Designing Operational Security Systems

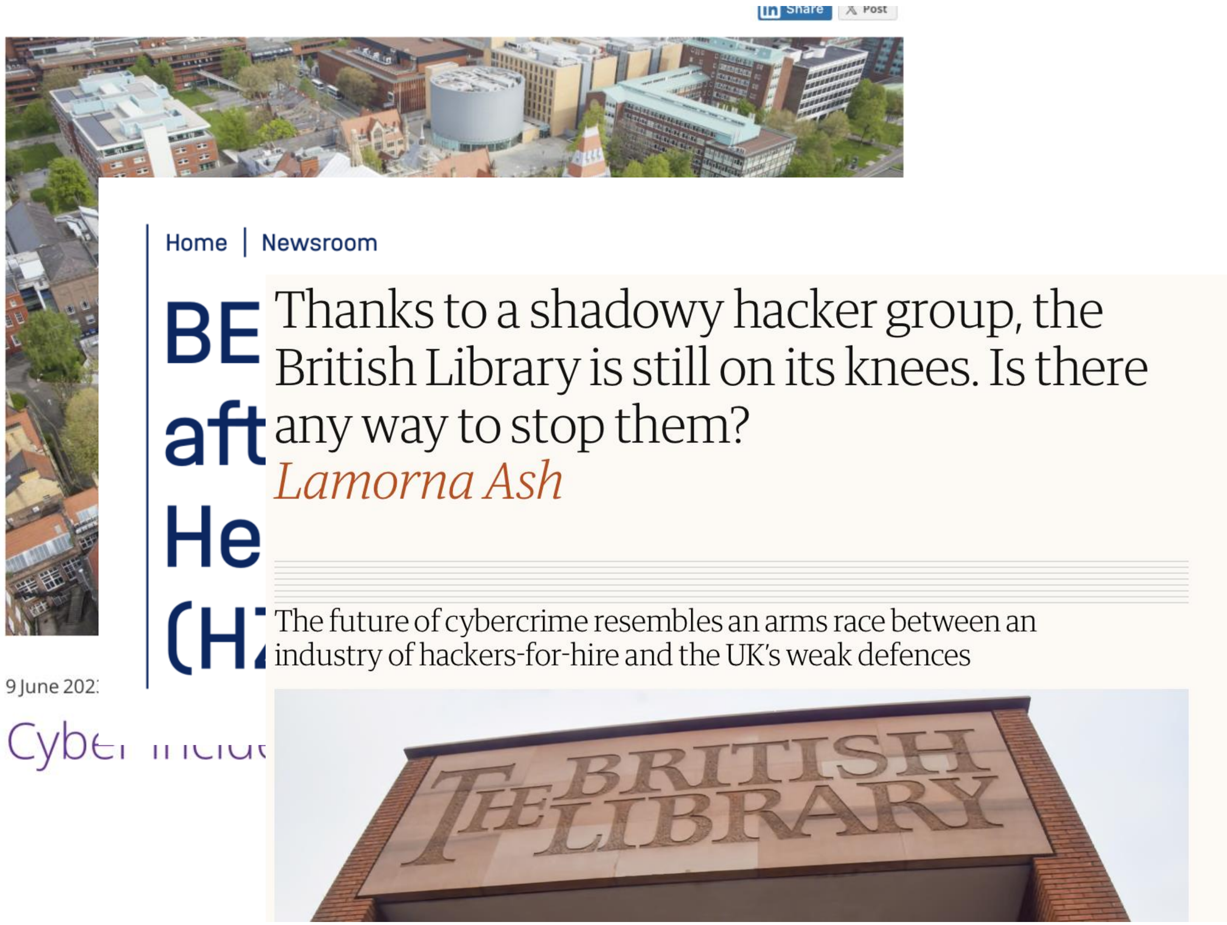
David Crooks (UKRI STFC)

david.crooks@stfc.ac.uk

On behalf of the SOC WG

Landscape

- The risk from cyber attack to organisations in the Research and Education (R&E) sector remains persistent and high
- Many highly visible examples: University of Manchester, British Library, HZB, …



Thanks to a shadowy hacker group, the British Library is still on its knees. Is there any way to stop them?

Lamorna Ash

The future of cybercrime resembles an arms race between an industry of hackers-for-hire and the UK's weak defences

What is the scope of our work?

