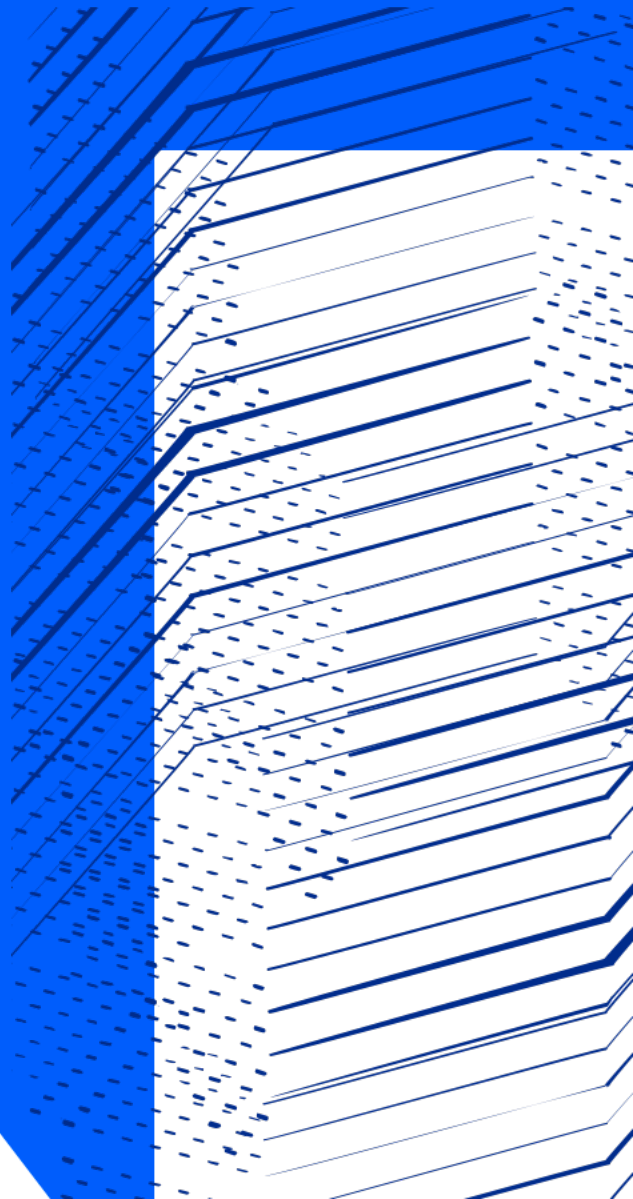
Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics



GridPP Security

David Crooks
david.crooks@stfc.ac.uk

GridPP 47, March 2022, Durham

Overview

1 Landscape

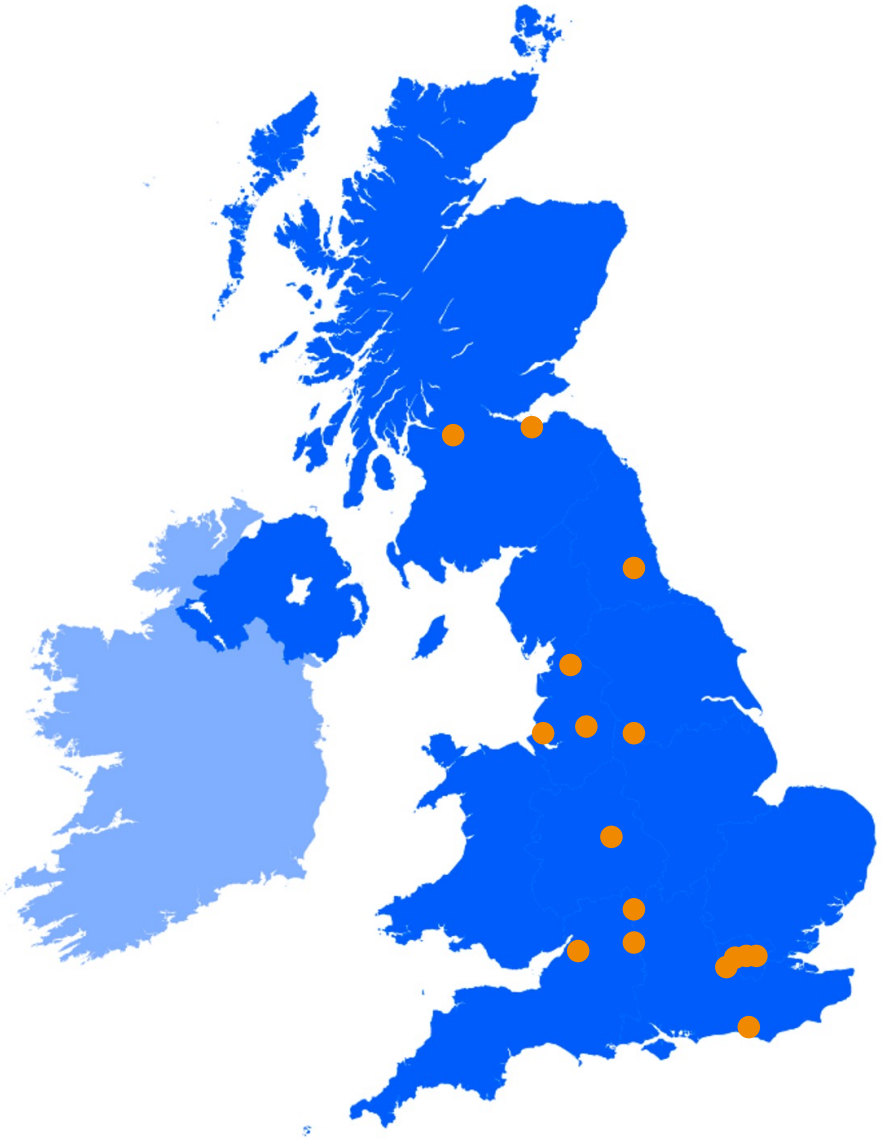
2 SVG update

3 CSIRT update

4 SOC updates

5 pDNS SOC

6 Next steps/conclusions



Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

Landscape

Landscape

- While broadly landscape is similar to 6 months ago, current events have focused the need for increased cybersecurity readiness

- Important for GridPP that we do this in a well-considered fashion. Make sure you:
  - have your incident response plans to hand
  - have your patching processes up to date
  - understand your authorisation mechanisms

Science and Technology Facilities Council

Scientific Computing

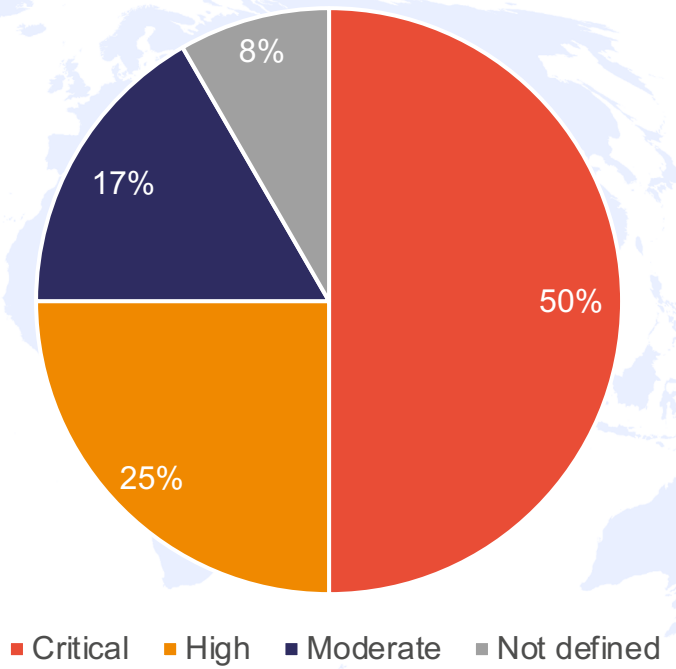
GridPP

UK Computing for Particle Physics

SVG update

SVG: Vulnerability issue handling

- Since Sept 2021
  - 32 Tickets created
  - 12 advisories issued to sites
  - **6 Critical**
  - 3 High
  - 2 Moderate
  - 1 not defined
- Some have multiple updates
- Should now use https://advisories.egi.eu after migration from older wiki platform



SVG Evolution: Deployment Experts Group

- Evolution of SVG process to include the DEG continues
- Ask for approval from OMB

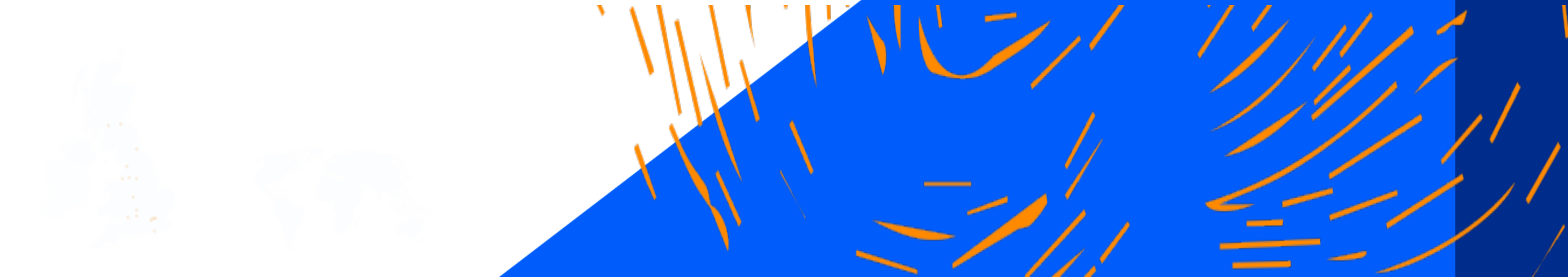
Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

Operational Security update



IRIS/GridPP Security Team update

- No incidents impacting GridPP since Sep 2021
- Vulnerability assessment reports continue to be really useful
  - Considering how we can improve this in the future

- Becoming increasingly clear that we really need a ticket system/collaborative space that can be used across GridPP/IRIS

Training

- Training is a key area of development
  - Thematic CERN School of Computing
  - STFC
  - GridPP
  - IRIS

- Aim for materials that we can reuse for GridPP/other purposes

- A syllabus is important!

EGI CSIRT SSC Update

- A quick SSC update
- There won’t be a challenge in March (!)
- We are now looking for alternative dates this year
- Very important that we have the preparation in place to undertake an effective challenge

UKRI STFC perspective

- STFC and UKRI are undergoing a process of a greatly increased priority for cybersecurity
  - What processes do we need?
  - What people do we need?
  - What technology do we need?

