restena

réseau · sécurité · .lu

LuCy
Se4RE

01101100 011101
01011000110
111100

Go Live - Workshop

10/03/2026

Co-funded by
the European Union

Agenda

1) Workshop - Part I
- 1 & 2 – Key points and Achievements
- 3 - Roadmap. What about the future ?
- 4 - Lucy Guichet & ecosystem - demo

Coffee break (15min)

2) Workshop - Part II
- 1 - SIEM overview
- 2 - Use case: from implementation to detection

3) Lunch – *Restena Office*

LuCy
Se4RE
01101100 011101
01011000110
111100

1. Key points

- Official start: 1st September 2023
- Duration: 36 months
- Recruitment of
  - A new System & Security Engineer *(David)*
  - A new (Junior) Security Analyst *(Denim)*
- Co-funded (50%) by the DIGITAL programme of the European Union

2. Achievements

Phase 1 – Tools evaluation

- Requirements
  - IPv6 support
  - Linux based
  - On-premises Deployment
  - Multi-tenancy
  - Scalability
  - High Availability

- Considerations
  - Integration capabilities: *zeek, suricata, MISP, Case management*
  - Budget and Resource Allocation
  - Use Cases
  - Feature Set

2023

2024

2025

2026

2. Achievements

Phase 1 – Tools evaluation

Product	Open-Source	Technology	Multi-Tenant	Customisation	Costs	Comments
Security Onion	Yes	ElasticSearch, Logstash, Kibana, Zeek, Suricata, others	No	No for muti-organisations	**€** (support and more)	resource-intensive workarounds needed
WAZUH	Yes	OpenSearch and others	Yes	Yes	**€** (support and more)	Installing agents at partners is too intrusive (XDR)
ELK (with Platinum subscription)	Yes	ElastiSearch, Logstash, Kibana and Platinum subscription	Yes	Yes	**€€**	Commercial licensing
OpenSearch	Yes	OpenSearch & Security Analytics	Yes	Yes	/	Close to ElasticSearch (already known). No cost BUT man power needed

2023

2024

2025

2026

2. Achievements

Phase 1 – Tools evaluation

Product	Open-Source	Technology	Multi-Tenant	Customisation	Costs	Comments
Security Onion	Yes	ElasticSearch, Logstash, Kibana, Zeek, Suricata, others	No	No for muti-organisations	**€** (support and more)	resource-intensive workarounds needed
WAZUH	Yes	OpenSearch and others	Yes	Yes	**€** (support and more)	Installing agents at partners is too intrusive (XDR)
ELK (with Platinum subscription)	Yes	ElastiSearch, Logstash, Kibana and Platinum subscription	Yes	Yes	**€€**	Commercial licensing
OpenSearch	Yes	OpenSearch & Security Analytics	Yes	Yes	/	Close to ElasticSearch (already known). No cost BUT man power needed

2023

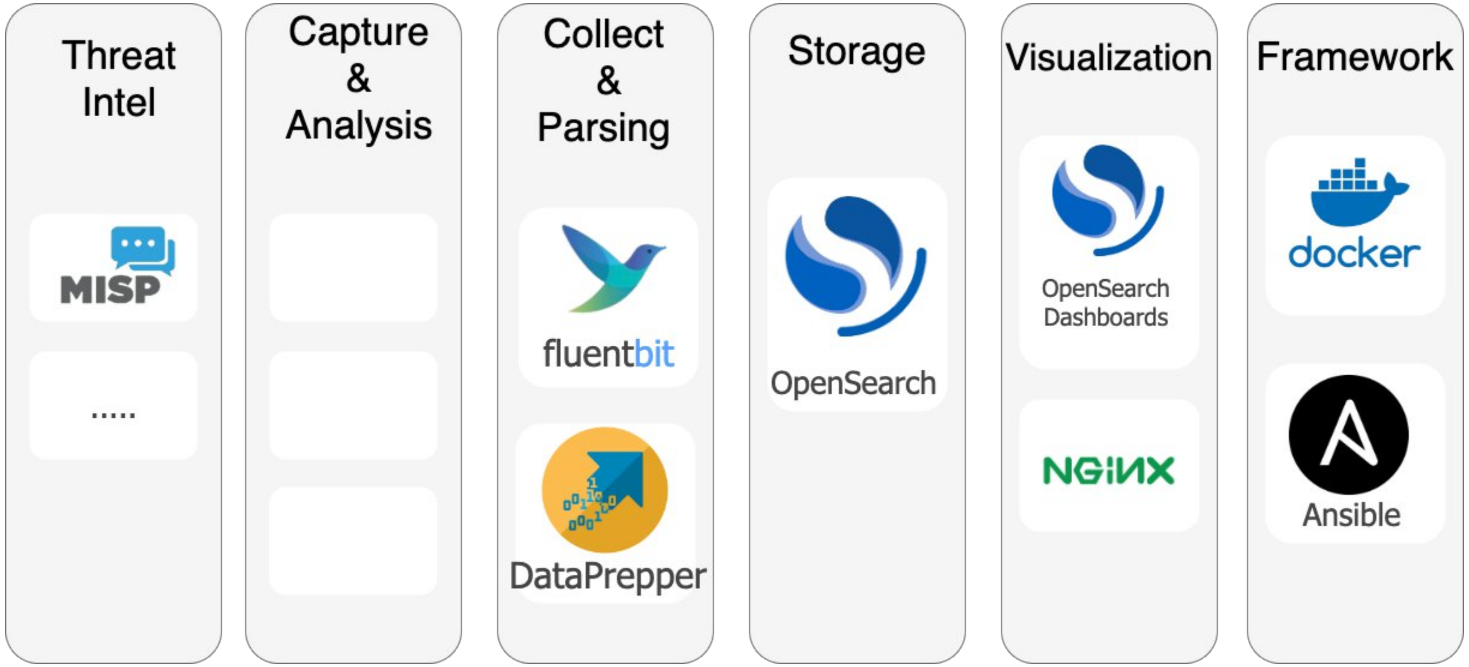
2024

2025

2026

2. Achievements

Phase 2 – Deployment and onboarding



Threat Intel

MISP

.....

