WISE 2016

WISE: a global trust community where security experts share information and work together, creating collaboration among different e-infrastructures

Alf Moens

Participants in WISE

- WISE is for the e-infrastructures, globally, both networking and super- and gridcomputing infrastructures.
- WISE was initiated by Géant SIG-ISM and SCI
- SIG-ISM: Information Security Management
- SCI: Security for Collaboration among Infrastructures
- "Launching" e-infrastructures:
  - Géant (European Research and education networks)
  - EGI (European Grid Infratsructure)
  - EUDAT (research data services)
  - PRACE (High Performance Computing)
- Participating communities
  - NRENs, HEP/CERN, the Human Brain Project, XSEDE, NCSA, CTSC

Working program 2016 – 5 topics

- Updating the SCI-framework
- Security Training and Awareness
- Risk Assessment
- Security Review and Audit
- Security in Big and Open Data

Events

- Barcelona 2015
- TNC2016 – Prague
- Xsede 2016 – Miami
- DI4R 2016 – Krakow

- Large steering committee

- Presentations from Xsede 2016 can be found on the wikihttps://wiki.geant.org/display/WISE/WISE+@XSEDE

Updating the SCI Framework

- **SCI (Security for Collaboration among Infrastructures) is a collaborative activity of information security officers from several large-scale infrastructures, including EGI, PRACE, EUDAT, WLCG, XSEDE and HBP. A version 1 document has been published - "A Trust Framework for Security Collaboration among Infrastructures".**
- **Review is under way and making good progress**
- **Please join Dave Kelsey and Adam Slagell!**

The SCI Framework – Areas addressed

- Operational Security
- Incident Response
- Traceability
- Participant Responsibilities
  - Individual users
  - Collections of users
  - Resource providers, service operators
- Legal issues and Management procedures
- Protection and processing of Personal Data/Personally Identifiable Information
- Also used by REFEDS, in an adapted form

SCIV2-WG Workplan 2016

7

- Self-assessments against Sections 4 (Operational Security) and 5 (Incident Response) in SCI version 1
  - To decide what guidance is needed and what words need to be changed. (completed)
- Produce draft guidelines for sections 4 and 5.
  - all topics considered and questions discussed (see wiki)
- Tune words of sections 4 and 5. (before WISE3 at DI4R)
  - And write the guidance for those sections
- Move on to other sections. (after WISE3 at DI4R)
- Aim for version 2 of the SCI document by the 12-month anniversary of the group (May 2017)
- After version 2 produced consider re-merging text with Sirtfi and Snctfi work (AARC and REFEDS)

STAA: Security Training and Awareness

- The WISE community we recognise that there is a broad need for security training and for awaress materials
- We also see there is a lot of material available
- This working group will:
  - Identify 5 to 10 most relevant training topics for the coming 3 years
  - collect good training practices;
  - collect information about relevant existing trainings by the infrastructures;
  - map out the need for organising joint training events on specific topics;
  - map out the need for developing trainings;
  - set up a basic training and awareness programme for organisations in the WISE community, identifying which trainings are needed.
- Chairs: Alf Moens (SURFnet) – Jim Marsteller (PSC)

STAA: Some example trainings

- XSEDE Information Security Training
- CTSC training materials, NSF Cybersecurity Summit
- Transit I and II
- Risk management workshops
- Géant DDOS workshop
- End user training / awareness sessions
- SANS
- …
- Your training?