- For GridPP
  - The needs of GridPP/WLCG are being placed clearly as part of these plans
  - Make sure that GridPP benefits from additional capabilities
    - STFC SOC/MISP…

Wellbeing / Security Team capabilities

- Security work has a notable risk to act as a stressor for staff
  - Repeated, urgent requests

- Work this year on additional areas the security team can support sites
  - Centralised monitoring services, etc…
  - **Leading to resource needs**

Pakiti

- EGI CSIRT now uses Pakiti v3

- New capability: sync CVE tagging with downstream pakiti instances, eg…
  - STFC central instance
  - Glasgow

- Are other sites interested in trying this out?
- Aim for something that all sites can/should use

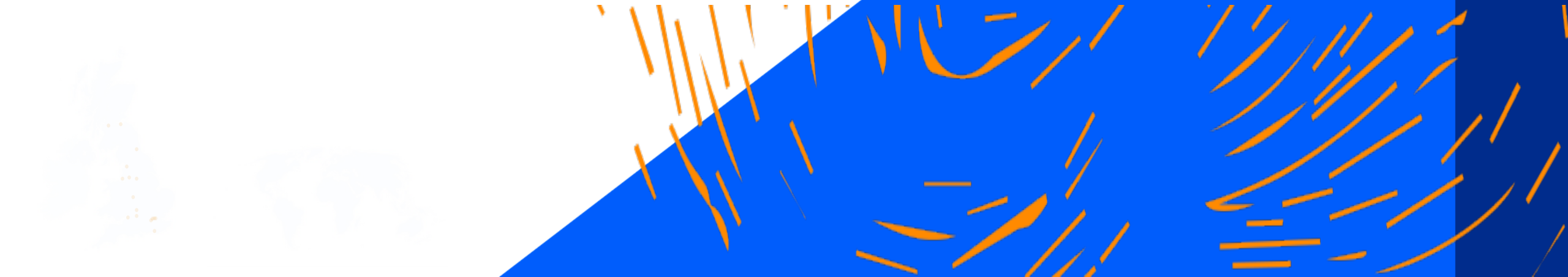
Science and Technology Facilities Council

Scientific Computing

GridPP

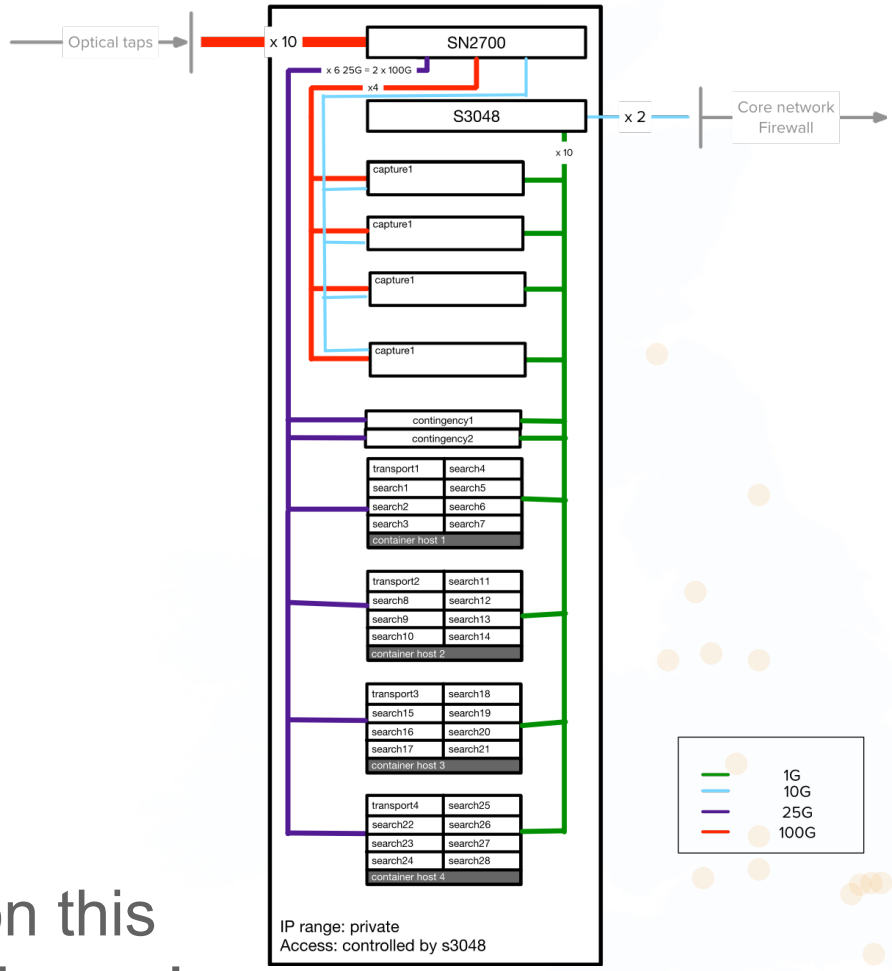
UK Computing for Particle Physics

SOC updates



STFC SOC update

- All hardware installed
- Network taps in place and ready for use
  - Start with LHCOPN link first
- Internal networking mostly prepared
- Deployment config in testing
  - Plan to deploy Zeek node very soon
- Thanks to Olivier who worked last 6 months on this
  - Welcome to Liam and James who are joining us!

