restena
réseau · sécurité · .lu

# LuCySe4RE

**Lu**xembourg **Cy**ber **Se**curity **4**

**R**esearch & **E**ducation

**Denim Latić & Cynthia Wagner**

TNC24 – Rennes - France

13 June 2024

tnc24
RENDEZVOUS À RENNES
Rennes, France | **10-14 JUNE 2024**

Co-funded by
the European Union

GÉANT


# Luxembourg Cyber Security 4 Research & Education Project


# Why LuCySe4RE?

## Motivation

- A lot of small organisations shape our R&E community
  - No or restricted security monitoring only
    - Lack of competences, interest and budget
- New EU directives show up quickly such as NIS2, CER …

- LuCySe4RE aims at Improving overall cybersecurity maturity and awareness within R&E

- Restena wanted to extend its security portfolio (s.a. SOC)
- Respect our philosophy of using open-source


# The long way to LuCySe4RE

## Collecting the requirements of an R&E community

- Lots of meetings cleared the situation ….
  - Our first impression : Mission impossible!
  - But: strong exchange between interested parties happened!
- From a technical perspective we identified:
  - Huge quantities of Logs, events to be processed → ✓
  - Data retention and requirements → ✓
  - Many types of data sources, appliances, applications, endpoints
    → let's start small for a first
  - Alerting --> ✓ already there via CSIRT
  - 24/7 SOC? → Please NO! Why?
- Form an awareness perspective: lots of different requirements

# The LuCySe4RE framework objectives

ASSESS THE STATUS QUO OF CYBERSECURITY PREPAREDNESS AND IMPROVE IT

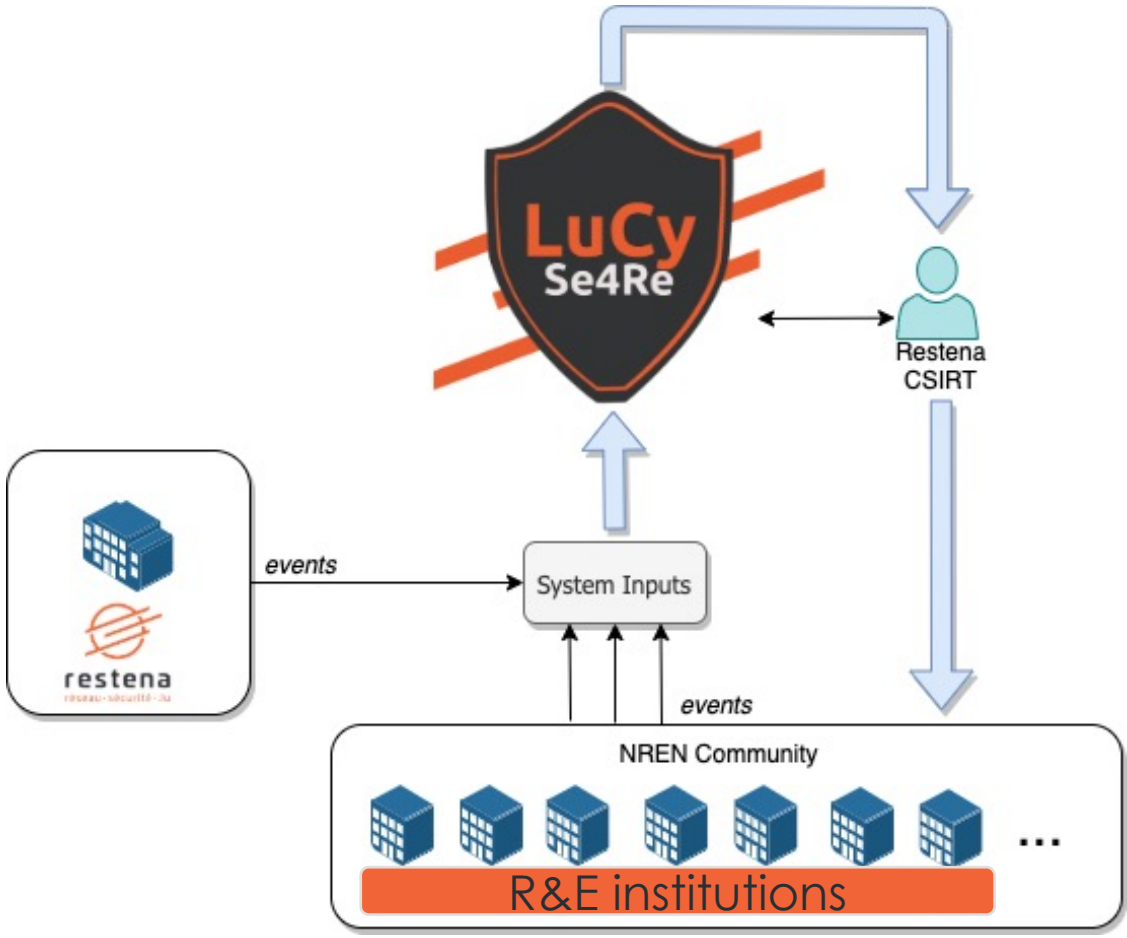
DEPLOY INNOVATIVE CYBERSECURITY SOLUTIONS AND MAKE THEM AVAILABLE AS SERVICE TO ORGANISATIONS IN THE LUXEMBOURG R&E SECTOR.

