Contribution ID: **8** Type: **not specified**

Building and operating a large scale Security Operations Center

Tuesday, 25 April 2017 17:05 (25 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 Security Operations Center (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 Center will be presented, as well as means to obtain and share relevant and accurate threat intelligence information. Various lessons learnt from building and operating the CERN SOC will be presented. This presentation also gives an update on the work performed in the WLCG Security Operations Center Working Group that aims to provide a scalable reference design applicable for a range of HEP sites.

Length of talk (minutes)

20

Scheduling constraints / preferences

Primary author: VALSAN, Liviu (CERN)

Presenter: VALSAN, Liviu (CERN)

Session Classification: Security and networking

Track Classification: Security & Networking