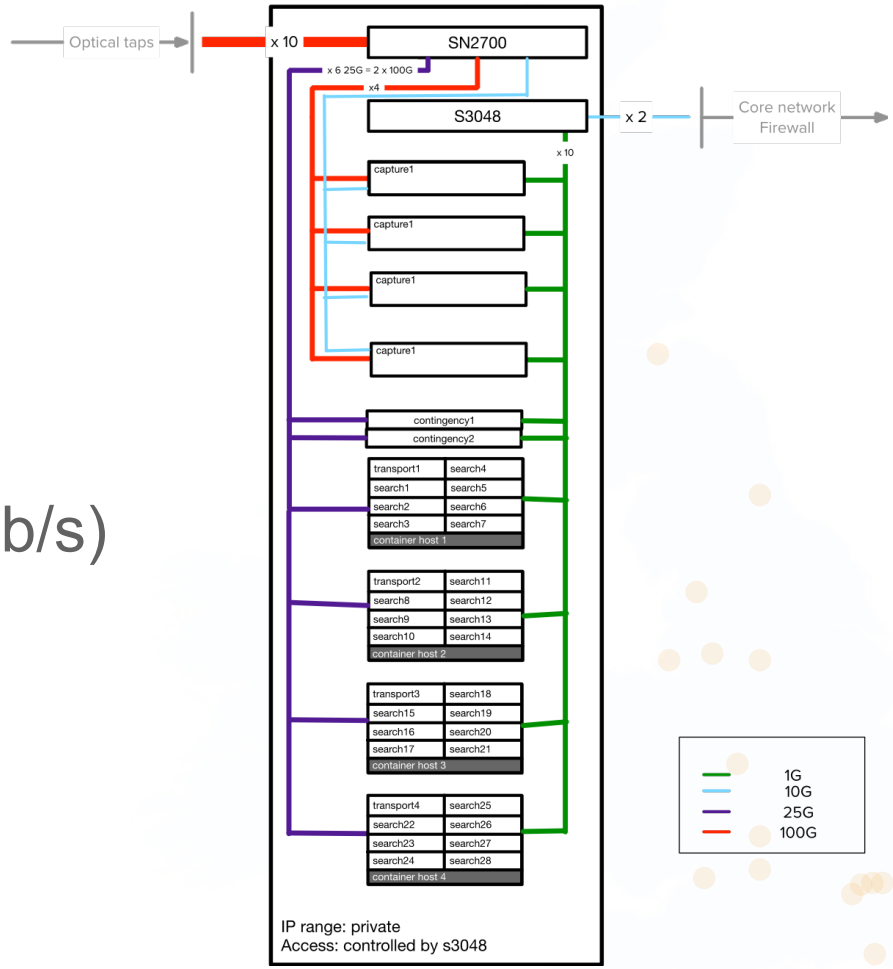


Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

STFC SOC zeek worker nodes

- 4 x zeek worker nodes each with:
  - 2 x 7H12 AMD (2 x 64 physical cores)
  - 1 TB RAM
  - 4TB SSD
  - 2 x ConnectX-6 100Gb/s cards (4 x 100 Gb/s)
  - 1 x Intel 25/10 Gb/s card (4 x 25/10 Gb/s)



Threat intelligence update

- Almost all Threat Intelligence contacts have access to the central R&E MISP instance
  - Small number of well-understood issues

- Plan for additional technical meeting (after Easter) to look more at using this intelligence

Wider SOC update

- SOC WG update at ISGC
- Initial work on Kubernetes SOC (CERN)
- Work on HA SOC services at Nikhef
- Share links to these once they are available

Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

pDNS SOC

Motivation

- Building a SOC is hard
  - Setting up a fully-fledged threat intelligence platform is extremely difficult for most sites
  - Deploying network monitoring + threat intelligence infrastructure is an unrealistic scenario for many sites
  - Only a very small fraction of WLCG sites have a production SOC

