Collaborative operational security

Security Operations Centre deployment models

David Crooks
Liviu Vâlsan

HEPiX Spring 2024, Paris

Agenda

- Environment update
- Deployment updates
- SOC Hackathon
- Lightweight approach

Environment update

- Threat to research and education remains persistent
- Recent examples include British Library
  - https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf
- Cyber Threat Intelligence (CTI) widely seen as vital to improve our capabilities
  - Jisc cyber threat intel sharing group (via MISP)
  - GEANT cyber intelligence sharing (NRENs)
  - In addition to our own work

STFC Deployment

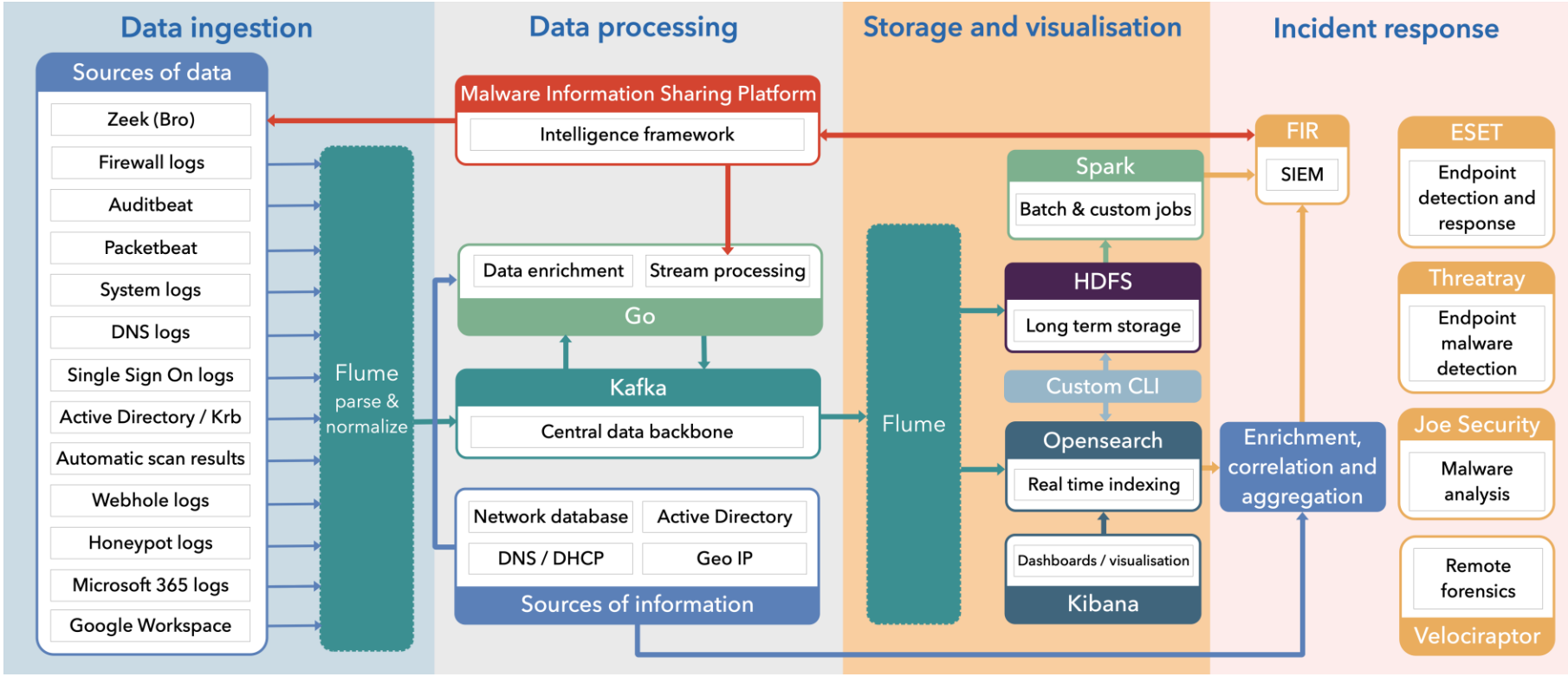
- Focus on config management
- Monitoring of both LHC OPN links being commissioned
  - Low capture loss monitoring for both links (~0.05% / worker thread)
  - Re-engineered load balancing structure in place on aggregation switch
- Security-first Aquilon archetype used for both VM and bare metal machines
  - Working with Rocky9
- OpenSearch cluster in place

