Infrastructure Security
(at EURISE workshop, Utrecht, 13 March 2019)

David Kelsey

UK Research and Innovation STFC

David Kelsey - who am I?

- Head of particle physics computing group at STFC UK Research and Innovation (Rutherford Appleton Laboratory)
- Various roles in *Security, Trust and Identity* since year 2000
  - EU CA Coordination Group -> EUGridPMA & IGTF
  - Security policies for GridPP (UK) & Worldwide Large Hadron Collider Computing Grid (WLCG)
  - WLCG/EGEE Joint Security Policy Group (JSPG)
  - EU-funded projects (EU DataGrid, EGEE, EGI-Inspire, EGI-Engage, AARC/AARC2, EOSC-hub)
  - FIM4R.org (Research Community Federated IdM requirements)
  - WISE & Security for Collaborating Infrastructures (SCI)
    - Since Spring 2018 - Chair of WISE steering Committee

Contents

- Security - why & how?
- Collaboration with others (WISE Community)
  - Security for Collaborating Infrastructures (SCI)
  - Sirtfi and Snctfi
- Security for Software Developers
- Security training
- Security policies

Why “Security”?

- EGI Operational Security – aims include
  - Maintain Confidentiality, Integrity, Availability
    - of services & data
  - Manage Security Risks
    - Risk assessment & mitigation
- Threats are constantly changing
  - Ongoing process of risk analysis
  - Constant evolution of policies, procedures & best practices

EGI CSIRT Activities

- Prevention of security incidents
  - Risk assessment & mitigation
  - Security Monitoring
  - Vulnerability Handling
- Incident Response
  - Support Infrastructure, community & service security teams
  - Digital forensics
  - Mitigation
- Security Drills & communication challenges
- Training and dissemination
- Security Policy Group

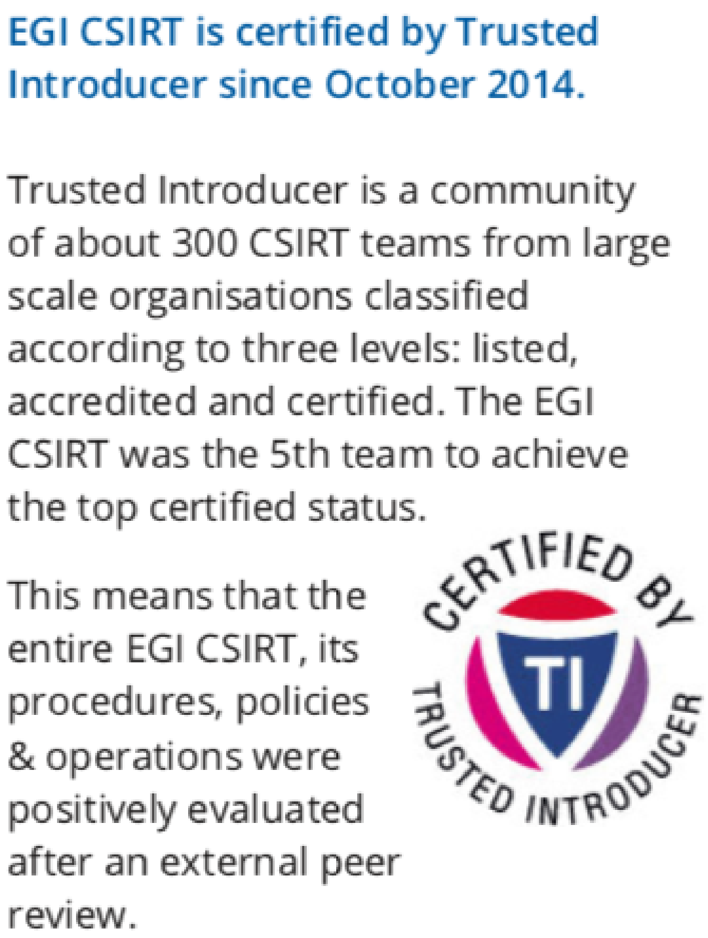
More details published in

https://www.egi.eu/wp-content/uploads/2017/07/EGI-CSIRT-report-July-2017.pdf

Keeping EGI secure

EGI CSIRT: Prevention - Response - Training

Trusted Introducer



EGI CSIRT is certified by Trusted Introducer since October 2014.

Trusted Introducer is a community of about 300 CSIRT teams from large scale organisations classified according to three levels: listed, accredited and certified. The EGI CSIRT was the 5th team to achieve the top certified status.

This means that the entire EGI CSIRT, its procedures, policies & operations were positively evaluated after an external peer review.

