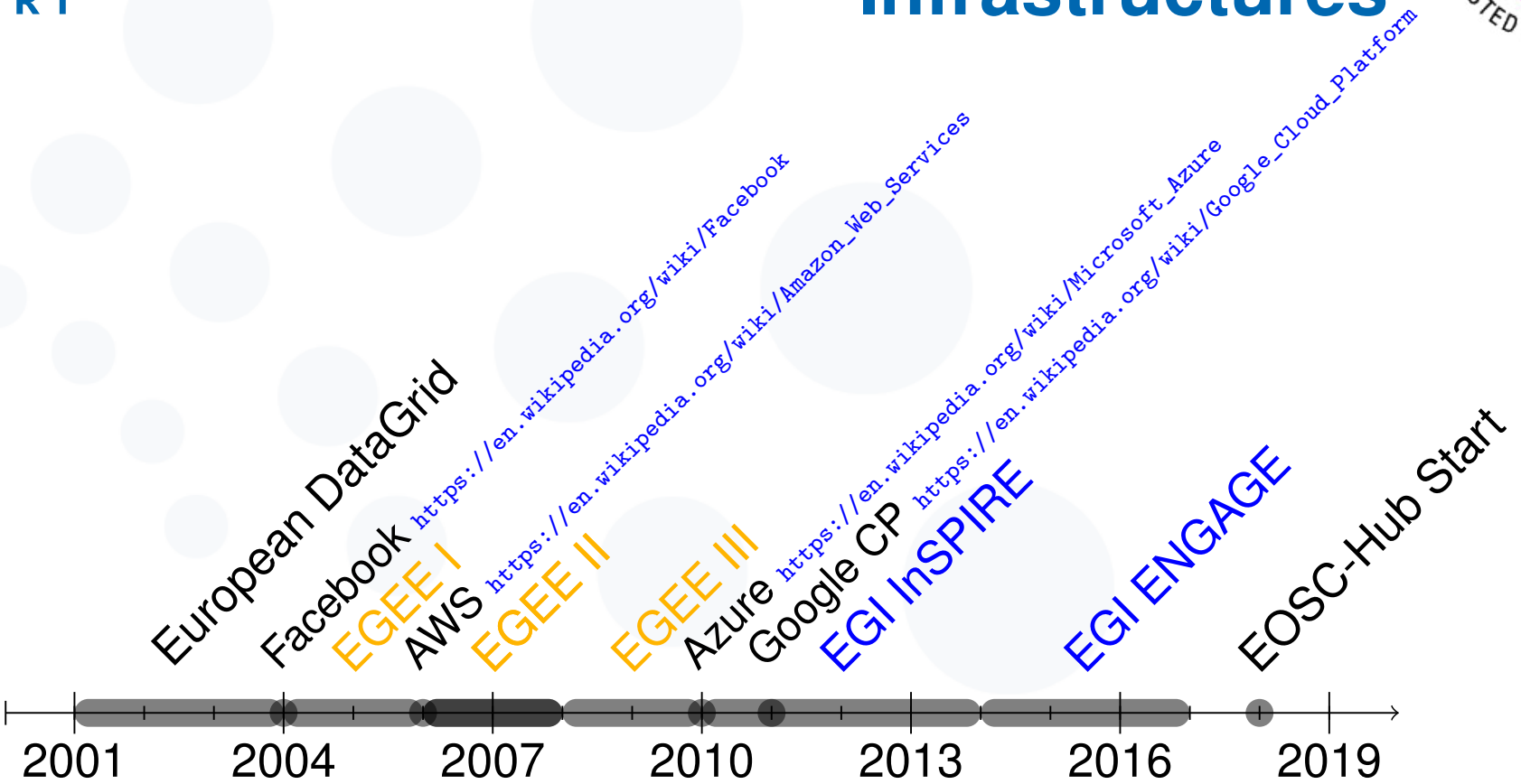
Towards cross infrastructure Operational Security in EOSC-hub