Capture & Analysis

Collect & Parsing

fluentbit

DataPrepper

Storage

OpenSearch

Visualization

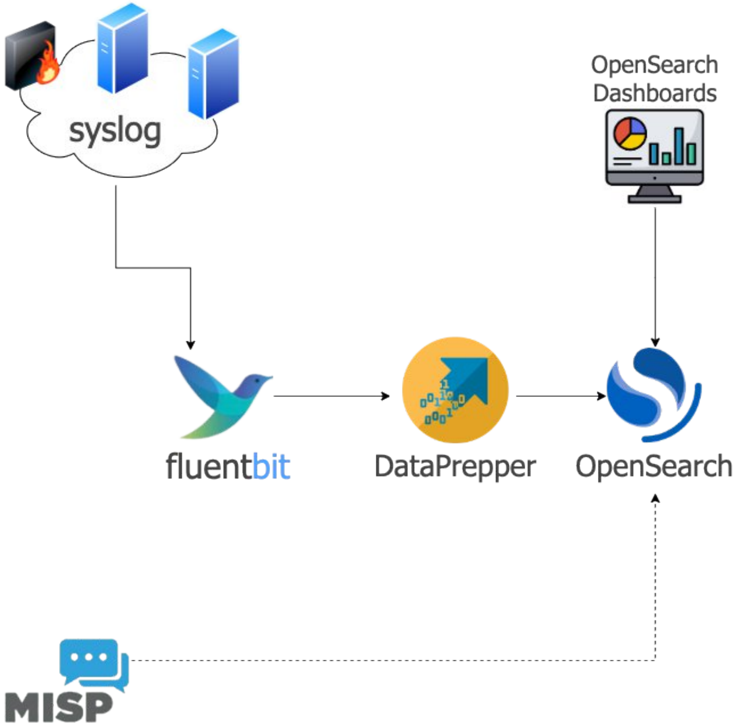
OpenSearch Dashboards

NGINX

Framework

docker

Ansible



syslog

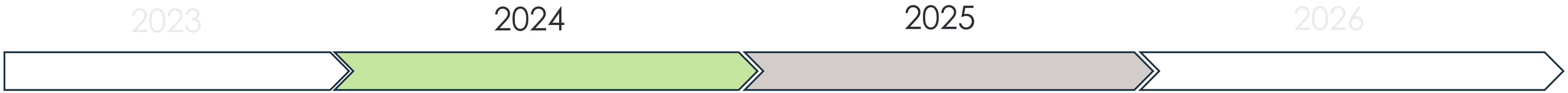
OpenSearch Dashboards

fluentbit

DataPrepper

OpenSearch

MISP



2023

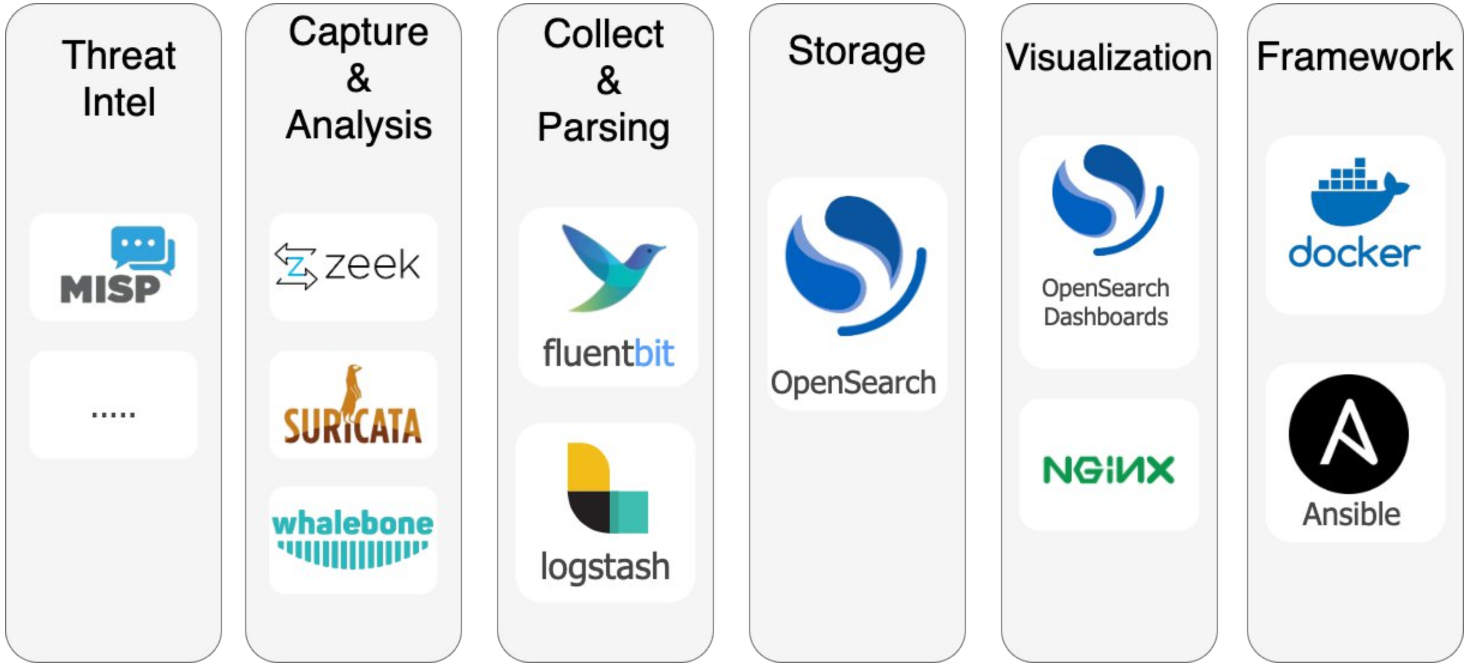
2024

2025

2026

2. Achievements

Phase 2 – Deployment and onboarding



Threat Intel: MISP, ...