TEACH AND RAISE AWARENESS OF CURRENT CYBERSECURITY THREATS, COUNTERMEASURES, AND USAGE OF RELEVANT TOOLING

PROVIDE SERVICE AT REDUCED/LOW COSTS

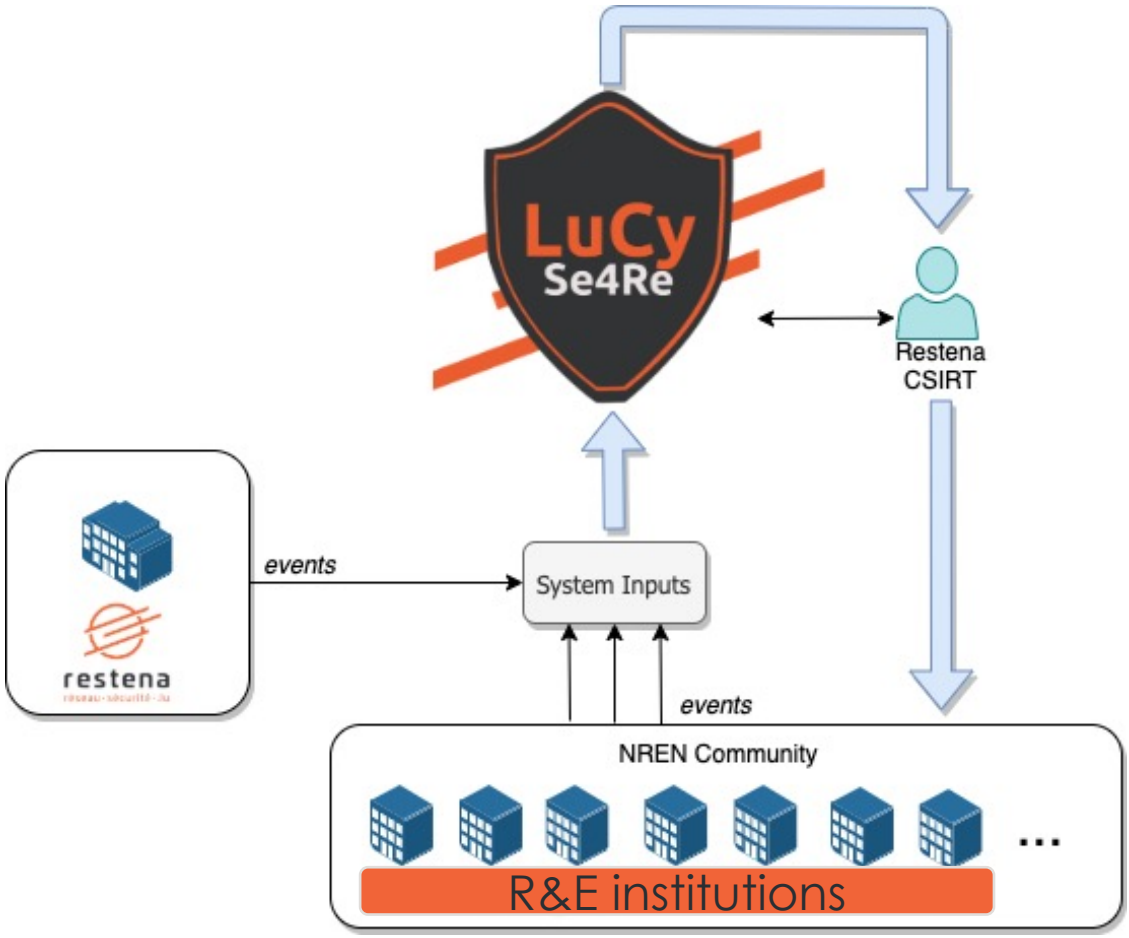
# Let's set the perimeter

- 