Contribution ID: **38** Type: **Oral Presentation**

Status update on the deployment of threat intelligence and operational security monitoring capabilities (Remote Presentation)

Tuesday, March 26, 2024 12:00 PM (20 minutes)

We have presented previously on the strategic direction of the Security Operations Centre working group, focused on building reference designs for sites to deploy the capability to actively use threat intelligence with fine-grained network monitoring and other tools. This work continues in an environment where the cybersecurity risk faced by research and education, notably from ransomware attacks, continues to be very high.

In this report we discuss recent developments in the community, including both updates on deployment of security tools as well as progress in the sharing of threat intelligence in different contexts

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