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

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

Introduction

Distributed Computing Infrastructures



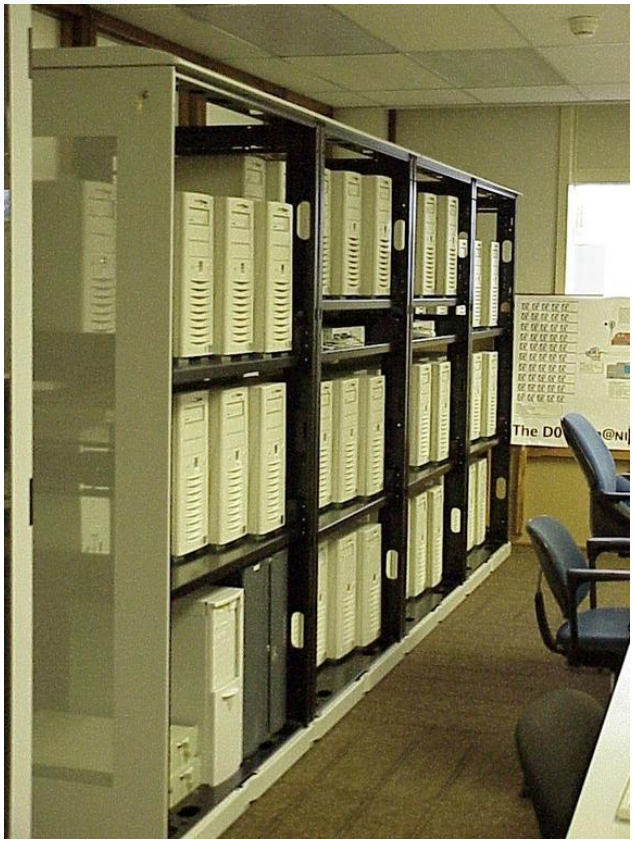
2003 WLCG Policy Group

2005 SVG, OSCT (evolved into)

2010 EGI-Foundation started, EGI CSIRT took over from OSCT

History

- EGEE I- III 2004 – 2010i.
- Middleware Development.
- Share cluster management expertises developed at RCs.
- Development of common Operational procedures/policies.



History

- EGEE I- III 2004 – 2010i.
- Middleware Development.
- Share cluster management expertises developed at RCs.
- Development of common Operational procedures/policies.

