EGI Security

David Kelsey

STFC-RAL

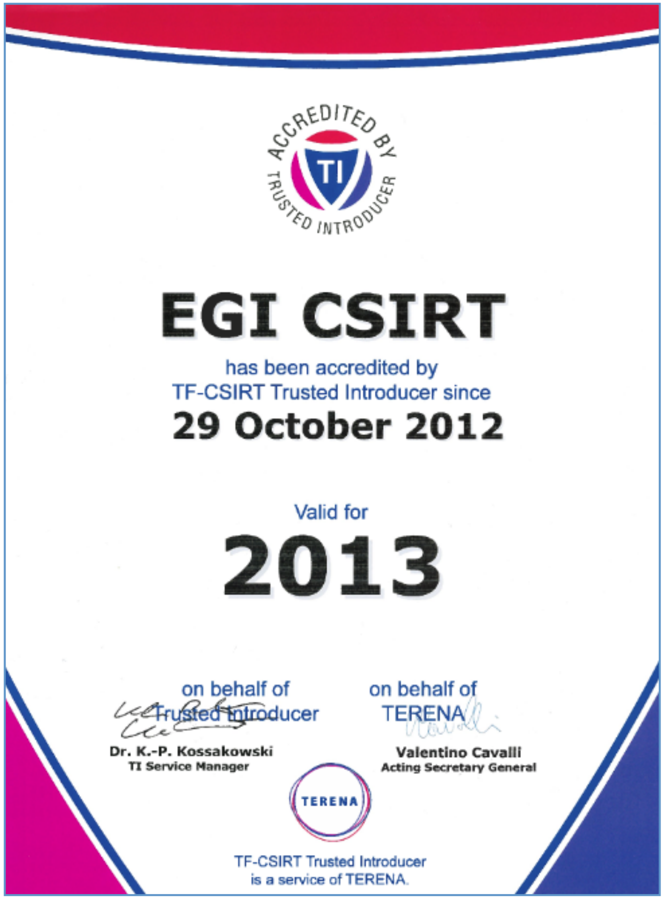
12 June 2014

EGI CSIRT

- Incident Prevention (security monitoring, security intelligence, assessment of known vulnerabilities with the support of SVG, preparation of advisories)
  - 6 EGI CSIRT alerts and advisories (xx critical, yy high risk)
    - Includes CVE-2013-2014 (linux kernel) and CVE-2014-0160 (Heartbleed)
  - 14 Software Vulnerability Group advisories (xx critical, zz high risk)
- Incident Response and Vulnerability Handling (incident handling including investigation, heads up, coordination with site CSIRTs, forensics, technical support, advisories, reports)
  - Support tickets: xx on critical vulnerabilities, yy on security incidents
  - 10 security incidents (2/PY1, 10/PY2, 3/PY3) including some unauthorised use of resources by registered users
    - Many stolen ssh passwords and brute-force ssh scan

EGI CSIRT Collaborations

- Oct 2012: Trusted Introducer accreditation
  - Member of TERENA TF-CSIRT
- – EGI CSIRT is a listed team in the European database of CSIRTs
  - 2013/4: Working towards full certification
- EGI-CSIRT collaborations
  - – Public and non-public vetted networks
    - FIRST and NREN CERTS
  - – Grid-SEC: coordinated response to cross-grid security incidents (vetted security representatives from WLCG, OSG, XSEDE, EGI)



ACCREDITED BY TRUSTED INTRODUCER

TI

EGI CSIRT

has been accredited by
TF-CSIRT Trusted Introducer since
29 October 2012

Valid for
2013

on behalf of
Trusted Introducer
Dr. K.-P. Kossakowski
TI Service Manager

on behalf of
TERENA
Valentino Cavalli
Acting Secretary General

TERENA

TF-CSIRT Trusted Introducer
is a service of TERENA.

Other Security achievements

- Security Service Challenges (SSC)
  - Framework has been improved
  - One NGI SSC was run (UK)
  - others delayed because of departure of key staff
- Several joint meetings with PRACE and EUDAT security teams
  - Including presentation of a three-day training course and certification
  - Jointly develop trust framework for security operations (SCI)
    - SCI paper V1 published in ISGC 2013 proceedings
- Central Emergency suspension mechanism deployed (Argus)
  - Procedures for this developed and adopted
- Many successful training courses given (forensics, logging, cluster management, incident handling) – EGI Tech Forum, ISGC2014, UK NGI
- Work on Federated Identity Management for Research, and new LoA profile in EUGridPMA (IOTA)

EGI Federated Cloud – multi pronged approach to advancing security

- Security Questionnaire for Technology Providers – to ensure technology complies with EGI security policy and is under security support
- Security Questionnaire for sites – will be part of certification process
- Traceability challenge to Federated cloud sites – CSIRT – in preparation
- Security monitoring for Federated Clouds – CSIRT- in planning
- Evolution of Software Vulnerability handling to encompass new technology – in planning
  - Relationship with Technology Providers is changing
- Federated Cloud Security Requirements – document planned
- Requirements on VM endorsement – in planning
- New security policies and policy revision - as needed
- Security Threat Risk assessment with Fed Cloud Focus – in planning