International Symposium on Grids & Clouds 2018 (ISGC 2018) in conjunction with Frontiers in Computational Drug Discovery (FCDD)

Contribution ID: **42** Type: **Oral Presentation**

Harnessing the Power of Threat Intelligence in Grids and Clouds: WLCG SOC Working Group

Tuesday, 20 March 2018 14:20 (20 minutes)

The modern security landscape affecting Grid and Cloud sites is evolving to include possible threats from a range of avenues, including social engineering as well as more direct approaches. An effective strategy to defend against these risks must include cooperation between security teams in different contexts. It is essential that sites have the ability to share threat intelligence data with confidence, as well as being able to act on this data in a timely and effective manner.

As reported at ISGC 2017, the WLCG [1] Security Operations Centres Working Group has been working with sites across the WLCG to develop a model for a Security Operations Centre reference design. This work includes not only the technical aspect of developing a security stack appropriate for sites of different sizes and topologies, but also the more social aspect of sharing data between groups of different kinds. In particular, since many Grid and Cloud sites operate as part of larger University or other Facility networks, collaboration between Grid and Campus/Facility security teams is an important aspect of maintaining overall security.

We discuss recent work on sharing threat intelligence, particularly involving the WLCG MISP [2] instance located at CERN. In addition, we examine strategies for the use of this intelligence, as well as considering recent progress in the deployment and integration of the Bro Intrusion Detection System at contributing sites.

An important part of this work is a report on the first WLCG SOC WG Workshop/Hackathon, a workshop planned at time of writing for December 2017. This workshop is planned to assist participating sites in the deployment of these security tools as well as giving attendees the opportunity to share experiences and consider site policies as a result. This workshop is hoped to play a substantial role in shaping the future goals of the working group.

[1] Worldwide LHC Computing Grid
[2] Malware Information Sharing Platform

Primary authors: Dr CROOKS, David (University of Glasgow); Mr VALSAN, Liviu (CERN)

Presenters: Dr CROOKS, David (University of Glasgow); Mr VALSAN, Liviu (CERN)

Session Classification: Networking, Security, Infrastructure & Operation Session

Track Classification: Networking, Security, Infrastructure & Operations