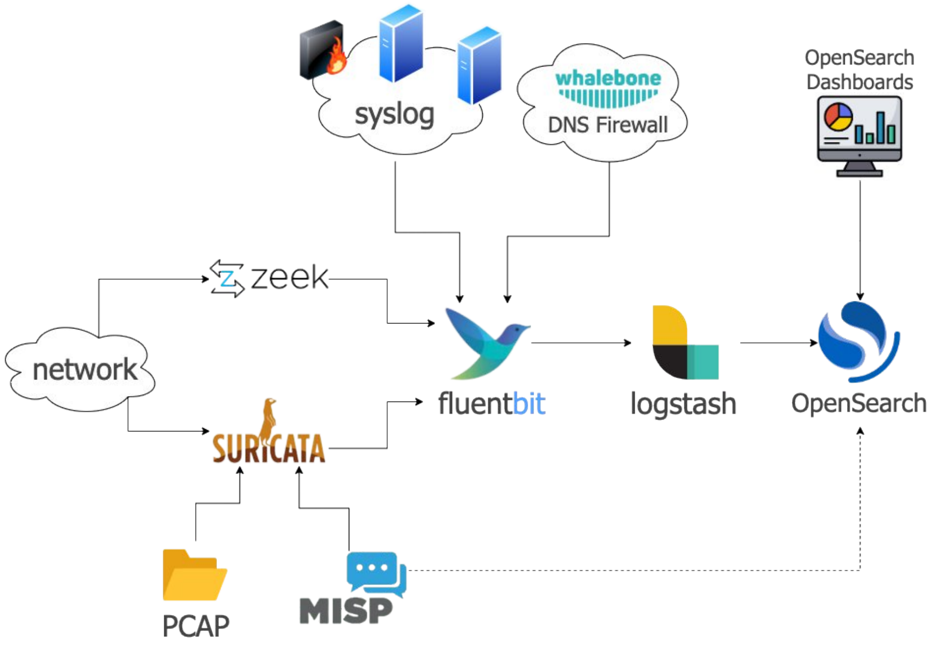
Capture & Analysis: zeek, SURICATA, whalebone

Collect & Parsing: fluentbit, logstash

Storage: OpenSearch

Visualization: OpenSearch Dashboards, NGINX

Framework: docker, Ansible

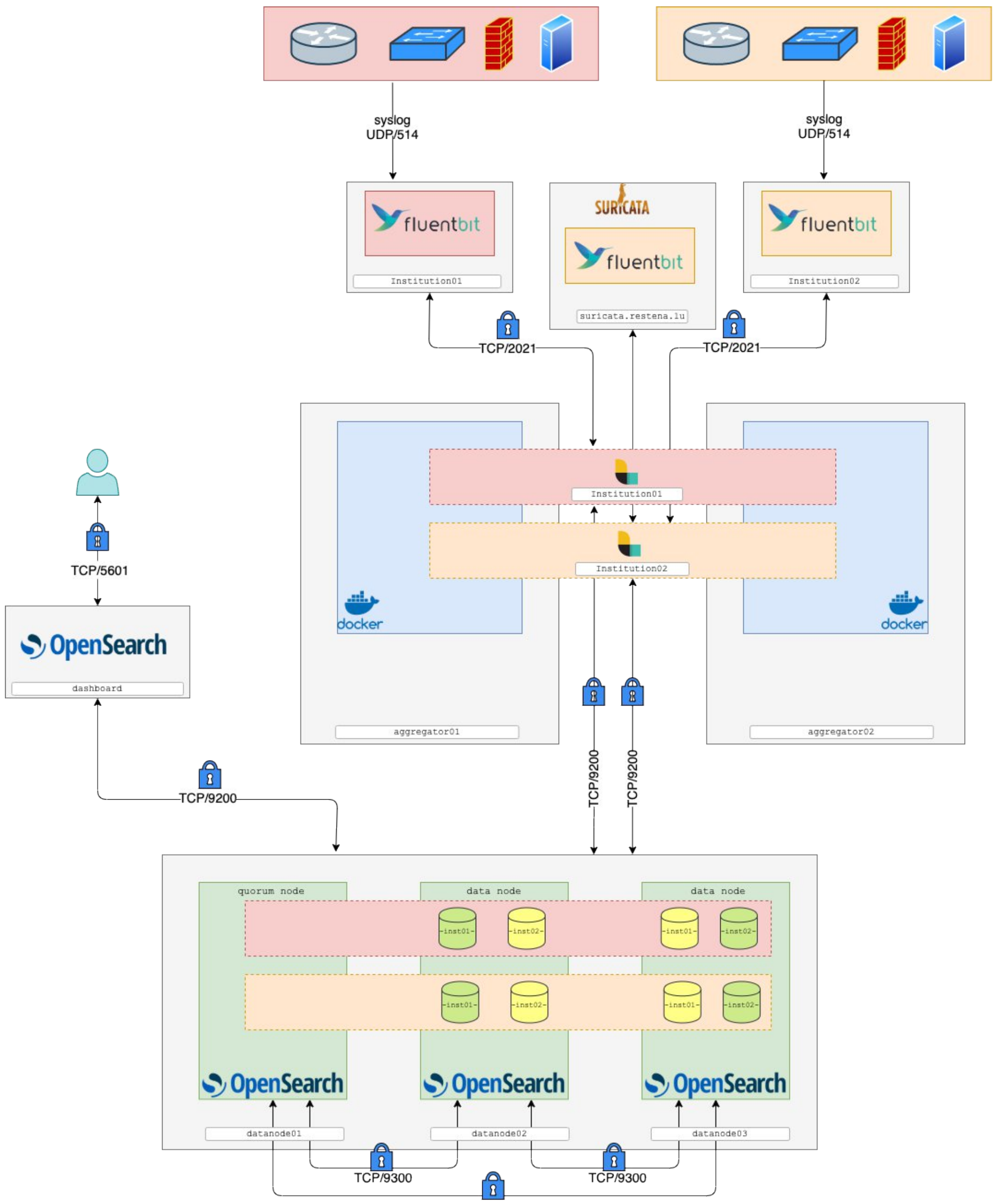


2023
2024
2025
2026

2. Achievements

Phase 2 – Deployment and onboarding

- Started small
- 2x Hypervisors running on VMware
    - 3x Data Nodes
    - 2x Aggregator Nodes
    - 1x VPN concentrator

