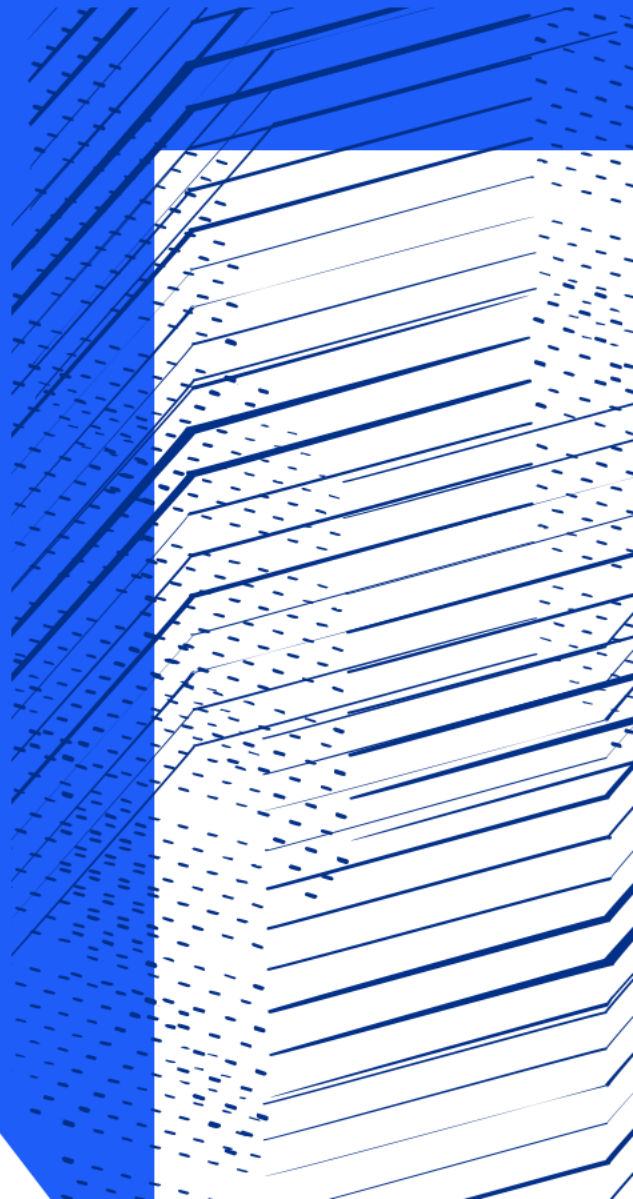
Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics



GridPP Security

David Crooks
david.crooks@stfc.ac.uk

GridPP 49, March 2023, Abingdon

Equality, Diversity and Inclusion

- Reflecting on recent events, I feel the responsibility to make a couple of comments

Equality, Diversity and Inclusion

- Reflecting on recent events, I feel the responsibility to make a couple of comments

- I am a queer cybersecurity professional
- I have a fair bit of privilege, and somewhat of a platform

#queercybersecurity

Equality, Diversity and Inclusion

- It is vital that we protect the right of those we work with to live and work as their authentic selves
- Trans Lives Matter
- Our community is built on collaboration
- We should make sure we extend these values to building diverse and inclusive workplaces

#translivesmatter

Landscape

- Intentionally left blank

Science and Technology Facilities Council
Scientific Computing

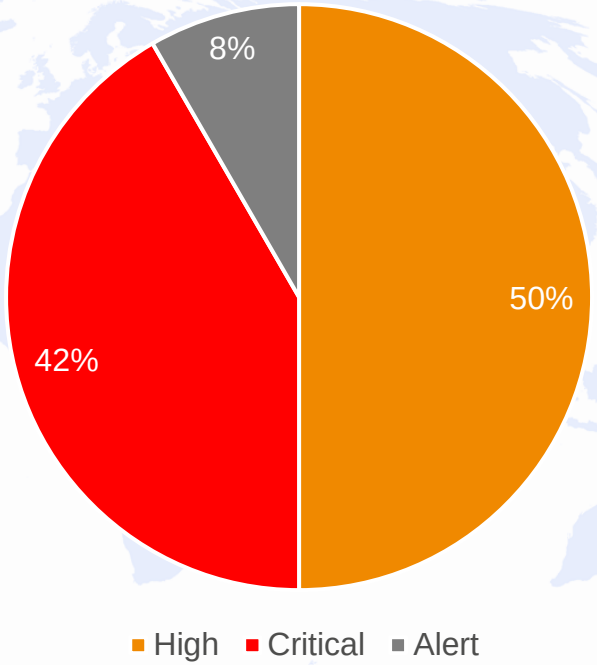
GridPP
UK Computing for Particle Physics