The WISE Community, SCI, training and policies

WISE Community – short history

- Started in October 2015 – Workshop – Barcelona
  - Jointly organized by SIG-ISM and SCI
- Community members come from Infrastructures across the world (including research infrastructures – LIGO, HEP, HBP) – all welcome
- Governed by a steering committee
  - Project managed by GEANT staff
- Real work done by Working Groups
- Meetings since mid 2017
  - NSF Cybersecurity Summit, USA – August 2017
  - STFC Abingdon, UK – February 2018
  - NSF Cybersecurity Summit, USA – August 2018
  - Next meeting (joint with SIG-ISM), Kaunas, Lithuania – April 2019

WISE mission

- *Why? The WISE community enhances best practice in information security for IT infrastructures for research.*
- *What? WISE fosters a collaborative community of security experts and builds trust between IT infrastructures, i.e. all the various types of distributed computing, data, and network infrastructures in use today for the benefit of research, including cyberinfrastructures, e-infrastructures and research infrastructures.*
- *How? Through membership of working groups and attendance at workshops these experts participate in the joint development of policy frameworks, guidelines, and templates.*

WISE meetings (Oct 2015, Feb & Aug 2018)

Barcelona, Spain

Abingdon, UK

Alexandria, VA, USA

Security for Collaborating Infrastructures (SCI)

- A collaborative activity of information security officers from large-scale infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, …
- Grew out of JSPG and IGTF – from the ground up
- We developed a *Trust framework*
  - Enable interoperation (security teams)
  - Manage cross-infrastructure security risks
  - Develop policy standards
  - Especially where not able to share identical security policies

Shared threats & shared users

- Infrastructures are subject to many of the same threats
    - Shared technology, middleware, applications and users
- User communities use multiple e-Infrastructures
    - Often using same federated identity credentials
- Security incidents often spread by following the user
    - E.g. compromised credentials
- Several e-Infrastructure security teams decided “we should collaborate”

SCI Document – version 1

- Proceedings of the ISGC 2013 conference

http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf

- The document defined a series of numbered requirements in 6 areas

PoS PROCEEDINGS OF SCIENCE

A Trust Framework for Security Collaboration among Infrastructures

David Kelsey[1]
STFC Rutherford Appleton Laboratory
Harwell Oxford, Didcot OX11 0QX, UK
E-mail: david.kelsey@stfc.ac.uk

Keith Chadwick, Irwin Gaines
Fermilab
P.O. Box 500, Batavia, IL 60510-5011, USA
E-mail: chadwick@fnal.gov, gaines@fnal.gov

David L. Groep
Nikhef, National Institute for Subatomic Physics
P.O. Box 41882, 1009 DB Amsterdam, The Netherlands
E-mail: davidg@nikhef.nl
http://orcid.org/0000-0003-1026-6606

Urpo Kaila
CSC - IT Center for Science Ltd.
P.O. Box 405, FI-02101 Espoo, Finland
E-mail: Urpo.Kaila@csc.fi

Christos Kanellopoulos
GRNET
56, Mesogion Av. 11527, Athens, Greece
E-mail: skanct@admin.grnet.gr

James Marsteller
Pittsburgh Supercomputer Center
300 S. Craig Street, Pittsburgh, PA 15213, USA
E-mail: jam@psc.edu