Infrastructure

Introduction, Users

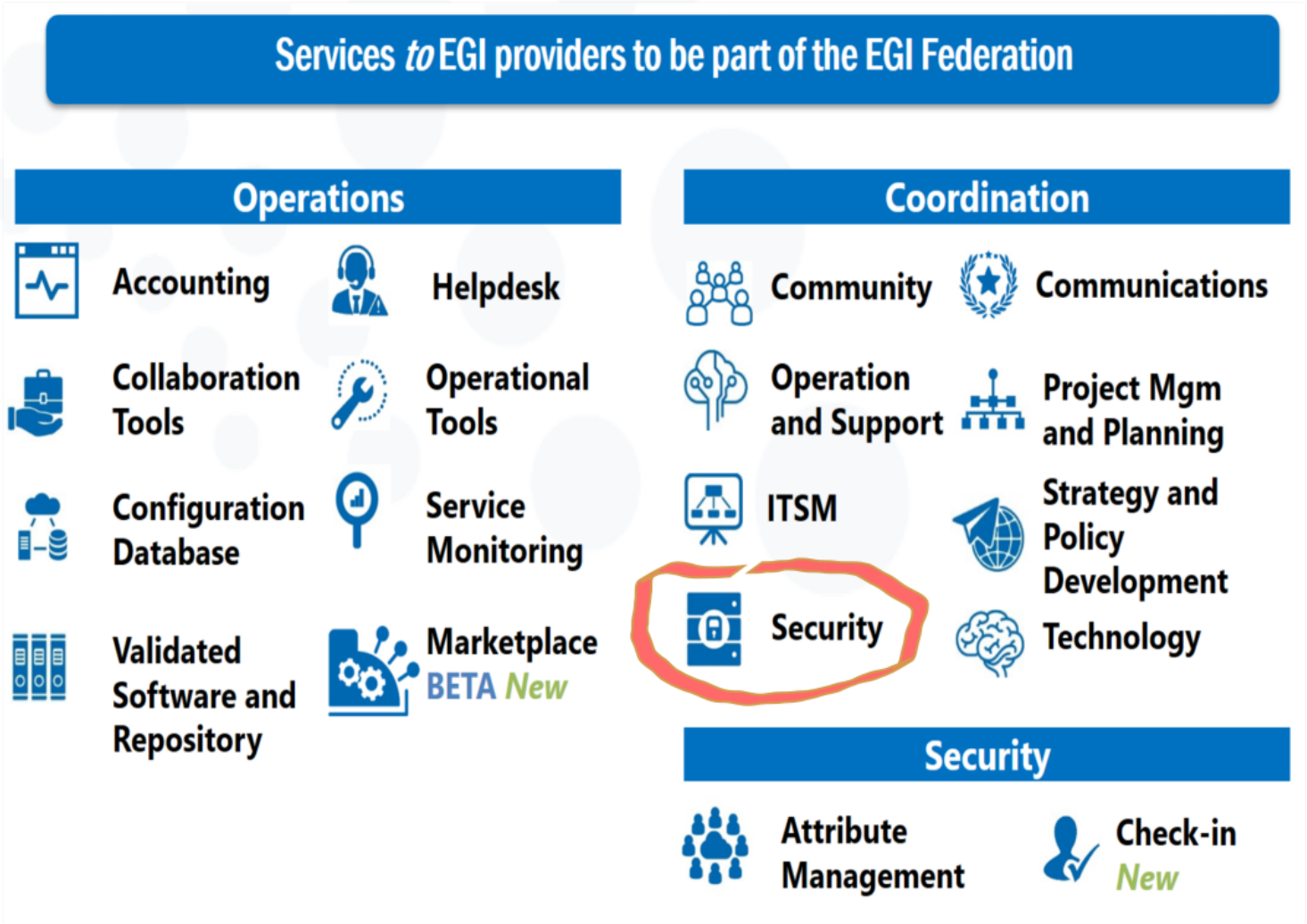
EGI: Advanced Computing for Research

EGI-Engage

EGI is a federation of over 260 computing and data centres spread across 40+ countries in Europe and worldwide

EGI delivers services to support scientists, international projects and research infrastructures

Introduction, Services provided



Introduction, Services provided

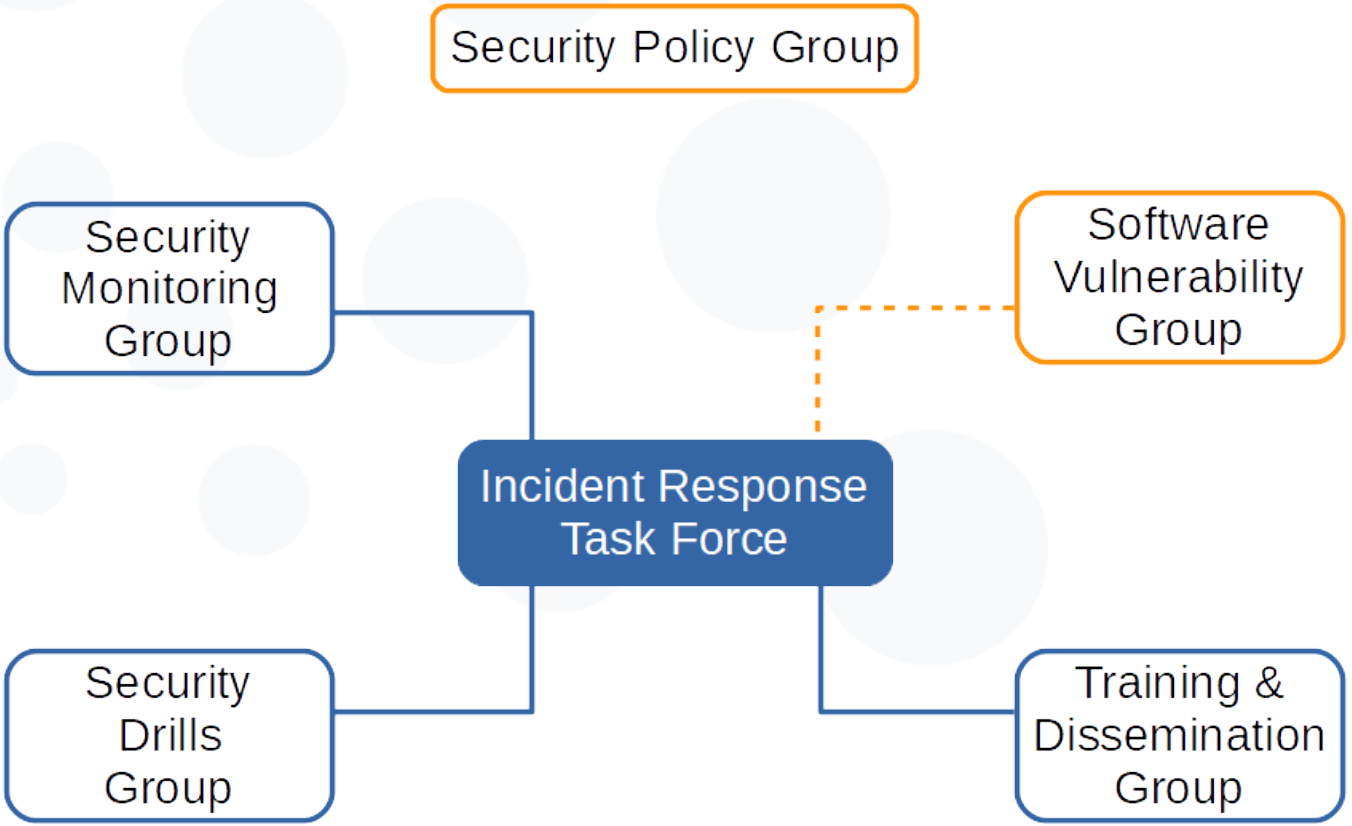
$\longrightarrow$ Central coordination needed.

