Contribution ID: **40** Type: **Oral Presentation**

WLCG SOC WG: Use of threat intelligence and deployment of SOC components at WLCG Tier-1 centres

Wednesday, 24 March 2021 14:00 (30 minutes)

The information security threats currently faced by the research community are not only sophisticated, but also in many instances highly profitable for the actors involved. Evidence suggests that targeted organisations take on average more than six months to detect a cyber attack; the more sophisticated the attack, the more likely it is that it will pass undetected for longer. Enabling sites to receive appropriate, technical and actionable threat intelligence is a cornerstone of the WLCG security strategy. The mandate of the WLCG SOC working group primarily includes the exploration of the technical aspects of developing operational security capabilities, through the design and implementation of various components of Security Operations Centers. The technological means of sharing threat intelligence is provided by the Malware Information Sharing Platform (MISP) which allows for considerable flexibility in the design of an information sharing network. The topology adopted by the working group focuses in the first instance on a purpose deployed central MISP instance hosted at CERN, which leverages existing trust partnerships. In addition, MISP allows for a number of methods to access threat intelligence data, including synchronising events to peer instances as well as direct access via a REST API.

Particular attention has recently been paid to the rollout of threat intelligence capabilities for the WLCG Tier 1 sites. This rollout represents a key milestone not only in providing an important security function for WLCG in its own right, but also in an operational rollout sense, gaining experience that can then be used for the benefit of Tier 2 sites.

This effort covers two aspects. The first is establishing the capability of Tier 1 sites to access the threat intelligence available through the CERN-hosted WLCG academic MISP instance. This will allow the sites to become familiar with the threat intelligence available and consider where it can be integrated within their existing Intrusion Detection and Intrusion Prevention Systems. The second aspect is the deployment, where necessary, of a minimally viable SOC following the SOC working group reference design. The approach taken is to work with individual sites following their specific circumstances. The goal of these activities is to provide sites with the threat intelligence and intrusion detection capabilities allowing them to quickly detect and defend against typical attacks.

We report on specific experiences of sites deploying SOC components and gaining access to threat intelligence, in addition to reporting on experience gained in integrating threat intelligence with existing Intrusion Detection and Intrusion Prevention systems.

Primary authors: Dr CROOKS, David (UKRI STFC); Mr VALSAN, Liviu (CERN)

Presenters: Dr CROOKS, David (UKRI STFC); Mr VALSAN, Liviu (CERN)

Session Classification: Network, Security, Infrastructure & Operations Session

Track Classification: Network, Security, Infrastructure & Operations