SCI How-to

U. Stevanovic, I. Neilson

WISE virtual meeting, 26 Oct 2020

https://wise-community.org/events
https://events.geant.org/event/209/

In collaboration with and co-supported
by EU H2020 EOSC-HUB and GN4-3

SCI – short recap

- Security for Collaborating Infrastructures (trust framework)
- V1 – 2013
  - Security Incident Response Trust Framework for Federated Identity
  - The Scalable Negotiator for a Community Trust Framework in Federated Infrastructures
- v2 – 2017 (current)
  - Revised
  - Simplified (and improved)
  - Endorsed by all major e-Infras!

SCI current progress

- Assessment sheet for v2 is provided
  - Assessment conducted for EGI
- Started work on SCI How-to guide
  - Helps explain how to comply with the framework, and explain ambiguities and unknowns
- https://docs.google.com/spreadsheets/d/1NNI7ZlsmxBoVxpDy4iYAamyd7BsIgcts/edit#gid=204520169
- https://docs.google.com/document/d/1O2UTrKD70erpmO5DVIgn_1xpFX3NfVae_BGKPHoFuWo/edit?pli=1#heading=h.xt9d2igjc9y4

SCI sections

- Operational Security
- Incident Response
- Traceability
- Participant Responsibilities
- Data Protection

Why How-to?

- SCI is a framework
  - Sometimes not detailed or prescriptive enough
- Different understanding of requirements
- Requirements may vary greatly in scope and complexity
  - OS1 – “A person or team mandated to represent the interests of security for the infrastructure”
  - OS3 – ““A security plan (e.g., architecture, requirements, controls, policies, processes) addressing issues, such as, authentication, authorisation, access control, physical and network security, risk mitigation, confidentiality, integrity and availability, disaster recovery, together with compliance mechanisms ensuring its implementation”

OS3 – Security plan

- “A security plan (e.g., architecture, requirements, controls, policies, processes) addressing issues, such as, authentication, authorisation, access control, physical and network security, risk mitigation, confidentiality, integrity and availability, disaster recovery, together with compliance mechanisms ensuring its implementation.”
- How to provide guidance for “a security plan” in an accessible way?
  - Simply referencing standards (e.g. ISO2700x) may not help the reader much
  - Trying to summarise reinvents the wheel and leaves a larger maintenance headache

OS2 – Risk Management Process

- “A process to identify and manage security risks on a regular basis.”
  - Again, accessible and adequate guidance is not easy to provide
- Possible points to address:
  - Data theft or loss (potential impact of data loss, personal data involved, protection of personal data, protection of users’ data)
  - Denial of service
  - Intrusion detection
  - Phishing/hacking/ransomware attacks
  - Unauthorized use of resources (botnets, cryptocurrency mining)
  - Detection of unauthorized/illegal data (adult material, illegal data)