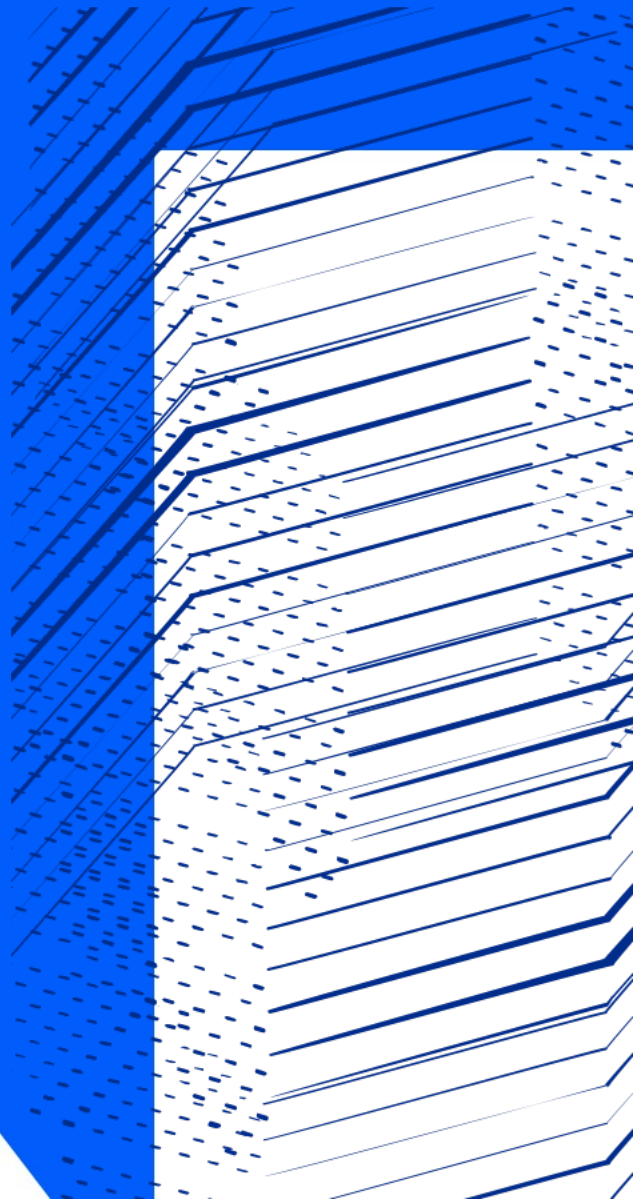
Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics