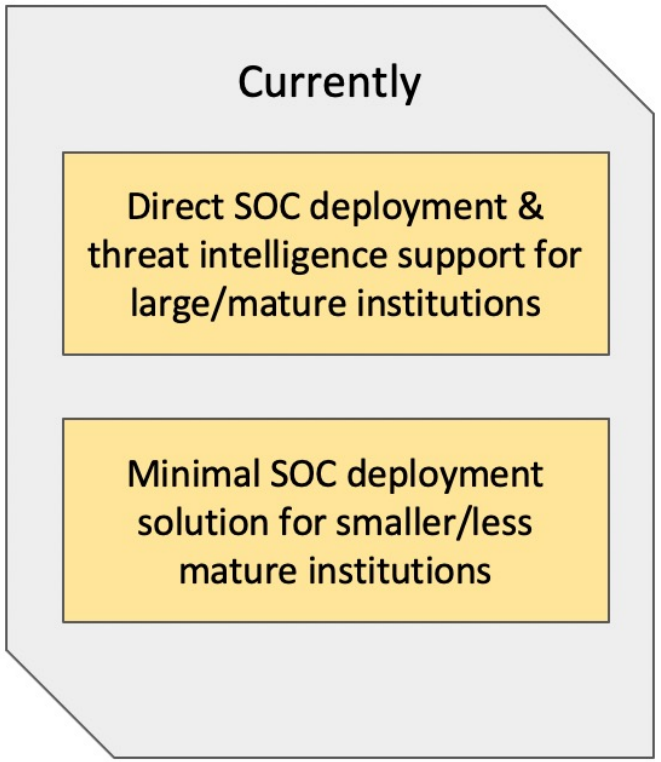
We have to lower the entry barrier

Passive DNS

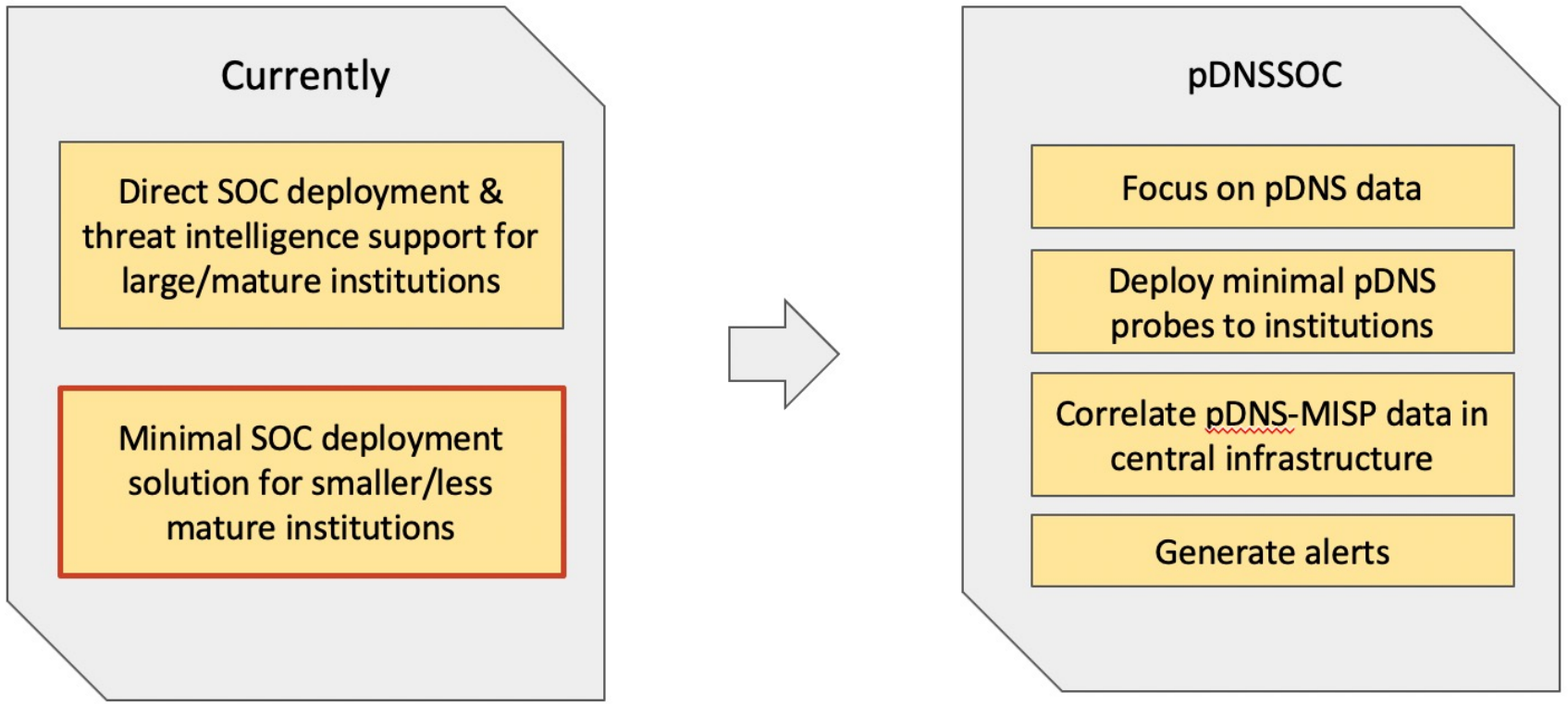
- What is passive DNS?
  - Historical DNS records originating from DNS server probes
  - Only DNS record - domain associations stored
  - DNS client information is stripped out, preserving privacy

- How can passive DNS data be useful?
  - Detect traffic to well-known malicious websites
  - Used in incident response lifecycle
  - Historical details beyond standard DNS