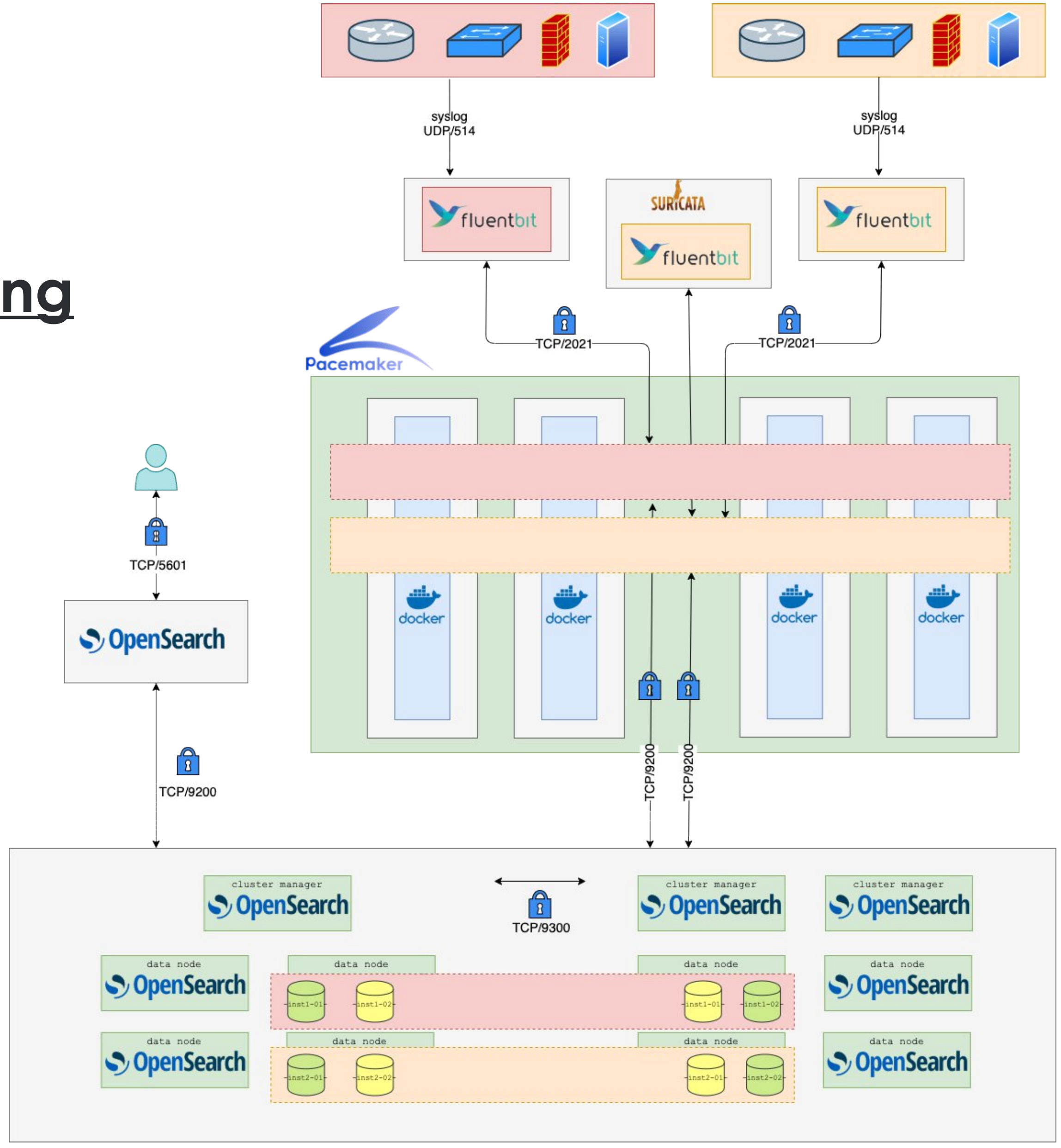


2023 2024 2025 2026

2. Achievements

Phase 2 – Deployment and onboarding

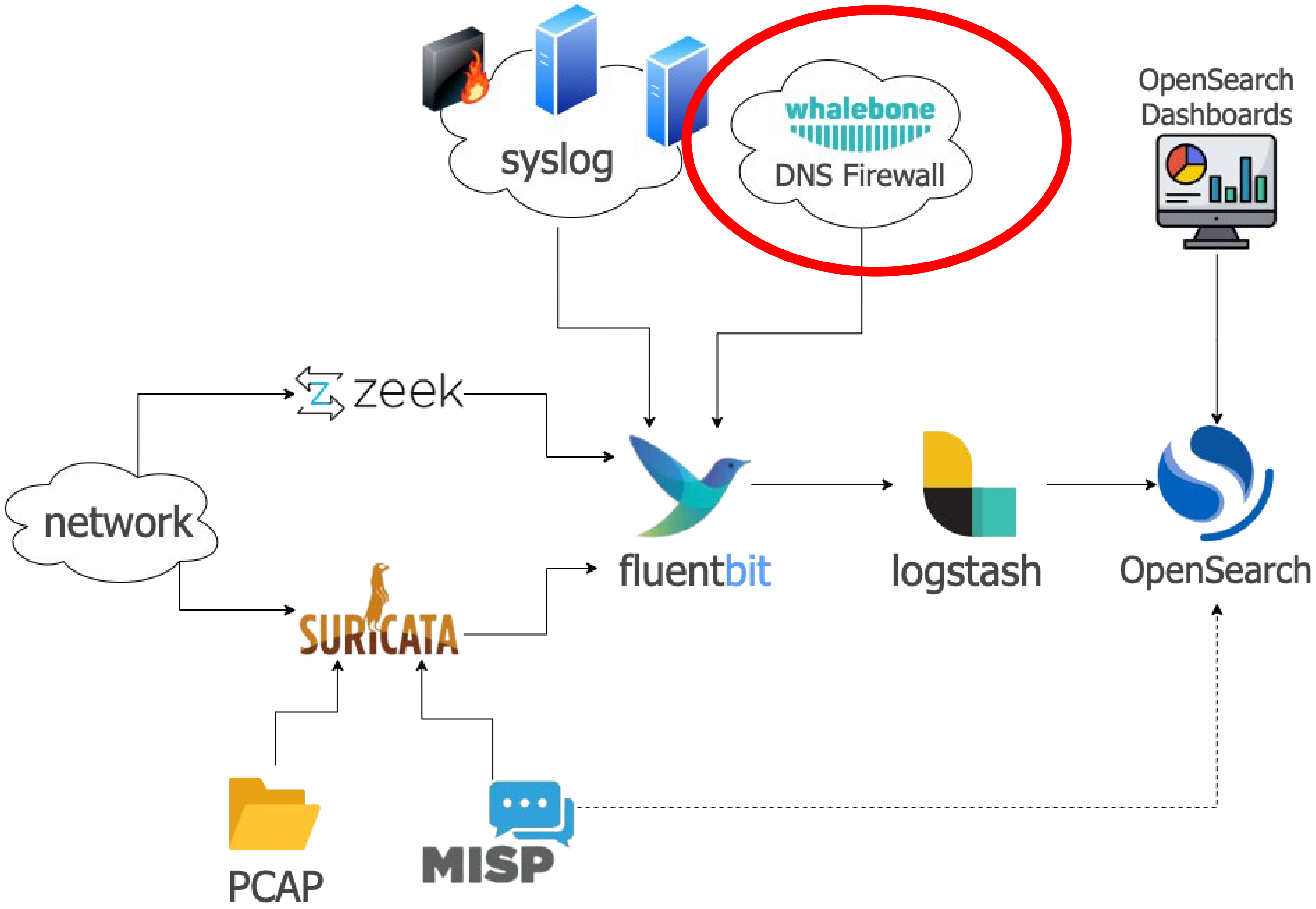
- 4x Hypervisors running on Proxmox
  - 8x Data Nodes
  - 3x Cluster Manager nodes
  - 4x Aggregator Nodes
  - 2x VPN concentrator
- Storage:
  - 2x 28TB for Hot search
  - 2x 72TB for Cold search (snapshots)