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



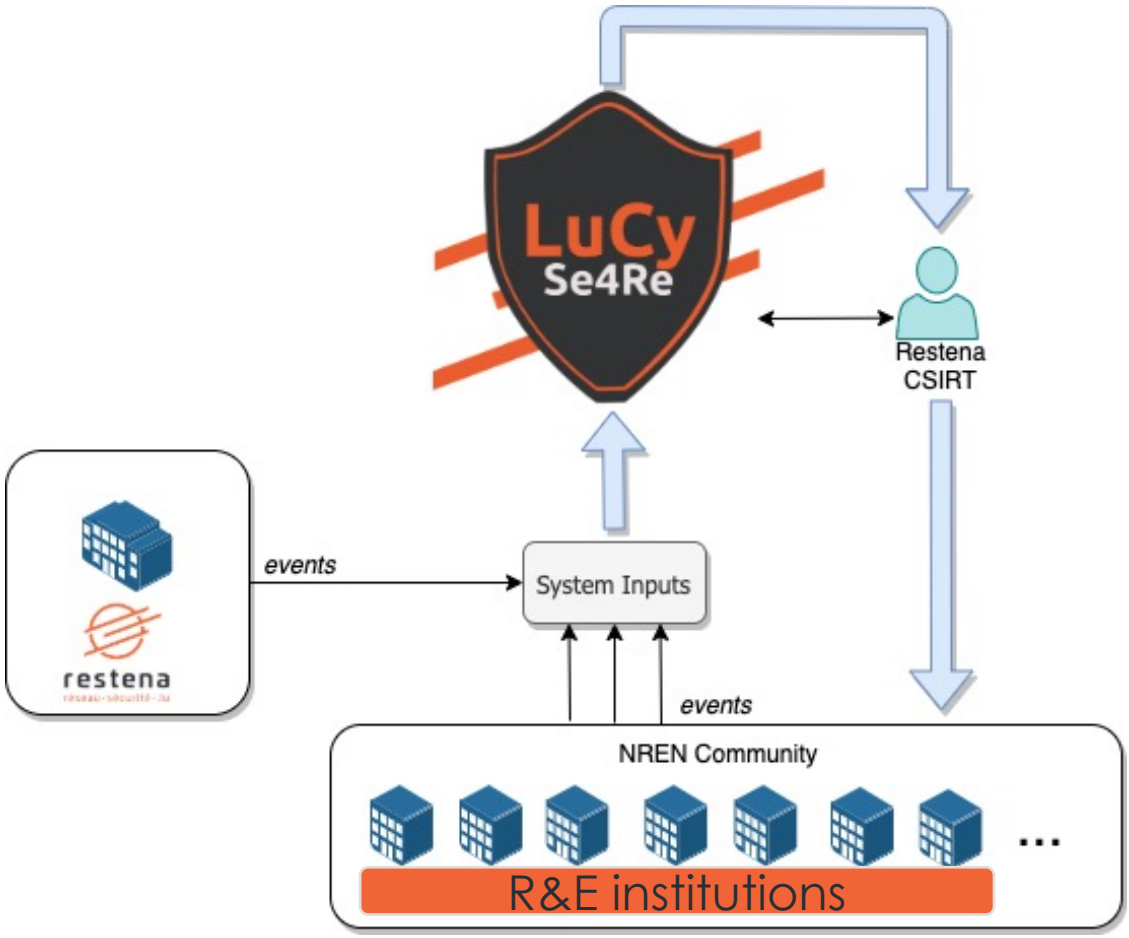
# Community benefits

- 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

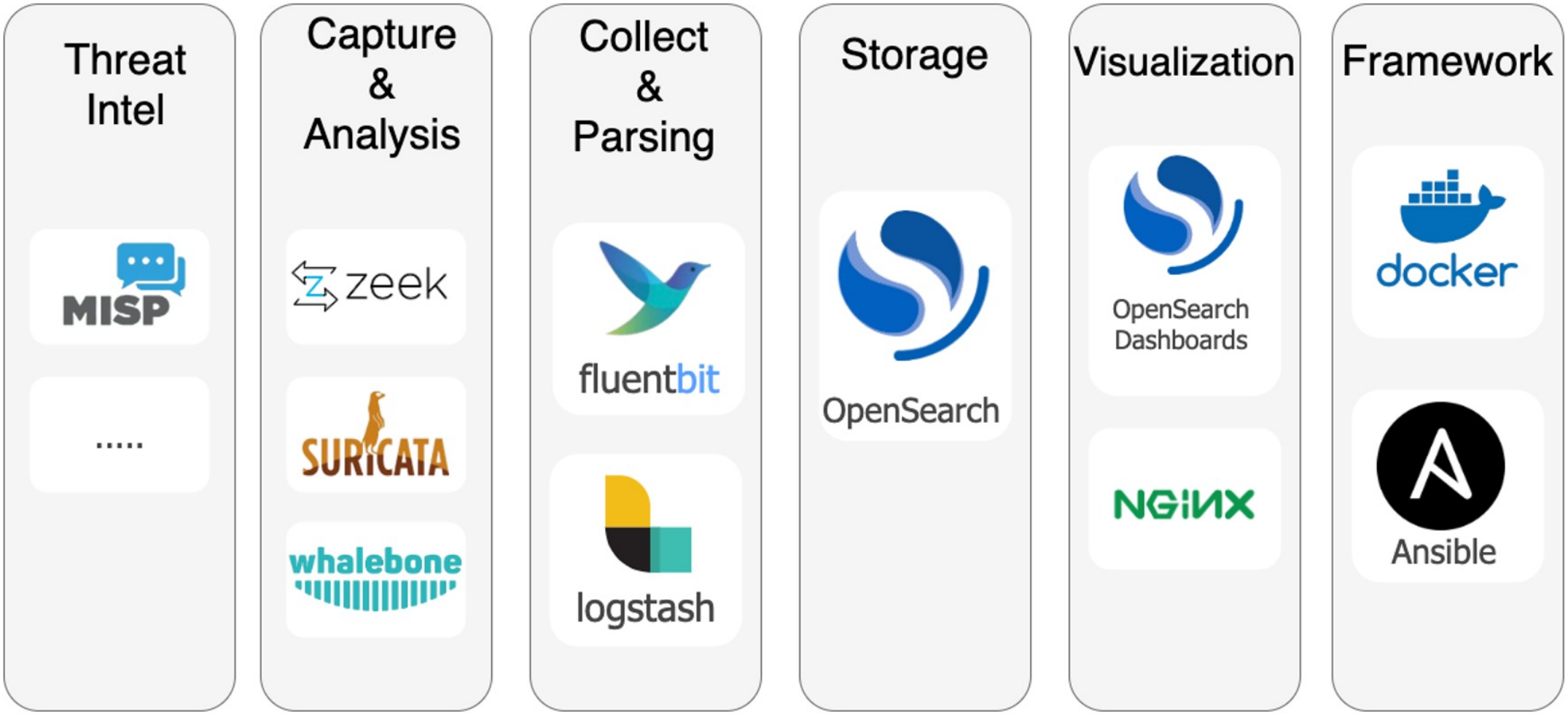


# So what is LuCySe4RE

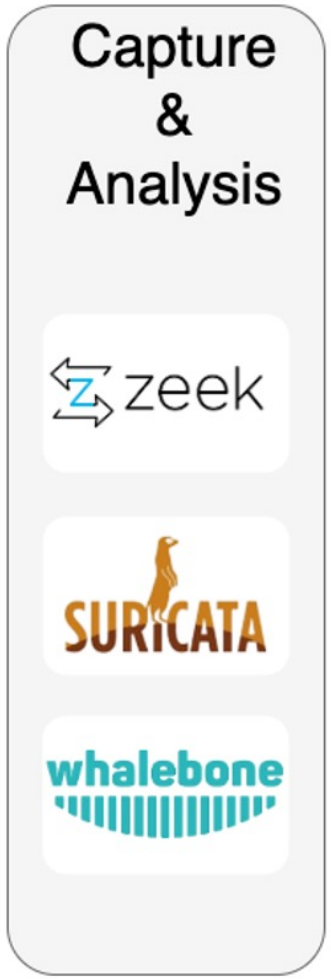
- Based on open-source technologies only
- Hardware has been reused and new hardware purchased
- On premises
- Other consequence: we will have an internal SOC team



