Contribution ID: **95** Type: **Oral Presentation**

Security exercises, which questions to ask and what to do with the answers

Tuesday, 26 March 2024 11:40 (20 minutes)

ecurity exercises can be seen as an experiment, one wants to investigate how good, for example, the expected computer security incident response activities of an organisation described in the procedures and policies match with real (measured) activities in an -as realistic as possible, but contained- created security incident situation.

The complexity of the created security situation depends on what to investigate. It ranges from measuring various aspects of incident response, like the security communication infrastructure used by the involved security teams, to “shaking the whole tree” situations where also the borders of the primarily addressed infrastructure and the interfaces to the security teams of depending or supporting infrastructures are challenged. An example would be Identity Providers that manage identities which can be used at compute services (like EGI FedCloud).

Since security exercises are costly and in addition even bare the risk to be harmful to collaborations in the area of operational security, we will focus in this talk rather on our experiences gained through organizing security exercises, or being part of campaigns, on what went wrong, what can be improved, what should be avoided in future runs.

For that purpose, and taking into account the similarity to scientific experiments we will also talk about how to design a security exercise, i.e. what are the questions you want to answer, how to identify and measure the relevant parameters, and finally what to do with the results.

Primary authors: CROOKS, David (UKRI STFC); GABRIEL, Sven (Nikhef/EGI)

Presenters: CROOKS, David (UKRI STFC); GABRIEL, Sven (Nikhef/EGI)

Session Classification: Network, Security, Infrastructure & Operations

Track Classification: Track 7: Network, Security, Infrastructure & Operations