Contribution ID: **108** Type: **not specified**

Threat Intelligence and Security Operations Centres: Collaborative Security

Thursday, 28 October 2021 18:50 (25 minutes)

The threat faced by the research and education sector from determined and well-resourced attackers has been growing in recent years and is now acute. We must act together as a community to defend against these attacks. A vital means of achieving this is to share threat intelligence - key indicators of compromise of an ongoing incident including network locations and file hashes - with trusted partners. We must couple this with 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. The WLCG SOC working group has been pursuing an interconnected network of SOC-equipped sites for several years. We report here on recent progress, including new deployments against multiple 100Gb/s sites, and future plans for the coming year.

Desired slot length

Speaker release

Yes

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

Presenter: CROOKS, David (UKRI STFC)

Session Classification: Network & Security

Track Classification: Networking & Security