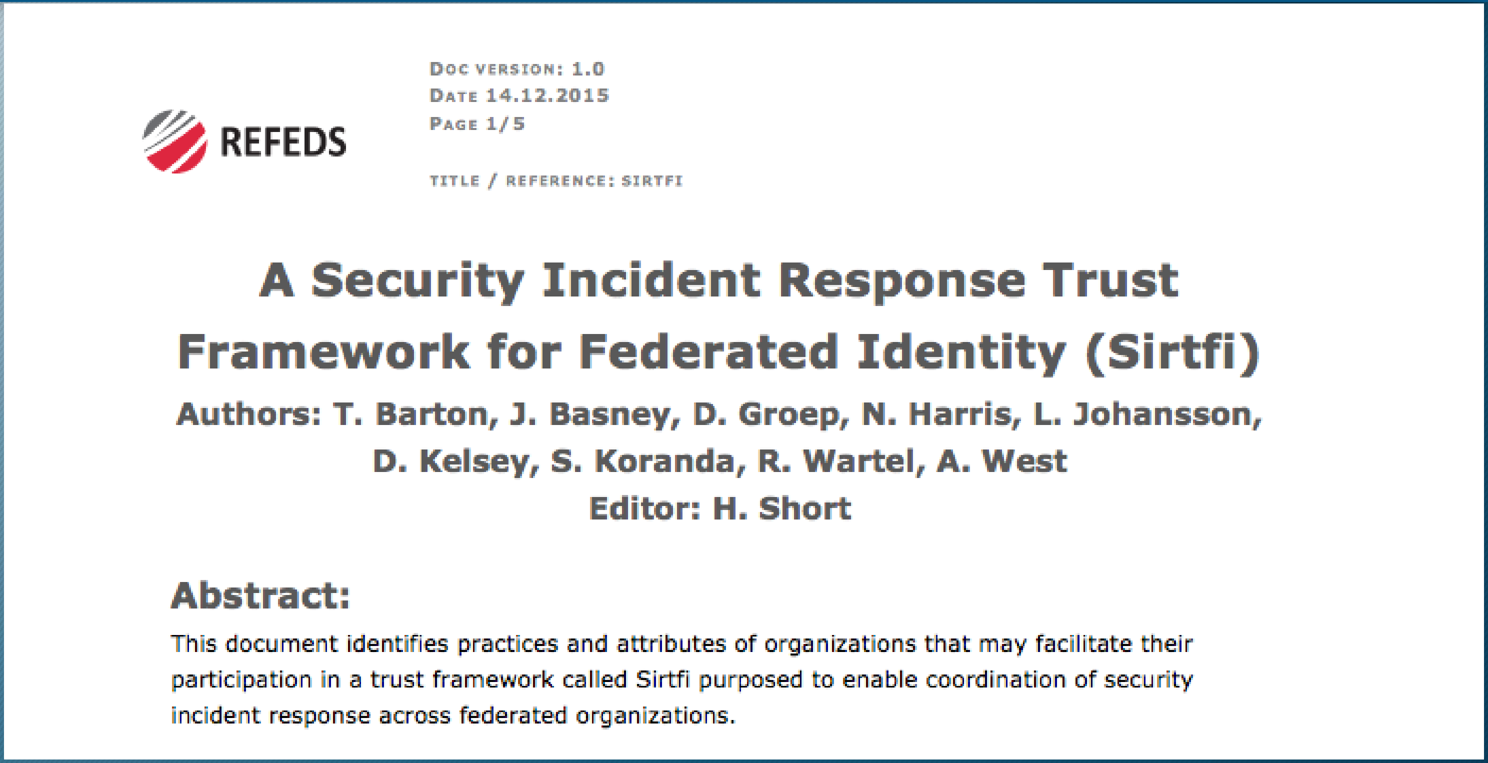
[1] Speaker

© Copyright owned by the author(s) under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike Licence.

http://pos.sissa.it

PoS(ISGC 2013)011

Sirtfi (2015)



REFEDS

Doc version: 1.0
Date 14.12.2015
Page 1/5

Title / Reference: Sirtfi

A Security Incident Response Trust Framework for Federated Identity (Sirtfi)

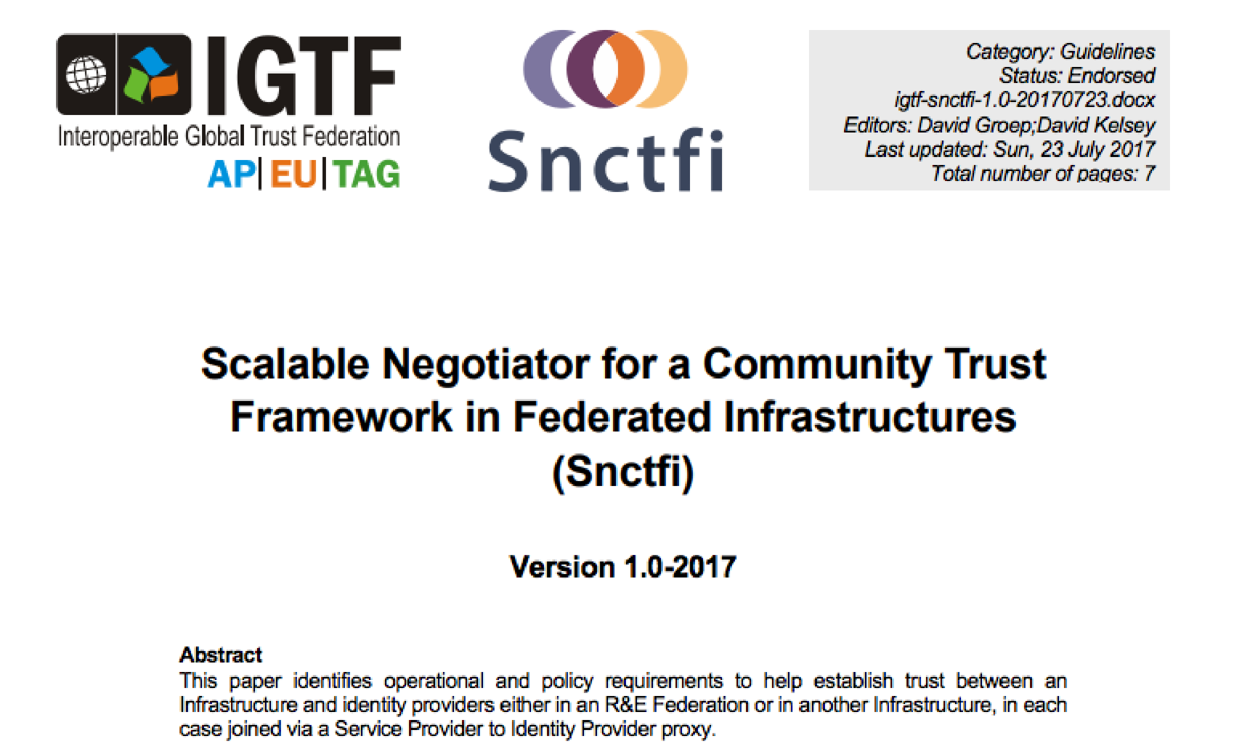
Authors: T. Barton, J. Basney, D. Groep, N. Harris, L. Johansson, D. Kelsey, S. Koranda, R. Wartel, A. West
Editor: H. Short

