Contribution ID: **65** Type: **not specified**

Building a large scale Security Operations Centre

Tuesday 13 October 2015 17:30 (20 minutes)

The HEP community is facing an ever increasing wave of computer security threats, with more and more recent attacks showing a very high level of complexity. Having a centralised Security Operations Centre (SOC) in place is paramount for the early detection and remediation of such threats. Key components and recommendations to build an appropriate monitoring and detection Security Operation Centre will be presented, as well as means to obtain and share relevant and accurate threat intelligence information. The presentation concludes that the key to achieve an appropriate response is to both build an efficient security infrastructure and a tight international collaboration, enabling information to be shared globally with trusted partners, and in particular between the various HEP sites.

Length of presentation (max. 20 minutes)

20

Primary author: VALSAN, Liviu (CERN)

Presenter: VALSAN, Liviu (CERN)

Session Classification: Security and Networking

Track Classification: Security & Networking