Contribution ID: **7** Type: **Oral Presentation**

# Collaborative operational security for Research and Education (Remote presentation)

*Tuesday, 21 March 2023 17:00 (30 minutes)*

We must protect and defend our environment against the cybersecurity threats to the research and education community, which are now acute having grown in recent years. In the face of determined and well-resourced attackers, we must actively collaborate in this effort across HEP and more broadly across Research and Academia (R&E).

Parallel efforts are necessary to appropriately respond to this requirement. We must both share threat intelligence about ongoing cybersecurity incidents with our trusted partners, and deploy the fine-grained security network monitoring necessary to make active use of this intelligence. We must also engage with senior management in our organisations to ensure that we work alongside any broader organisational cybersecurity development programmes.

We report on recent developments in the Security Operations Centres (SOC) Working Group, established by the WLCG but with membership encompassing the R&E sector. The goal of the Working Group is to develop reference designs for SOC deployments and empower R&E organisations to collect, leverage and act upon targeted, contextualised, actionable threat intelligence. This report will include recent experience in deploying SOC capabilities for the first time including network topology considerations, hardware and software provisioning strategies. We also report on experience using containerised SOC training environments in the security thematic CERN School of Computing held in Split in the summer of 2022.

Finally, we discuss ongoing work in the broader community to develop common practices in cybersecurity to support our common response in this area.

**Primary authors:** CROOKS, David (UKRI STFC); VALSAN, Liviu (CERN)

**Presenters:** CROOKS, David (UKRI STFC); VALSAN, Liviu (CERN)

**Session Classification:** Network, Security, Infrastructure & Operations

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