- We must work together to improve the cybersecurity posture of our organisations and infrastructures.

- Before focusing on operational security tools, pause to consider the full scope of the work to be done in this area

- Must have clear picture of this scope, and then make a plan to execute.

Developing strategy and plans

- Introduce two tools that could be of use in building a vision and strategic plan for an organization – or infrastructure

- Trusted CI Framework

- NIST Cybersecurity Framework
  - (as example; other frameworks exist!)

Trusted CI

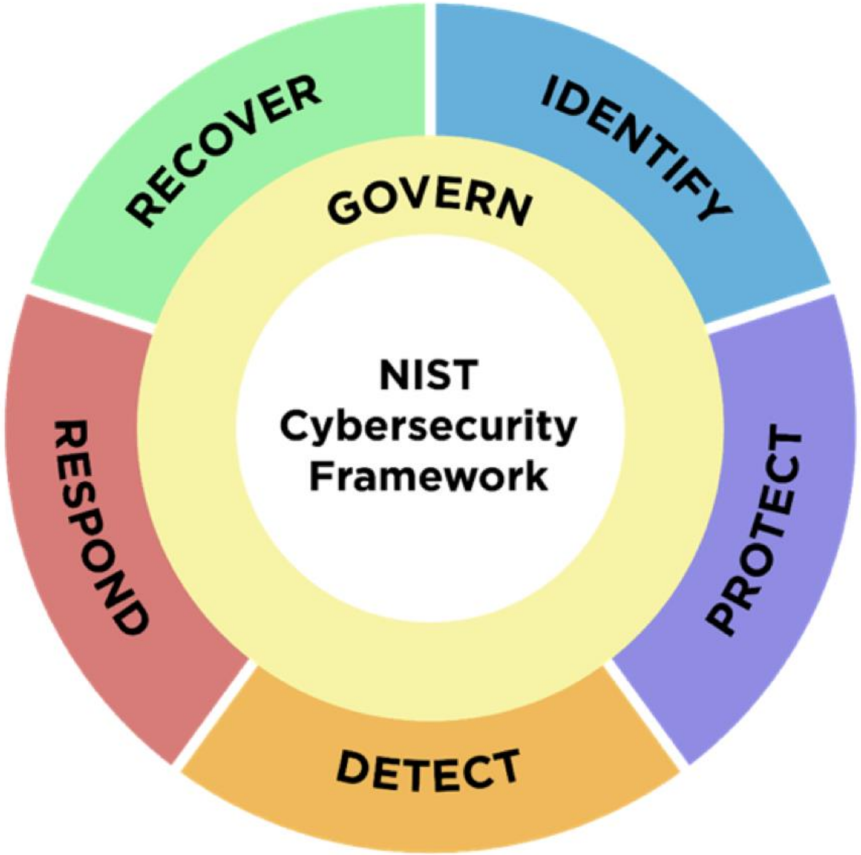
- Trusted CI is the NSF Cybersecurity Center of Excellence
- Cybersecurity experts with experience working with US science and engineering communities
- The team draws from best operational practices and includes leaders in the research and development of new methodologies and high-quality implementations.

