

Trust and Incident Response Cooperation Frameworks

David Crooks

Who am I?

- David Crooks
- GridPP Security Officer
- Member of EGI CSIRT Incident Response Task Force
- Used to be System Manager at Glasgow Tier-2
- Originally (a long time ago!) I worked in Gravitational Waves and on the early development of Advanced LIGO

What is security for?

- Confidentiality
 - Applying appropriate protections to keep data secure
- Integrity
 - Consistency and trustworthiness of data
- Availability
 - Services/data are available when they're expected to be

Confidentiality

- Are there appropriate controls on access to our data?
 - May depend on the nature of the data, but always important

Integrity

- Can we trust our data?
- Now?
- Reproducing results in the future?

Availability

- What is the cost of an incident in terms of outages?
 - Reputation
 - Service availability
 - What happens if there is a major incident at conference time?
 - Particularly in times of heightened stress, want to have procedures in place.

Components of security

- Trust and policy
 - What does the community determine to be acceptable?
 - How does a community interact with its sites, and other communities?
 - Do I know how other parts of the community will respond?
- Operational Security
 - Incident prevention
 - Incident response
 - Training and documentation
- Authentication and Authorisation Infrastructure
 - Other ongoing work, but important part of security fabric

Distributed community

- Shared threats
- Shared users
- Shared access mechanisms
- Shared response
 - Intelligence is a key element in responding to attacks

Distributed security

- Particular features of security in a distributed environment
- Who handles incident response?
 - What are the boundaries of this response?
- Who is responsible?

Maturity

- Everything is a process
- If you look at any mature security function, based on years of development
- Iterative process

Case study

EGI CSIRT

- Specifically distributed team
- Components
 - Policy
 - Drills
 - Monitoring
 - Incident Response
 - (Vulnerability Assessment)

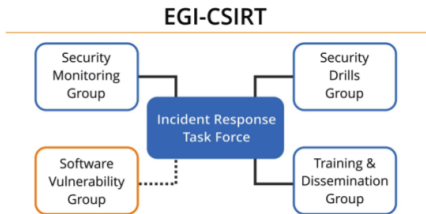


- current NGIs, Sites, ... <https://goc.egi.eu/portal/>
- Production Sites 450 (certified 343)
- NGIs 39 (some consist of multiple countries)

Policy framework in EGI provides CSIRT with:

- Have the infrastructure responsive to vulnerabilities
- Have the infrastructure ready to contribute in Incident Response (IR), logs etc
- Have the infrastructure to actively contribute in IR, information sharing
- Have a possibility to enforce actions (escalations)

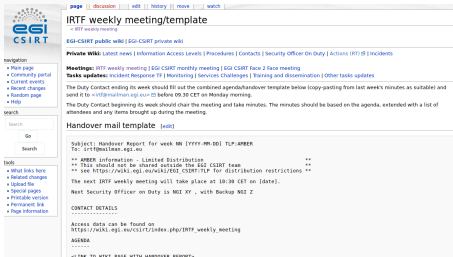
- Project wide coordination of operational security activities.
- Procedure / Policy development, testing these in . . .
- Security Service Challenges
- Security Monitoring
- Enforcing procedures/policies
- Allows for centralized tools (suspending IDs infrastructure wide, also on Christmas eve)
- Interfacing to other (Grid/NREN/VO) CSIRTs



The EGI Computer Security and Incident Response Team (EGI-CSIRT) provides operational security for the EGI Infrastructure. This includes responding to computer security incidents affecting the infrastructure, which is carried out by co-ordinating the incident handling activities in the NGIs/EIROs, RCs, VOs, and where applicable interacting with partner Infrastructures CSIRTs and CSIRT communities with which EGI-CSIRT has a trust relationship.

<https://documents.egi.eu/secure/ShowDocument?docid=385&version=12>

- Rota: Security Officer on Duty (IRTF members 6)
- Handover, follow up in RT-IR
- Security Dashboard: Results from Monitoring, SVG
- Communication end points in Goc-DB , ... are tested



The screenshot shows a wiki page for the IRTF weekly meeting template. It includes a navigation menu, a search bar, and a table of contents. The main content area contains the following text:

IRTF weekly meeting/template
 IRTF weekly meeting

EGI-CSIRT public wiki | EGI-CSIRT private wiki

Private Wiki: Latest news | Information Access Levels | Procedures | Contacts | Security Officer On Duty | Actions IRTF @ | Incidents

Navigation:
 • Main page
 • Community portal
 • Current events
 • Recent changes
 • Random page
 • Help

Meetings: IRTF weekly meeting | EGI-CSIRT monthly meeting | EGI-CSIRT Face 2 Face meeting

Tasks updates: Incident Response TF | Monitoring | Services Challenges | Training and dissemination | Other tasks updates

The Duty Contact ending its week should fill out the combined agenda/handover template below (copy-pasting from last week's minutes as suitable) and send it to irtf@mainline.egi.eu before 09:30 CET on Monday morning.

The Duty Contact beginning its week should chair the meeting and take minutes. The minutes should be based on the agenda, extended with a list of attendees and any items brought up during the meeting.