Abstract:

This document identifies practices and attributes of organizations that may facilitate their participation in a trust framework called Sirtfi purposed to enable coordination of security incident response across federated organizations.

https://refeds.org/sirtfi

Snctfi (2017)



IGTF
Interoperable Global Trust Federation
AP|EU|TAG

Snctfi

Category: Guidelines
Status: Endorsed
igtf-snctfi-1.0-20170723.docx
Editors: David Groep;David Kelsey
Last updated: Sun, 23 July 2017
Total number of pages: 7

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)

Version 1.0-2017

Abstract
This paper identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

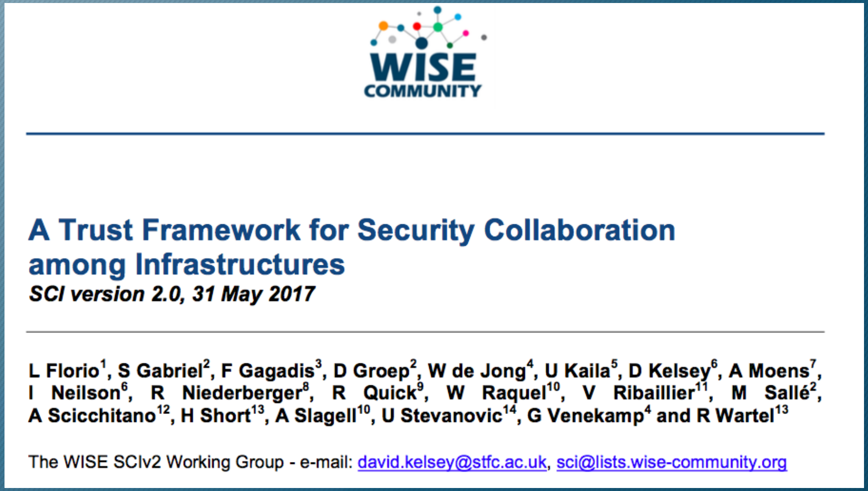
https://www.igtf.net/snctfi/

WISE SCI Version 2

- Aims
  - Involve more stakeholders
  - Address any conflicts in version 1
  - Add/remove topics/areas
  - Revise all wording of requirements
  - Simplify!
- SCI Version 2 was published on 31 May 2017
- https://wise-community.org/sci/

SCI Version 2 – published 31 May 2017

WISE COMMUNITY



WISE COMMUNITY

A Trust Framework for Security Collaboration among Infrastructures

SCI version 2.0, 31 May 2017

L Florio[1], S Gabriel[2], F Gagadis[3], D Groep[2], W de Jong[4], U Kaila[5], D Kelsey[6], A Moens[7], I Neilson[6], R Niederberger[8], R Quick[9], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[10], U Stevanovic[14], G Venekamp[4] and R Wartel[13]