Vulnerability risk assessments

- 23 Vulnerabilities reported
- 12 advisories sent
  - **5 Critical Risk**
  - 6 High Risk
  - 1 ‘Alert’

- EGI SVG is adapting its methods for dealing with software vulnerabilities
  - increased infrastructure inhomogeneity

- https://advisories.egi.eu



PREVENTION

RESPONSE

IRIS/GridPP Security Team update

- No incidents involving GridPP since GridPP48
- IRIS Security Confluence area still in planning
- Talk about Site Security Survey and SSC in a moment

Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

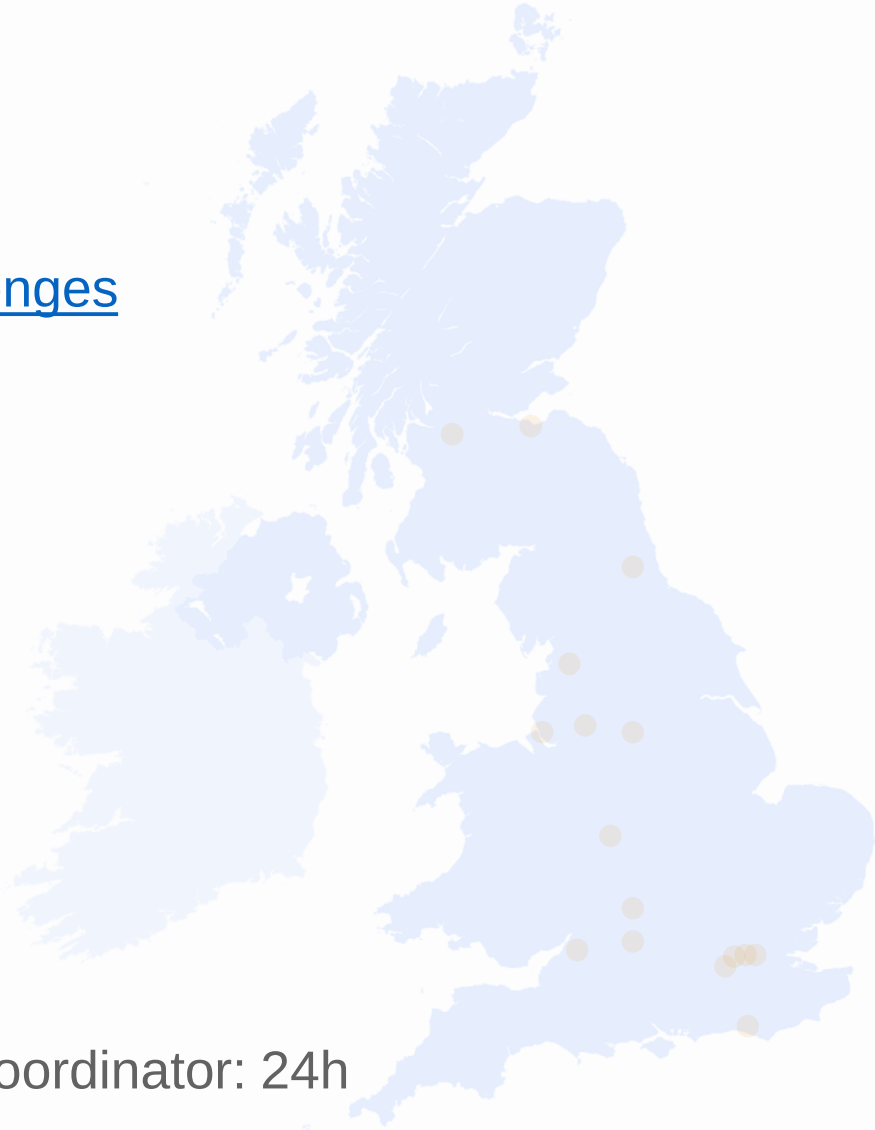
Training

- IRIS Security Workshop in January very successful
- Plan for repeat in the middle of the year
  - Risk management module continuing to be developed
- Start planning for later in the year