Trusted CI Framework

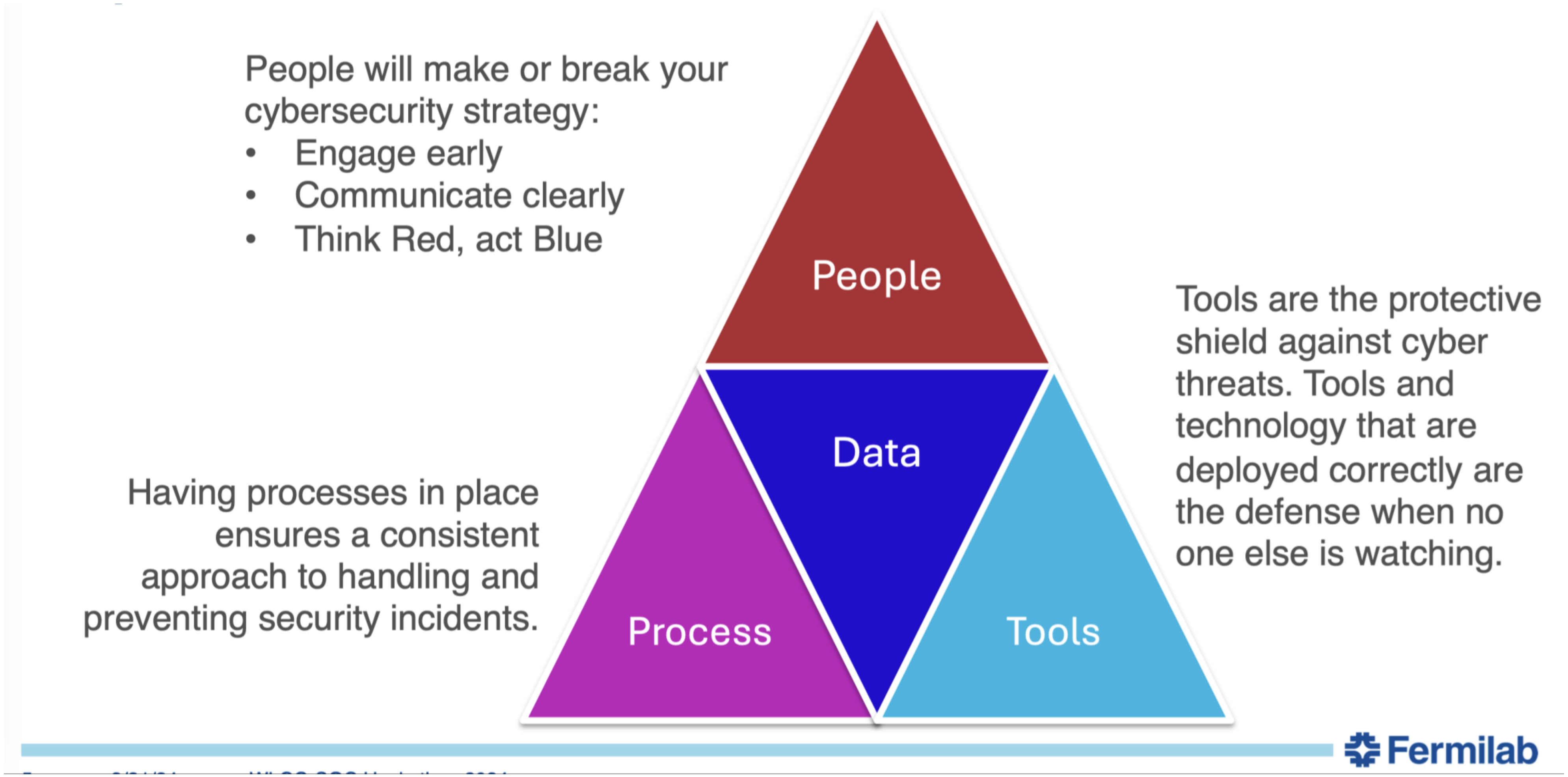
- Trusted CI Framework
  - An approach to support organisations building cybersecurity programmes and strategic plans. Specifically agnostic of other cybersecurity frameworks and technology, this could be of interest for the DRI
  - Representation on Advisory Board by Dave Kelsey on behalf of the WISE Community
    - International involvement
  - 4 pillars: Mission Alignment, Governance, Resources, and Controls
  - 16 “Musts”: Concrete requirements for establishing a cybersecurity program

NIST Cybersecurity Framework

- GOVERN
- IDENTIFY
- PROTECT
- **DETECT**
- RESPOND
- RECOVER



People, Process, Tools and Data



People will make or break your cybersecurity strategy:

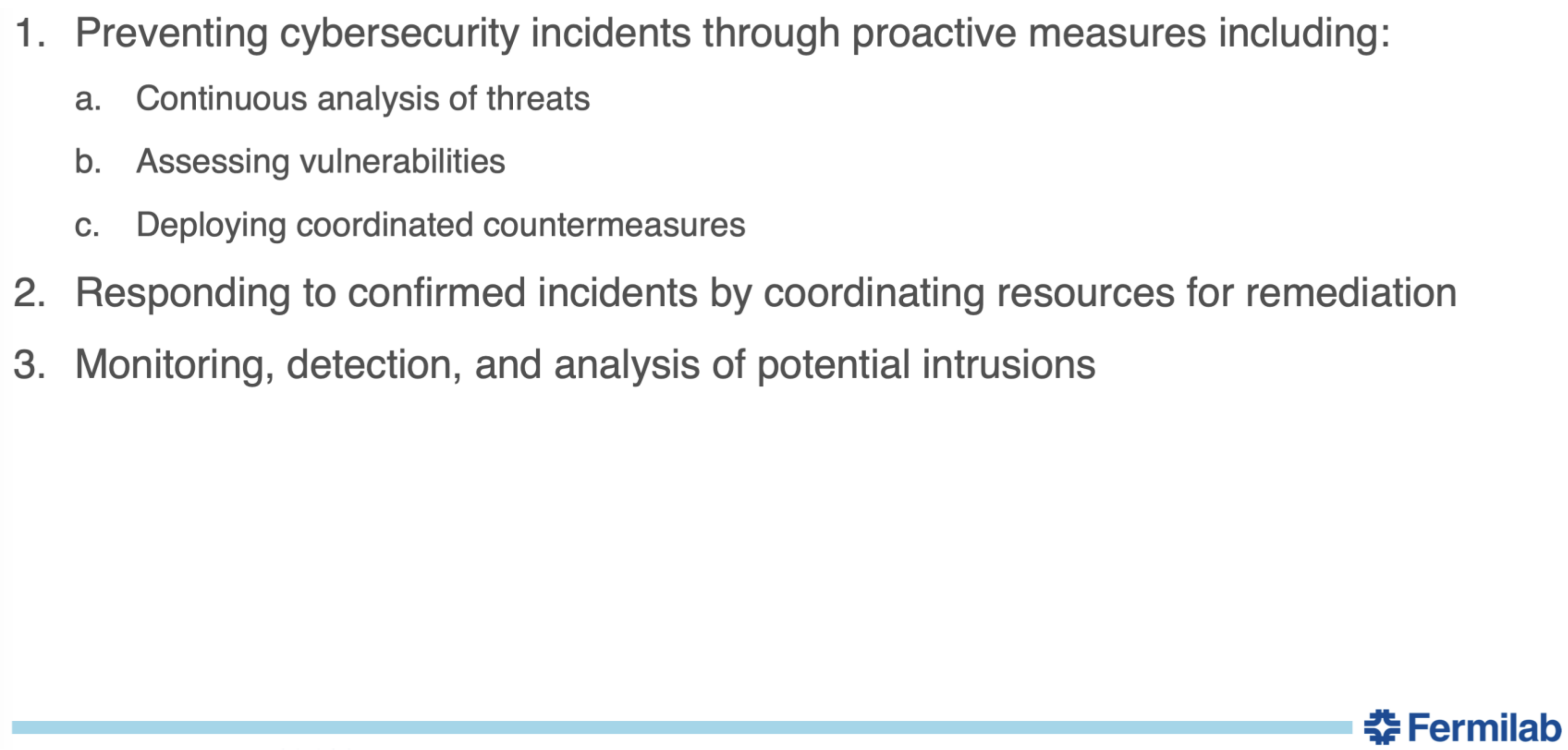
- Engage early
- Communicate clearly
- Think Red, act Blue

Having processes in place ensures a consistent approach to handling and preventing security incidents.

Tools are the protective shield against cyber threats. Tools and technology that are deployed correctly are the defense when no one else is watching.

