SCCC-JWG

Security Communications Challenge Coordination Joint Working Group

Co-chairs: David Groep (Nikhef), Hannah Short (CERN)

Joint Working Group: in collaboration with SIG-ISM, IGTF, and REFEDS

Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have either explicit or implicit expectations on their remit, responsiveness, and level of confidentiality maintained. However, it is a well-recognised fact that data that is not verified becomes stale: security contact information that is appropriate at time of enrolment in an infrastructure may later bounce, or have different 'characteristics'.

In order to achieve its goals of fostering trust between infrastructures that span multiple areas of interest (service provider ensembles, identity providers, organisations and institutions, national federation operators and incident response teams), having this effort established as a *joint* working group between all relevant stakeholders is seen as a key trust element. To underline this goal, the SCCC working group strives to be joint between WISE, SIG-ISM, IGTF, REFEDS, and is open to other pertinent communities.

The SCCC WG will address the following aspects of security communications challenge (CC) coordination:

- Coordination of 'CCs recipient groups' among participating infrastructures
  making sure that targets are not overload by coinciding or overlapping challenges, for example by designating a lead infrastructure for each category of targeted entities
- Transitivity of trust in CC results between infrastructures
  for example by specifying the level of disclosure detail for CCs between trusted infrastructures, by using an SCI evaluation framework approach to it, or by coordination of testing and success criteria.
  How can requests for CCs between infrastructures be handled, e.g. in response to changing needs or a changed risk assessments; or as remediation after an incident in which communications did not meet expectation.
- Definition of CC models and classification
  the 'depth' of the CC testing is a balance between the level of trust gained (more profound testing and good results gives more trust) and expediency (asking the recipient to respond to a mail or click a link consumes less resources than requesting forensic investigation of a simulated incident of deliberately unknown nature).
- Frequency of CCs
  simple communications challenges are often performed one or several times per year (e.g. for TF-CSIRT, by SURFcert for the SURFconext federation, EGI Operations on their sites). Complex challenges are less frequent (e.g., the 'black-box traceability' trials of the EGI Security Service Challenges tale place once every 1-2 years). Following a CC model classification, propose an appropriate frequency for each class.

The SCCC-WG should thereafter become a standing interest group in the WISE-community that maintains a timetable of planned CCs (to prevent overlap), provides a lightweight mechanism to request and coordinate CCs, and promotes the sharing of results with qualified peer infrastructures.

Documents	Draft terms of reference for the WISE contingent of the Joint Working Group (July 2018, presented to SIGISM April 2019)
Presentations	Introduction to the SCCC group at the joint SIGISM-WISE meeting (Kaunas, 2019)