2023 2024 2025 2026

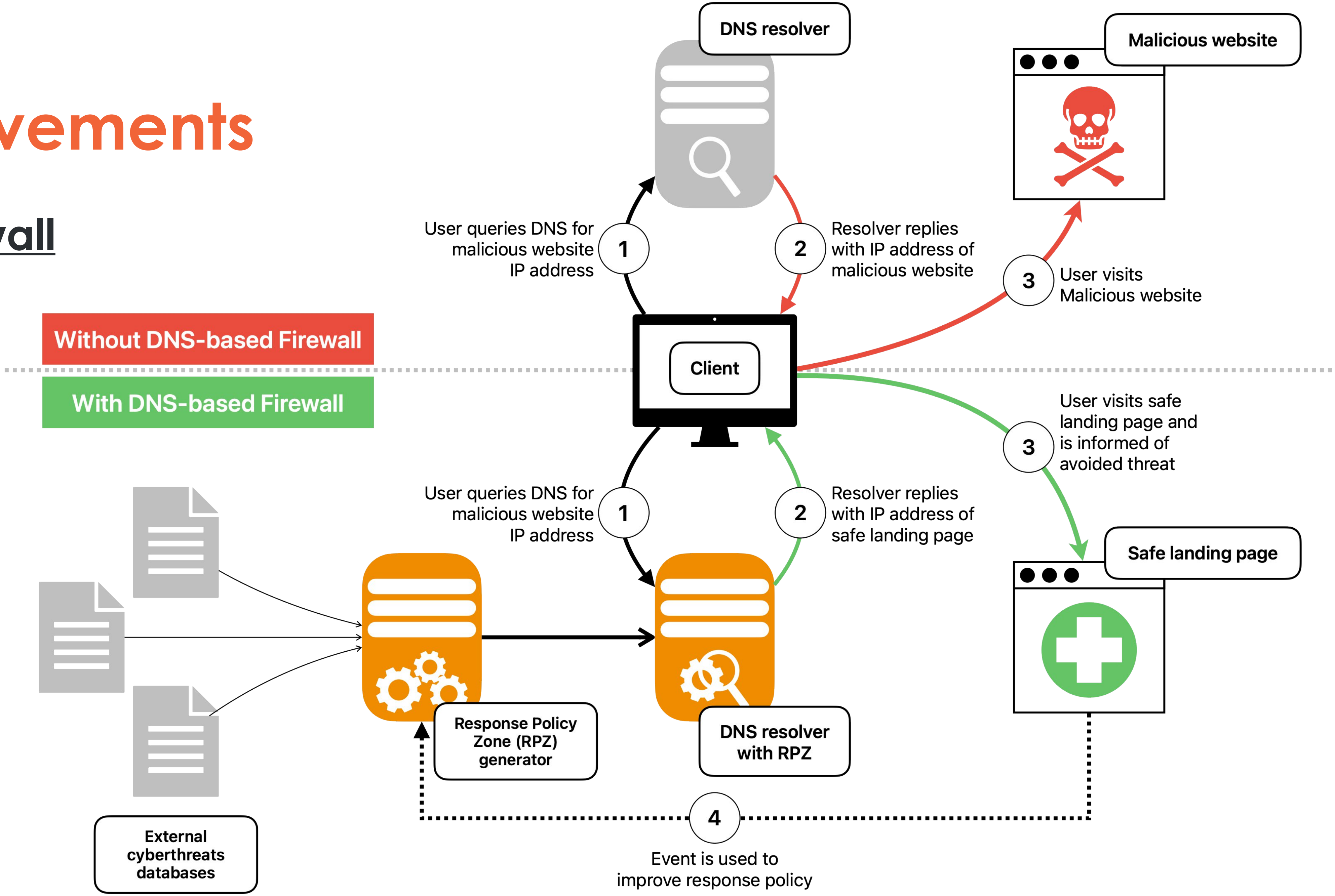
2. Achievements

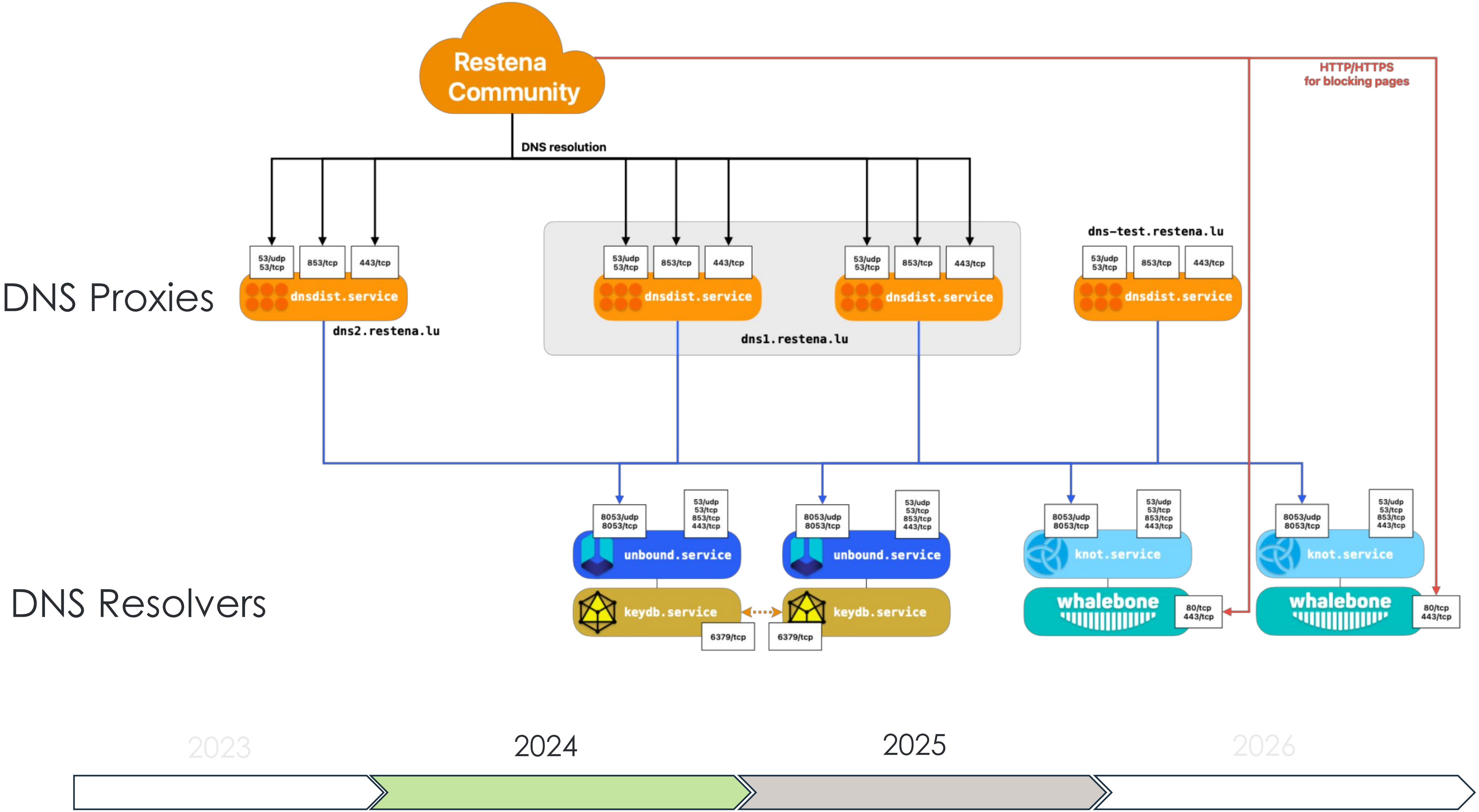
Phase 2 – Deployment and onboarding – *DNS Firewall*



