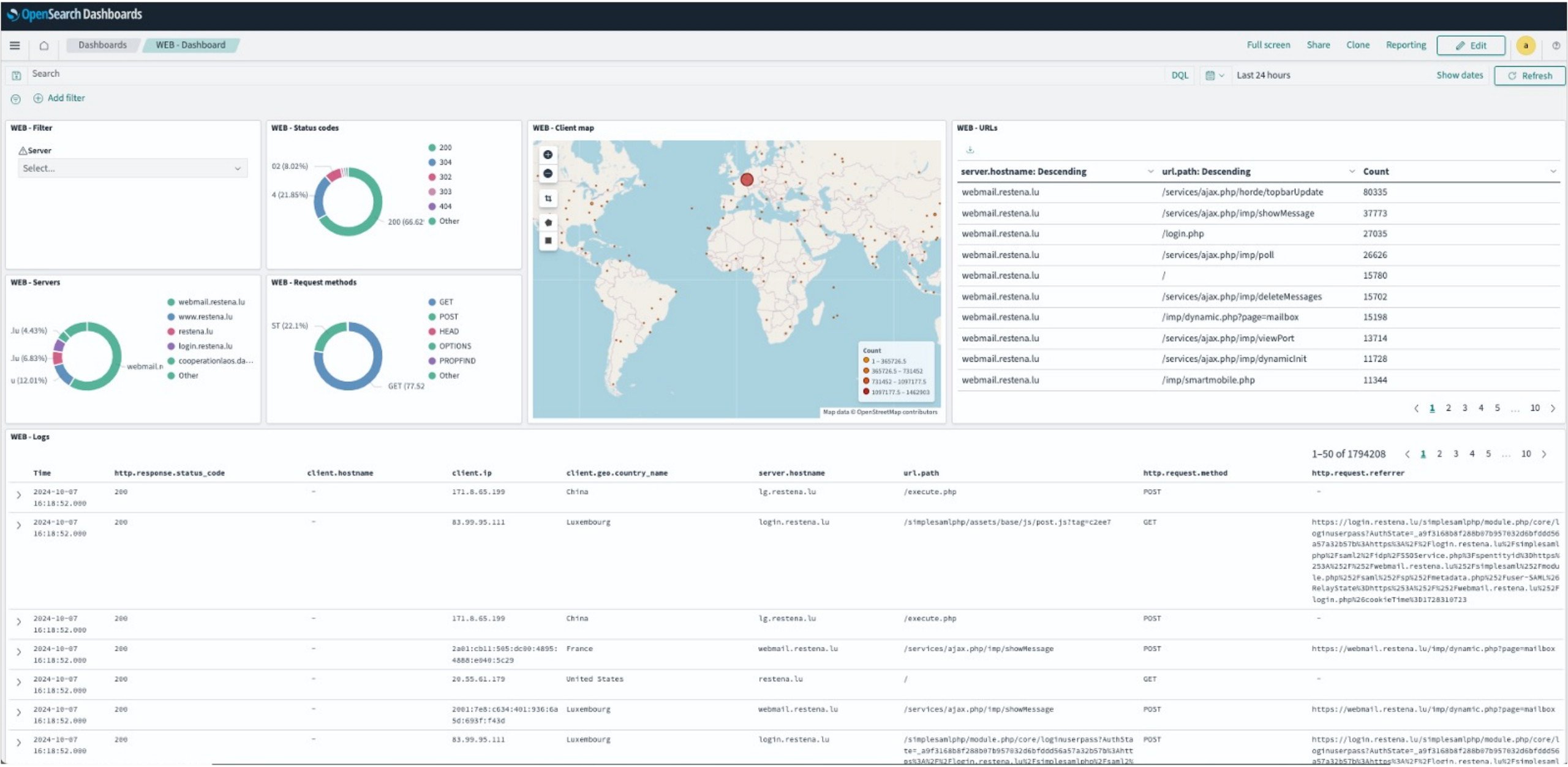
How does LuCy help?