EGI-CSIRT, EUDAT Security

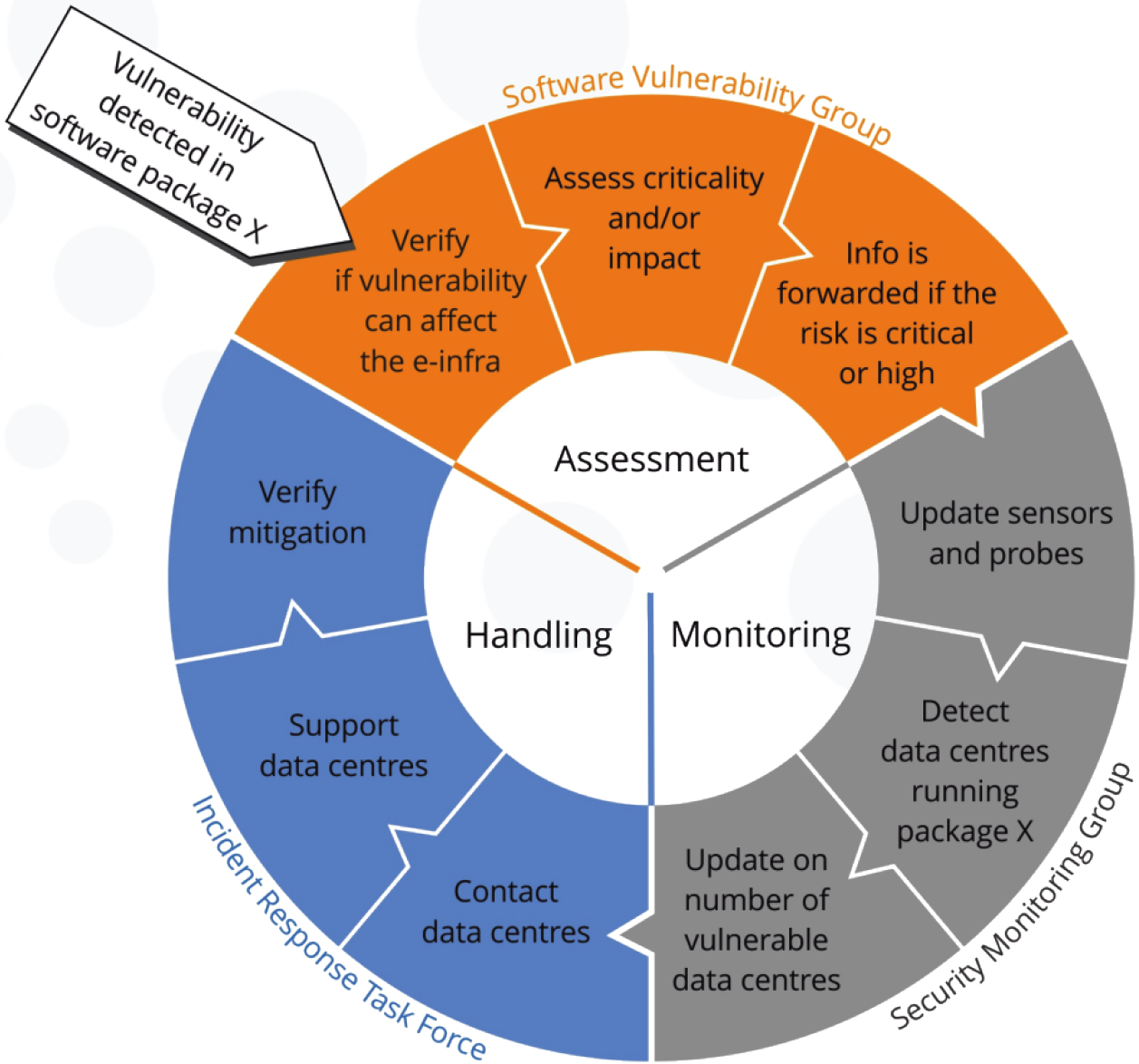
Federated e-infrastructure and security

- EGI CSIRT:
  - Security officers & experts from NGIs
  - Partial time involvement, other duties
  - Activities: Prevention, Response & Training