2. Achievements

DNS Firewall


DNS resolver
Malicious website
User queries DNS for malicious website IP address
1
2
Resolver replies with IP address of malicious website
3
User visits Malicious website
Without DNS-based Firewall
With DNS-based Firewall
Client
User visits safe landing page and is informed of avoided threat
3
User queries DNS for malicious website IP address
1
2
Resolver replies with IP address of safe landing page
Safe landing page
Response Policy Zone (RPZ) generator
DNS resolver with RPZ
External cyberthreats databases
4
Event is used to improve response policy



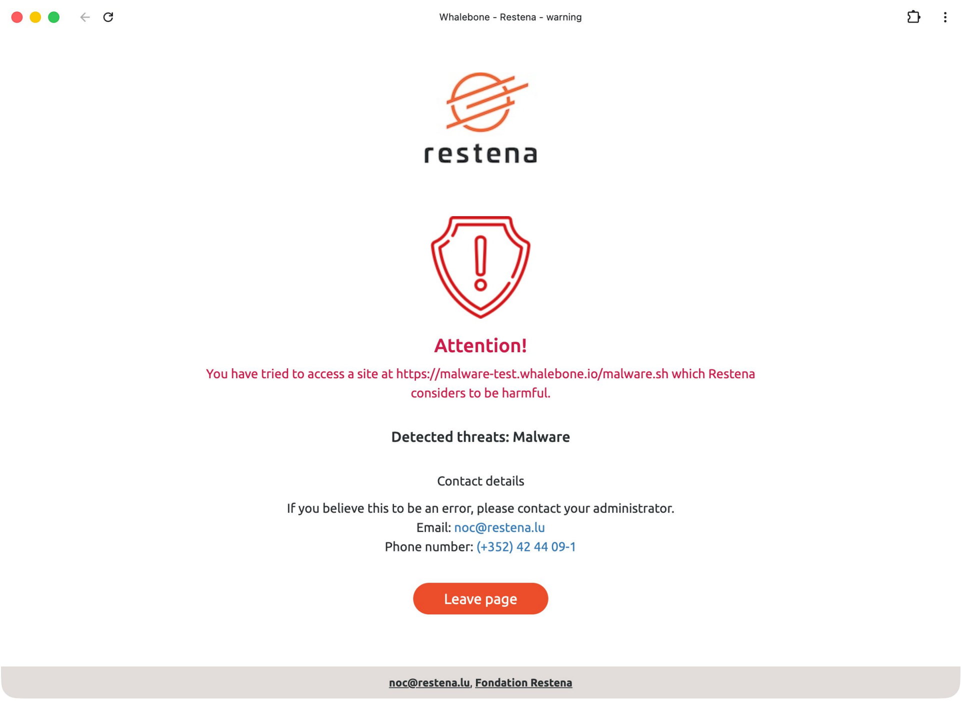
DNS Proxies

DNS Resolvers

2. Achievements

DNS Firewall

DNS Firewall blocking page



Attention!

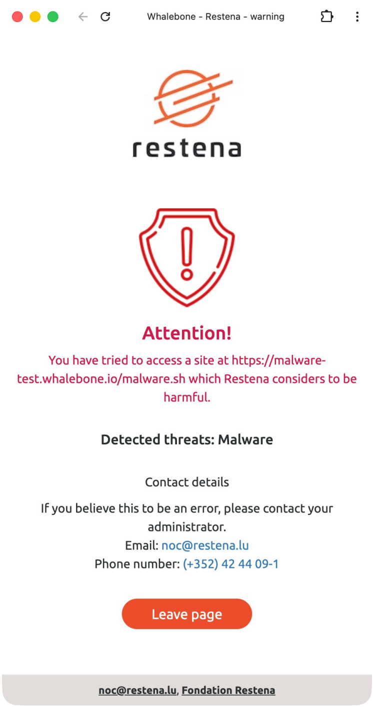
You have tried to access a site at https://malware-test.whalebone.io/malware.sh which Restena considers to be harmful.

Detected threats: Malware

Contact details

If you believe this to be an error, please contact your administrator.
Email: noc@restena.lu
Phone number: (+352) 42 44 09-1

noc@restena.lu, Fondation Restena



Attention!