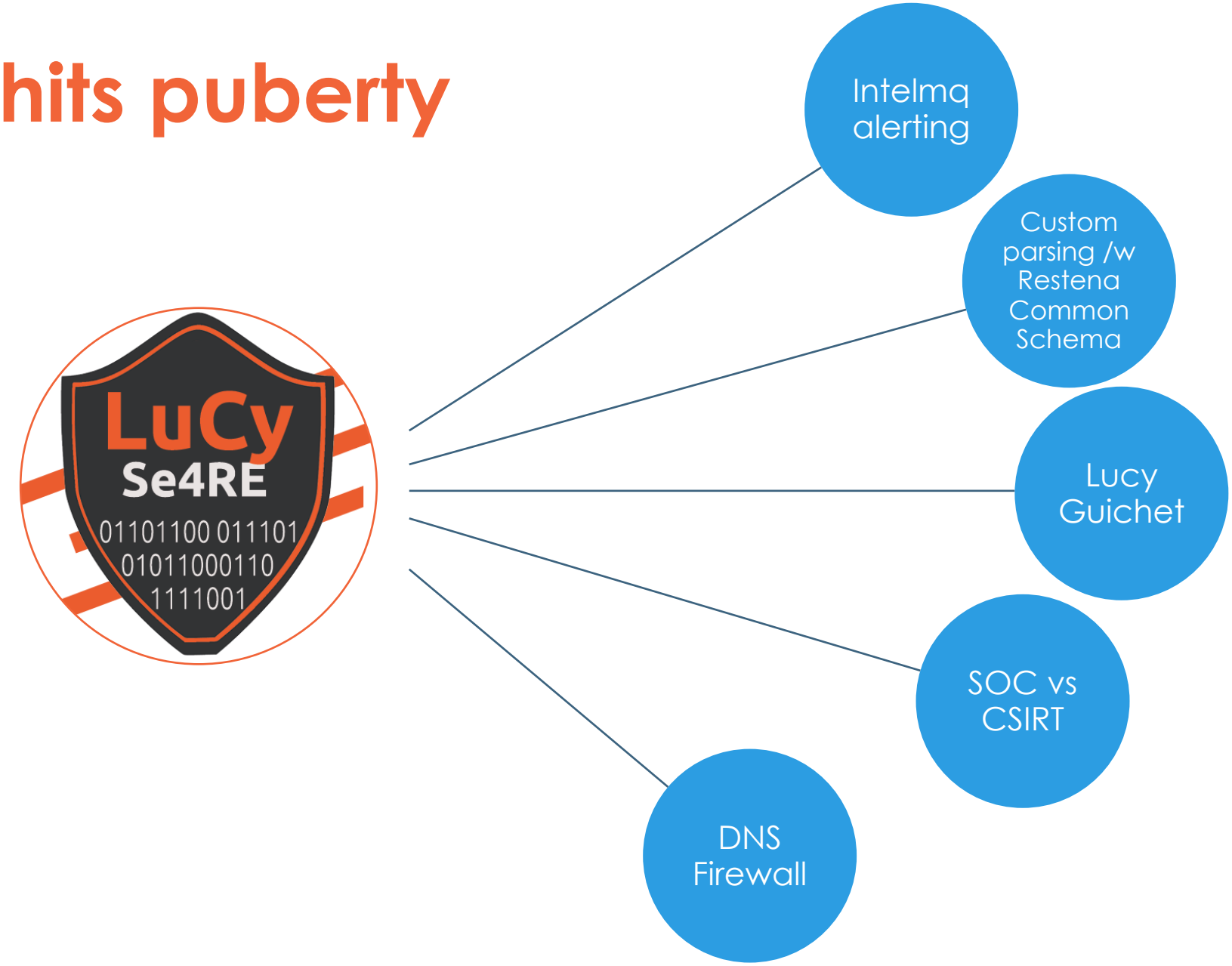
- Low costs for R&E institutions
- Detection of sector specific threats
- Adapted to R&E needs
- Compliant with new EU directives

The inner workings of LuCy




OpenSearch Dashboards
Dashboards
WEB - Dashboard
Full screen
Share
Clone
Reporting
Edit
Search
DQL
Last 24 hours
Show dates
Refresh
Add filter
WEB - Filter
Server
Select...
WEB - Status codes
02 (8.02%)
4 (21.85%)
200 (66.62
200
304
302
303
404
Other
WEB - Client map
Count
1 – 365726.5
365726.5 – 731452
731452 – 1097177.5
1097177.5 – 1462903
Map data © OpenStreetMap contributors
WEB - URLs
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 - Servers
.lu (4.43%)
.lu (6.83%)
u (12.01%)
webmail.n
webmail.restena.lu
www.restena.lu
restena.lu
login.restena.lu
cooperationlaos.da...
Other
WEB - Request methods
ST (22.1%)
GET (77.52
GET
POST
HEAD
OPTIONS
PROPFIND
Other
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 hits puberty

