UKRI Science and Technology Facilities Council

IRIS Security

IRIS Collaboration meeting, Cambridge, January 13th 2026

David Crooks
david.crooks@stfc.ac.uk
On behalf of the IRIS Security Team

iris

Landscape + overview

- Broad status the same: high, persistent risk

- Considerable focus on compliance → Risk
  - Organisational focus

- Security team continuing to develop, no changes in the roster

Science and Technology Facilities Council

iris

Security Handbooks

- First draft of site security handbook for GridPP – and potentially IRIS – has been completed and handed to Lancaster and Glasgow
  - Gain site feedback before broader distribution

- Focus on key controls: likely to require some work especially in documentation
  - Not a full framework assessment, but hopefully useful in that regard

- Recent addition was a maturity model: ultimate aim for level 2, but useful to note any 3s.

Level	Description
0	Not known/not in place
1	Known verbally
2	Known and documented
3	Known, documented and peer reviewed

Security Handbooks

- Security contact
- Central logging configuration
- Asset management process
- Network map including relation to central network
- Access control structure, including local, site and organisational firewalls
- Approach to system hardening
- Patching process, noting applicable organisational policies
- Local incident response and recovery procedure
- Monitoring capabilities including local and organisational where relevant
- Security documentation, processes, procedures lifecycle

Security Detection

- Previously mentioned pDNSSOC as a tool to correlate DNS logs with threat intelligence

- Now replaced by Unicor, maintained by Romain Wartel and the SAFER community

- Ingests DNS logs or other JSON formatted records and correlates with MISP threat feeds
    - Builds alert notifications with context and sends to security teams

Unicor pilot

- Focussed initially on GridPP, intention with core Tier 2s to implement Unicor as lightweight incident detection mechanism
  - Pilot underway at Lancaster

- Goal here is not a unified regional Security Operations Centre, but contribution to the overall work of securing our organisations
  - Building relationships with central teams

DRI Update

- Next DRI Cyber Security workshop now in planning stages – hopefully to be held in Edinburgh around April

- Active planning now taking place around CAF workshops

- NFCS N+ project underway to contribute cyber security elements to the overall roadmap
  - Likely to include additional workshops

- Specific project on online cyber security training for research computing
  - Focus initially on induction style course, useful in different contexts

Skills and Training

- Upcoming training events
  - ISGC, Taipei, March: additional track added to conference focused on security training (less directly relevant to IRIS, but part of overall training development)

  - Next Thematic CERN School on Computing will be held again at Cosener's House in Abingdon
    - 27th September to 3rd October (Sunday to Saturday, school M-F)

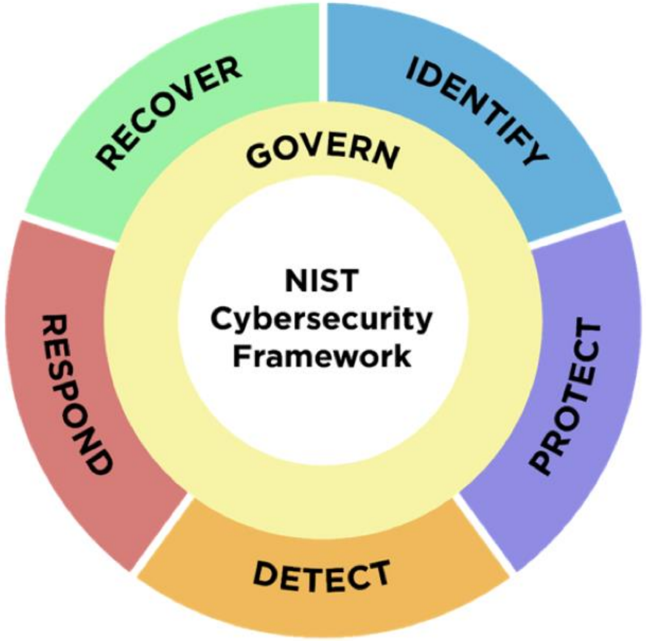
- Should design an IRIS security training day this year

CERN School on Security

- Aimed at system managers expected to work with security in their day-to-day role
  - As opposed to cybersecurity professionals – but typically have a small number of these as well
  - Cover security lifecycle of a service

Risk management
Security architecture
AAI
Logging and Traceability
Virtualisation + cloud security
Container security
Vulnerability management
Application security

Security Operations Centres
Security operations
Incident response management
Forensics
Incident response exercise



Policy

- Mentioned policy in the summer; a review of our existing policies needs to be a focus for this year
  - https://www.iris.ac.uk/security/

- Parallel work needed for EGI and WLCG

- AARC TREE project (AARC and AARC 2 provided policy toolkit used by IRIS) almost complete
  - Experience from IRIS has greatly benefited that activity

Exercises

- Something that has been discussed over the past few years
- Compare and contrast with the EGI Service Security Challenges that run against the WLCG infrastructure every few years
  - Heavyweight, in depth activity
- For IRIS, propose a lighter-weight approach, identifying a specific area to focus on in the first instance
  - Could include technical and pure tabletop elements

Summary

- In a continued high risk environment, security governance and risk management are key areas for development
- Understand impact for IRIS: engage with broader DRI activities

- Skills and training vital additional strand

- Need to plan IRIS security exercises

- Upcoming work
  - Site Security Checklist work
  - Unicor pilot → Tier2 deployments

Science and Technology Facilities Council

Thank you

Science and Technology Facilities Council

@STFC_Matters

Science and Technology Facilities Council

Science and
Technology
Facilities Council

Questions?