GridPP Security

David Crooks
david.crooks@stfc.ac.uk

GridPP 46, September 2021, Ambleside

Overview

1 Landscape

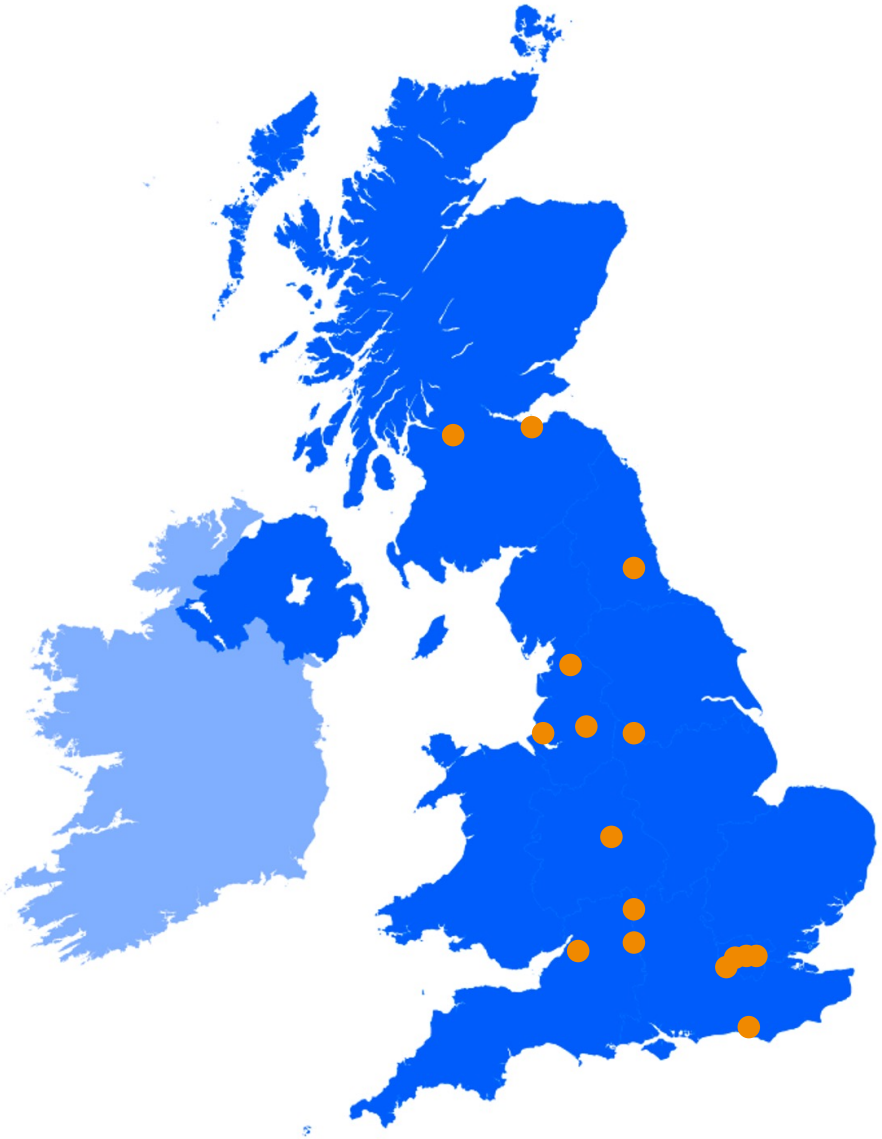
2 SVG update

3 Security team/CSIRT update

4 Distributed Research Trust and Security

5 STFC SOC Project

6 The next 6-12 months



Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Science and Technology Facilities Council