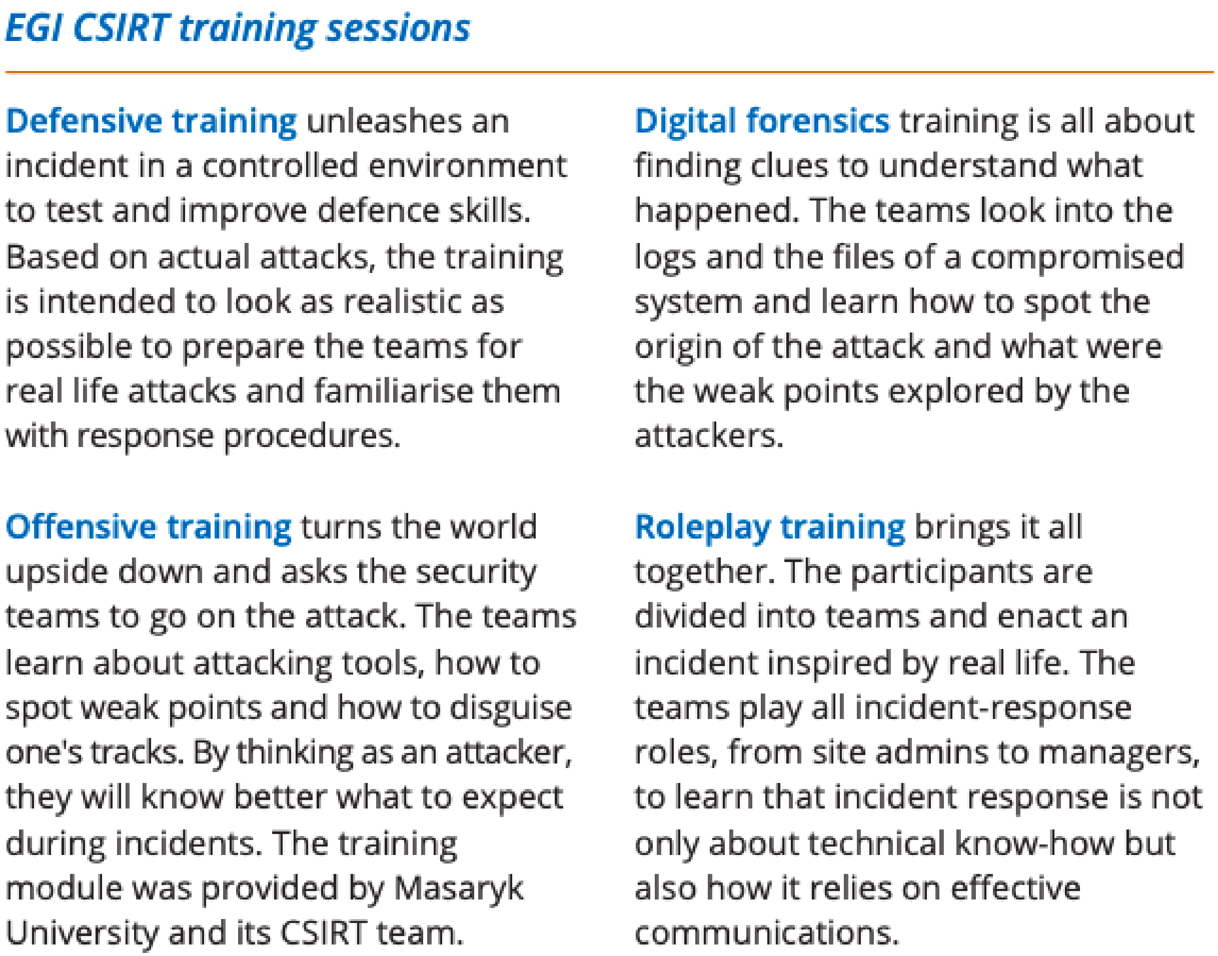
The WISE SCIv2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

https://wise-community.org/sci/

Endorsement of SCI Version 2 at TNC17 (Linz)

- 1st June 2017
- *Infrastructures endorse the governing principles and approach of SCI, as produced by WISE, as a medium of building trust between infrastructures, to facilitate the exchange of security information in the event of a cross-infrastructure incident, and the collaboration of e-Infrastructures to support the process. These Infrastructures welcome the development of an information security community for the Infrastructures, and underline that the present activities by the research and e-Infrastructures should be continued and reinforced*
- Endorsements have been received from the following infrastructures; EGI, EUDAT, GEANT, GridPP, MYREN, PRACE, SURF, WLCG, XSEDE, HBP
- https://www.geant.org/News_and_Events/Pages/supporting-security-for-collaborating-infrastructures.aspx

EGI Security training



EGI CSIRT training sessions

Defensive training unleashes an incident in a controlled environment to test and improve defence skills. Based on actual attacks, the training is intended to look as realistic as possible to prepare the teams for real life attacks and familiarise them with response procedures.

Offensive training turns the world upside down and asks the security teams to go on the attack. The teams learn about attacking tools, how to spot weak points and how to disguise one's tracks. By thinking as an attacker, they will know better what to expect during incidents. The training module was provided by Masaryk University and its CSIRT team.

