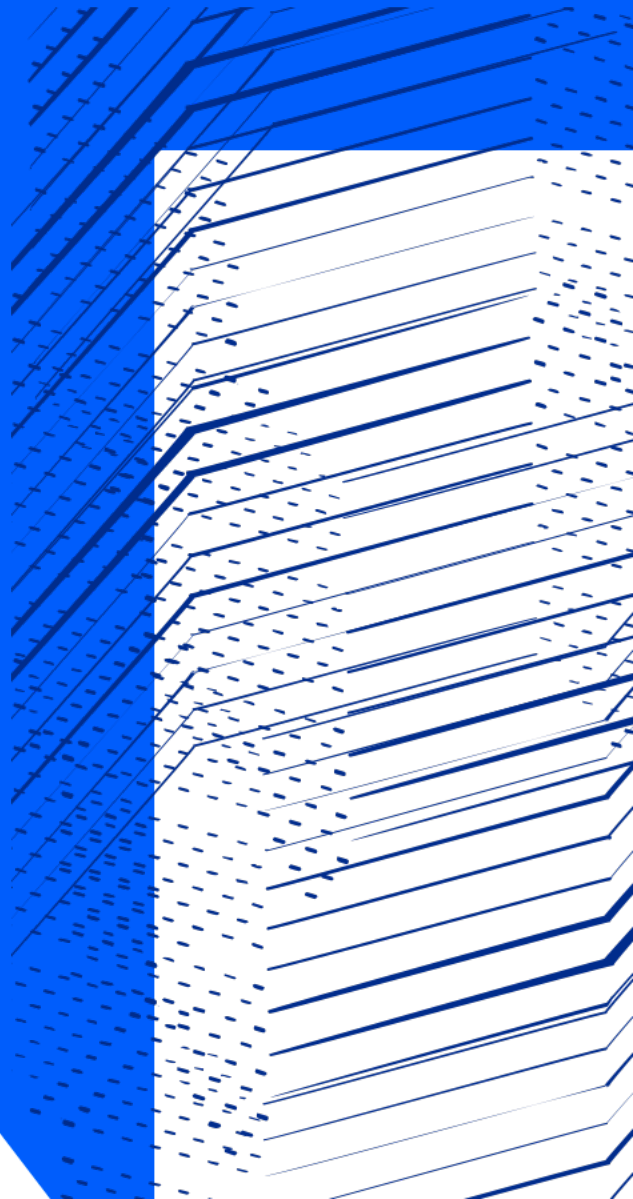
Science and Technology Facilities Council

Cybersecurity

David Crooks
david.crooks@stfc.ac.uk

GridPP Security Officer
Chair, STFC Cybersecurity Group
Project Leader, DRI Cybersecurity

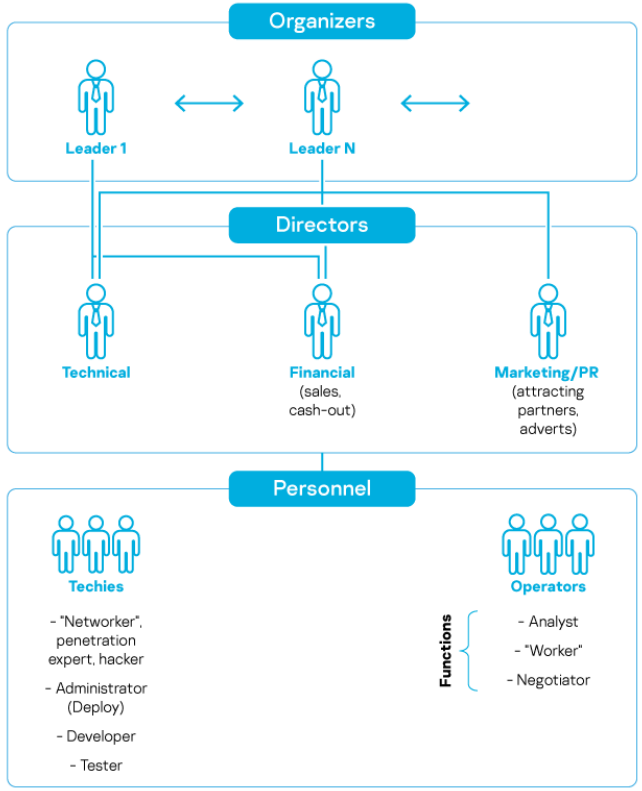


Modern cybersecurity environment

- The world has changed
  - In the past, biggest risk for academic security
  - Relatively simple, untargeted attacks
  - Belief that research computing was major risk

