

Deploying Security Operations Centre capabilities

Thursday, 19 March 2026 12:00 (20 minutes)

Supported by the work of the Security Operations Centre Working Group that has been reported on at ISGC previously we have built experience across the Research & Education community deploying security operations centre capabilities. This work has used the reference design of the working group, developed to provide guidance on the elements required to deploy a Security Operations Centre, in various ways. A recent addition to the working group has been a focus on people and process.

In this presentation we will report on the lessons learned from the experience of deploying these capabilities from the perspective of different organisations, to support others in developing their own activities. While the technology stack is an important element of this work, the sustained staffing and processes needed are a vital part of this work.

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

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

Session Classification: Networking, Security & Operations - I (11:00 - 12:40)

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