STFC Deployment

- Kafka and logstash are done and working in development
  - Next are config management and deployment to hardware
- New MISP instance in testing
  - Based on Jisc deployment model
  - Onboarding UKRI infosec team
    - Following snag fixing network connectivity
- Working across STFC to building operational processes
  - Broader STFC SOC project underway + UKRI activity

CERN Deployment

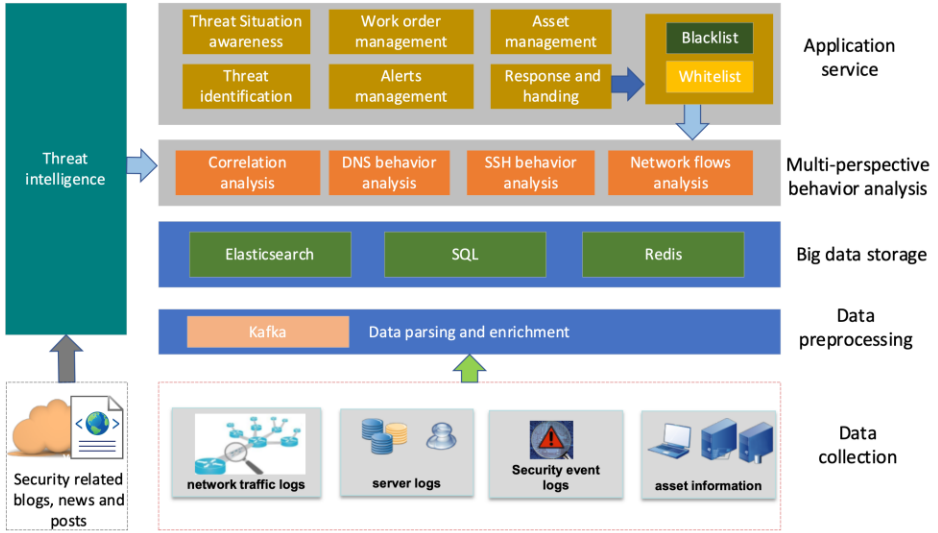
- Additional data sources
- Migrated from Elasticsearch to Opensearch



Status update: IHEP

IHEP SOC

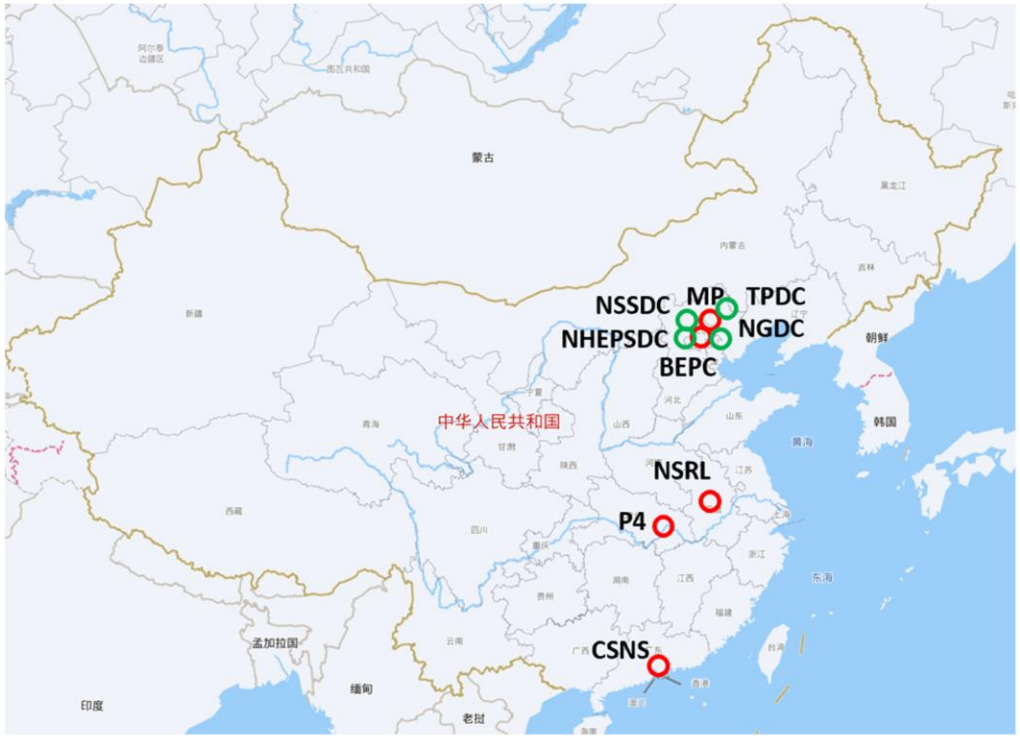
- The Security Operation Center(SOC) proposed in 2021 in IHEP is effective
  - minimize cybersecurity risks
  - improve security operations
- Five data processing layers



