

# Who doesn't need to be WISE?

*Bringing into reality global information security collaboration*

Alessandra Scicchitano  
GÉANT - Project Development Officer

# WISE - what is it?

- Wise Information Security for Collaborating E-infrastructure
- A trusted global framework where security experts can share information on different topics like risk management, experiences about certification process and threat intelligence keeping a special focus on e-infrastructures.

# How everything started

- Joint effort of GEANT SIG-ISM (Special Interest Group on Information Security Management) and SCI (Security for Collaboration among Infrastructures)
- Workshop in Barcelona Spain, October 2015.
- 50 participants



# How everything started

- Main idea: 4 big e-infrastructures EGI, EUDAT, GEANT and PRACE getting together to facilitate the exchange of experience and knowledge on security.
- But also NRENs, XSEDE, NCSA, CTSC and communities like HEP/CERN, HBP and many others participated.
- A profound need for a real collaboration became evident

# WISE - The new born community



*WISE Workshop - Barcelona Supercomputing Center - October 2015*



# Activities

- Led by a Steering Committee
- Two face-to-face meetings a year
- The main work happens through working groups.
- Five WGs:
  - Updating the SCI framework (SCIV2-WG)
  - Security Training and Awareness (STAA-WG)
  - Security Review and Audit (SRA-WG)
  - Risk Assessment WISE (RAW-WG)
  - Security in Big and Open Data (SBOD-WG)

# SCIV2-WG

## Updating the SCI framework:

- Already existing framework created by the SCI group  
[http://pos.sissa.it/archive/conferences/179/011/ISGC%202013\\_011.pdf](http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf)
- SCIV2-WG will work towards version 2 of the SCI document that will become the 1<sup>st</sup> WISE framework defining best practices, trust and policy standards for collaboration.
- A wider range of stakeholders will be involved, specifically the NRENs, whose security issues were not present in the first version.
- <https://wise-community.org/updating-the-sci-framework/>

# SCIV2-WG

The WG has just defined the direction of the work and chose the first topic the group will focus on:

- How to share vulnerabilities among e-infrastructures



# STAA-WG

## Security Training and Awareness:

- Training is wanted and needed for security professionals, systems and network managers and engineers, users of the infrastructures and for decision makers, for a wide range of topics.
- Main activities of the WG:
  - Collecting good training practices
  - Collecting information about relevant existing trainings at the infrastructures
  - Set up a basic training and awareness program for organizations in the WISE community, identifying which trainings are needed
- <https://wise-community.org/training-and-awareness/>

# STAA-WG

The WG Security Training and Awareness will first do an inventory:

- What are the target groups for security awareness? What materials are already available and what practices can NRENs share?
- What are the most important subjects for security training?
- Which free/open training or training materials are available?
- Which commercial trainings are available?
- The purpose is to identify the training needs and make a first match with available training material.



# RAW-WG

## Risk assessment WISE:

- Large e-infrastructures are vulnerable for high impact security incidents because of the relative easy way that an incident may spread among partner organizations because of the collaborative services that exist among the constituent organizations. So it is important that each member organization has a trusted level of implemented security procedures.
- The objective of the WG is to provide e-infrastructures and their member organizations with guidelines on how Risk Assessments can be effectively implemented.
- <https://wise-community.org/risk-assessment/>

# SRA-WG

## Security Review and Audit:

- A proven method to obtain objective and comprehensive information about the current state of information security is to perform security reviews and security audits
- Some of the activities of the WG:
  - Follow and contribute to the development of security audits and reviews among the constituents
  - Share related best practices for implementations
  - Contribute to development of security standards and frameworks
- <https://wise-community.org/review-and-audit/>



# SBOD-WG

## Security in Big and Open Data:

- The WG focuses on security issues that arise when dealing with Big and Open data especially within the e-infrastructures.
- Main activities of the WG:
  - list and discuss already existing studies and state of the art the starting point for the rest of the work.
  - work on a list of issues particularly important for e-infrastructures and on a set of recommendations on how to minimize the impact of these issues.
- <https://wise-community.org/security-in-big-and-open-data/>

# SBOD-WG

- Published a draft of the case statement  
<https://wiki.geant.org/display/WISE/Case+Statement>
- Working on providing a clear definition of what is big and open data for the WG.



# Participate in WISE

- Interested in any of the the working group subjects?
- Subscribe to the workgroup mailinglist on the WISE website
- Contact the workgroup chair and let's work together
- The Working groups are starting their work now

[www.wise-community.org](http://www.wise-community.org)

Thank you

Questions?

[alessandra.scicchitano@geant.org](mailto:alessandra.scicchitano@geant.org)