Evolving Operational Security for the EOSC era

Sven Gabriel sveng@nikhef.nl, Nikhef, EGI-CSIRT
Urpo Kaila urpo.kaila@csc.fi, CSC, EUDAT
Introduction
History

- EGEE I- III 2004 – 2010
- Middleware Development
- Cluster management expertise at sites
- Operational procedures/policies
History

- EGEE I- III 2004 – 2010
- Middleware Development
- Cluster management expertise at sites
- Operational procedures/policies
- EGEE I- III 2004 – 2010
- Middleware Development
- Cluster management expertise at sites
- Operational procedures/policies
EGI-CSIRT, EUDAT Security
EGI CSIRT is certified by TI(2014), framework that facilitates the collaboration of 200+ CSIRTs from Edu, Finance, Gov, Mil, ISPs
Incident Prevention: SVG, SM, IRTF, Set of highly integrated Monitoring and communication tools

If you find a vulnerability
Please report it to the Software Vulnerability Group:
report-vulnerability@egi.eu.

Please do not discuss the vulnerability in open forums or blogs, as this may compromise our mitigation strategies.
Example Incident Response

- Situation: Massive Bitcoin Mining on the Infrastructure.
- Spotted by alerted RC Admins (Unusual usage pattern spotted in the monitoring).
- Investigations revealed 26 RCs affected, approx. 30,000 jobs.
- Activity could quickly attributed to a particular Identity.
- Using central suspension, IR was in effect after a couple of hours. Incident Contained.
- After advanced forensics investigation attribution possible.
Collaborative Data Infrastructure

Collaboration of **Thematic** and **Generic Service** Providers

Community Repositories (thematic data centres)

Based on a **Partnership Agreement** specifying OLAs and SLAs

EUDAT generic data service provider storage, workflows, processing, archive
Production Infrastructure
EUDAT Security

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

- Common F2F meeting held in Helsinki (Nov 2017)
- Policy
  - Full cross-review, alignment, and create road-map.
  - AUP alignment & GDPR are early priorities.
- Procedures
  - Alignment of the Incident Response Procedures.
  - Ensure maintained contact details to all sites are available.
- Incident Response
  - EUDAT Security observing member in EGI-CSIRTs IRTF
- Incident Prevention
  - Monitoring EGI and EUDAT teams to review options for collaboration.
  - Vulnerability: SVG will investigate possible collaborations.
- Next F2F scheduled for Jan. 2018
Thank you for your attention!

http://csirt.egi.eu/
https://wiki.egi.eu/wiki/SVG:SVG