Status update: IHEP

Applications

- The DSOC has been applied to institute of high energy physics (IHEP) and deployed in 5 collaborative large scientific facilities and 4 scientific data centers



SOC Hackathon 2024

- Recent hackathon in CERN in March
- 24 participants in person
  - 11 organisations from 6 countries represented
- ~9 online

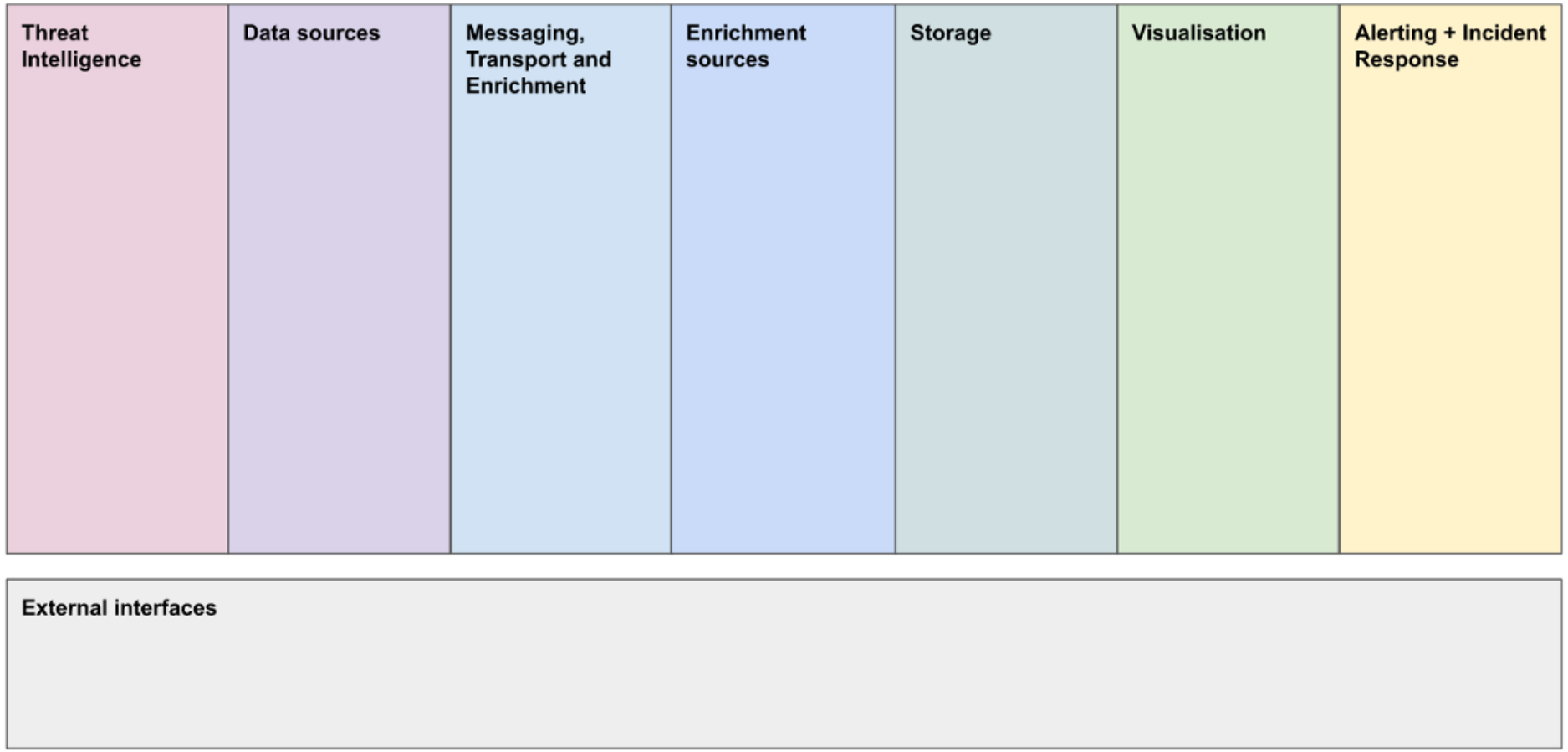
- More of a single track discussion model than previous
  - Aim to move back to breakout model next time

