The 3rd WISE Workshop took place on 27 September 2016 in Krakow, Poland, prior to DI4R conference. There were 30 people registered, 8 of them were last minute comers. https://eventr.geant.org/events/2473 All the participants introduced themselves and the newcomers have been added to the WISE mailing list.

The agenda and all slides shown are available at:
https://wiki.geant.org/display/WISE/WISE+@DI4R

Magda Haver from GÉANT welcomed everybody. Alessandra Scicchitano, who has been leading WISE sent her apologies.

Dave Kelsey (STFC; EGI) presented an overview of WISE. "Wise Information Security for Collaborating E-infrastructures is a trusted global framework where experts representing main infrastructures come together to facilitate exchange of knowledge on security".
Established as a global effort of GÉANT, SIG-ISM and SCI with main goal to build trust between infrastructures and their management, it is also information sharing and giving e-infrastructures possibility to set up security policies to work together in a secure way. Dave presented future plans – WISE is nearly 1 year old now and needs review of working groups work, structure and frequency of the meetings and topics. Alessandra Scicchitano is leaving GÉANT and Hannah Short from CERN will replace her as the WISE Coordinator.

Important is to identify what is unique about R&E and infrastructures. Involvement from other communities is very much welcome. Dave showed how to subscribe to working groups mailing lists and invited the audience to stay actively involved.

Currently, the main work of WISE happens through working groups (presentations followed by chairs).

1. **SCIV2 WG** (chair- Dave Kelsey) - A Trust Framework for Security Collaboration among Infrastructures is a collaborative activity of information security, where the officers from large-scale infrastructures (EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, HBP) developed a trust framework in order to enable interoperation (security teams), manage cross-infrastructure security risks, develop policy standards. The WG is building on the SCI document version 1, and now working on version 2, where a wider range of stakeholders will be involved, conflicts from version 1 will be addressed and new topics and areas will be identified. Dave stressed that the group does not compete with others and it is not operational security/trust group. Presented work plan and talked about meetings and next steps. Invited and encouraged more people to join, also via mailing list.

   Discussions about certification. Self assessment and peer reviewing would be first step - for the community and organisation itself.

2. **STAA-WG** Security Training and Awareness (chair Alf Moens, SURF). Alf addressed "competing vs collaborating" issue and talked about communities involved in security – TF-CSIRT, SIG-ISM, NREN-CERT and national communities. The WISE community recognizes that there is a broad need for security training and materials. Alf presented main objectives of the group - identify training topics, collect good training practices and set up training and awareness programme. Gave examples of past and existing

trainings as well as target groups. The STAA group will not develop trainings but encourage to share training practices and experiences.
Fotis Gagadis asked question about creating a list of regulations; Alf advised to consult Andrew Cormack. Irina Mikhailava mentioned ENISA (they approach things at national level and could provide a framework.)

3. **SBOD-WG** Security in Big and Open data (chair Ralph Niederberger). The work of this group focuses on high level security issues that arise when dealing with big and open data especially within the e-infrastructures. Ralph talked about definitions and association with open and big data and presented examples from LHC, SKA, EUDAT and HBP. How can this be handled - SBOD is looking for use cases on data archives that contain huge amounts of data for different communities in order to search for communalities. Are the solutions usable for everyone? The objective is to come up with models to community, that can be documented. Ralph invited everyone to stay involved - visit the website and subscribe to the mailing list.

4. **RAW-WG** (chair Urpo Kaila) Risk Assessment Best Practices on Risk Management. Research infrastructures face very similar risks and can greatly benefit from sharing information about methods for risk assessment and risk management. Also the controls are often similar. WISE WG's should cover core security domains - security management policy sharing/harmonization, risk management, operational security incident coordination training, security of partner management/stakeholders compliance, technical security. Presented examples of sharing best practices and types of risks – strategic, operational and damage. Most typical risk is stolen account. 'My risk is your risk'. Next steps for the WG will be sharing risks registers and tools and methods for risk management. The WG will continue working through VCs, mailing list and meetings. A review and audit of Risk Assessment should be done.

Irina Mikhailava – Head of GÉANT Learning and Development presented GÉANT Internship Programme. GÉANT is currently seeking host sites for the internships, that will run from January to June 2017 and end with the student's attendance at TNC2017 https://tnc17.geant.org/ . The program is funded by GÉANT and covers possible intern's compensation fee and student's travel and accommodation at TNC2017. GÉANT's L&D team is also eager to learn and brainstorm about topics and areas of collaboration (eg. what is the main challenge from technical and from research perspective?) Contact nadia.sluer@geant.org

Linda Cornwall - STFC spoke about cloud security risks and their mitigation in the context of activities and discussions within the EGI federated cloud. The EGI Federated Cloud has been operational since May 2014 and has 21 cloud resource centres. The various EGI security groups are working with the EGI Federated cloud to integrate the security activities and methodology of work. A new security threat risk assessment highlights a lot of the problems with federated infrastructures especially clouds. Security risks are higher in the Cloud, with less control over what people do, what software is in use, and who has privileged access. EGI works on risk mitigation, but collaboration with others is necessary. Reports are available, please contact Linda.Cornwall@stfc.ac.uk.

