Contribution ID: **57** Type: **Oral Presentation**

# Collaborative threat intelligence and security operations centres

*Tuesday, 22 March 2022 12:00 (30 minutes)*

The threat faced by the research and education sector from determined and well-resourced cyber attackers has been growing in recent years and is now acute. A vital means of better protecting ourselves is to share threat intelligence - key Indicators of Compromise of an ongoing incidents including network observables and file hashes - with trusted partners. We must also deploy the technical means to actively use this intelligence in the defence of our facilities, including a robust, fine-grained source of network monitoring. The combination of these elements along with storage, visualisation and alerting is called a Security Operations Centre (SOCs).

We report on recent progress of the SOC WG, mandated to create reference designs for these SOCs, with particular attention to work being carried out at multiple 100Gb/s sites to deploy these technologies and a proposal to leverage passive DNS in order to further assist sites of various sizes to improve their security stance.

We discuss the plans for this group for the coming year and the importance of acting together as a community to defend against these attacks.

**Primary authors:** ARVANITIS, Christos (CERN); CROOKS, David (UKRI STFC); VALSAN, Liviu (CERN); WARTEL, Romain (CERN)

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

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

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