SOC Hackathon 2024

- Lightweight solutions for facilities with fewer resources
- Identifying concrete plans for different infrastructures
  - Including WLCG
- Deployment of MISP docker solution developed by Jisc
  - And development of OIDC config options: pull request open on Github project
  - Support for Shibboleth looks promising
- Development of Zeek docs
  - And documentation processes
- Deeper look at using MISP
  - Taxonomies, Feeds, Warning Lists, …
- People and process

SOC Models

- Recall from [last time]
- Look at different SOC Models
- Focus on lightweight approach here



How to get involved?

- As always in this type of work, two kinds of participation

    1. Specific domain interest or early adopter
    2. Rolling out capabilities through participation in $infrastructure

- Vast majority of this work so far is in the domain of early adopters
    - What should sites be doing?

- People and processes
    - New part of work of SOC WG (see Jeny's talk)
    - Part of *people*, *process* and technology components of a SOC

People

- Who do you have available to do this work?
  - Are you a 0/0.25FTE system manager supporting a small cluster?
  - Do you have a reasonably sized* ops team/ dedicated security/networking staff
  - How good is your connection to your central security team(s)
    - Or vice versa!

* *or* Are you a Tier-1

People

- Unless you have a ~dedicated team likely do not want to deploy full-scale SOC
  - "SOC in a box" concept not appropriate given reliance on particular network topologies/circumstances
- Who is going to deploy systems **and** who is going to respond to alerts?
  - Including, where appropriate, on-call

Process

- What are your existing incident response + incident detection processes?

- Once you deploy a set of tools, important to understand how you are going to use the output
  - What distributed options are available to you?

Lightweight sites

- In WLCG, very likely that the majority of sites will not deploy full-scale SOCs
  - **Unless** as part of an organisational activity