STAA: clarification of the goals

- We are not going to develop trainings
- We will work on encouraging the sharing and joint development of trainings:
  - Organise special topic trainings
- We will identify and recommend a good training practice
- We will identify good trainings based upon your experience

- Where should the focus be?
  - Special topics: DDOS mitigation, monitoring, log file analysis
  - End user training and awareness
  - Security management, security governance and compliance

STAA: training target groups

- Management/governance
- Systems management, system administrators
- Network engineers
- User coordinators
- Users
- Software developers
- Acquisition

STAA: Training subjects

Subject	Target group
Laws & Regulations (privacy, export)	Systems management, users
Secure Software development	User, user coodorinator, contractor
System hardening	System admin, network engineering
Monitoring and logging	System admin, network engineering, respnse teams
Forensics	Response teams
Incident respons and analysis	Response teams

Participate in WISE -STAA

- Interested in any of the the working group subjects?
- Contact the workgoup chair and let's work together
- Subscribe to the workgroup mailinglist on the WISE website
- Submit your training ideas to the inventory page or send an e-mail to the list or to alf.moens@surfnet.nl

- www.wise-community.org

Security Review and Audit

The main activities for SRA-WG are to:

- follow and contribute to the development of security audits and reviews among the constituents;
- share related best practices for implementations;
- promote related research and disseminate findings of reviews;
- contribute to the development of security standards and frameworks;
- promote peer reviews.

- Chair: Urpo Kaila (CSC, EUDAT)

Security Review and Audit

- Review or Audit?
- Security of infrastructure
- Your processes
- For compliance
- For proving trust
- For proving effectiveness of security
- After major incidents
- Before launching major changes
- Review of SCI-compliance?

Workgroup Risk Assesment

16

- Risk assessment is the overall process of risk identification, risk analysis and risk evaluation
- It is key in order to be in control of your security as part of the implementation of an Information Security Management System (ISMS)
- The implementation of effective security controls depends very much on a reliable risk assessment, so that the right measures can be taken

Workgroup Risk Assesment - Why

17

- Don’t want to reinvent the wheel, but use what is already there
- Need for practical information for large e-Infrastructures and NRENs
- Enhance trust among e-infrastructures
- Collaboration with SIG ISM of GEANT
  - Open for external partners
  - Draft available of document describing risk mgmt

Workgroup Risk Assesment - Definitions

18

- Risk Assessment is the process where an organisation analyses the risks of its business processes, systems and services based on
  - Likelihood
  - Impact with respect to
    - Confidentiality, integrity, availability
- Management of risks is
  - Mitigation, acceptance, delegation (outsourcing)

Workgroup Risk Assesment - Activities

19

- Create risk registers for specific NREN and e-Infrastructures services
- Evaluation of tools for Risk Assessments
- Evaluation of standards for risk management
- Collection of metrics
  - So how are you doing. Which metrics to use (e.g. see NIST document 800-55)

Workgroup Risk Assesment - How

20

How do we work

- Emails are the means of communication of the working group
- will mainly meet via teleconferences, but if needed face-to-face meetings also will be considered and organised
- Membership and how to share information has to be defined
- You can subscribe to our mailing lists

- https://wiki.geant.org/display/WISE/RAW-WG
- **Chair: (Jules Wolfrat - PRACE, SURFsara - retired)**
  Vice-Chair: Urpo Kaila - CSC, EUDAT

WG Big and Open Data

- The Security in Big and Open Data (SBOD) working group focuses on security issues that arise when dealing with big and open data especially within the e-infrastructures. Security issues in this context concentrate on confidentiality, integrity and availability. Confidentiality regulates access to the information, integrity assures that the information is trustworthy, i.e. has not been changed without authorisation, and availability guarantees access to the information by authorised people at any time.

- Alessandra Scicchitano (Géant)
- Ralph Niederberger (Jülich Supercomuting Center, EUDAT)

WG – SBOD - targets

- The SBOD-WG focuses on security issues that arise when dealing with big and open data especially within the e-infrastructures.
- Security issues in this context concentrate on (as stated above):
  - Confidentiality regulates access to the information,
  - Integrity assures that the information is trustworthy, i.e. has not been changed without authorisation
  - Availability guarantees access to the information by authorised
- people at any time.
- SBOD intends to focus on high level security issues only.
- CSIRT issues are out of scope.

Working program 2016 – 5 topics

- Updating the SCI-framework
- Security Training and Awareness
- Risk Assessment
- Security Review and Audit
- Security in Big and Open Data