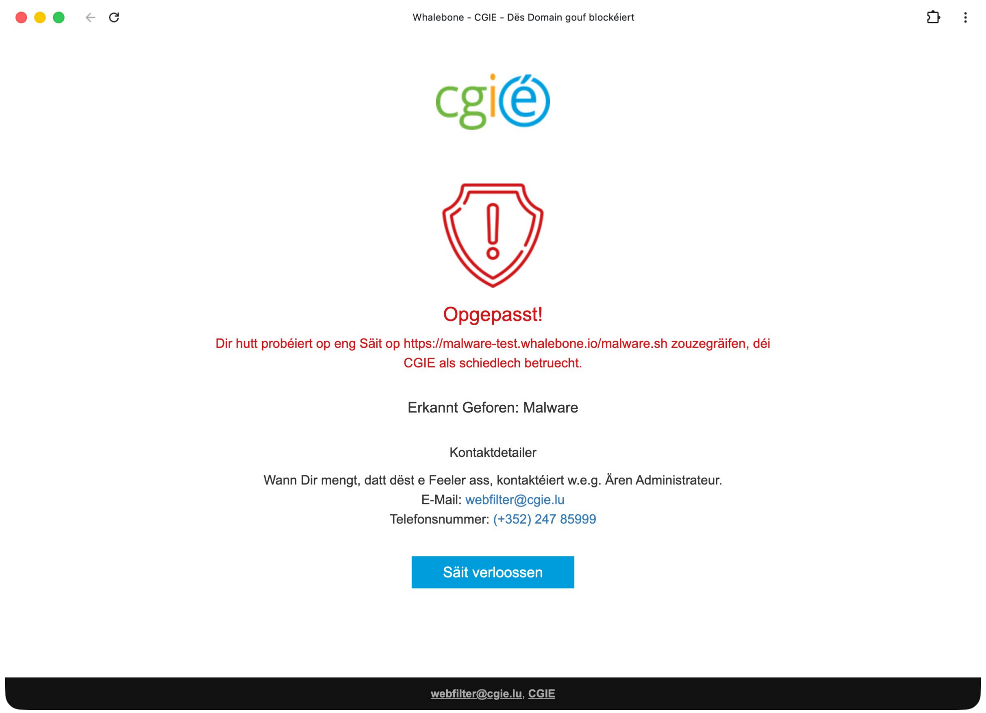
You have tried to access a site at https://malware-test.whalebone.io/malware.sh which Restena considers to be harmful.

Detected threats: Malware

Contact details

If you believe this to be an error, please contact your administrator.
Email: noc@restena.lu
Phone number: (+352) 42 44 09-1

noc@restena.lu, Fondation Restena



Opgepasst!

Dir hutt probéiert op eng Säit op https://malware-test.whalebone.io/malware.sh zouzegräifen, déi CGIE als schiedlech betruecht.

Erkannt Geforen: Malware

Kontaktdetailer

Wann Dir mengt, datt dëst e Feeler ass, kontaktéiert w.e.g. Ären Administrateur.
E-Mail: webfilter@cgie.lu
Telefonsnummer: (+352) 247 85999