Scientific Computing

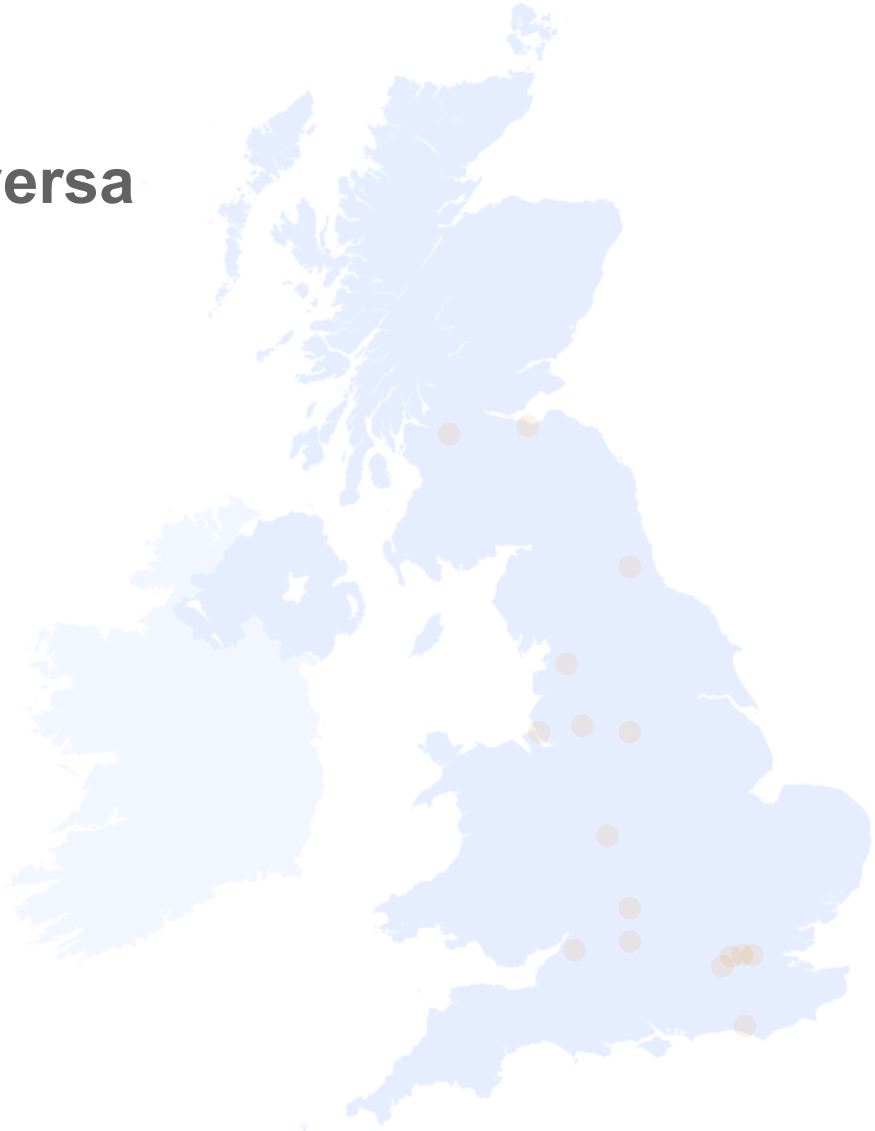
GridPP

UK Computing for Particle Physics

Landscape

Landscape

- **Institutional security is grid security and vice versa**



Science and Technology Facilities Council

Scientific Computing

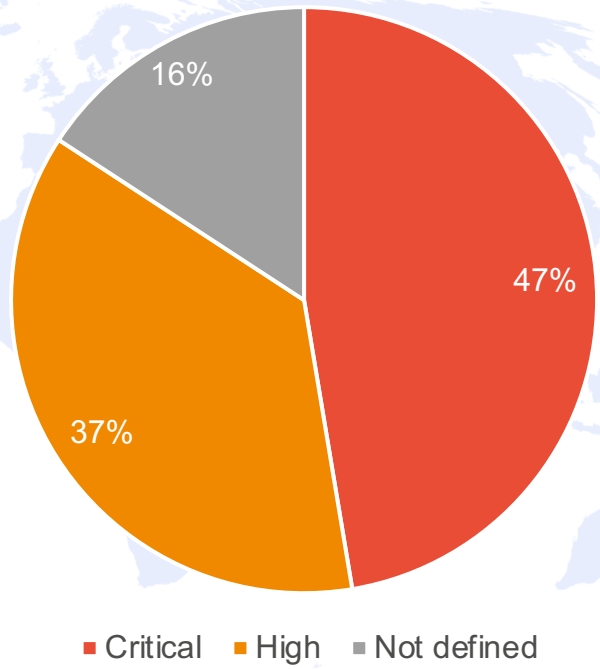
GridPP

UK Computing for Particle Physics

SVG update

SVG: Vulnerability issue handling

- Since Oct 2020
  - 33 Tickets created
  - 19 advisories issued to sites
  - **9 Critical**
  - 7 High
  - 3 not defined
    - 1 which will NOT be made public
- Some have multiple updates
- **NB**: for advisories due to become public in August, this has been delayed until September due to holiday season



SVG Evolution: Deployment Experts Group

- Build set of experts in different software to accurately assess the risks of vulnerabilities in our increasaingly heterogeneous software environment
- Getting DEG going hasn't taken place
  - hope to do this soon
- Thanks to all who have offered your help
  - Vital part of ongoing assessments
    - Accuracy

SVG Evolution: EOSC

- SVG will handle vulnerabilities in EGI ACE scope rather than EOSC
  - EGI, the EGI UMD/CMD, and software used by EGI
  - Update of previous plans more focussed on EOSC
  - Scope will depend on DEG participation
- For EOSC – likely to be mainly best practice
  - Collaboration with a WISE working group
  - Some EOSC services may be included
- More info in coming weeks when finalized
- Abstract submitted for EGI conference
  - *"The EGI Software Vulnerability Group (SVG) - what we do and how we are evolving."*

Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

Security Team/ CSIRT update

IRIS/GridPP Security Team update

- No incidents impacting GridPP since Oct 2020
- New procedure gathering specific site updates for all advisory broadcasts
  - Staying in touch with sites
  - Tracking changes in infrastructure
- Updated backup duty accordingly
  - Maintaining an internal dashboard of these reports
  - New weekly handover meeting
    - Following IRTF example

EGI CSIRT SSC

- Planned for this year
- Same format of activity over working week
- Designed to be global challenge
- Timescales will be announced in advance
  - Recommend sites start reviewing incident response procedures this month
  - Carrying out a review at RAL
  - Happy to discuss!

Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

Distributed Research Trust and Security

Distributed Research Trust and Security

- Within STFC, in Scientific Computing and Particle Physics, we have decades of experience in distributed security
  - Information security management
  - Trust, policy and assurance
  - Identity management
  - Operational security
- **Distributed Research Trust and Security**
  - **DRTS**
- Members of this team coordinate all security and identity management activity in GridPP and IRIS

Science and Technology Facilities Council
Scientific Computing

DRTS

GridPP
UK Computing for Particle Physics

Distributed Research Trust and Security

- Ian Collier
- David Crooks (lead)
- Linda Cornwall
- Tom Dack
- Will Furnell
- Jens Jensen
- Dave Kelsey
- John Kewley
- Ian Neilson

Science and Technology Facilities Council
Scientific Computing

DR TS

GridPP
UK Computing for Particle Physics

Distributed Research Trust and Security

- This team provides a centre of excellence in distributed research security
  - Important for collaboration in UK-wide activities
- Aim to support existing and new Digital Research Infrastructure in STFC and UKRI
- Ultimate goal to help steer development of DRI program

- *drts@stfc.ac.uk*

Science and Technology Facilities Council
Scientific Computing

DRTS

GridPP
UK Computing for Particle Physics

Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

STFC SOC Project

STFC SOC project

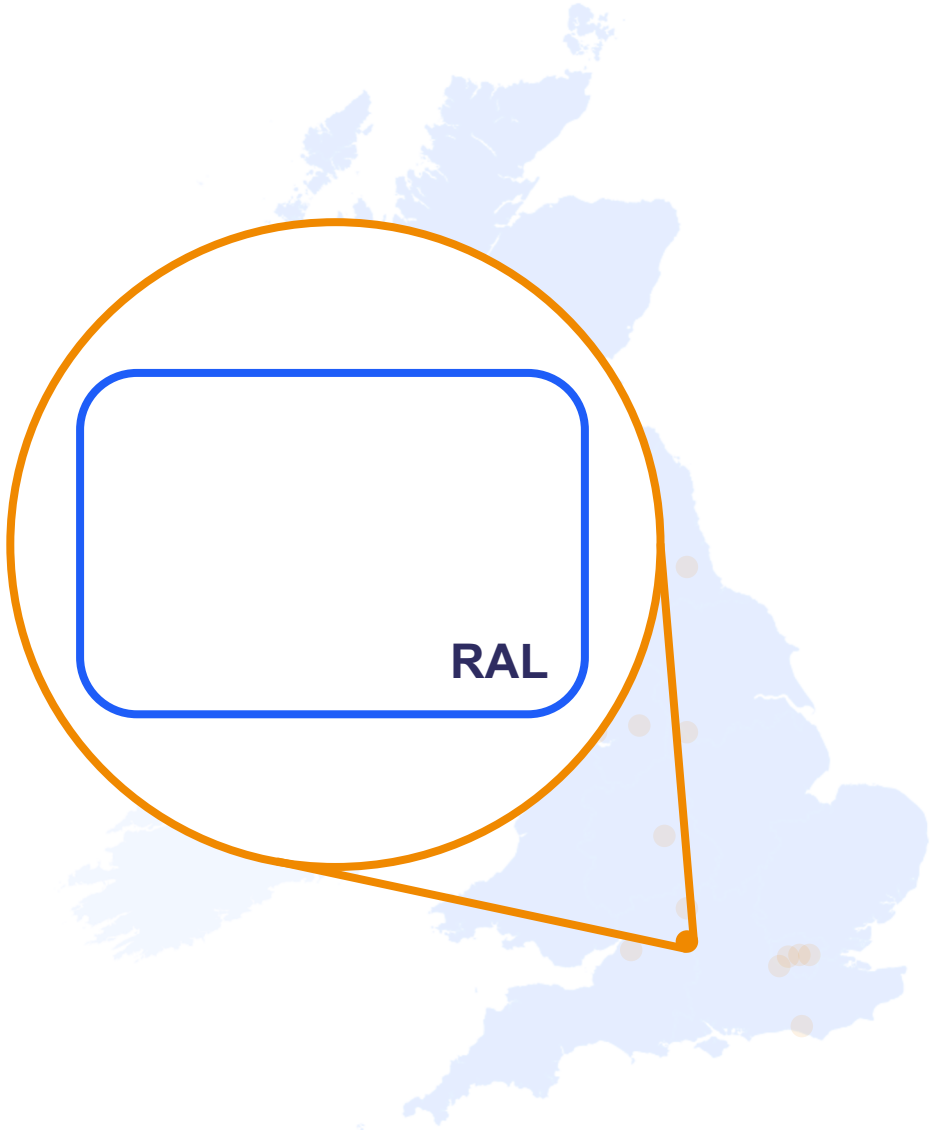
- Priority security project at STFC
- Add capability to monitor **all** traffic entering and exiting RAL campus, correlated with threat intelligence
- High visibility, ambitious project
- Multiple goals
  - Primarily of security of STFC itself
  - Future goal: multi-site version to also cover Daresbury, Boulby, Chilbolton and UK ATC
  - Take a leading role in our community in the deployment of this capability

Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

STFC SOC project

- Priority security project at STFC
- Add capability to monitor **all** traffic entering and exiting RAL campus, correlated with threat intelligence
- High visibility, ambitious project
- Multiple goals
  - Primarily of security of STFC itself
  - Future goal: multi-site version to also cover Daresbury, Boulby, Chilbolton and UK ATC
  - Take a leading role in our community in the deployment of this capability

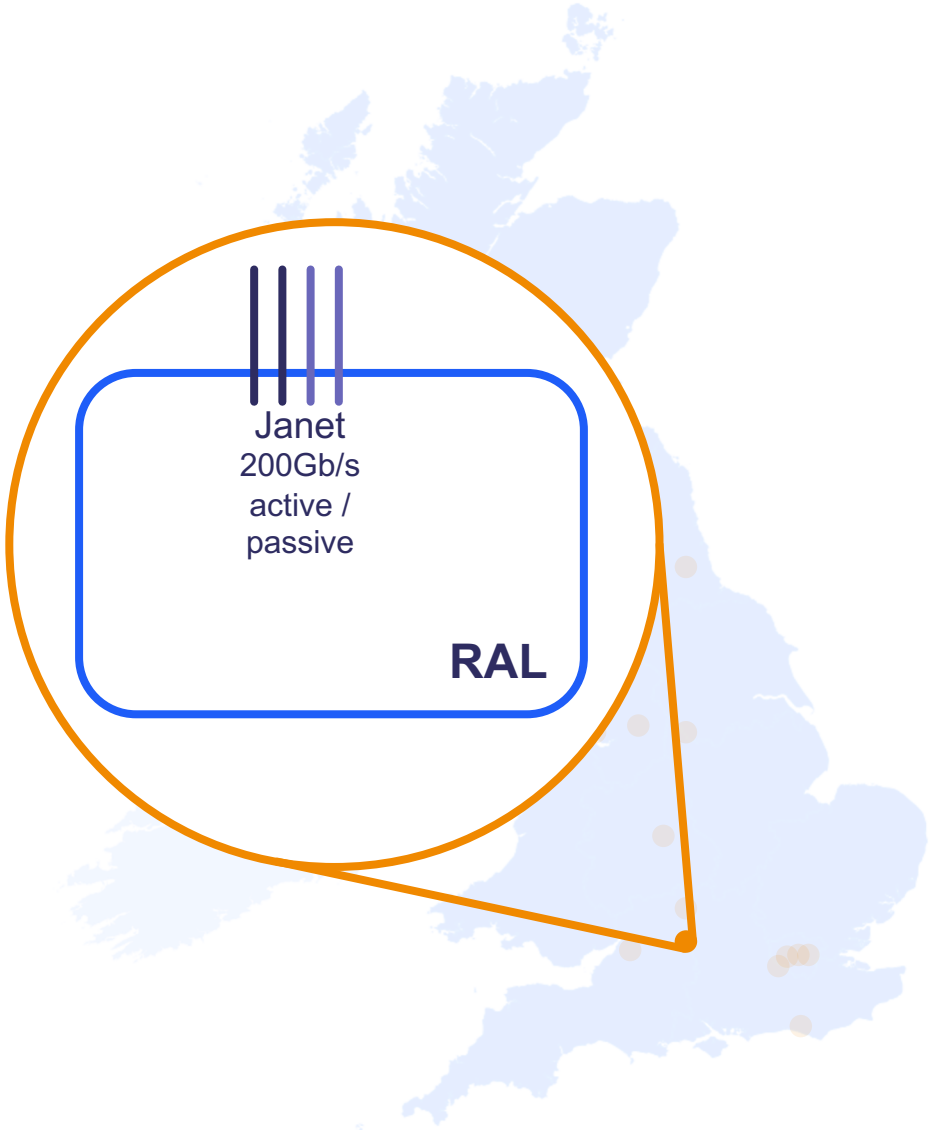


Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

STFC SOC project

- Priority security project at STFC
- Add capability to monitor **all** traffic entering and exiting RAL campus, correlated with threat intelligence
- High visibility, ambitious project
- Multiple goals
  - Primarily of security of STFC itself
  - Future goal: multi-site version to also cover Daresbury, Boulby, Chilbolton and UK ATC
  - Take a leading role in our community in the deployment of this capability