Ralph Niederberger - “Security in PRACE & HBP”. Network and security create net of trust via WISE Community work. Both PRACE as well as HBP are collaborating e-infrastructures where security risks are dependent not only on the security policies of the own infrastructure. Security policies and procedures have to be setup globally, which help to circumvent those additional risks. These activities are the ones WISE community is undertaking so contributing to this work will make future e-infrastructures more secure.

Ralph talked about PRACE Security Forum, presented the organizational chart, spoke about policies and procedures as well as risk reviews. Collaboration with other projects and activities enables exchange of information about incidents and vulnerability information.

Human Brain Project has more than 100 partners. Ralph spoke about the subprojects, presented infrastructure and partnership scheme. The security setup is very similar to PRACE security (but also direct access possible). Showed user access to the HBP portal.

Do you have ways to have special protection? No, we don’t know which data user is working on. It is evaluated at scientific level. Alf - we had discussions on classification. What kind of privacy related info you have? We provide supercomputing cycles. User responsible for his data and what he provides.

Daniel Kouril – CESNET “Handling security incidents in e-infrastructures: balancing prevention and response”.

Daniel talked about EGI CSIRT and its mission to maintain secure EGI via a dedicated incident response team, but also focusing on prevention. Involvement of sites is necessary and transferring responsibilities to take actions. What is the right balance between prevention and response? What is changed by clouds?

Discussion - How much response/prevention/education. Education does not need to be risk averse. Sven - we have various levels in infrastructures. We tried to educate admins to provide at least first steps of including response. You can not do this with users - they are not interested; admins are. Also reason for endorsement policy. Ralph - admins need to do security training. Admin can set up service, users can’t. Focus stays on user and possible prevention of educations. Are they any other prevention issues? Fotis: right amount based on org needs.

Rob Quick - Indiana University – “Getting to know the SWAMP”
The SWAMP, or Software Assurance Marketplace, is no-cost resource available to the software community to promote a more stable and secure software ecosystem. It is funded by US Department of Homeland Security and is operational since 2014. It offers 19 software analysis tools and works also with commercial tool vendors. Audience is software developers, researchers, infra operators, educators and students. Rob talked about key attributes as well as challenges. Software developers need effective continuous software assurance capabilities to integrate into their development workflows.

Drew Leske – Compute Canada – “History and Current State of Compute Canada Security”
Canada’s Advanced Research Computing Platform is currently consolidating data centres and

expanding base of expertise. Compute Canada is a national not-for-profit organization supporting advanced research computing. ARC is the core, the goal is to share experience and wisdom, scripture, infrastructure, information and alerts; formalize, centralize and accelerate cooperation. National Security Council and the Compute Canada Security Program will continue implementation of the governance model, security portal, as well as working on issues of privacy and confidentiality.

Maciej Miłostan – PSNC – "Secure access to e-infrastructure in context of NREN security management practices". Maciej presented his organization, its security management in R&D HPC centres and status of cybersecurity management. Main structures related with cybersecurity are PSNC Cybersecurity department, PIONIER CERT, NOC and IBCh IS team. Maciej talked about law regulations and technical security measures - procedures, trainings and in general cybersecurity being embedded into lifecycle of developed products. Future plans consist of completing all elements of ISMS, building a regular SOC for internal and external purposes of research, education, public administration and certifications.

Fotis Gagadis, GÉANT- "Framework called enterprise security architecture - SABSA model" In today's environments security officers and managers lead its organisations and engineers to enhance the capabilities of their environments and protect its assets by applying multiple practices across board of operations. To ensure that they have to guide organisations through compliance with various practices, most of the times organisations have to rely on old methods of security and trends. The overall approach of Enterprise Security Architecture methodology is to ensure that security follows the business needs. Security officers should suggest practices and solutions that are adequate to the business environment to ensure re-usability of concepts, cost effectiveness, business driven decisions and human oriented objectives for security leading to a harmonised environment. On this project the security team followed and shared the results of this methodology being used within the corporate environment for one of the current projects.

Outcome from discussion:

- We should do a better marketing of WISE globally focusing on research communities. Involvement of other communities is also important.

- Other topics that should be addressed are (but we need to identify leaders):
    - Cloud Security
    - Threat Intelligence Sharing
    - Privacy issues
    - Vulnerability Handling
    - IPv6 Security
    - Laws and Regulations

- Current working groups will continue, SCIV2, security awareness, big and open data, and hopefully review and audit.

- Deliverable should be events and best practices, website, wiki, news letters.

- Can we define one achievement/goal for year 2?

- Peer reviewing and self assessment

- What’s scheduled for next 12 months:

  - use cases
  - training for security officer
  - engaging young talents
  - materials to be put together by the community
  - ask chairs to set date for deliverables
  - proceed with website and Wiki, inform people where we are
  - SC has role to have other communities involved and make WISE initiative global (including inviting new members of SC)
  - setting up ‘community within communities’ - make contact and share experiences.