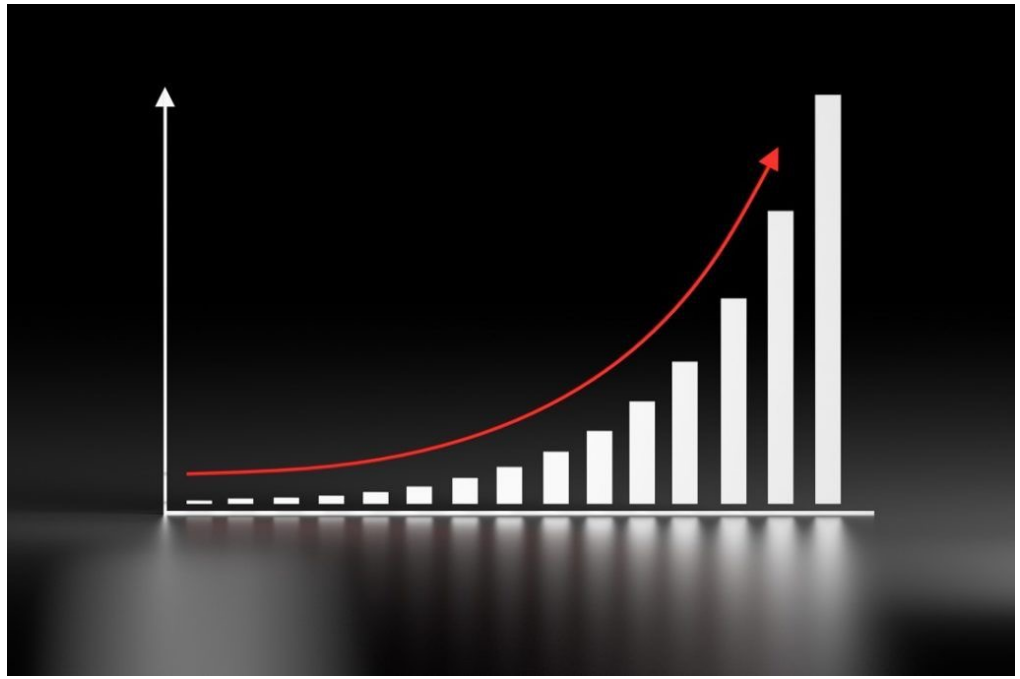


What's to come! LuCy's future

- August 2026 → End Of EU funding
- Anomaly Detection
- Case management
  - Integration of FlowIntel

flowintel

- Threat Intel / IOC
  - Evaluation of commercial feeds
  - Improve scoring mechanism



Planned outcomes and surprises

- SIEM with tooling
- Formal education activities
  - Lectures on incident mgmt
  - Digital Learning Hub lectures
- Awareness
  - Tip-sheets & Posters
  - Conferences

    Cyberday.lu & DataPrivacyDay.lu
  - Protecting the most vulnerable
  - Web-filtering for >50k students









Planned outcomes and surprises





- More formal education activities
  - Lectures on Ansible, Email forensics, DNS Security, IPv6 & security …
- TALON cyber-crisis exercise
  - From zero to game-master in a few weeks
- BENELUX Security and Privacy Meeting co-founder
- LuCy implemented on Luxembourgish cyber-range for Cyber-fortress exercise

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



Wrapping up!



We didn't just build a SIEM — we built a foundation for long-term cooperation in cybersecurity with peers – who wanted!



Open-source SIEM is a viable and effective alternative. Collaboration significantly amplifies impact. Technology alone is not enough—people and processes matter.



LuCy demonstrates that it is possible to build effective, sustainable, and collaborative cybersecurity solutions through open-source and shared effort



The success is the team that kept going despite the fallbacks!

Thank you!
Questions?

And yes, we do have our SOC now!



This is a real building set, not generated by AI !