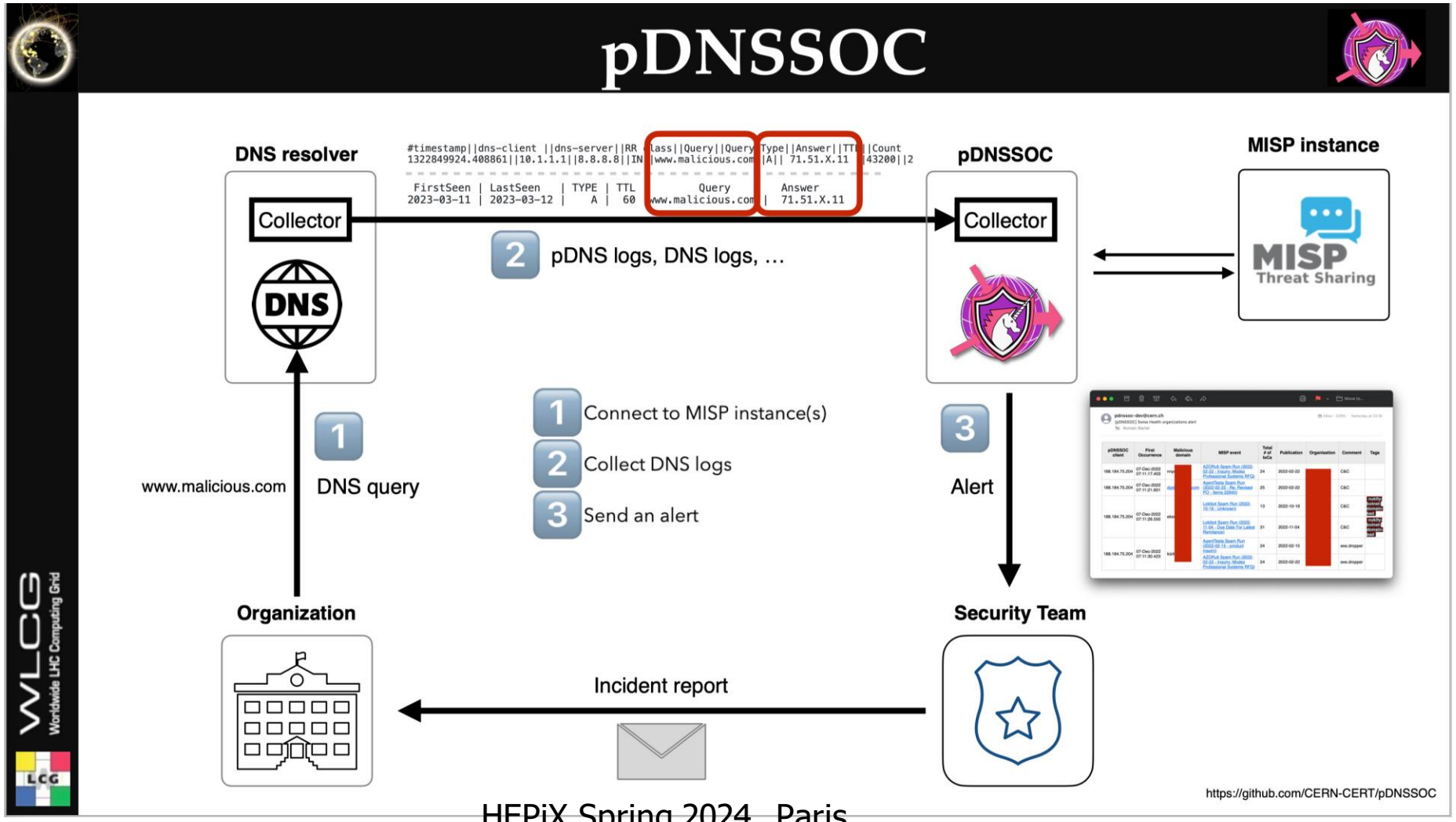
- Focus on "bang for buck"
  - pDNSSOC

pDNSSOC

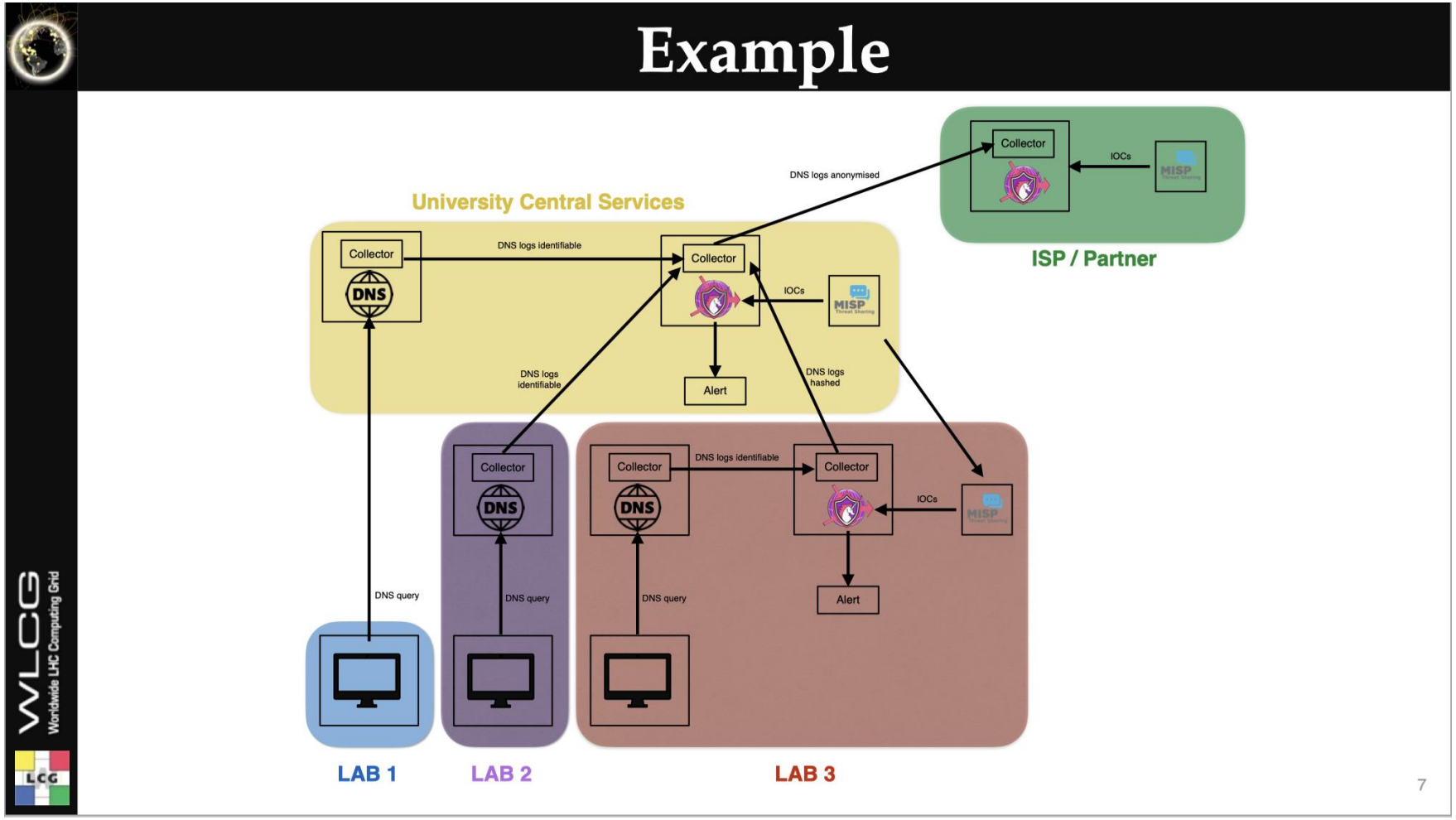
- Deploying a full-scale SOC requires sustained effort, people, processes and technology
- Many/most smaller facilities or sites may not be in a position to take this route
- Identify lightweight "80%" alternative that can make best use of threat intel without significant resource
  - DNS