- This is no longer the case
  - Determined, well-resourced attackers
  - 9-5 jobs working on malware services
  - Phishing and identity theft are major risk
  - Research computing security can be major asset

- Big business: we are targets



kaspersky

Science and Technology Facilities Council

https://securelist.com/russian-speaking-cybercrime-evolution-2016-2021/104656/

UKRI Digital Research Infrastructures

- UKRI Digital research and innovation infrastructure (DRI) underpins the research and innovation ecosystem.
- It enables us to solve problems, and to analyse and understand complex topics on any subject.
- This is possible because digital infrastructure allows us to work with data and computation efficiently and securely, at scale.

UKRI Science and Technology Facilities Council

DRI Cybersecurity

- The cybersecurity risk to the DRI community is now acute having grown in recent years
- We can and must work together, recognising and celebrating the diversity of our research communities
- This project will focus on building trust between DRI participants to share information about ongoing incidents
- To effectively use this information we must have
  - a technical way of sharing information that supports automation
  - fine-grained monitoring, focused on network monitoring in the first instance

UKRI Science and Technology Facilities Council

DRI Cybersecurity

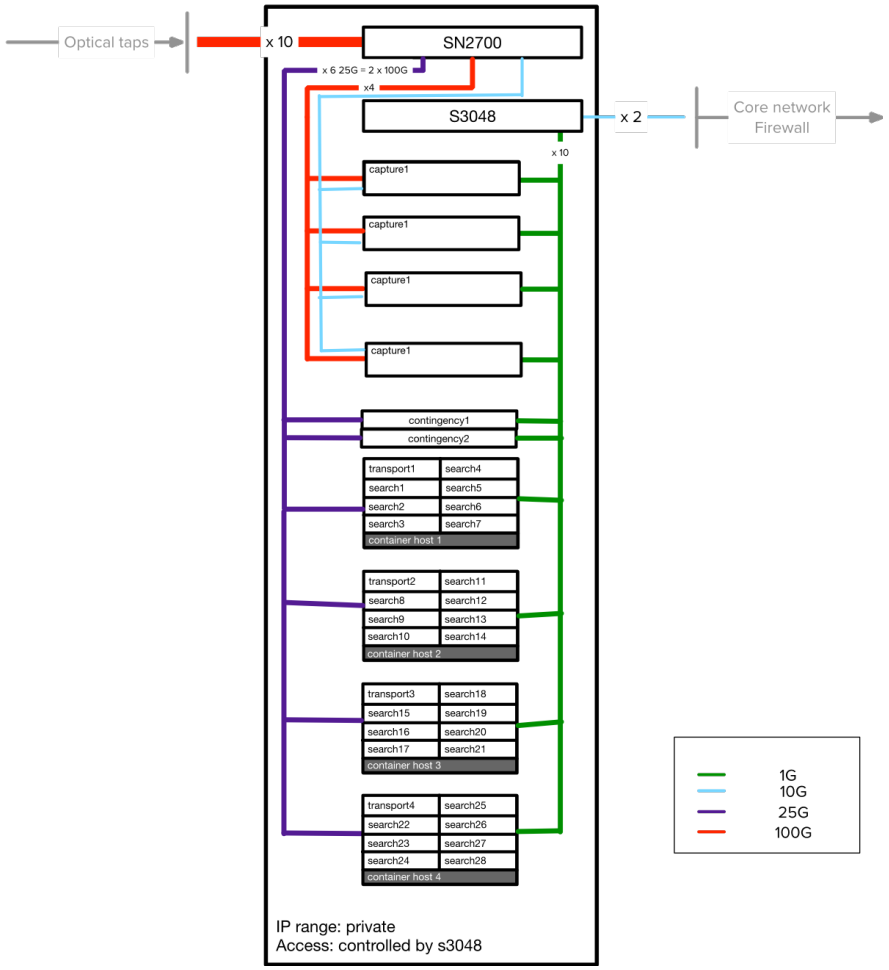
- The cybersecurity risk to the DRI community is now acute having grown in recent years
- We can and must work together, recognising and celebrating the diversity of our research communities
- This project will focus on building trust between DRI participants to share information about ongoing incidents
- To effectively use this information we must have
  - a technical way of sharing information that supports automation
  - **fine-grained monitoring, focused on network monitoring in the first instance**