# Current LuCySe4RE state of architecture



# Current LuCySe4RE state of architecture




## Capture & Analysis

Zeek: parsing of network traffic

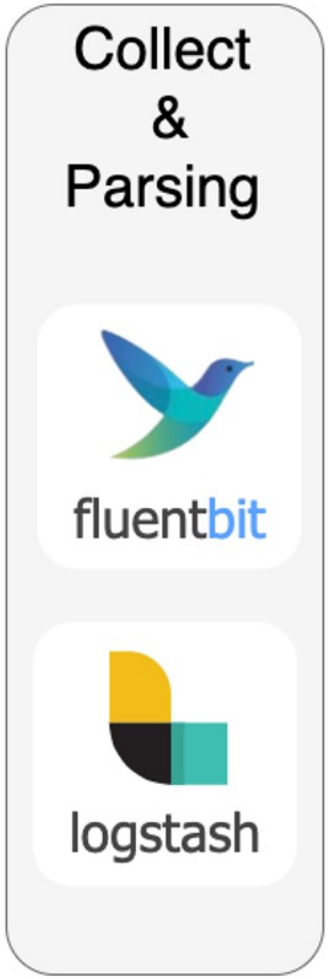
Suricata: Online and Offline

- Online: live network

- Offline: PCAP files

Whalebone: secure DNS resolution