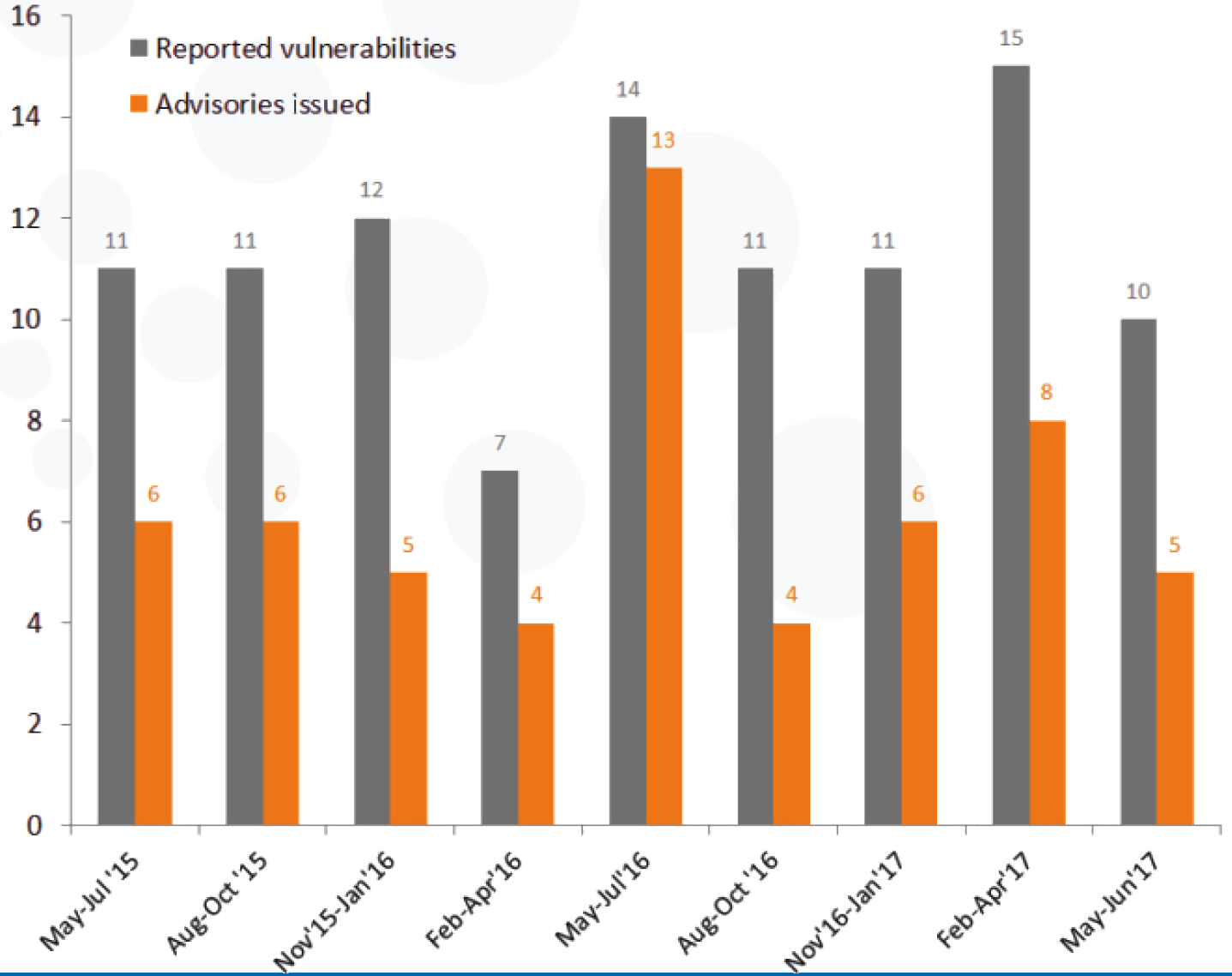
EGI CSIRT Activities & collaborations



Prevention


Vulnerability detected in software package X
Software Vulnerability Group
Verify if vulnerability can affect the e-infra
Assess criticality and/or impact
Info is forwarded if the risk is critical or high
Assessment
Verify mitigation
Update sensors and probes
Handling
Monitoring
Support data centres
Detect data centres running package X
Contact data centres
Update on number of vulnerable data centres
Incident Response Task Force
Security Monitoring Group