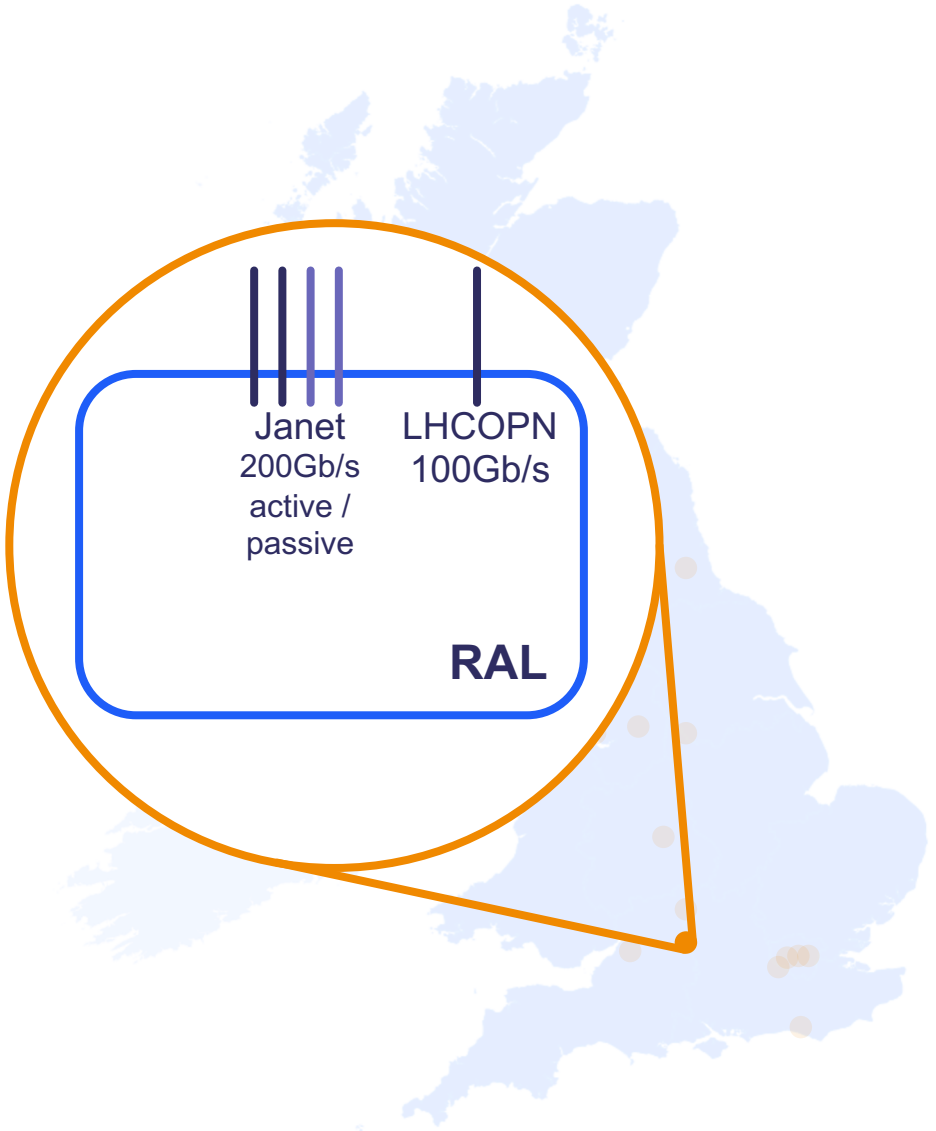


Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

STFC SOC project

- Priority security project at STFC
- Add capability to monitor **all** traffic entering and exiting RAL campus, correlated with threat intelligence
- High visibility, ambitious project
- Multiple goals
  - Primarily of security of STFC itself
  - Future goal: multi-site version to also cover Daresbury, Boulby, Chilbolton and UK ATC
  - Take a leading role in our community in the deployment of this capability