# Current LuCySe4RE state of architecture




## Collect & Parsing

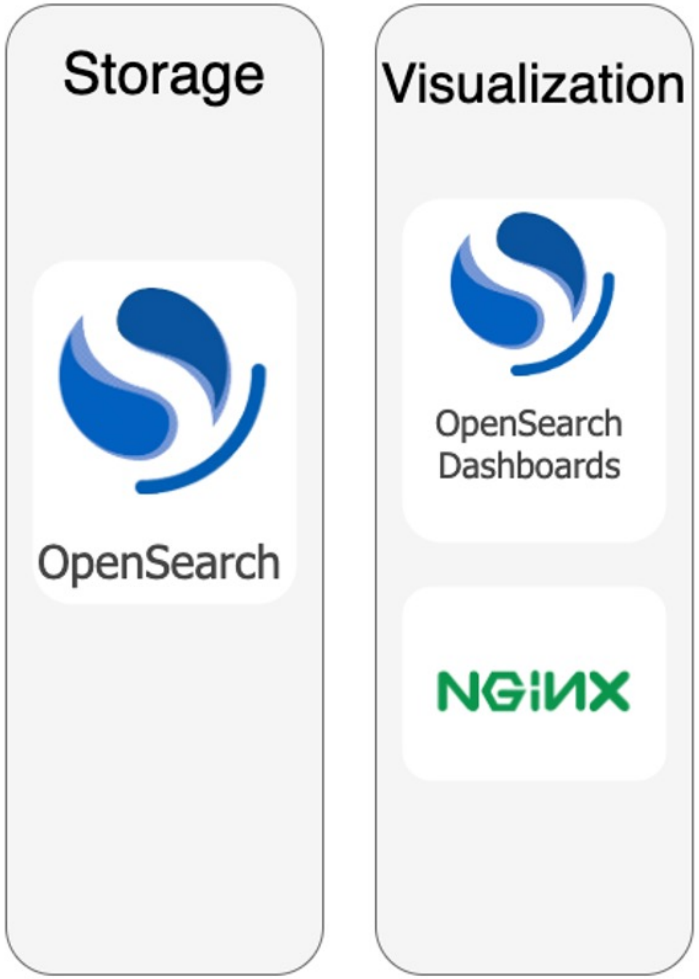
Fluentbit: Log collector

- Acquisition of logs per institution

Logstash: Parse & transform data

- Compatibility with Opensearch

# Current LuCySe4RE state of architecture




## Storage & Visualization

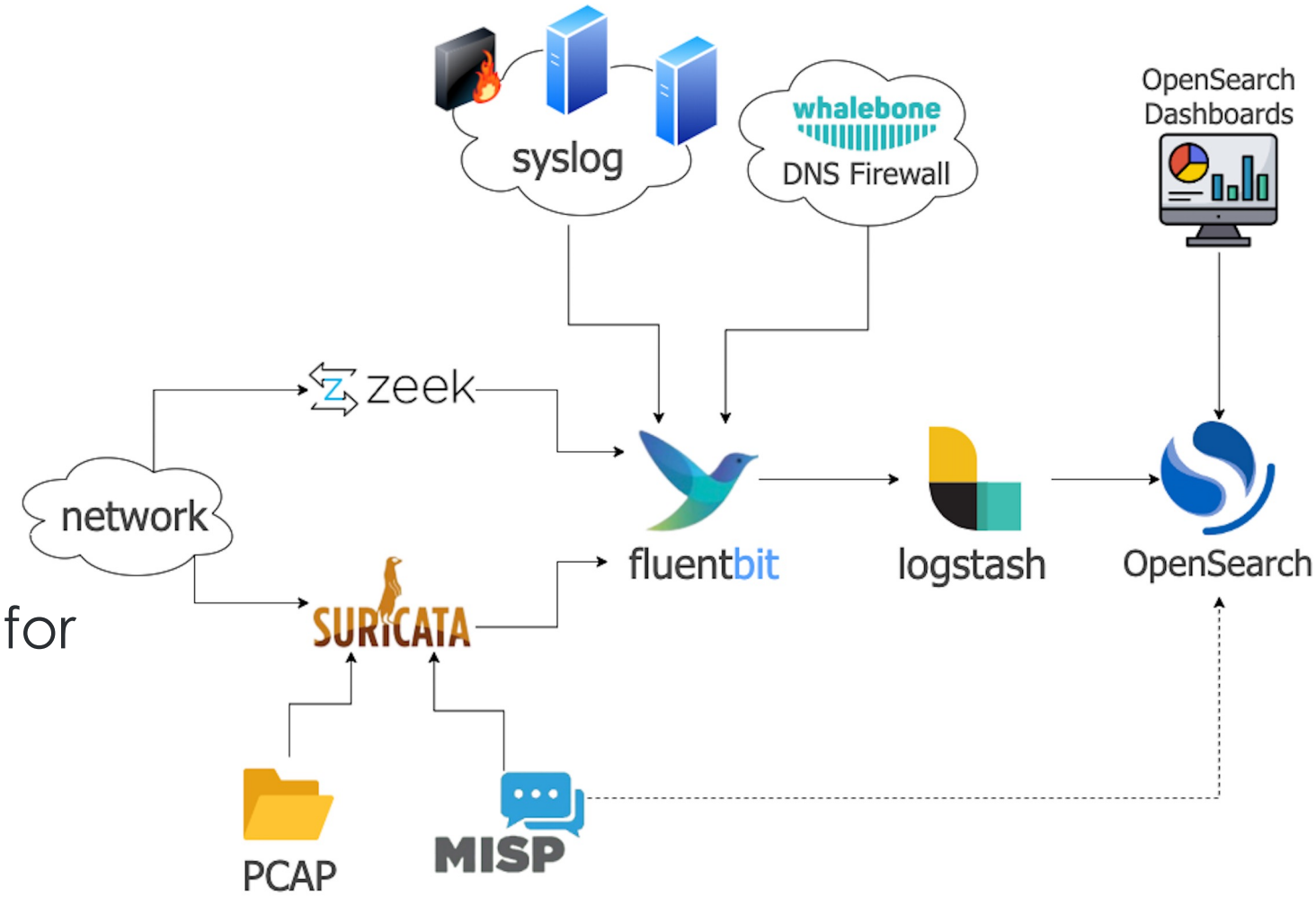
Why OpenSearch?

