International Symposium on Grids & Clouds 2017 (ISGC 2017)

Contribution ID: **16** Type: **not specified**

WLCG Security Operations Centres Working Group

Tuesday, 7 March 2017 14:20 (20 minutes)

Security monitoring is an area of considerable interest for sites in the Worldwide LHC Computing Grid (WLCG), particularly as we move as a community towards the use of a growing range of computing models and facilities. There is an increasingly large set of tools available for these purposes, many of which work in concert and use concepts drawn from the use of analytics for Big Data. The integration of these tools into what is commonly called a Security Operations Centre (SOC), however, can be a complex task - the open source project Apache Metron (which at the time of writing is in incubator stage and is an evolution of the earlier OpenSOC project) is a popular example of one such integration. At the same time, the necessary scope and rollout of such tools can vary widely for sites of different sizes and topologies. Nevertheless, the use of such platforms could be critical for security in modern Grid and Cloud sites across all scientific disciplines.

In parallel, the use and need for threat intelligence sharing is at a key stage. Grid and Cloud security is a global endeavour - modern threats can affect the entire community, and trust between sites is of utmost importance. Threat intelligence sharing platforms are a vital component to building this trust as well as propagating useful threat data. The MISP software (Malware Information Sharing Platform) is a very popular and flexible tool for this purpose, in use at a wide range of facilities in different domains across the world.

In this context we present the work of the WLCG Security Operations Centres Working Group, which was created to coordinate activities in these areas across the WLCG. The mandate of this group includes the development of a scalable SOC reference design applicable for a range of sites by examining current and prospective SOC projects & tools. In particular we report on the first work on the deployment of MISP and the Bro Intrusion Detection System at a number of WLCG sites, including areas of integration between these tools. We also report on our future roadmap and framework, which includes the Apache Metron project.

Summary

We present the work of the WLCG Security Operations Centres Working Group, which was created to coordinate work on analytic security platforms across the WLCG (a more detailed description being in the abstract). The mandate of this group includes the development of a scalable SOC reference design applicable for a range of sites by examining current and prospective SOC projects & tools. In particular we report on the first work on the deployment of MISP and the Bro Intrusion Detection System at a number of WLCG sites, including areas of integration between these tools. We also report on our future roadmap and framework, which includes the Apache Metron project.

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

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

Session Classification: Network, Security, Infrastructure & Operations I

Track Classification: Networking, Security, Infrastructure & Operations