- pDNSSOC

pDNSSOC


pDNSSOC
DNS resolver
#timestamp||dns-client ||dns-server||RR class||Query||Query Type||Answer||TTL||Count
1322849924.408861||10.1.1.1||8.8.8.8||IN ||www.malicious.com ||A|| 71.51.X.11 ||43200||2
FirstSeen | LastSeen | TYPE | TTL | Query | Answer
2023-03-11 | 2023-03-12 | A | 60 | www.malicious.com | 71.51.X.11
Collector
DNS
2 pDNS logs, DNS logs, …
pDNSSOC
Collector
MISP instance
MISP Threat Sharing
1 Connect to MISP instance(s)
2 Collect DNS logs
3 Send an alert
www.malicious.com
1 DNS query
3 Alert
Organization
Security Team
Incident report
https://github.com/CERN-CERT/pDNSSOC

pDNSSOC


Example
University Central Services
Collector
DNS
DNS logs identifiable
Collector
IOCs
MISP
DNS logs anonymised
Collector
IOCs
MISP
ISP / Partner
DNS logs identifiable
DNS logs hashed
Alert
Collector
DNS
Collector
DNS
DNS logs identifiable
Collector
IOCs
MISP
Alert
DNS query
DNS query
DNS query
LAB 1
LAB 2
LAB 3
7

pDNSSOC

- What do you need to deploy pDNSSOC?

- A(ccess to a) DNS infrastructure
- Somewhere that can correlate DNS with MISP
  - Regional?
- Someone to respond to alerts
  - Including some level of false positives

