Science and Technology Facilities Council

Scientific Computing

iris

IRIS Security

January 2023, ROE

David Crooks
david.crooks@stfc.ac.uk

Overview

- Landscape
- IRIS Security: last year
- Training + Security Workshop summary
- DRI Cybersecurity + broader activity
- IRIS Security: this year

Who am I?

- GridPP/IRIS Security Officer
  - WLCG incident response team (EGI CSIRT)
- Acting as Head of Cybersecurity for Scientific Computing
- Chair of the STFC Information Security Group
- Project leader for DRI Cybersecurity
- Member of GEANT 5-1 security work package
  - High speed network monitoring

Landscape

- We remain in a heightened cybersecurity risk environment

- Geopolitical situation + cybercrime
- Ransomware
- Phishing

- We continue to learn hard lessons from the international HPC incident in 2020
  - **But** provides fertile ground for improvement: see later

IRIS Security over the last year

- No IRIS scoped incidents
- Emanuele Simili and Stuart Rankin have joined the security team from Glasgow and Cambridge
  - Jon Wakelin has moved on
- Continue to operate the On Duty rota and polling sites for updates on specific vulnerabilities in GridPP
  - Consulting with DiRAC and cloud sites and developing how we could expand on this

IRIS Security over the last year

- Focus on training
  - Summary of yesterday's workshop in a moment and our roadmap
- Community policy going through continued development
  - led by Ian Neilson
- Completed SCIv2 Framework Assessment of IRIS Security maturity
  - A Trust Framework for Security Collaboration among Infrastructures

Training approach

- Developing and overall syllabus for IRIS Security training

- Closely aligned with and building on other work
  - EGI CSIRT: thematic CERN School of Computing on Security
  - Work to develop training within STFC
  - EOSC Future: online training modules (planned)

- Look at areas of focus for cybersecurity
  - (Those familiar with NIST Cybersecurity Framework may recognize these!)

Identify

- What do we have and how do we structure our processes?

- Asset management
- Risk management
- Governance

Protect

- What safeguards can we put in place to protect our systems from attack?

- Security controls
- Architecture
- Training!

Detect

- What monitoring and telemetry do we have access to to detect suspicious traffic in our environment?

- Network monitoring/IDS
- Central logging
- Threat Intelligence
- Security Operations Centres

Respond

- How do we respond in the case of an incident?

- Security team/CSIRT structures
- Incident response procedures
- Exercises!

Recover

- How do we recover from an incident?

- Recovery procedures (including final incident reports)
- Continuous improvement
- Communications

Identify and Protect

- Focus on elements of the first two of these:
  - Security architecture
  - Risk management

IRIS Security Workshop

- Held in this room yesterday

- 10 in person attendees, around the same online for the morning
  - Introduction and training plans
  - Security Architecture
  - Risk Management

- In person exercises in the afternoon
  - Enthusiastic discussion on risk management!
    - Important aspects at technical and management layers
  - Recent Slovenian VEGA HPC deployment used as example for a security architecture exercise

IRIS Security Workshop

- Sven Gabriel and Barbara Krasovec from the EGI CSIRT very welcome as instructors
  - In principal planning in progress to repeat this later in the year for people who would have liked to attend but were unable to
- Particular thanks to Bob and Mark!
- Next steps
  - Use feedback and roadmap to plan next workshops
  - Planned Security Operations Centre workshop/hackathon ~May/June could provide training opportunity
  - See later IAM talk for nice AAI training exercise in development

Digital Research Infrastructure

- Look at our broader R&E community
- The threat from cybersecurity attacks to the UK research and education sector is acute having growing over recent years
- We must work together to protect and defend our community in the face of determined and well-resourced attackers
- We **must** collaborate and share information about ongoing incidents between our organisations

DRI Opportunities and Risks

- With its role underpinning UK research, it is vital that the DRI system be trustworthy and provide the assurance necessary to protect the assets and reputation of those using it

- With the open risk appetite necessary to support innovative computing infrastructures, it is vital that these risks be managed appropriately

- A key part of this process is an effective approach to cybersecurity

DRI Cybersecurity

- A new project to develop **a common approach to cybersecurity across the DRI landscape**
  - Essential in our current environment
  - Building on experience from leading work for research infrastructures nationally and internationally