Let’s talk People and Process

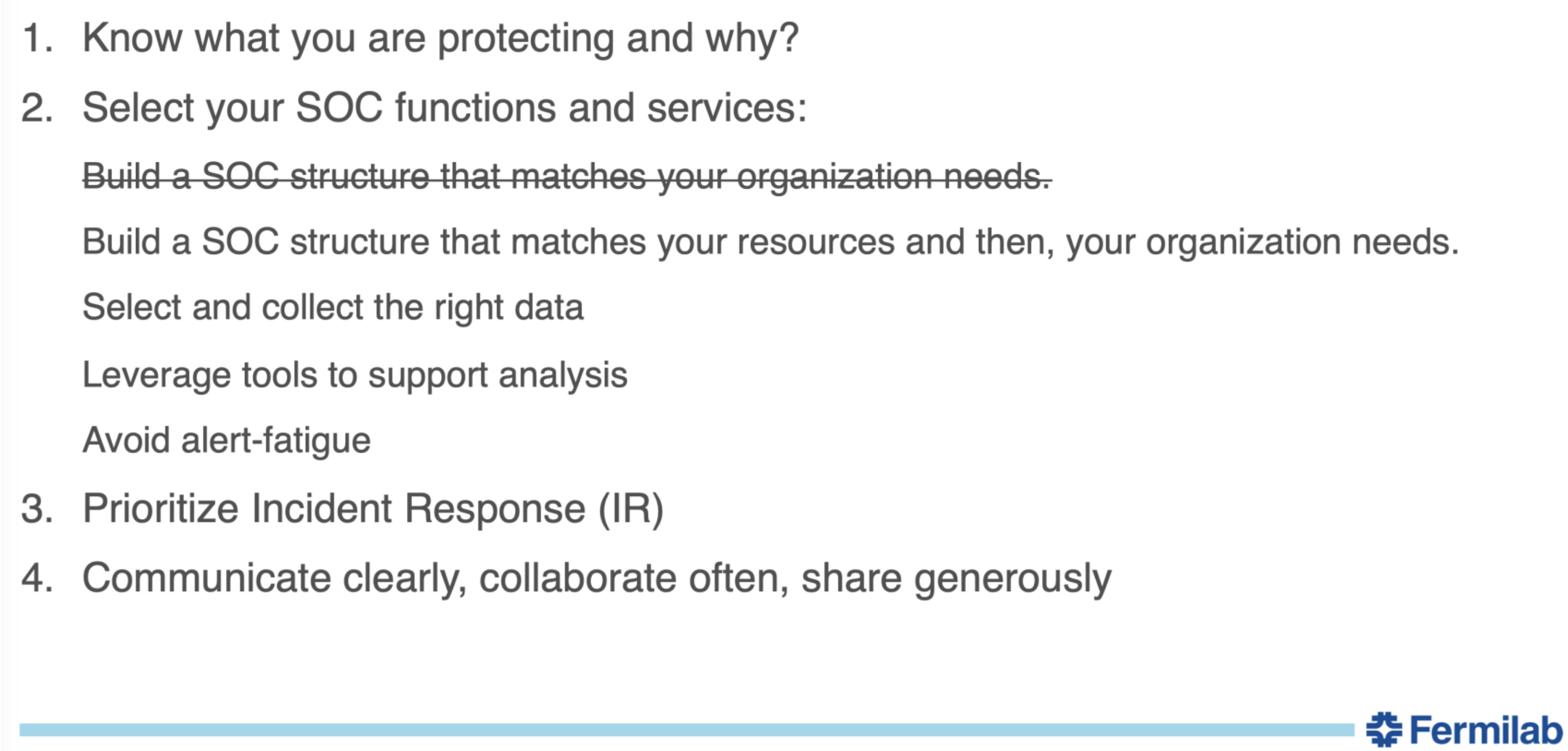
SOC Processes



1. Preventing cybersecurity incidents through proactive measures including:
   a. Continuous analysis of threats
   b. Assessing vulnerabilities
   c. Deploying coordinated countermeasures
2. Responding to confirmed incidents by coordinating resources for remediation
3. Monitoring, detection, and analysis of potential intrusions

Let’s talk People and Process

The People Component



1. Know what you are protecting and why?
2. Select your SOC functions and services:

   ~~Build a SOC structure that matches your organization needs.~~

   Build a SOC structure that matches your resources and then, your organization needs.