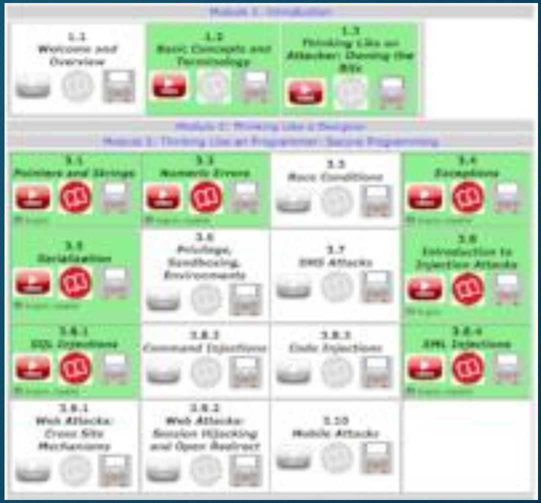
Digital forensics training is all about finding clues to understand what happened. The teams look into the logs and the files of a compromised system and learn how to spot the origin of the attack and what were the weak points explored by the attackers.

Roleplay training brings it all together. The participants are divided into teams and enact an incident inspired by real life. The teams play all incident-response roles, from site admins to managers, to learn that incident response is not only about technical know-how but also how it relies on effective communications.

EGI.eu offers ISO27001 training

Security & software developers

- Training & guidance
- https://wiki.egi.eu/wiki/SVG:Secure_Coding
- https://wiki.egi.eu/wiki/SVG:Software_Security_Checklist
- https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/
- https://trustedci.org/trainingmaterials