UKRI Science and Technology Facilities Council

STFC Security Operations Centre Project

- Monitor all STFC-RAL traffic and correlate it with threat intelligence
  - R&E MISP instance hosted by CERN
  - Monitoring will include
    - 2x100Gb/s Janet and
    - 2x100Gb/s LHCOPN links

- Following initial pilot phase, natural progression to other STFC sites
  - Design in discussion

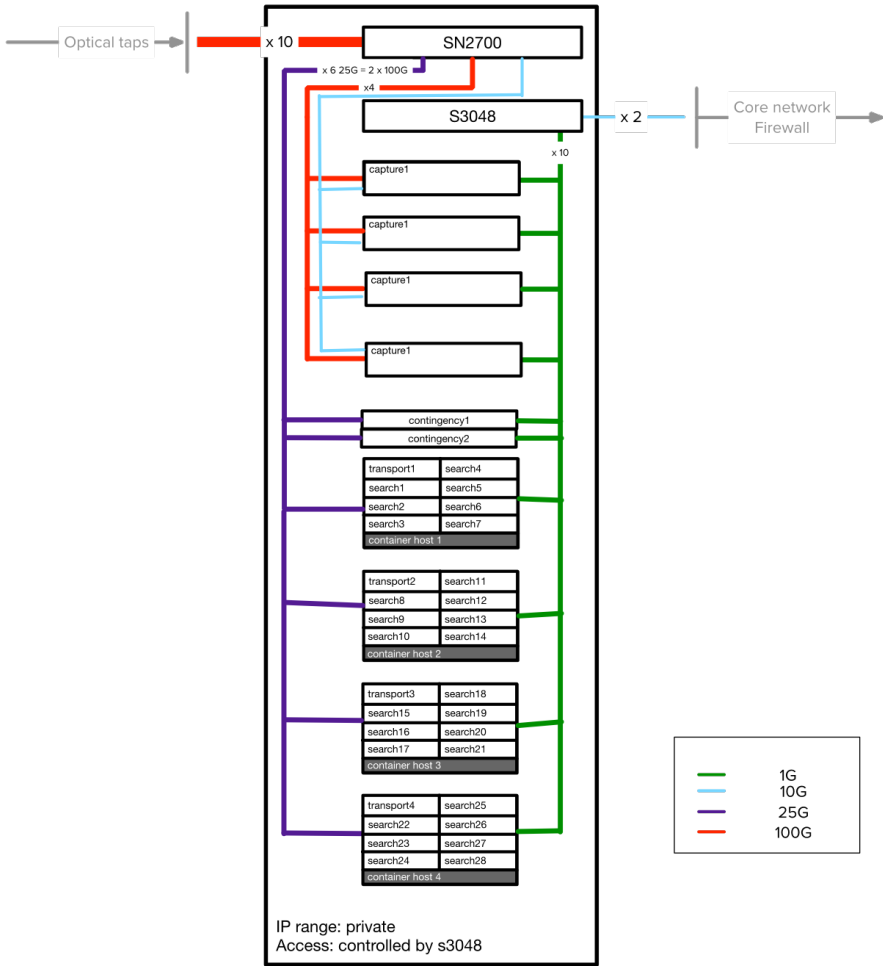


Science and Technology Facilities Council

Hardware config [capture]

- Networking
  - 32x100Gb/s aggregation switch
  - 1Gb/s rack management/admin switch
  - Optical taps

- Network capture nodes x4
  - 256 cores
  - 1TB memory
  - 4TB SSD storage
    - Zeek nIDS is not I/O bound
  - 4x100 Gb/s capture interfaces
  - 25 Gb/s internal networking