   Select and collect the right data

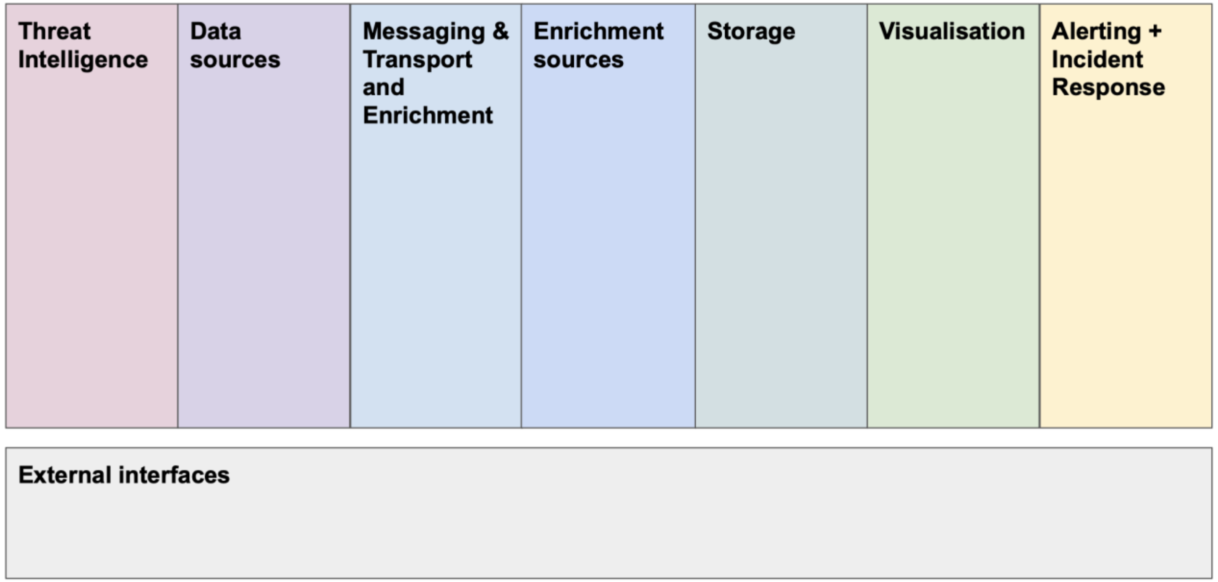
   Leverage tools to support analysis

   Avoid alert-fatigue
3. Prioritize Incident Response (IR)
4. Communicate clearly, collaborate often, share generously

Let’s talk People and Process

SOC Models

- Since last CHEP, new reference designs for Security Operations Centres (SOCs) by SOC WG.
- Focus here on identifying ways forward for majority of sites where deploying full-scale facility is not practicable (or not without central support, etc…)