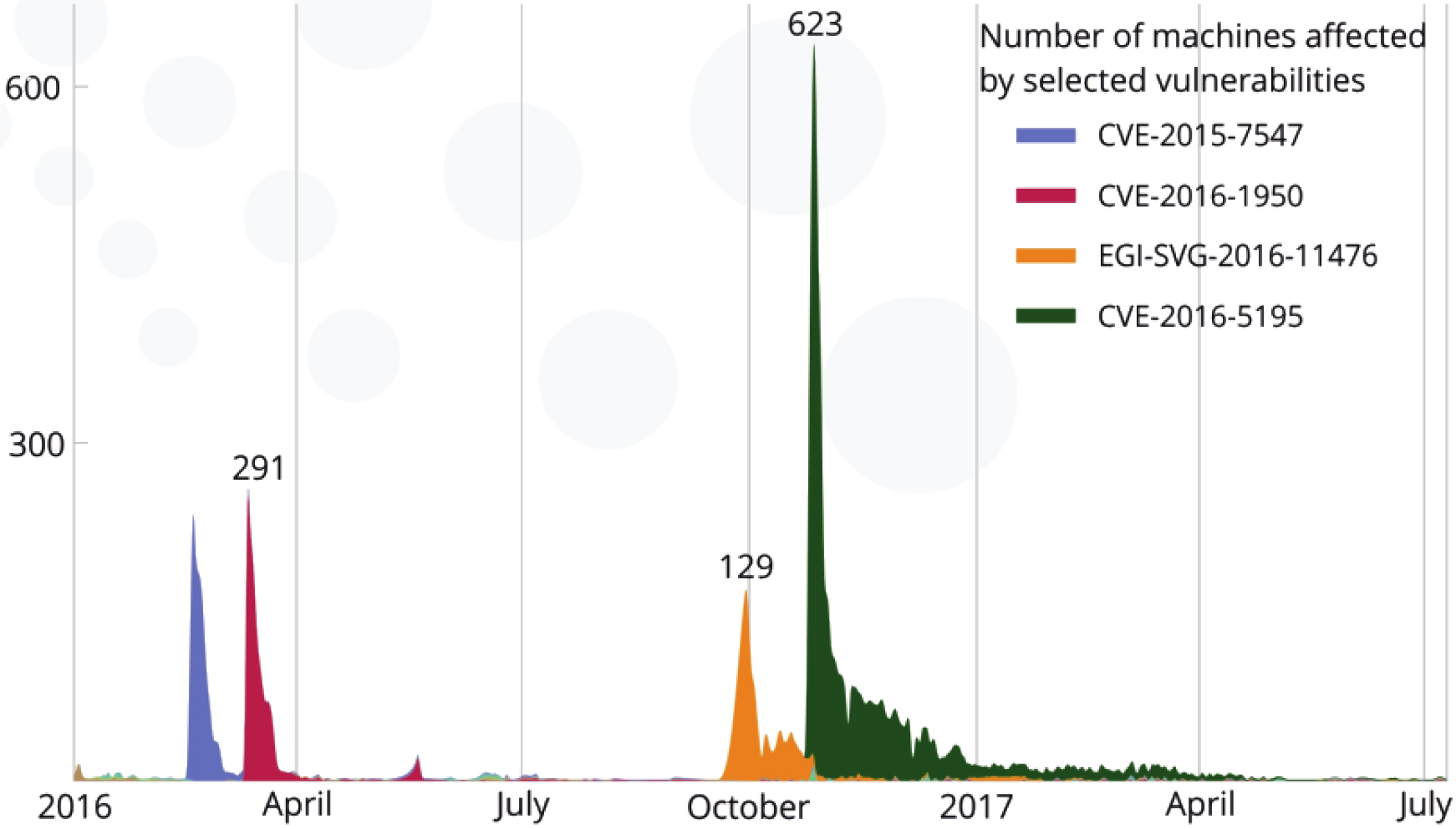
Prevention: Vulnerability reported



Prevention: Classifying vulnerabilities

- Advisories: Critical, High, Medium, Low, (Alert)
- Always to be patched, but with different priority & impact
- Only Critical is actively followed-up by the CSIRT
- Escalation possible (e.g. High -¿ Critical)

Prevention: Vulnerability hunt



Prevention: Getting help from EGI Operation

- Following data centres vulnerabilities
  - Time consuming (esp. waves)
  - Requires almost no security knowledge
  - Requires good site contacts
- Currently evaluating involving EGI Operations

Response

- IRTF roles:
  - Coordinate response: contacts, overview, actions...
  - Help with forensics analysis, guide site admins
- 44 incidents since 2010:
  - 2010-2013: SSH bruteforce, trojans, bots
  - 2013-2014: AUP violations (Bitcoin mining)
  - 2014-2017: User VM compromise (basic errors)

Response: VENOM

- Rootkit identified by an EGI site
- IRTF and site expert analysis:
  - Identify all persistence mechanisms $\rightarrow$ *IoCs*
  - Reverse the backdoor protocols $\rightarrow$ *remote scanner*
- Recursive take down possible:
  - Collect network activity from compromised systems
  - Remotely scan systems for the backdoor
  - Contact owner with IoCs for confirmation

Response: VENOM – *takedown*

- Few systems in Europe
  - Contacted directly
  - Backdoor found but no network traces
- More cases in the US
  - Forwarded to colleagues
  - Partial follow-up: 25 server identified
- Criminals & goals still unknown...

Security Challenges

- Simulate incidents over several sites
- Test all links in the chain:
  - Site security: Communication, setup & response
  - IRTF: coordination & help
  - SPG: Policies

Security Challenges 2017: Federated Cloud

- Scenario: user VMs starts DDOS & Crypto-mining
- Response:
  - 2 sites reported DDOS within few hours hours
  - Most sites suspended VMs within a day
  - Many out-of-office contributions!
- Some issues identified (e.g. suspension)
  But also very good participation from sites!