pDNSSOC

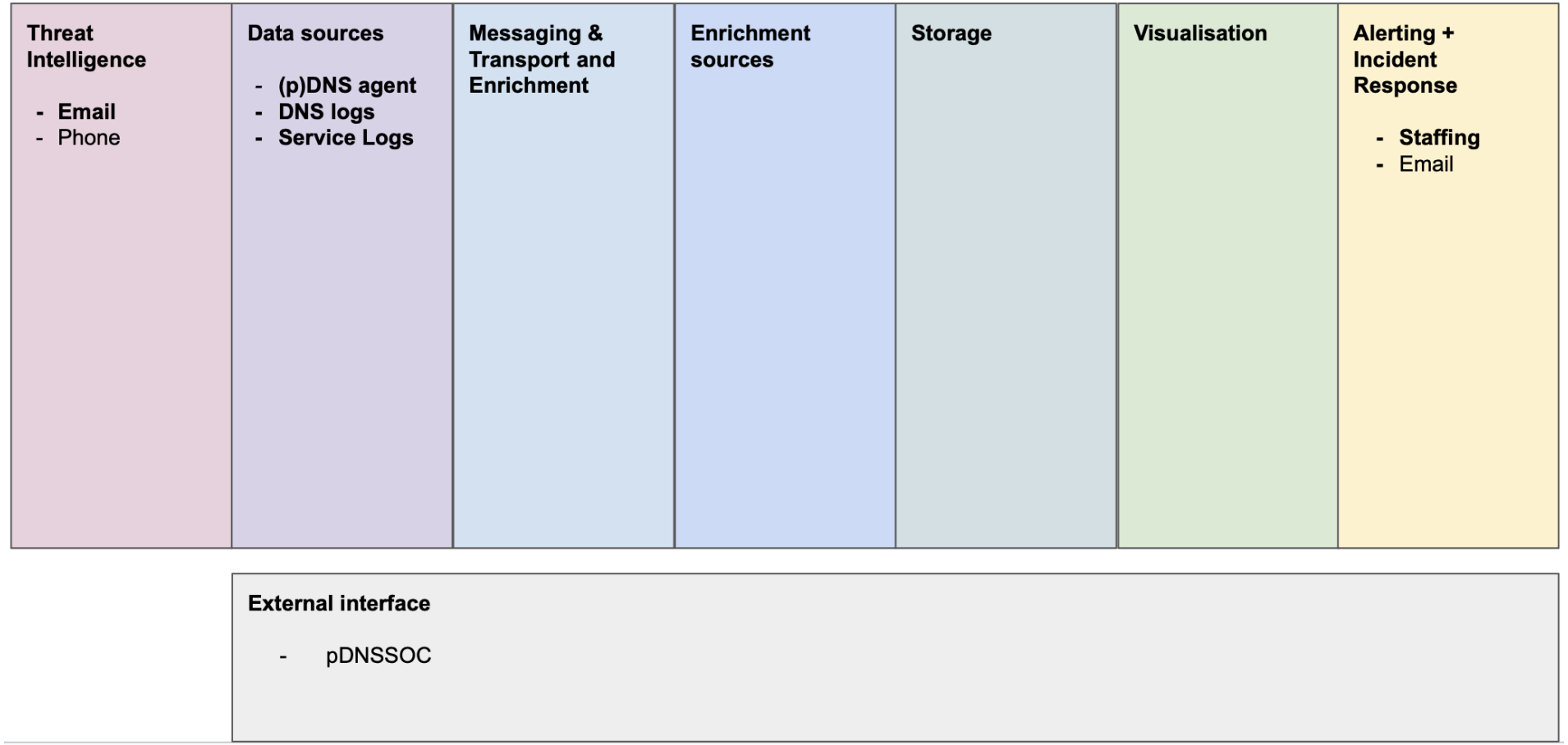
- What to do next/what do we need?

- We need people to use pDNSSOC in real/test environments
- We (SOC WG) are planning some development meetings
  - Welcome participation

- We need to design the larger structures to use this effectively
  - (Federated, distributed) teams providing support

- Pau Cutrina working with both DK-CERT and RedCLARA in South America, valuable experience to be gained

Lightweight SOC Model



Training

- PocketSOC-NG again used in security school in 2023
  - Similar to first edition
  - Retuning of access mechanism and refactoring of material

- Graduate project in place at STFC to improve deployment process and training materials, to begin in a few weeks
  - Goal of straightforward deployment to cloud environment with scalable number of clients

SOC Hackathon (Late 2024)

- Initial planning already underway for next edition
- Aim for ~9 month cadence: split between once and twice a year
- Plan for next hackathon in November (avoiding December)
  - Perhaps shortly after next HEPiX
  - A chance for a ~BoF meet-up there?
  - Looking for volunteers to host
    - Jisc has offered to host in their London offices
- Identify work that the working group should engage with over the next months to provide best basis for workshop

Possible GridPP/IRIS testbed

- Would like to be in a position to discuss in detail site experience
  - Proposing that GridPP/IRIS could be a useful testbed in the UK

- Focus on plan for different sites across GridPP/IRIS
  - Existing+organisational full-scale SOC work
  - How and where pDNSSOC can play a role
    - For example STFC could play role of regional correlation/alerting centre
  - How does the Jisc intel sharing group play a role?

Next steps

- Continuing theme of this work is identifying where a full-scale SOC is appropriate, versus a lightweight approach using something like pDNSSOC
- Goal for this year is to have clear guidance, infrastructure dependent
- Underlying driver continues to be the importance of threat intelligence
- People and processes are vital for a long term, full-scale SOC activity
- Get involved!
  - Talk to me and join the active keybase community


egi
CSIRT

WISE
COMMUNITY

WLCG
Worldwide LHC Computing Grid

Questions?