Handover mail template [edit]

Subject: Handover Report for week NN (YYYY-MM-DD) TLP:AMBER
 To: irtf@mainline.egi.eu

** AMBER information - Limited Distribution **
 ** This should not be shared outside the EGI CSIRT team **
 ** See https://wiki.egi.eu/wiki/EGI_CSIRT_TLP for distribution restrictions **

The next IRTF weekly meeting will take place at 10:30 CET on [date].
 Next Security Officer on Duty is NO2 XY , with Backup NO2 Z

CONTACT DETAILS

 Access data can be found on
https://wiki.egi.eu/wiki/index.php/IRTF_weekly_meeting
 AGENDA

 <LINK TO WIKI PAGE WITH HANDOVER REPORT>

SIM3 and Trusted Introducer

- Example of work on maturity models
- GEANT TF-CSIRT
- Trusted Introducer



SIM3 : Security Incident Management Maturity Model

SIM3 m&XVIII
Don Stikvoort, 30 March 2015

© S-CURE bv and PRESECURE GmbH 2008-2015 ;
The GEANT Association (home for TF-CSIRT) and
SURFnet bv, have an unlimited right-to-use providing
author and copyright statement are reproduced; changes
only by copyright holders S-CURE and PRESECURE.

Thanks are due to the TI-CERT "certification" WG (Serge
Droz, chair, Gosard Bazic, Marek Maj, Ugo Kalla, Klaus-
Peter Kosakowski, Don Stikvoort) and to Jimmy
Arvidsson, Andrew Connack, Lionel Ferret, Aart Jochem,
Peter Jorg, Chris Malagon, Kevin Meynck, Alf Moosa,
Andri Oostervik, Carol Overton, Ronald Reijers, Jacques
Schoutman, Bert Stals and Karel Vietsch for their valuable
contributions.

Contents

Starting Points	2
Basic SIM3	3
SIM3 Reporting	4
SIM3 Parameters	6
O - "Organization" Parameters	7
H - "Human" Parameters	8
T - "Tools" Parameters	9
P - "Processes" Parameters	10

WISE Community

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.*

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”

Security for Collaborating Infrastructures (SCI-WG)



- A collaborative activity of information security officers from large-scale infrastructures
 - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, HBP...
- Grew out of EGEE/WLCG 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

SCI version 1 (2013) - children



- Both separate derivatives of SCI version 1
- REFEDS **Sirtfi** - The Security Incident Response Trust Framework for Federated Identity
 - requirement in FIM4R version 1 paper
 - <https://refeds.org/sirtfi>
- AARC/IGTF **Snctfi** - The Scalable Negotiator for a Community Trust Framework in Federated Infrastructures
 - For scalable policy - Research Services behind a SP/IdP proxy
 - <https://www.igtf.net/snctfi/>



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.



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.

WISE SCI Version 2



- Aims
 - Involve wider range of stakeholders
 - GEANT, NRENS, Identity federations, ...
 - Address any conflicts in version 1 for new stakeholders
 - Add new topics/areas if needed (and indeed remove topics)
 - 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



A Trust Framework for Security Collaboration among Infrastructures

SCI version 2.0, 31 May 2017

L Florio¹, S Gabriel², F Gagadis³, D Groep², W de Jong⁴, U Kaila⁵, D Kelsey⁶, A Moens⁷,
I Neilson⁶, R Niederberger⁸, R Quick⁹, W Raquel¹⁰, V Ribaillier¹¹, M Sallé²,
A Scicchitano¹², H Short¹³, A Slagell¹⁰, U Stevanovic¹⁴, G Venekamp⁴ and R Wartel¹³

The WISE SCIV2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

Sections of V2 paper



- In this document, we lay out a series of numbered requirements in five areas (operational security, incident response, traceability, participant responsibilities and data protection) that each Infrastructure should address as part of promoting trust between Infrastructures
- I will now show an example of some text from SCI V2

4. Incident Response [IR]

Each *infrastructure* has the following:

- [IR1] A process to maintain security contact information for all *service providers* and communities.
- [IR2] A documented Incident Response procedure. This must address: roles and responsibilities of individuals and teams, identification and assessment of incidents, minimisation of damage to the *infrastructure*, response and recovery strategies to restore *services*, communication and tracking tools and procedures, and a post-mortem review to capture lessons learned.
- [IR3] The capability to collaborate in the handling of security incidents with affected *service providers*, communities, and *infrastructures*, together with processes to ensure the regular testing of this capability.
- [IR4] Policies and procedures to ensure compliance with information sharing restrictions on incident data exchanged during collaborative investigations. If no information sharing guidelines are specified, incident data will only be shared with other security teams on a need to know basis, and will not be redistributed further without prior approval.



AARC

AARC

- The **Authentication and Authorisation for Research and Collaboration (AARC)** initiative was first launched in May 2015 to address the increased need for federated access and for authentication and authorisation mechanisms by research and e-infrastructures.

AARC2 Policy Development Kit

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



Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	Google Doc
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Google Doc
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.	Google Doc
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.	Google Doc
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.	Google Doc
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	Users (view)	This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.	Google Doc
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.	Google Doc
Acceptable Use Policy	Infrastructure Management (for baseline) & Research Communities (for community specific restrictions)	Users (abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.	Google Doc

IRIS Proposal

- Submitted a proposal to develop first version of
 - Trust framework
 - Incident response cooperation framework
- Myself, Ian Neilson and Dave Kelsey

Trust framework

- Using our experience, build the policies that IRIS need at this stage
- A typical initial set of policies may comprise
 - Top Level Security Policy
 - What are the individual roles involved
 - Tie policies together
 - Acceptable Use Policy
 - What we expect of users
 - Privacy Policy
 - Required now particularly in light of GDPR

Incident response cooperation framework

- What incident response capabilities are in use now?
- Who could we contact at sites and experiments about security?
- Building trust
- Build from there

Conclusion

- In a distributed community, security is a community endeavour
- Collaboration enriches the whole
- Trust between community members is key
 - How do we engender that?
- Security should act to support the community to promote that trust and allow normal operations to proceed in a secure, well understood environment
 - And if something *does* happen, have the trust over how people will react