Training

- Usually at conferences or dedicated for NGI/NREN
- Different session types:
  - Defensive
  - Offensive
  - Digital forensics
  - Roleplay
- Contact us for organizing trainings!

Ongoing Challenge: Federated Cloud Security

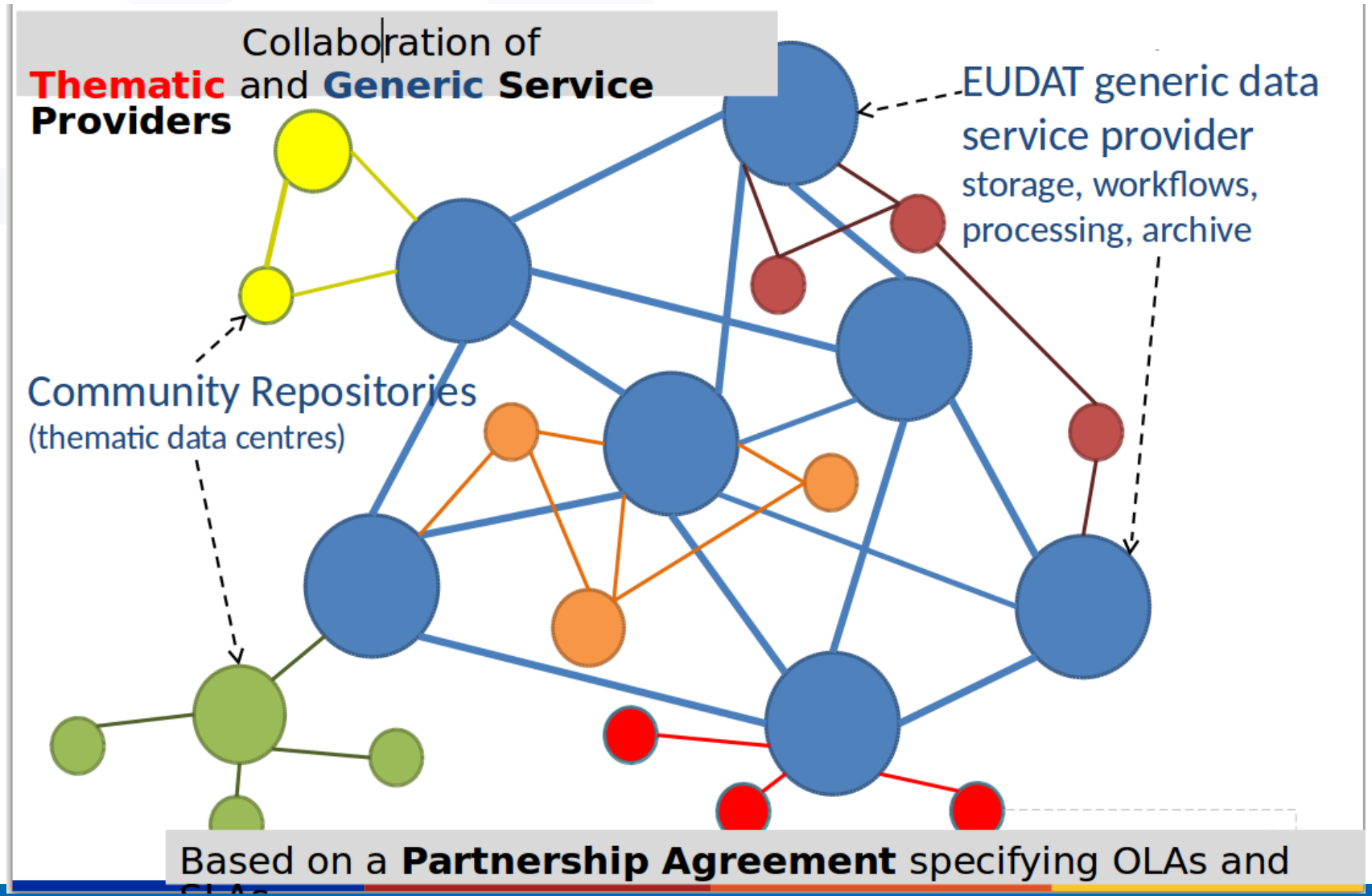
- EGI continues to develop Federated Cloud
- Cloud is difficult for users:
  - Full sysadmin, responsible for everything
  - Often directly exposed on the internet
- Most of recent incidents Cloud related

→ How to make the cloud *user-proof*?