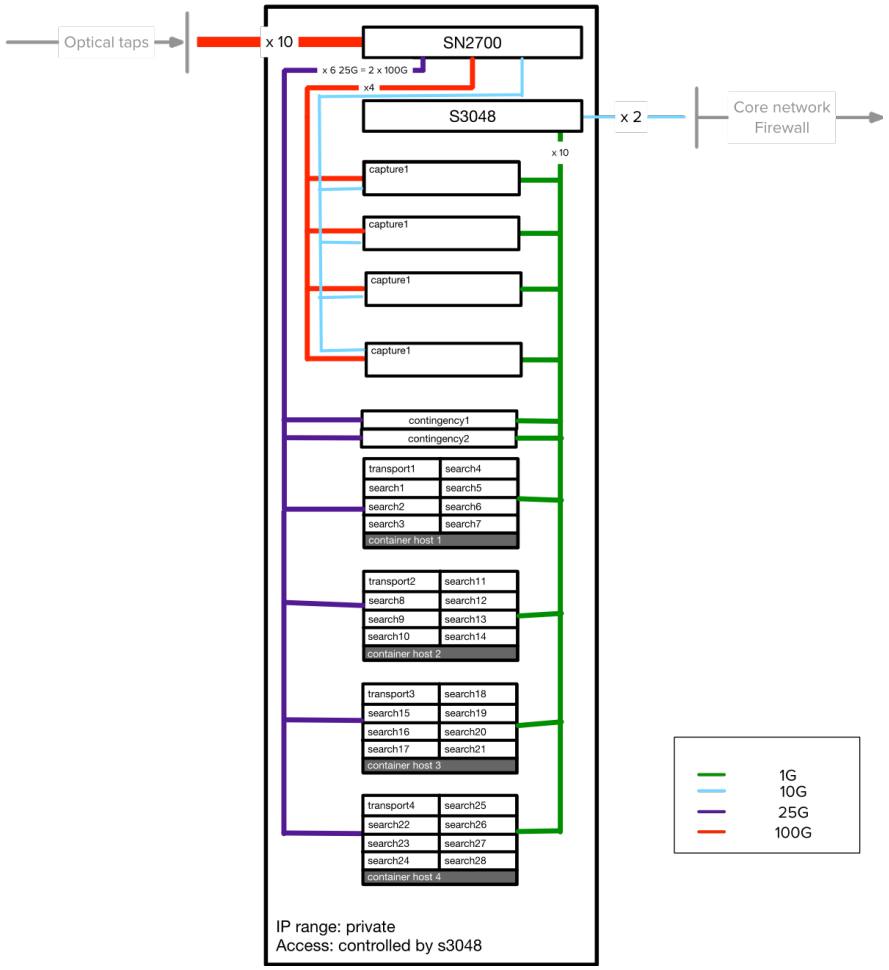


Science and Technology Facilities Council

Hardware config [storage/messaging]

- In-house managed 400GB raw ES cluster
  - Storage nodes x4
    - 48 cores
    - 1TB memory
    - 96TB SSD storage
    - 25 Gb/s networking