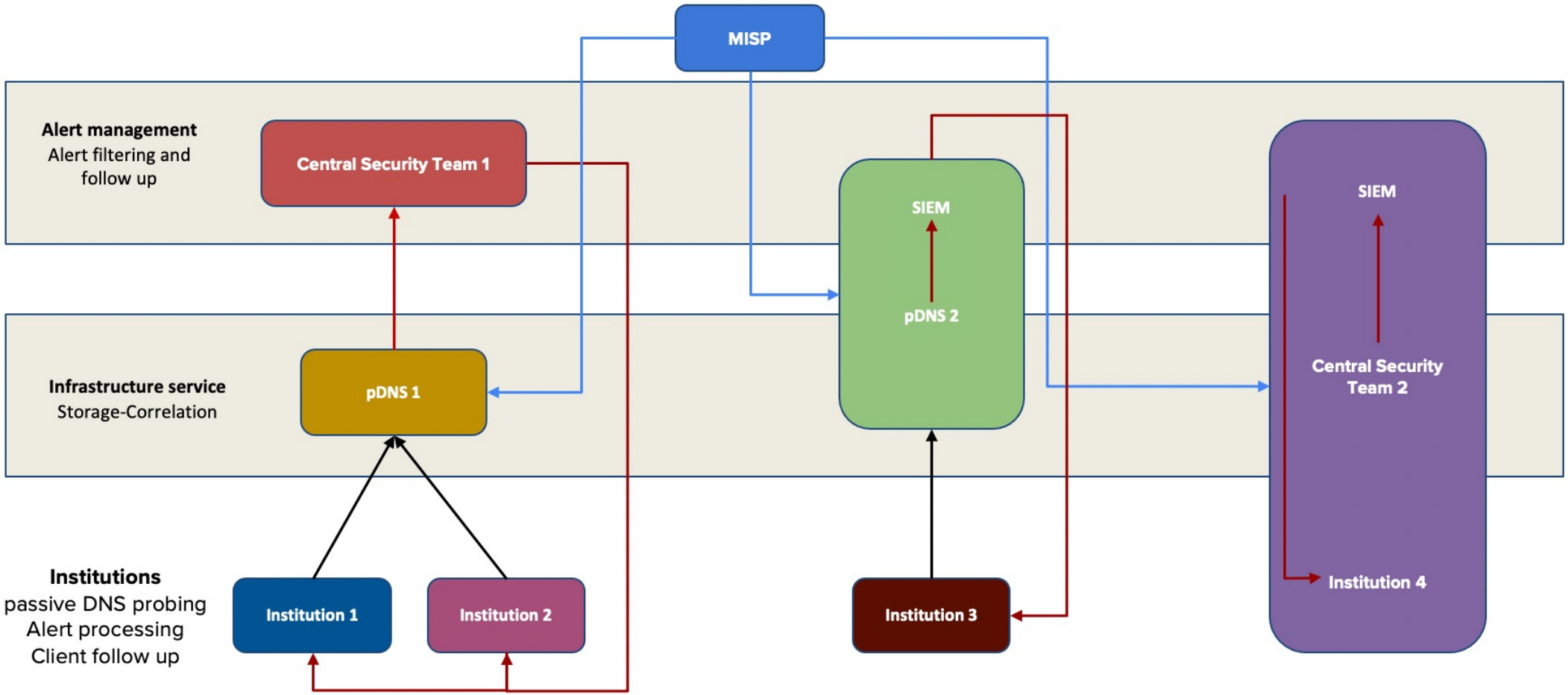
Current approach



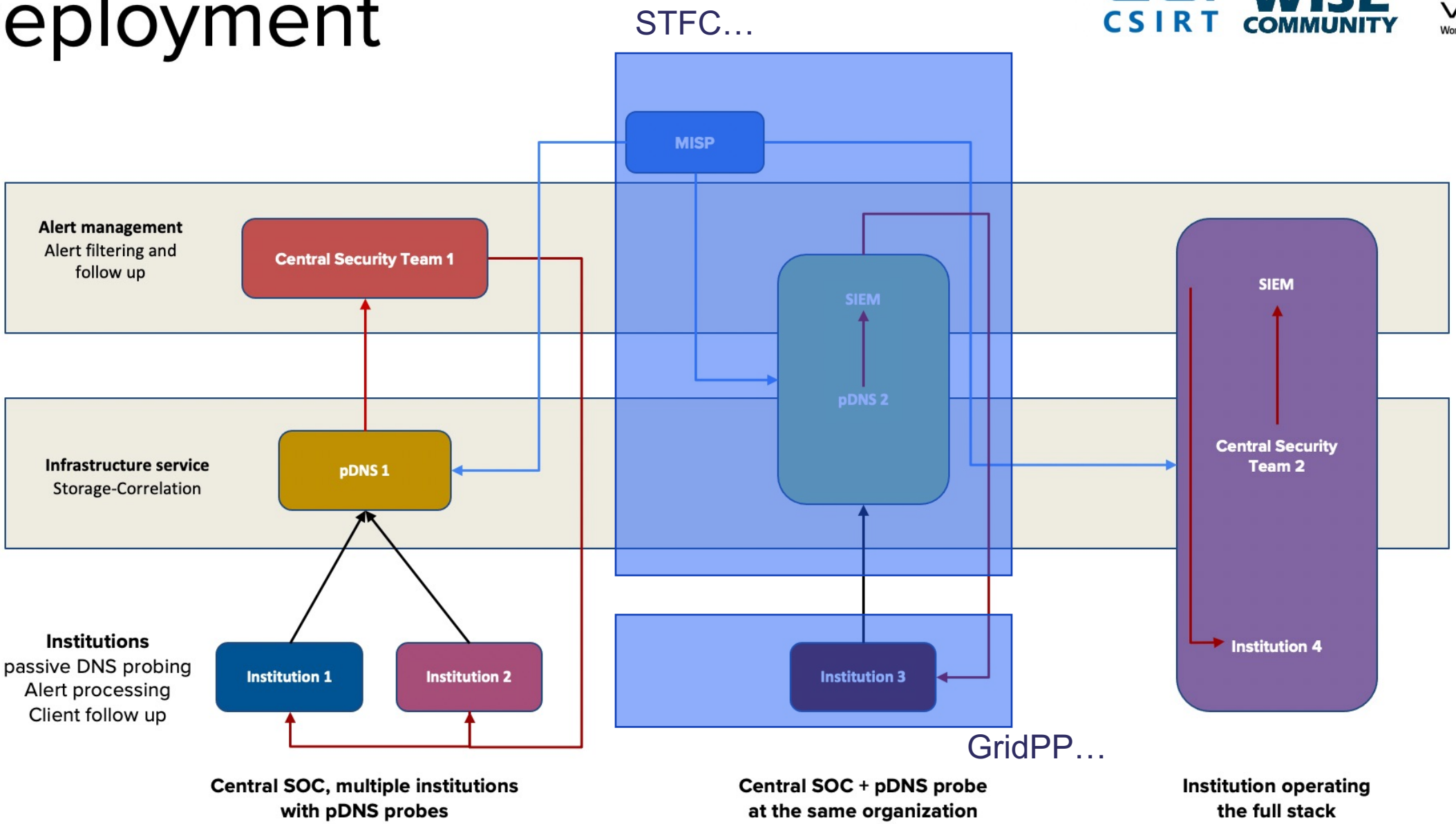
Passive DNS(pDNS) based SOC



Deployment


MISP
Alert management
Alert filtering and follow up
Central Security Team 1
SIEM
pDNS 2
SIEM
Central Security Team 2
Infrastructure service
Storage-Correlation
pDNS 1
Institutions
passive DNS probing
Alert processing
Client follow up
Institution 1
Institution 2
Institution 3
Institution 4
Central SOC, multiple institutions with pDNS probes
Central SOC + pDNS probe at the same organization
Institution operating the full stack

Deployment


STFC…
MISP
Alert management
Alert filtering and follow up
Central Security Team 1
SIEM
pDNS 2
SIEM
Infrastructure service
Storage-Correlation
pDNS 1
Central Security Team 2
Institutions
passive DNS probing
Alert processing
Client follow up
Institution 1
Institution 2
Institution 3
Institution 4
GridPP…
Central SOC, multiple institutions with pDNS probes
Central SOC + pDNS probe at the same organization
Institution operating the full stack

Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

Next steps / Conclusion

Next steps

1. *Access central threat intelligence by all GridPP/IRIS sites*
2. **Central logging review at all sites**
   - **Anticipate that many / all will have this in place**