Module 1: Introduction

1.1 Welcome and Overview	1.2 Basic Concepts and Terminology	1.3 Thinking Like an Attacker: Owning the Bits	

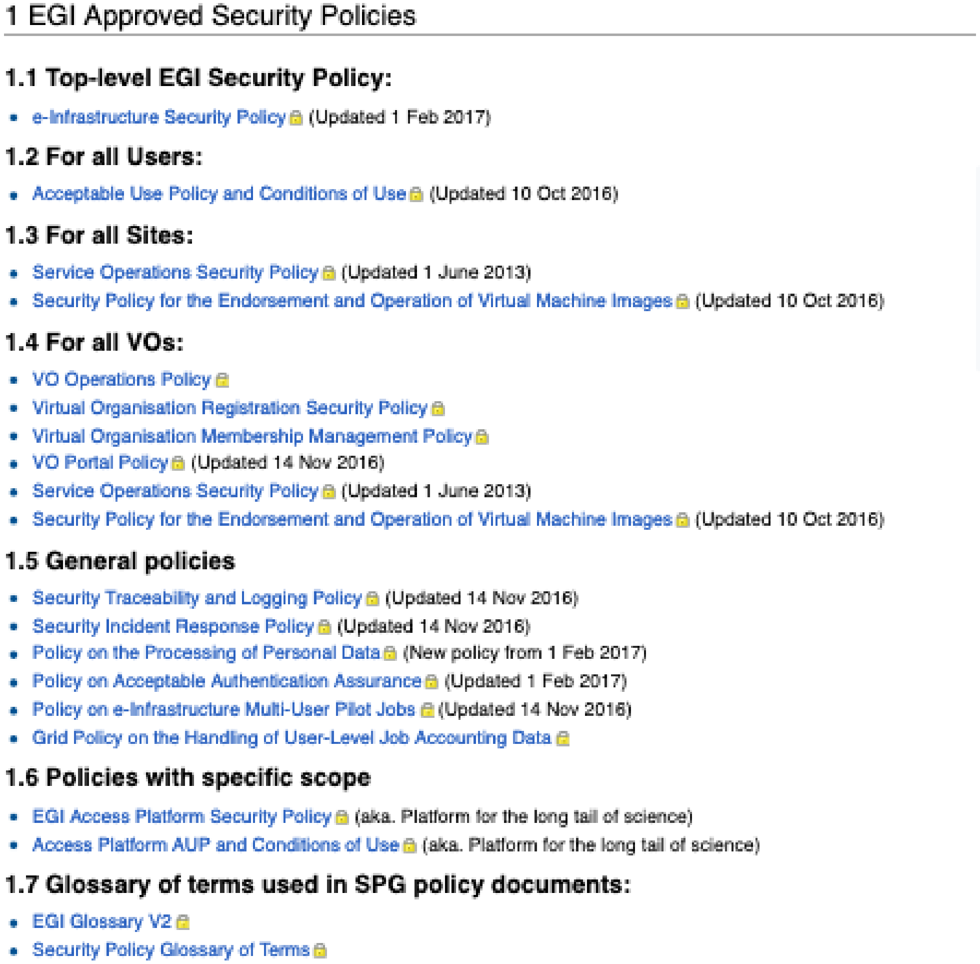
Module 2: Thinking Like a Designer

Module 3: Thinking Like an Programmer: Secure Programming

3.1 Pointers and Strings	3.2 Numeric Errors	3.3 Race Conditions	3.4 Exceptions
3.5 Serialization	3.6 Privilege, Sandboxing, Environments	3.7 DNS Attacks	3.8 Introduction to Injection Attacks
3.8.1 SQL Injections	3.8.2 Command Injections	3.8.3 Code Injections	3.8.4 XML Injections
3.9.1 Web Attacks: Cross Site Mechanisms	3.9.2 Web Attacks: Session Hijacking and Open Redirect	3.10 Mobile Attacks	

- Software assurance tool – code analysis https://www.mir-swamp.org

EGI/EOSC-hub Security Policy



1 EGI Approved Security Policies

1.1 Top-level EGI Security Policy:

- e-Infrastructure Security Policy (Updated 1 Feb 2017)

1.2 For all Users:

- Acceptable Use Policy and Conditions of Use (Updated 10 Oct 2016)

1.3 For all Sites:

- Service Operations Security Policy (Updated 1 June 2013)
- Security Policy for the Endorsement and Operation of Virtual Machine Images (Updated 10 Oct 2016)

1.4 For all VOs:

- VO Operations Policy
- Virtual Organisation Registration Security Policy
- Virtual Organisation Membership Management Policy
- VO Portal Policy (Updated 14 Nov 2016)
- Service Operations Security Policy (Updated 1 June 2013)
- Security Policy for the Endorsement and Operation of Virtual Machine Images (Updated 10 Oct 2016)

1.5 General policies

- Security Traceability and Logging Policy (Updated 14 Nov 2016)
- Security Incident Response Policy (Updated 14 Nov 2016)
- Policy on the Processing of Personal Data (New policy from 1 Feb 2017)
- Policy on Acceptable Authentication Assurance (Updated 1 Feb 2017)
- Policy on e-Infrastructure Multi-User Pilot Jobs (Updated 14 Nov 2016)
- Grid Policy on the Handling of User-Level Job Accounting Data

1.6 Policies with specific scope

- EGI Access Platform Security Policy (aka. Platform for the long tail of science)
- Access Platform AUP and Conditions of Use (aka. Platform for the long tail of science)

1.7 Glossary of terms used in SPG policy documents:

- EGI Glossary V2
- Security Policy Glossary of Terms

- EGI Security Policy Group
- All policies are deliberately general and re-usable
- https://wiki.egi.eu/wiki/SPG:Documents

- *Policies now being re-visited and modified by EOSC-hub ISM task (4.4) using the AARC Policy Development Kit (to move to WISE)*

In EOSC-hub – we use the AARC PDK as starting point

Security Policies – AARC2

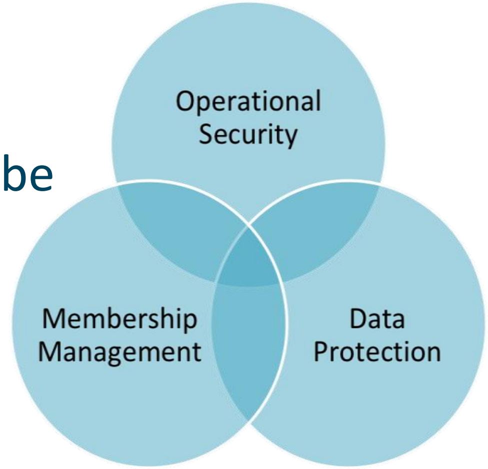
Policy Development Kit

https://aarc-project.eu/policies/policy-development-kit/

Will move to WISE for Sustainability

Which policies?

- SCI paper (*A Trust Framework for Security Collaboration among Infrastructures)*
- SNCTFI (*Scalable Negotiator for a Community Trust Framework in Federated Infrastructures)*
  - Top level policy
    - Operational Security
    - Membership management
    - Data protection
- Consider current best practices (EGI, CERN, ELIXIR, TrustedCI, etc.)
- Policies started from EGI versions
  - And then modified
- Some other policies (Infrastructure-related) will need to be handled by WISE/EOSC-hub



A common AUP - motivation

To make a recommendation for the content of an Acceptable Use Policy (AUP) to act as a baseline policy (or template) for adoption by research communities

