EOSC-hub
WP4.4 Security (ISM)

David Kelsey
STFC

EOSC-hub Task Leaders, 9 Jan 2018
Amsterdam

Evolving Operational Security for the EOSC era

Sven Gabriel svengᵃnikhef.nl, **Nikhef, EGI-CSIRT**
Urpo Kaila urpo.kailaᵃcsc.fi, **CSC, EUDAT**

www.egi.eu

EGI-Engage is co-funded by the Horizon 2020 Framework Programme of the European Union under grant number 654142

EGI-CSIRT, EUDAT Security

EGI CSIRT Activities & collaborations

EGI CSIRT is certified by TI(2014), framework that faclitates the collaoration of 200+ CSIRTs from Edu, Finance, Gov, Mil, ISPs

Incident Prevention

Incident Prevention: SVG, SM, IRTF, Set of highly integrated Monitoring and communication tools

EUDAT Security

- EUDAT Operational Security security@eudat.eu
- EUDAT CSIRT csirt@eudat.eu
- Site Security Contacts
- Security Assessments
- Risk Management
- Infrastructure Security

Task 4.4: Information Security Management

Lead STFC; Participants: CSC, JUELICH, CERN, CESNET, Nikhef, GRNET, STFC

- *Total amount of effort = 113 PM*

- This task will develop and implement the policies and procedures to ensure consistent and coordinated security operations across the services provided in the catalogue

- Security across distributed service providers will be based on an up-to-date policy framework including operational and incident response policies, participant responsibilities, traceability, legal aspects, and the protection of personal data
  - These policies and procedures will complement the security best practices implemented by the individual service providers
- The task will coordinate an incident response task force (IRTF) to make sure that routine issues and security events are handled properly by the service providers, and to provide specialised expertise in forensics and coordination for large scale incidents that threaten multiple providers

T4.4 (2)

- The task will also handle software vulnerabilities with the purpose to minimize the risk to the services and the users
- Another goal of the task is to build trust and create effective interoperability with the actors outside of the project such as other e-Infrastructures, with key Research Infrastructures, and – when appropriate – with dedicated security groups in Europe (TF-CSIRT, GÉANT) and in the US

- Other “Security” related activities (Tools,monitoring, AAI, …) housed elsewhere in EOSC-hub

EGI CSIRT F2F meetings

15-17 November 2017

- Hosted by CSC, Helsinki
- Urpo Kaila (EUDAT Security Officer)

- Integration of EUDAT to CSIRT/IRTF
  - Ongoing collaboration of several years
  - Spent several hours discussing plans for EOSC

Next meeting at CERN – 29-31 Jan 2018

- Urpo and Ralph Niederberger (FZJ) will attend

- Get the work underway
- Finalise year 1 plans – especially 1st 6 months

T4.4 – plans for 1st year

- During P1 – main aims
  - Ongoing coordination of security operations (the day jobs!)
  - Ongoing collaboration with other security activities
  - Integration of EGI and EUDAT teams – not full merger
  - With broader range of services and providers
- Policy
  - Full cross-review, alignment, create road-map, update as necessary
  - AUP alignment & GDPR are early priorities (in collaboration with AARC2)
  - Service policy?

T4.4 plans (2)

- Alignment of Procedures, particularly incident response
  - Top priority is to ensure that we have good contact details of all participants
- Incident Response
  - EUDAT security officer(s) to join IRTF – members of T4.4
  - Then see how to change things in future

Incident Prevention

- Monitoring (not T4.4)
  - EGI and EUDAT teams to review together what to do in future
- Vulnerability
  - SVG will investigate how the teams can best work together
  - Need to handle an even wider range of services

T4.4 – plans (3)

- Other important ongoing activities
  - Training and dissemination
    - Starting with ISGC2018 in Taipei (March)
  - Membership of (indeed leadership of) WISE
    - starting with upcoming workshop in Abingdon 26-28 Feb
    - SCI working group, Risk management, …
    - Coordination with other e-Infrastuctures and RIs
  - Liaiason/collaboration with AARC2, IGTF, etc
  - TF-CSIRT, GEANT

Deliverables

- Security team will need to contribute to WP4 deliverables as required
- D4.1 Operational requirements for the services in the catalogue
- D4.2 Operational Infrastructure Roadmap

Milestones?

- Not yet

Questions?

My own questions

- How do we handle GDPR / Data protection?
  - Several WPs are working in this area
  - We have an existing EGI security policy framework handling protection of personal data in operational logs, accounting, monitoring (not data in general)
  - And AAI attribute release (with GEANT & AARC2)
- Do we (T4.4) need to collect “usage” statistics?
    - Security policies? (what do we count?)

Other questions?