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

# LuCySe4RE data pipeline

- Suricata offline and online
- Syslog from institutions

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



# Awareness and education

- Awareness-raising and prevention material
  - Best practices and posters
- Training courses
  - A collaboration with the Luxembourg Digital Learning Hub has been set up
  - From the requirements topics cover:
    incident management, Ansible, DNS Security, IPv6 (no comment pls)
- Conferences
  - Cyberday.lu (save the date: 10 October 2024)
  - dataprivacyday.lu (save the date: 28 January 2025)

# Assessing the R&E security maturity level

**Motivating the R&E community for security**

- 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

## The Baselining toolset

- Assessment frameworks are very costly and not really adapted to R&E
  - We slightly adapted the actual GEANT Security Baseline tool for the assessments

- The GEANT Security Baseline tool (https://security.geant.org/baseline/)
  - Assessment tool for security based on well-known standards adapted to NRENs → help to set up security programmes
  - Assesses institutions on different topics s.a. organisation, operations, legal and technical areas
  - Assessment result in 3 levels of maturity (L1: baseline, L2: advanced, L3:expert)
  - Assessment tool not to underestimate, strong requirement to achieve L1: Baseline

# Assessing the R&E security maturity level

## The Baselining process –the PRE-LuCYSe4RE assessment

| Organisation | Score Level | ALL LuCySe4RE SCORE Level |
|---|---|---|
| Org 1 | 0 | 0 |
| Org 2 | 0 | |
| Org 3 | 0 | |
| Org 4 | 1 | |

**4 participating R&E institution were assessed 3 reported to 2024**

Assessment done by RESTENA-CISO in collaboration with R&E institution CISO

**Achieving the Baseline L1: not achieved**

1 institution being certified in ISO27001:2013 achieved L1

# Assessing the R&E security maturity level

**The Results confirm the requirements!**

- Digging deeper into the security maturity assessment results
  - The requirements identified during the proposal are confirmed here
  - Some weak points taken from the assessment to highlight :
    - 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 on-going 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)

# Merci!

tnc24
RENDEZVOUS À RENNES
Rennes, France | 10-14 JUNE 2024

Contact:
admin@restena.lu

Co-funded by
the European Union

Grant : LuCySe4RE - 101127864