- To facilitate -
  a) a more rapid community infrastructure 'bootstrap'
  b) ease the trust of users across infrastructures
  c) provide a consistent and more understandable enrolment for users.
- Adoption of a single policy preferred to modifying a template

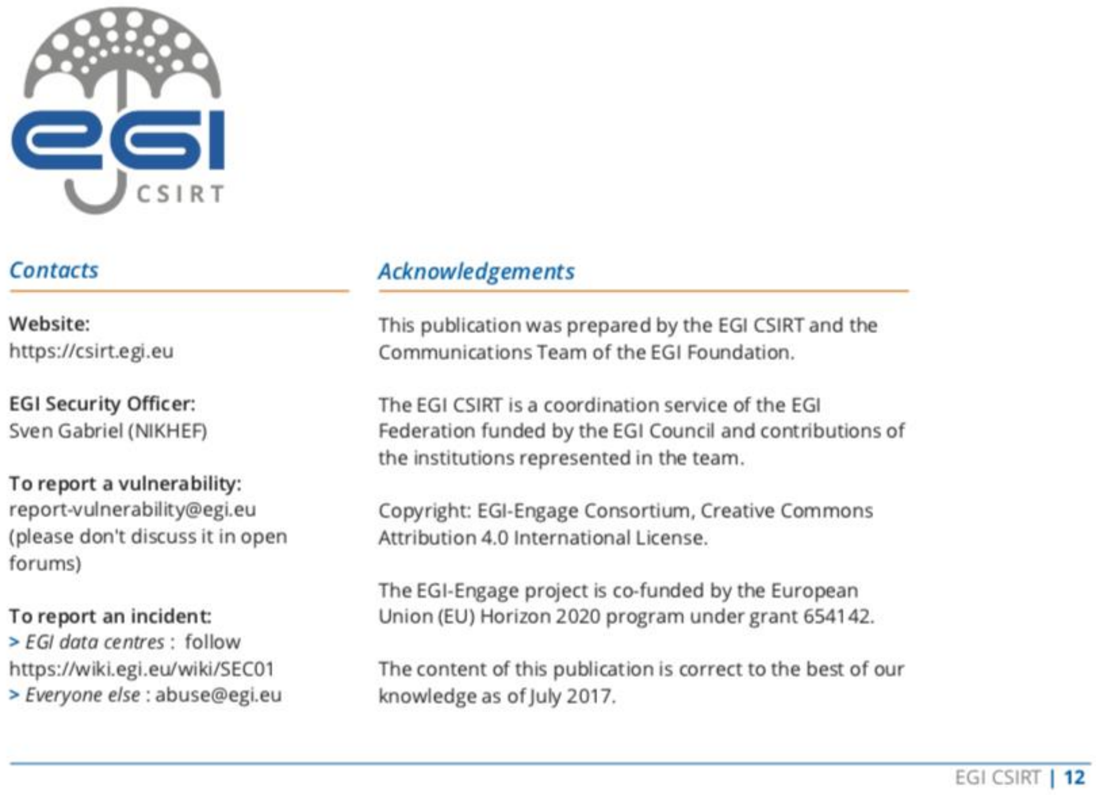
How will this Baseline AUP used?

- Forms part of the information shown to a user during registration with his/her community
- AUP provides information on expected behaviour and restrictions
- "baseline" text can, optionally, be augmented with additional, community or infrastructure specific, clauses as required, but the numbered clauses should not be changed
- The registration point where the user is presented with the AUP may be operated directly by the user's research community or by a third party on the community's behalf

AUP use (2)

- Other information shown to user during registration
- Privacy Notice - information about the processing of their personal data together with their rights under law regarding this processing
- Service Level Agreements - information about what the user can expect from the service in terms of quality such as reliability and availability
- (Optional) Terms of Service

More Information



CSIRT

Contacts

Website:
https://csirt.egi.eu

EGI Security Officer:
Sven Gabriel (NIKHEF)

To report a vulnerability:
report-vulnerability@egi.eu
(please don't discuss it in open forums)

To report an incident:
> *EGI data centres* : follow https://wiki.egi.eu/wiki/SEC01
> *Everyone else* : abuse@egi.eu

Acknowledgements

This publication was prepared by the EGI CSIRT and the Communications Team of the EGI Foundation.

The EGI CSIRT is a coordination service of the EGI Federation funded by the EGI Council and contributions of the institutions represented in the team.

Copyright: EGI-Engage Consortium, Creative Commons Attribution 4.0 International License.

The EGI-Engage project is co-funded by the European Union (EU) Horizon 2020 program under grant 654142.

The content of this publication is correct to the best of our knowledge as of July 2017.

EGI CSIRT | 12

Thank you for your attention.

Questions?