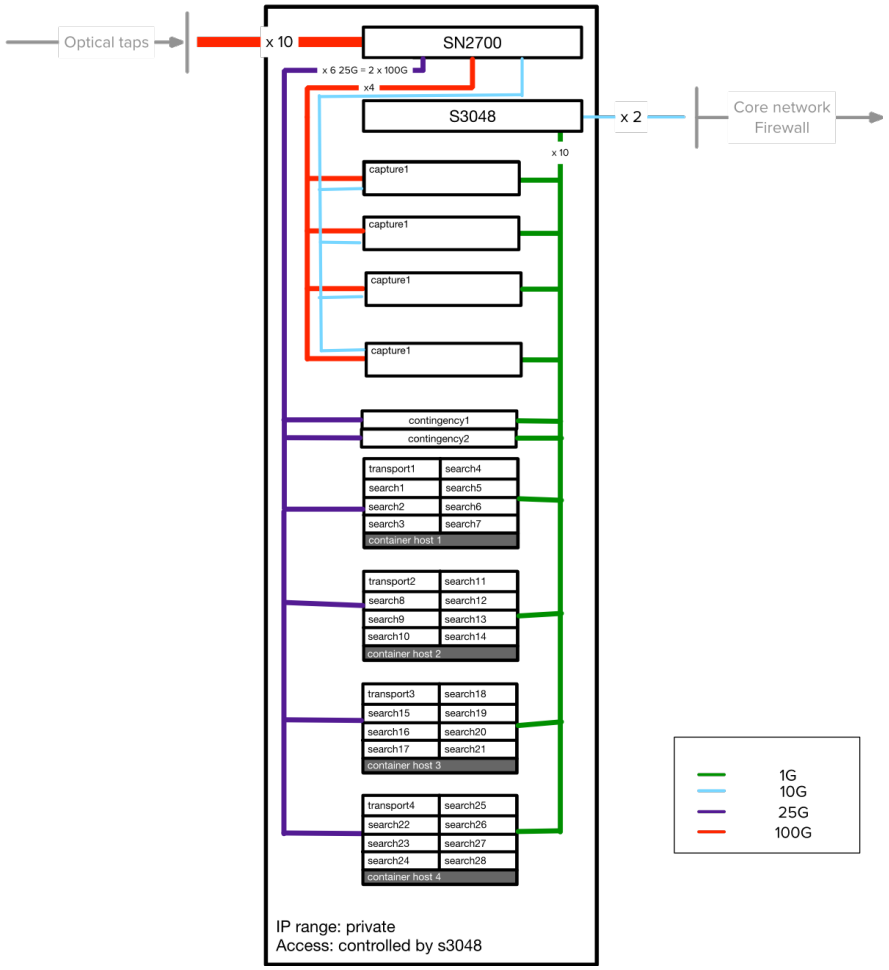
- Messaging/supporting services servers x2
  - 24 cores
  - 256 GB memory
  - 960GB storage
  - 25 Gb/s networking



Science and Technology Facilities Council

What's next?

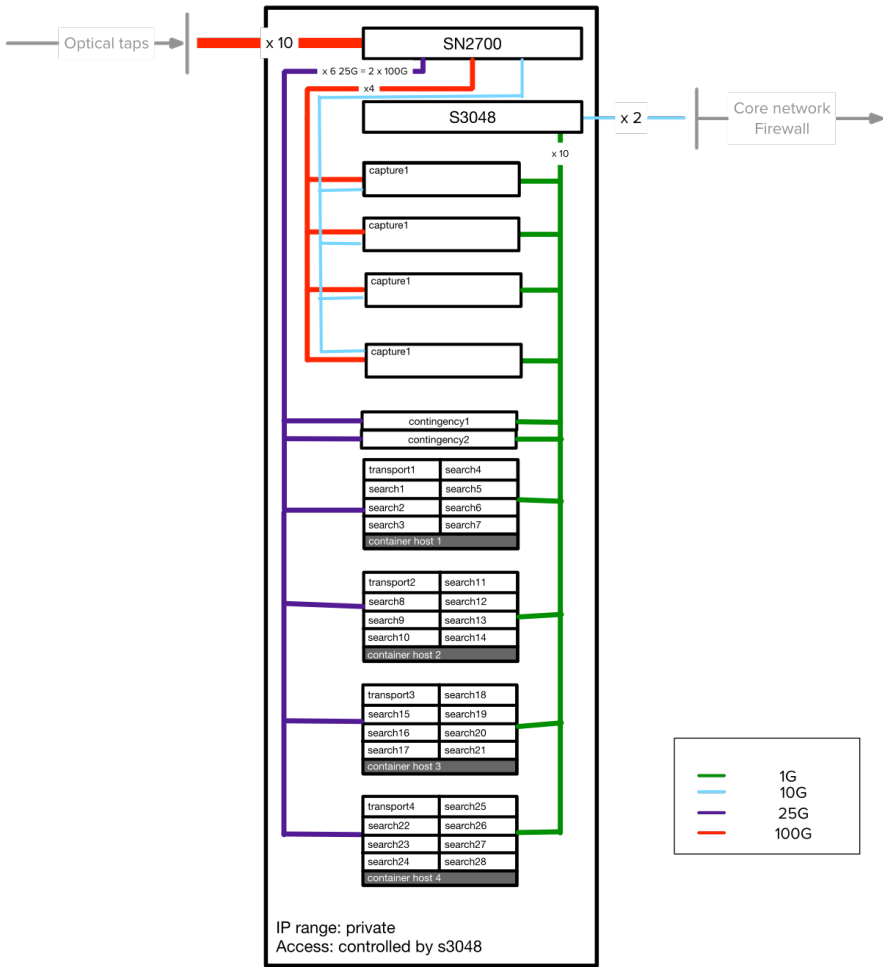
- STFC
  - Multiple sites
- UKRI
  - Multiple councils
- UKRI DRI
  - Work across research organisations nationally



