Coordinating Operational Security in EGI (and EOSC)

Matthew Viljoen
Service Delivery and Information Security Lead, EGI Foundation

22 June 2023

Dissemination level: Public
Disclosing Party: EGI Foundation
Recipient Party: e-IRG, Malmö
EGI – A truly distributed infrastructure

https://goc.egi.eu/portal/
Possible approaches to security

Centrally managed vs. Federated

- Central mandating of policies
- Central security/IR

- Autonomous members
- Federation agrees on policies
- Centrally distributed secure default configurations (ACLs) but final decision rests on member providers
EGI-CSIRT and security operations

EGI providers are autonomous (final decisions/actions taken by the providers)

EGI-CSIRT and the security team provide:
- Advisories on how to deal with vulnerabilities
- Security Monitoring
- Incident Response, Forensics coordination/support
- Training, drills, vulnerability/risk assessments
- Policy development and enforcement

Security team can eject insecure sites from the production infrastructure
Vulnerability response within EGI
One recent incident...

Access attempted to multiple resources by same actor

- Resource
- Identity provider
- Gateway
Approach

- Increasingly complex attacks. Federated incidents require federated approach to incident response
  - Trust and collaboration as a community
  - Collective security operations/incident response
- Policies properly adhered to a necessity
- Close collaboration needed between different e-Infrastructure CSIRT teams
  - Assessed frequently by joint security exercises

Security is everyone’s concern!
Thank you!

Contact: egi-ace-po@mailman.egi.eu
Website: www.egi.eu/projects/egi-ace

EGI Foundation
@EGI_elnfra

EGI-ACE receives funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no. 101017567.