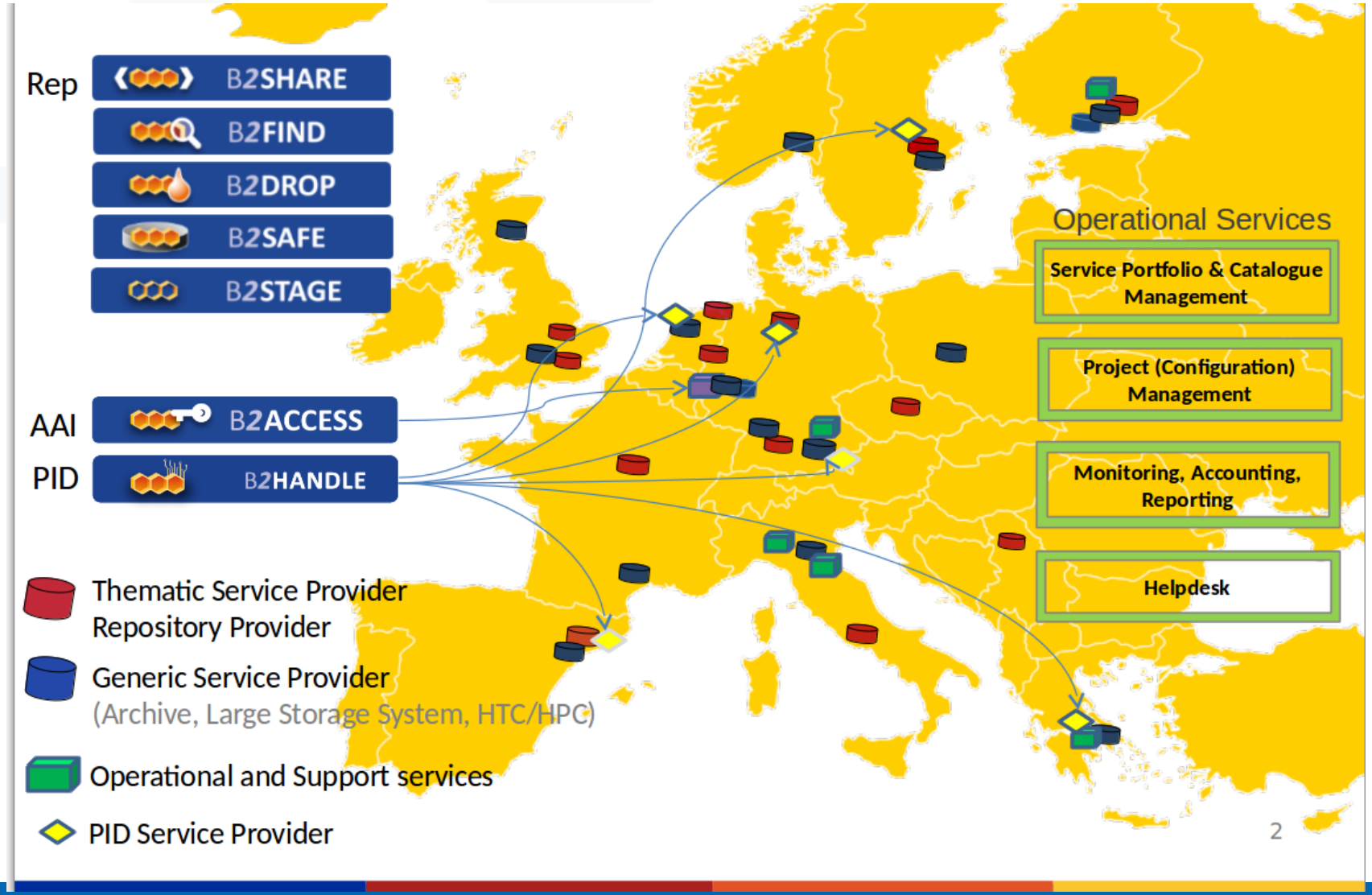
Ongoing Challenge: Federated Identity

- Simpler access to the grid (home institute credentials)
- New participants in incident response:
  - Home institutes (compromised identities, AUP violation,...)
  - Token translation services, VO portals
- How to maintain security levels?
  - Emergency suspension?
  - Incident reporting?

Collaborative Data Infrastructure



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

EUDAT EGI-CSIRT Coordination Integration II

- Operational Security needs to be backed by a set of agreed Policies.
- Differences in the Operational Security set up, and level of interaction with the RCs.
- Operational Security Services can not just be expanded to partner Infras.
- Harmonization of Policies Procedures, in progress.
- Communications framework has to be re-designed.

EUDAT EGI-CSIRT Communications

- Who, what, why? . . . some examples
- ”Vertical” Communications are different from ”Horizontal” Communications.
- Executive summary has different content then an advisory for site admins.
- Heterogeneous infra requires targeted communications, assessment needs more experts.
- Communications to peer infras need to be improved.
- Communication endpoints to AAI available/tested (Challenge run by Hannah Short)

EUDAT EGI-CSIRT Communications

$\longrightarrow$ Meeting scheduled.

Thank you for your attention!

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

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