Science and Technology Facilities Council

What's next?

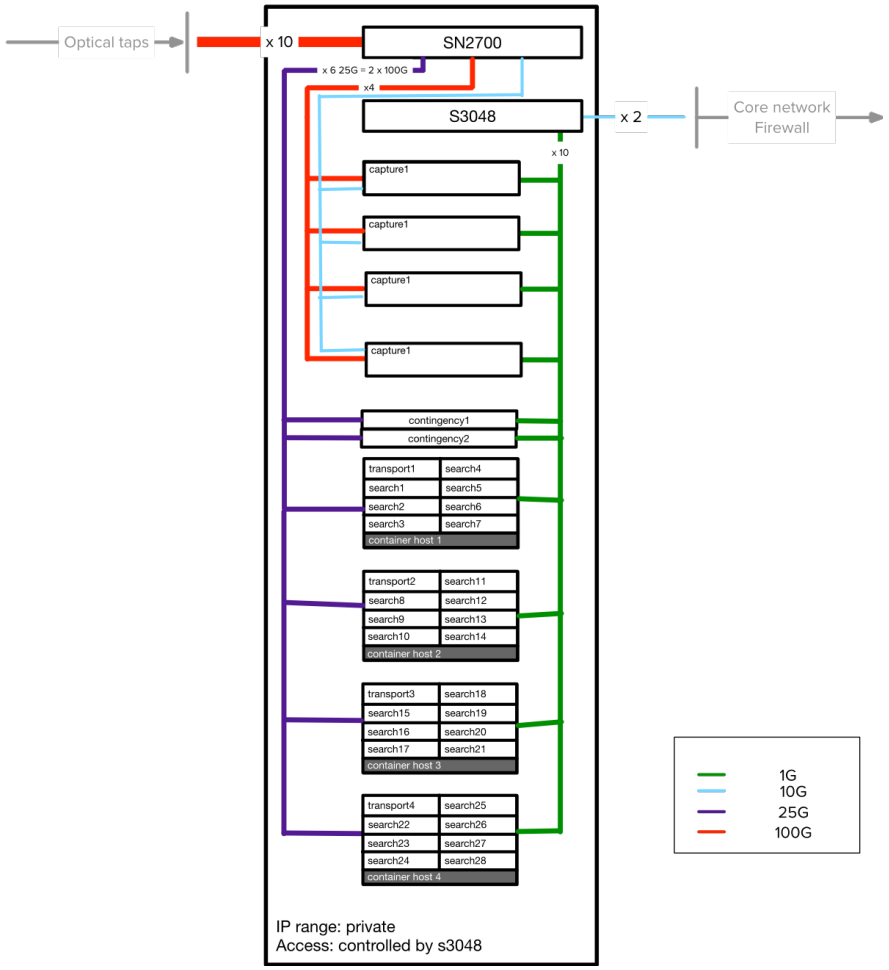
- As we look across our organisations, what solutions will work for which?
  - Some may have capabilities already
  - Some may want an in-house open source solution
  - Some may want/need a commercial/commercially supported option



Science and Technology Facilities Council

Areas of interest

- Packet broker switches
  - Vs optical taps
- Blue Field DPUs
- Network capture at multiple 100 Gb/s
- Area of very active development over the next few years



Science and Technology Facilities Council

UKRI Science and Technology Facilities Council

Thank you

Science and Technology Facilities Council @STFC_Matters Science and Technology Facilities Council