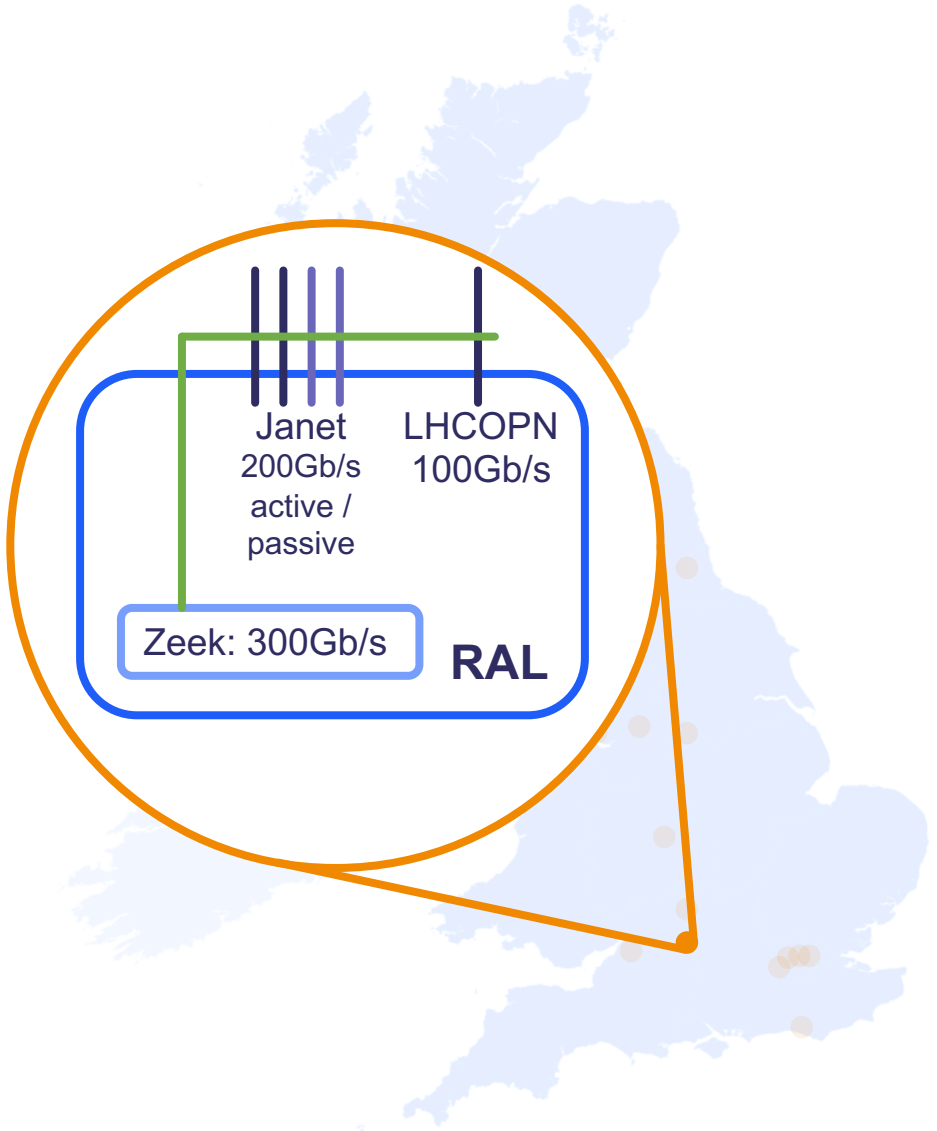


Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

STFC SOC project

- Priority security project at STFC
- Add capability to monitor **all** traffic entering and exiting RAL campus, correlated with threat intelligence
- High visibility, ambitious project
- Multiple goals
  - Primarily of security of STFC itself
  - Future goal: multi-site version to also cover Daresbury, Boulby, Chilbolton and UK ATC
  - Take a leading role in our community in the deployment of this capability