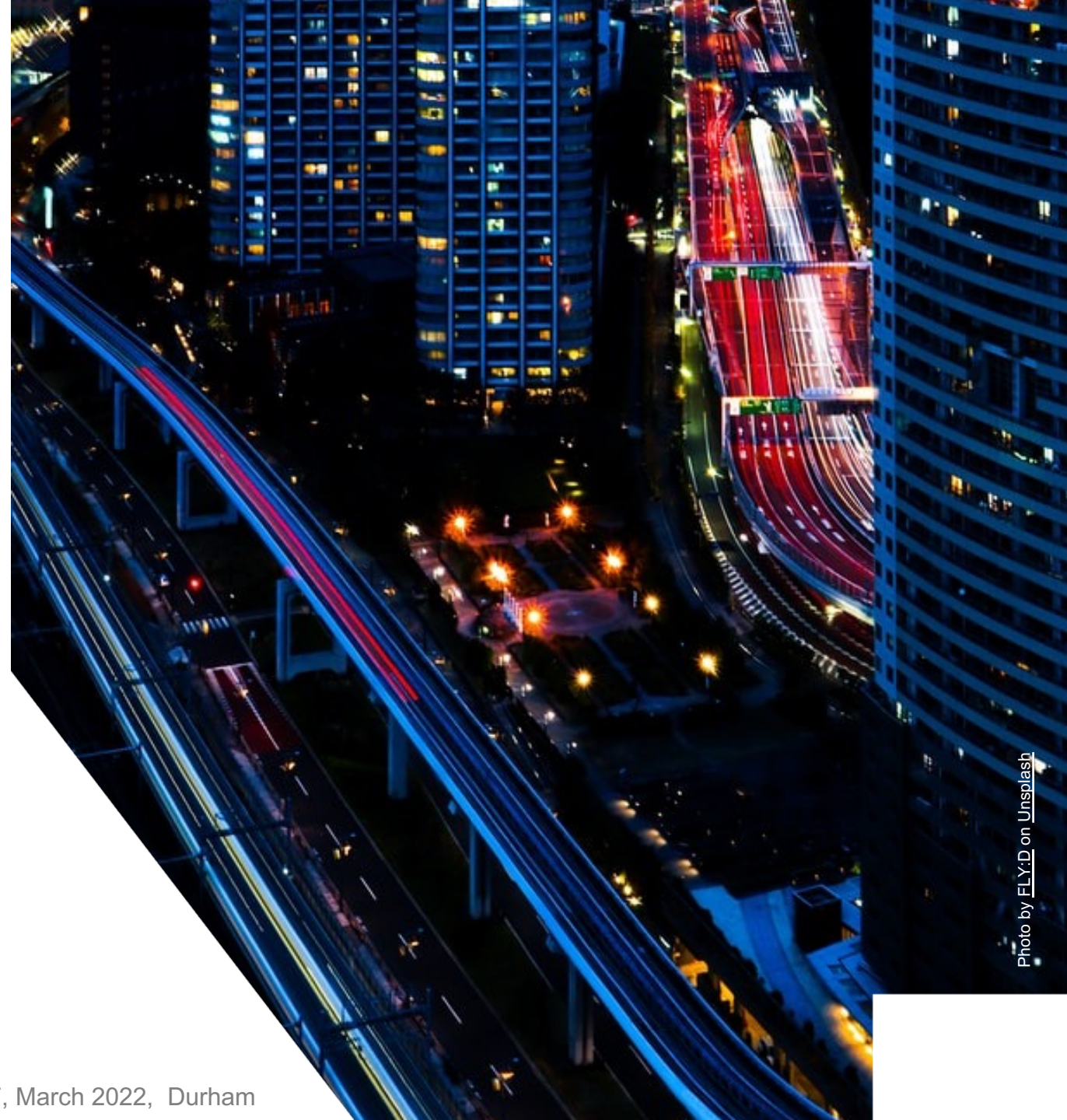


Photo by FLY:D on Unsplash

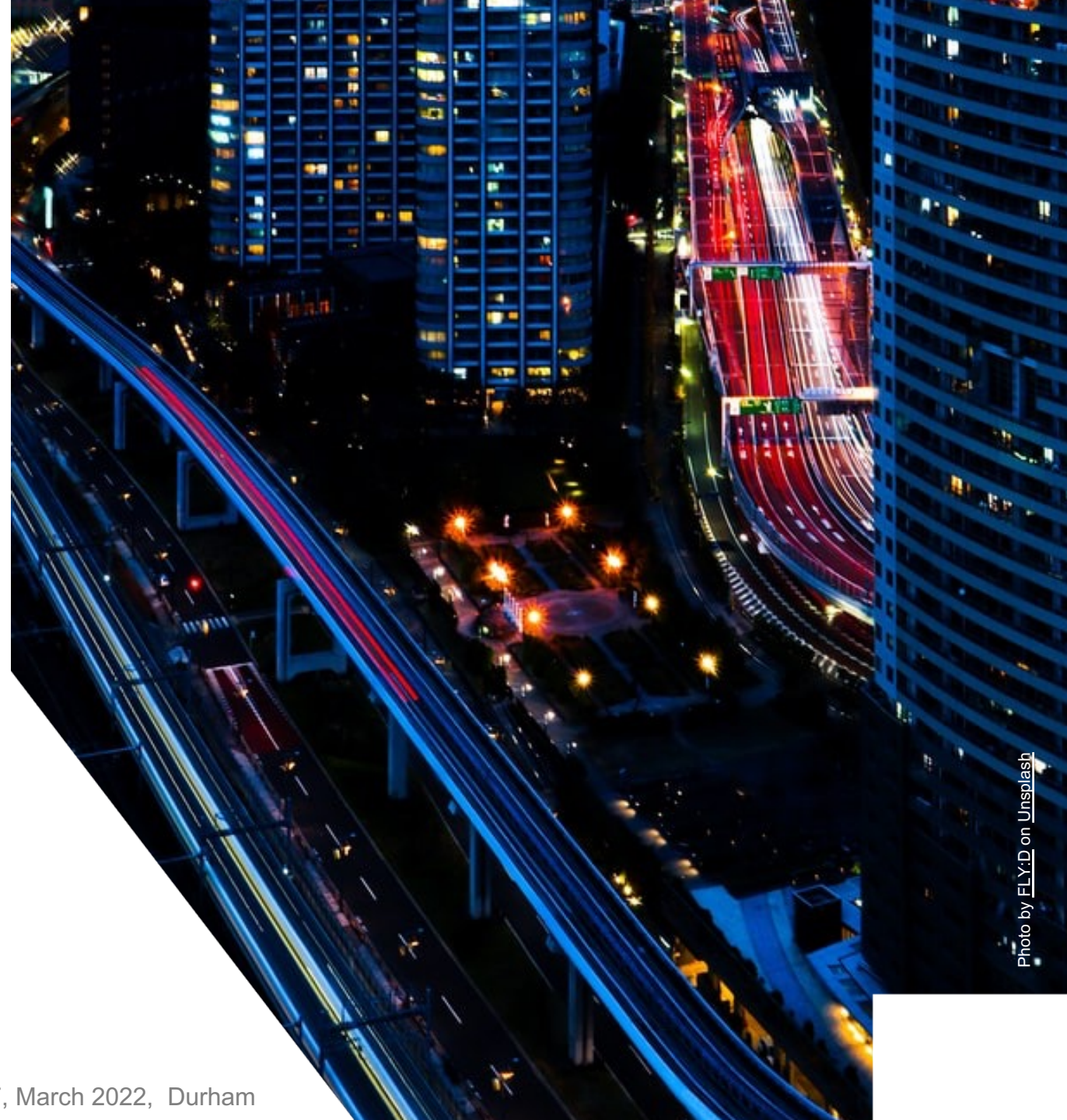
Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Conclusions

- Cybersecurity readiness is of immediate importance
  - Essential for sites to prepare **but**
  - Prepare carefully
    - Continuous sprinting is not useful
    - Long term processes are key

- (Inter)national context continues to be vital
  - What steps are your organisations taking?



Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Science and Technology Facilities Council

Scientific Computing

Questions?