- Next Security thematic CERN School of Computing has been discussed for October
  - Programme committee needs to meet to plan next steps

EGI CSIRT SSC Update

- Underway this week for CMS sites
  - https://confluence.egi.eu/display/EGIBG/Security+challenges
- GridPP channels:
  - Security-discussion
  - GridPP Security Mattermost
- Focus on communications
- Per site operations, target time, office hours
  - initial feedback: 4h
  - found malicious job/processes/stop them: 4h
  - ban problematic certificate: 4h
  - contain the malicious binary and sent it to the incident-coordinator: 24h



EGI CSIRT SSC Forensics

- The Forensics part of the SSC is managed via https://ssc.egi.eu/.
  - Optional activity of the Site Security Challenge (SSC).
  - By taking part in this game, you will be able to submit answers to additional questions
- The game will focus on selected areas of digital forensics
  - Refer to the information in the Forensics Howto.
- Post-SSC, opt-in to have results added to the final report.
- To register and get started, visit https://ssc.egi.eu/instructions

PREVENTION
DETECTION
RESPONSE

Site Security Survey

- Since last GridPP, IRIS/GridPP Security Team has worked on Security Survey
- Effectively ready to launch now, will activate post-SSC
- Use to build a picture of site plans over next year

Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Cybersecurity Assessment Framework

- NCSC CAF
- Step up from Cyber Essentials(+)
- UKRI in the process of showing compliance in the next years
  - Governance this year
- Recommend becoming familiar with this as could prove important in the coming years
  - Particularly at management levels

Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Digital Research Infrastructure

- DRI Congress held at beginning of March
- Coincident with launch of Future of Computing report
  - Now backed in most recent budget
  - Call for 10 year computing strategy

- Clear that we need a long-term DRI Cybersecurity strategy

- Now considering a number of 1 day DRI Cybersecurity workshops through new financial year

Digital Research Infrastructure

- Focus on common challenges and goals
- Identify early adopter sites we can support to deploy SOC capabilities
- £800k available from April for resource/hardware that can be made available across the UK
  - Use the workshops for planning

Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Security Operations and Engineering Team

- First full iteration of SCD Security Operations and Engineering team in place
  - James Acris
  - Liam Atherton
  - Callum Pollock

- Primary focus is deployment of STFC SOC components
    - Followed by other key SCD/STFC security monitoring
    - Central Pakiti

- Building to include other aspects of cybersecurity
- Important part of developing (SCD/STFC) cybersecurity profession

STFC SOC update

- All deployment will take place with new security-focused Aquilon archetype
  - Now in place
- Traffic now flowing from LHCOPN tap to zeek capture nodes
  - Begin characterisation and tuning work
- OpenSearch deployed on virtual cluster prior to installation on hardware nodes
- New MISP deployment underway using NUKIB config
  - Czech National Cyber and Information Security Agency
  - Containerised based on CentOS Stream 8