Threat Intelligence

Data sources

Messaging & Transport and Enrichment

Enrichment sources

Storage

Visualisation

Alerting + Incident Response

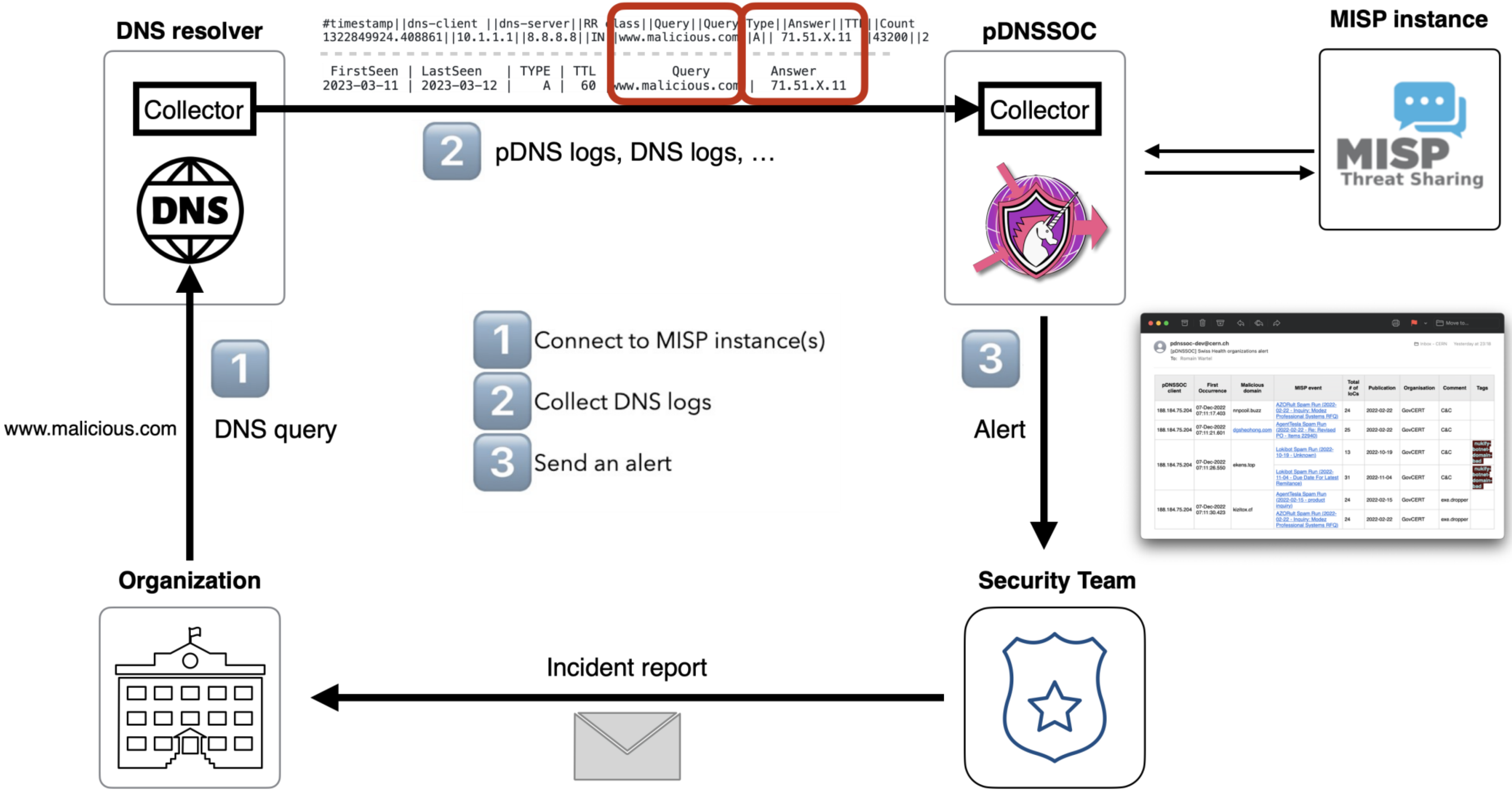
External interfaces

[Collaborative Operational Security: The future of Cybersecurity for Research and Education]

pDNSSOC

- pDNSSOC is a lightweight “80% SOC” solution focused on correlating DNS logs with Threat Intelligence
- Specifically designed to be low impact to deploying site
  - Minimum deployment is a sensor installed in DNS infrastructure
  - Does require external centre performing correlation and alerting

pDNSSOC outline



```
#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
```

1 Connect to MISP instance(s)

2 Collect DNS logs

3 Send an alert

pdnssoc-dev@cern.ch
[pDNSSOC] Swiss Health organizations alert
To: Romain Wartel

Inbox - CERN   Yesterday at 23:18

pDNSSOC client	First Occurrence	Malicious domain	MISP event	Total # of IoCs	Publication	Organisation	Comment	Tags
188.184.75.204	07-Dec-2022 07:11:17.403	nnpooil.buzz	AZORult Spam Run (2022-02-22 - Inquiry: Modez Professional Systems RFQ)	24	2022-02-22	GovCERT	C&C	
188.184.75.204	07-Dec-2022 07:11:21.601	dgsheohong.com	AgentTesla Spam Run (2022-02-22 - Re: Revised PO - Items 22940)	25	2022-02-22	GovCERT	C&C	
188.184.75.204	07-Dec-2022 07:11:26.550	ekens.top	Lokibot Spam Run (2022-10-19 - Unknown)	13	2022-10-19	GovCERT	C&C	nukify-botnet-domain-bad
			Lokibot Spam Run (2022-11-04 - Due Date For Latest Remitance)	31	2022-11-04	GovCERT	C&C	nukify-botnet-domain-bad
188.184.75.204	07-Dec-2022 07:11:30.423	kizitox.cf	AgentTesla Spam Run (2022-02-15 - product inquiry)	24	2022-02-15	GovCERT	exe.dropper	
			AZORult Spam Run (2022-02-22 - Inquiry: Modez Professional Systems RFQ)	24	2022-02-22	GovCERT	exe.dropper	

pDNSSOC status

- Work underway using pDNSSOC in a number of organisations
  - Danish e-infrastructure Consortium (DeiC)
  - RedCLARA: SICURA-LAC]

- Very interested in hearing of other organisations who may wish to help test this solution

- With long term support could be extremely powerful across WLCG

Upcoming meetings

- **This Autumn/Fall!**
  - SOC Hackathon taking place 2-4 December in UK
    - https://indico.cern.ch/event/1441326/
    - Registration closes on Friday
    - Hosted by our friends at Jisc
  - Dedicated SOC session + post-meeting SOC Hackathon @ HEPiX
    - https://indico.cern.ch/event/1450798/
    - Planning actively underway

Summary

- The deployment of security tools has to sit within an overall cybersecurity plan
  - Tools and frameworks available to help in the development of this

- Technological solutions require understanding of processes and people

- pDNSSOC is an option for deploying lightweight monitoring across a broad scope
  - Further testing need and volunteers welcome!

Questions?