- Aims to establish **a common cybersecurity defence framework across the DRI landscape**
  - An initial phase funded at £1m (resource + capital)

Status

- This work will focus initially on building trust between DRI participants to support information sharing 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
- The first phase of the DRI Cybersecurity project will develop these capabilities with **a core of early adopters**
  - Following an initial workshop in early 2023
- IRIS has a vital role to play in this broader activity
  - Identify senior organizational cybersecurity leaders to include in workshop
  - Key infrastructure representatives

National context

- The DRI Cybersecurity project takes place alongside existing national work
  - Jisc with a National R&E Network perspective
  - NCSC with a national and government perspective
- The perspectives shown on the next page are complimentary and strengthen our overall ability to defend and protect our R&E community
- I will have the chance to brief Cabinet Office on this planned work in a couple of weeks

National context

NCSC	DRI Cybersecurity	Jisc
“We support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public.”	“Represents the perspective digital research infrastructures including innovative workflows and large-scale data management.”	“Jisc is the UK digital, data and technology agency focused on tertiary education, research and innovation..”

International context

- The proposed work to develop a common approach to cybersecurity **from a research perspective** across the UK's research and education environment is unique within Europe

- Notable opportunity to provide an example for other countries in building this combination of capabilities and common approaches

International context

- The DRI Cybersecurity project is working alongside international partners including
  - GÉANT: The collaboration of European National Research and Education Networks (NRENs)
  - Trusted-CI: lead[ing] in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.

- GÉANT 5-1 developments in this area on the international stage will be closely aligned with work in the DRI

UK focused frameworks

- Commonly used frameworks in the UK include ISO27k and CyberEssentials(+)

- Their use will depend on the organization
  - UKRI is using the NIST Cybersecurity Framework as a development tool

- Want to highlight a couple of UK frameworks that might become more important: govs.007 and CAF

govs.007

- Government Functional Standard

- *This standard applies to the planning, delivery and management of government security activities.*
- *It includes risk management, planning and response for physical, personnel, cyber and technical security in departments and their arm's length bodies, as well as industry.*
- *Other public sector organisations, devolved or local, may find this standard useful.*

Cybersecurity Assessment Framework

- NCSC CAF
- The CAF is being introduced as part of a new programme aimed at improving government cyber security. Outside of government, the organisations likely to find the CAF collection most useful fall into three broad categories, namely
  - organisations within the UK Critical National Infrastructure (CNI)
  - organisations subject to Network and Information Systems (NIS) Regulations
  - organisations managing cyber-related risks to public safety

Impact for IRIS

- NCSC CAF in particular has the potential to become increasingly important in our sector so is worth being familiar with this

- Linking to DRI work: a benefit of building a UK R&E cybersecurity community including **HTC**, **HPC** and **Cloud**
  - We can work together on responses to frameworks
  - Some/most/all current frameworks do not necessarily fit well with research computing (more open risk appetite)
  - A community response would be a powerful tool

IRIS Security this year

- Risk management at IRIS and service level
- Working with IRIS communities and lifecycle management
  - Onboarding
- Security plan (documentation)

- Service catalogues/asset management: GOC DB

- Cybersecurity Services for IRIS
  - Recently created Scientific Computing Security Engineering Team
  - Deploying Security Operations Centre for Harwell Campus
  - Roadmap to (re)deploy Pakiti patch monitoring system for STFC
  - Allow us to provision prototype for IRIS

IRIS Security this year

- Risk management at IRIS and service level
- Working with IRIS communities and lifecycle management
  - Onboarding
- Security plan (documentation)

SCIv2 Framework Assessment

- Service catalogues/asset management: GOC DB

- Cybersecurity Services for IRIS
  - Recently created Scientific Computing Security Engineering Team
  - Deploying Security Operations Centre for Harwell Campus
  - Roadmap to (re)deploy Pakiti patch monitoring system for STFC
  - Allow us to provision prototype for IRIS

IRIS Security this year

- Enhanced detection capabilities
  - Threat Intelligence and Security Operations Centres
  - Coupled with broader DRI development
- Work with IRIS resource providers, communities and services
  - How to practically apply our approved policies
  - Continue to build common security culture
- As DRI Cybersecurity project proceeds, identify development needs and opportunities for IRIS vs broader community

iris

Thank you - Questions?

Science and Technology Facilities Council

Scientific Computing