Contribution ID: **39** Type: **not specified**

Harnessing the power of threat intelligence for WLCG cybersecurity

Wednesday 16 October 2019 09:50 (25 minutes)

The information security threats currently faced by WLCG sites are both sophisticated and highly profitable for the actors involved. Evidence suggests that targeted organisations take on average more than six months to detect a cyber attack, with more sophisticated attacks being more likely to pass undetected.

An important way to mount an appropriate response is through the use of a Security Operations Centre (SOC). A SOC can provide detailed traceability information along with the capability to quickly detect malicious activity. The core building blocks of such a SOC are an Intrusion Detection System and a threat intelligence component, required to identify potential cybersecurity threats as part of a trusted community. The WLCG Security Operations Centre Working Group has produced a reference design for a minimally viable Security Operations Centre, applicable at a range of WLCG sites. In addition, another important factor in the sharing of threat intelligence is the formation of appropriate trust groups.

We present the status and progress of the working group so far, including both a discussion of the reference SOC design and the approach of the working group to facilitating the collaboration necessary to form these groups, including both technological and social aspects. Threat intelligence and the formation of trust groups in our community will be the focus of the WLCG SOC WG workshop that will be taking place immediately following HEPIX, during 21-23 October 2019. We emphasise the importance of collaboration not only between WLCG sites, but also between grid and campus teams. This type of broad collaboration is essential given the nature of threats faced by the WLCG, which can often be a result of compromised campus resources.

Speaker release

Yes

Desired slot length

Authors: CROOKS, David (Science and Technology Facilities Council STFC (GB)); VALSAN, Liviu (CERN)

Presenter: CROOKS, David (Science and Technology Facilities Council STFC (GB))

Session Classification: Networking and Security

Track Classification: Networking & Security