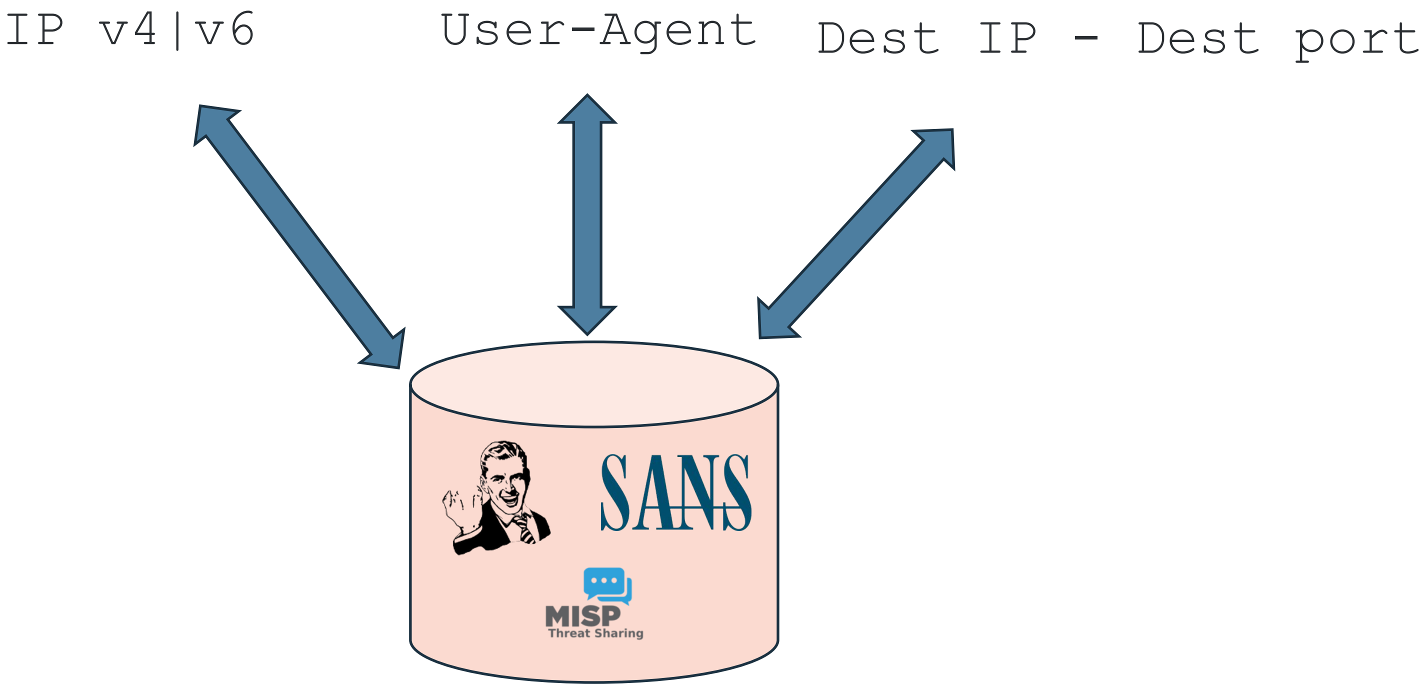
webfilter@cgie.lu, CGIE

2023
2024
2025
2026

2. Achievements

Phase 2 – Deployment and onboarding

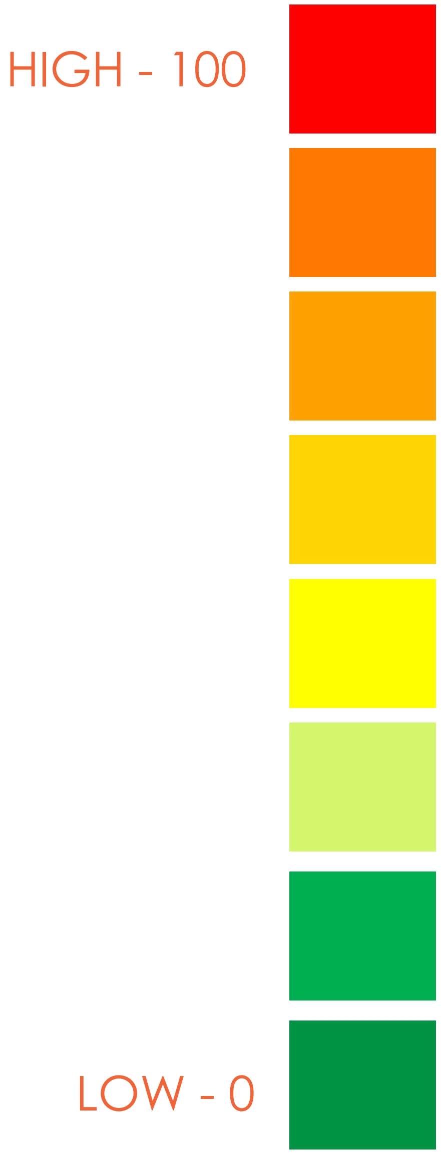
Threat Enrichments Indicator – Scoring & Confidence



IP v4|v6

User-Agent

Dest IP - Dest port



2. Achievements

Phase 2 – Deployment and onboarding

Step1

uni.lu
UNIVERSITÉ DU LUXEMBOURG

LISER
LUXEMBOURG INSTITUTE OF SOCIO-ECONOMIC RESEARCH

Step2

cgié

LUXEMBOURG INSTITUTE OF HEALTH

bts >> cybersecurity

Lycée Guillaume Kroll

2023

2024

2025

2026

3. What about the future ?

- August 2026 -> End Of EU funding
  - No worries, we will continue to maintain the systems
- Consolidation

zeek SURICATA

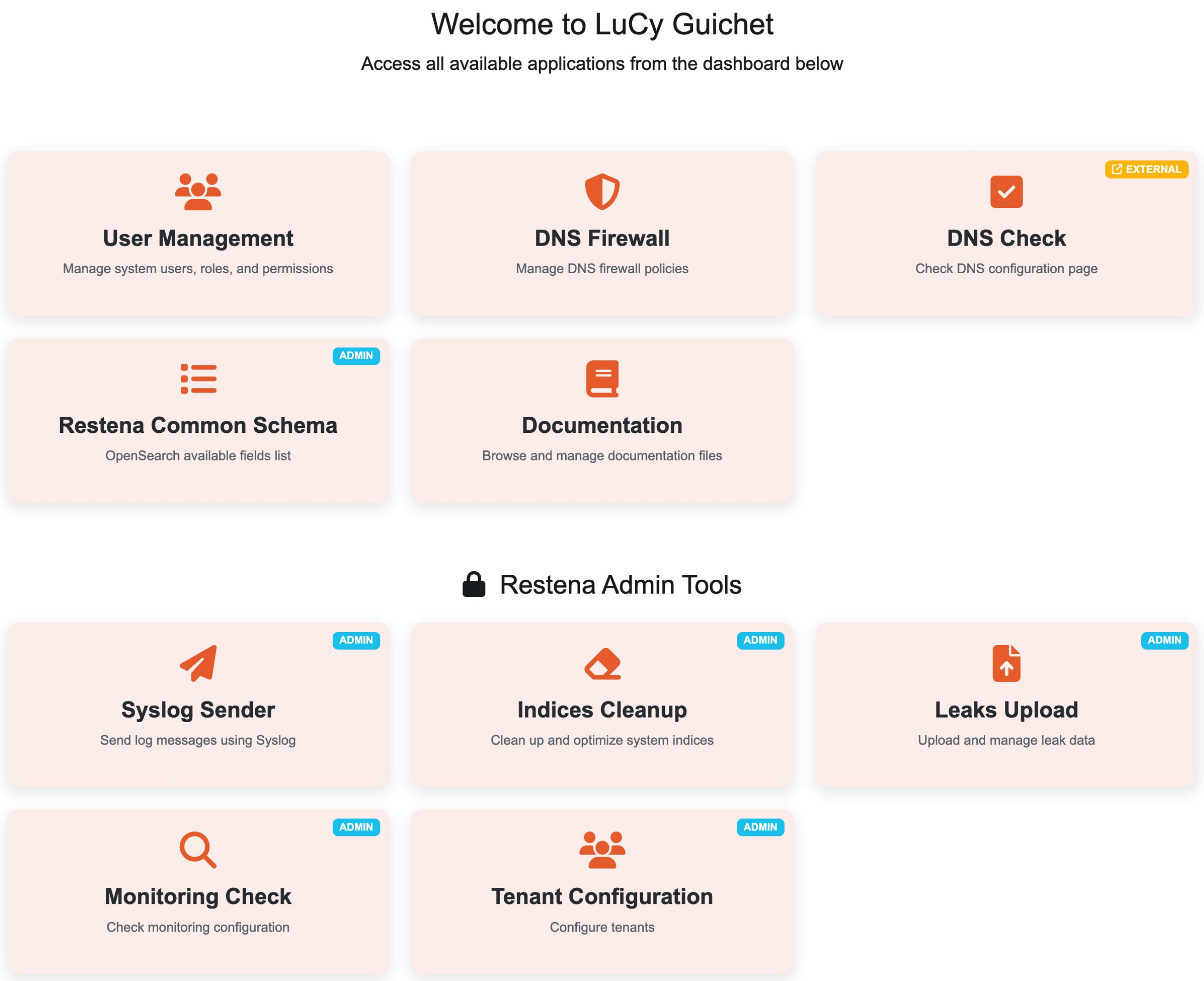
- Anomaly Detection
- Case management
  - Integration of FlowIntel

flowintel

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

4. LUCY Guichet

DEMO



Welcome to LuCy Guichet

Access all available applications from the dashboard below

User Management
Manage system users, roles, and permissions

DNS Firewall
Manage DNS firewall policies

EXTERNAL
DNS Check
Check DNS configuration page

ADMIN
Restena Common Schema
OpenSearch available fields list

Documentation
Browse and manage documentation files

Restena Admin Tools

ADMIN
Syslog Sender
Send log messages using Syslog

ADMIN
Indices Cleanup
Clean up and optimize system indices

ADMIN
Leaks Upload
Upload and manage leak data

ADMIN
Monitoring Check
Check monitoring configuration

ADMIN
Tenant Configuration
Configure tenants

And more demonstrations…

Thank you.

Cynthia WAGNER: cynthia.wagner@restena.lu

Isidore MORENO: isidore.moreno@restena.lu