SOC Hackathon

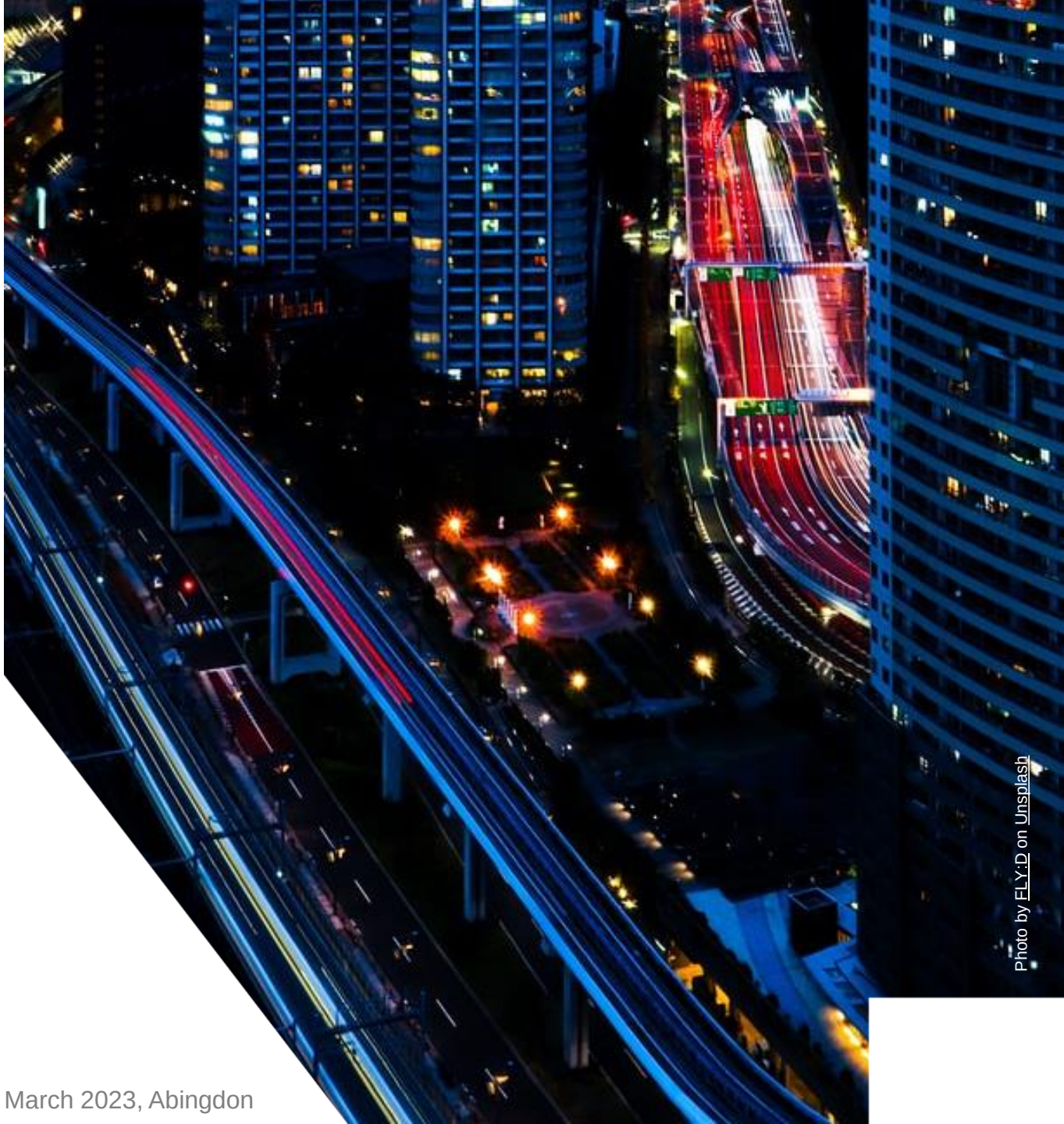
- Dates now confirmed for next SOC WG SOC Hackathon
  - **w/c 14th August**
  - https://indico.cern.ch/event/1268239/
- Hosted at Cosener's
  - Garden Room + 3 break-out rooms for 5 days
  - ~1 day status updates and 4 days technical work
- Potential for higher level discussions in parallel
  - Keen to include UKRI and DRI participants

Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Conclusion

1. Landscape and high priority of cybersecurity remain the same
2. Workshops and SSC will both provide training throughout this year
3. Security Survey will let us make plans for each sites needs
4. DRI Cybersecurity will become increasingly important with workshops being planned

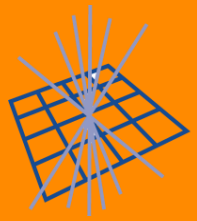


Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

Science and Technology Facilities Council

Scientific Computing



GridPP

UK Computing for Particle Physics

Questions?