Contribution ID: **18** Type: **Oral Presentation**

CaaS: Challenge as a Service - Modernizing the SSC framework

Wednesday, 26 August 2020 14:00 (20 minutes)

For years, EGI has run Security Service Challenges to assess and keep aware incident response teams within its community. Nikhef has, as part of this community, been tasked with the role of Red Team, developing anything and everything needed to systematically monitor properties related to the challenge. This means there is a need for a flexible software stack, enabling various payloads and forms of delivery. After all, the grid infrastructure is quite heterogeneous, while at the same time relatively inflexible. As a result, projects have introduced internal standardization, adding an additional axis to the available interfaces.

With digital threads becoming more and more imminent (cryptocoin mining, network attacks), SSCs have become more popular, and we have noticed an increased demand for training by simulation - while at the same time noticing an increase of non-technical communications challenges. In order to increase our flexibility, and thus being able to help with more of these challenges, we decided to design a new modular SSC framework, integrating more than a decade of SSC experience with the newer technologies that are available.

This development effort has been coupled with research into the deployment of mini-grids for exercises. The individual exercises have run are confronted with lost time due to the irregularity of environments we encounter, and/or decrease real-world value as they normally lack the batch systems that are a vital part of the normal challenges. With a mini-grid under our control, we are able to more independently debug issues with submission, and more easily integrate new deployment schemes, as well as acting as an infrastructure operations team during exercises.

Primary author: ROORDA, Jouke (Nikhef)

Co-author: Dr GABRIEL, Sven (Nikhef/EGI)

Presenter: ROORDA, Jouke (Nikhef)

Session Classification: Network, Security, Infrastructure & Operations Session

Track Classification: Network, Security, Infrastructure & Operations