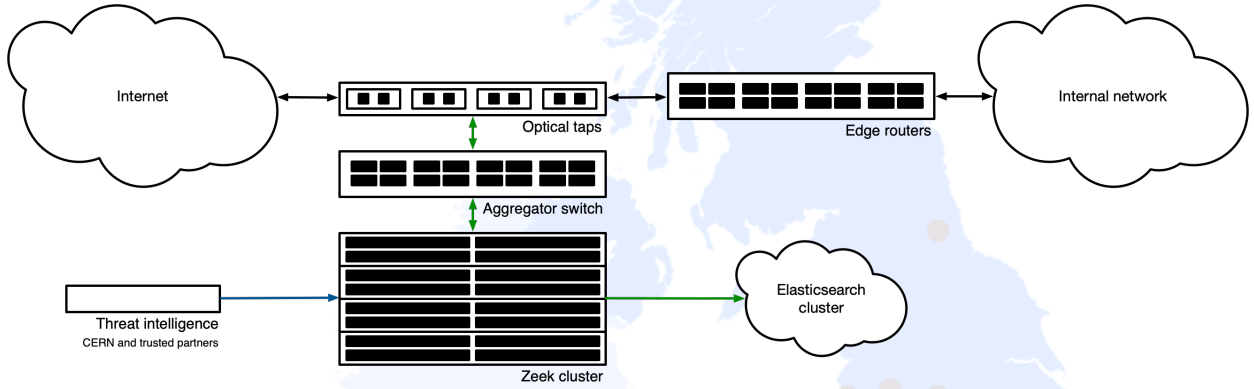


Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

STFC SOC project

- Priority security project at STFC
- Add capability to monitor **all** traffic entering and exiting RAL campus, correlated with threat intelligence
- High visibility, ambitious project
- Multiple goals
  - Primarily of security of STFC itself
  - Future goal: multi-site version to also cover Daresbury, Boulby, Chilbolton and UK ATC
  - Take a leading role in our community in the deployment of this capability

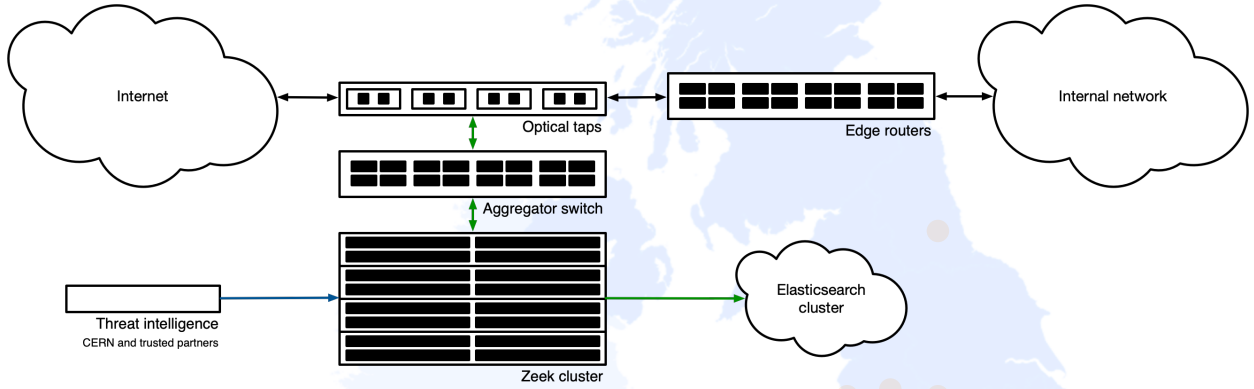


Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

STFC SOC project: GridPP/IRIS

- Project uses Tier1 Worker Nodes
- Provide ratified specification suitable to monitor throughputs up to multiple 100Gb/s links
- Understand what would be appropriate for GridPP/IRIS sites
  - In consultation with central security teams, build proposal to deploy technology at all sites appropriate to circumstances
    - Including staffing



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

The next 6-12 months

Next 6 months

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
3. Then understand what it would take to install SOC technology at sites appropriate to circumstances

Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Next 6 months

4. Understand where to locate SOCs – edge of institution is optimal
   - Security of institutions is security of GridPP/IRIS sites and vice versa
   - Talk to central teams – please send them my way!

Photo by FLY:D on Unsplash

Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Next 12 months

- Host **Distributed Security Forum**
- Invitations to
  - All central teams in GridPP and IRIS
  - IRIS Security Team
  - Jisc / Janet CSIRT
  - EGI CSIRT
  - WLCG Security Officer
- Matters of common interest
- Forward planning

Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Summary

- Our sector faces an acute threat
- We have the tools and processes to protect ourselves
- **And importantly** help protect our institutions and community
- We must work together

Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics


UKRI
Science and
Technology
Facilities Council
Scientific Computing
Questions?


UKRI
Science and Technology Facilities Council
Scientific Computing
Thank you
scd.stfc.ac.uk
@SciComp_STFC