Contribution ID: **44** Type: **Oral Presentation**

Collaborative Operational Security

Wednesday, 19 March 2025 14:20 (20 minutes)

The WLCG Security Operations Centre Working Group has been working on establishing a common methodology for the use of threat intelligence within the academic research community. A central threat intelligence platform allows working group members to easily exchange indictors of compromise (IoCs) of ongoing security incidents and to use this information to secure their own infrastructures. This capability also enhances the ability of participating organisations to respond effectively to multi-site security incidents across the community.

We discuss the current extent of this trust group, including examples of sites that have deployed MISP instances themselves as well as those that are using the central instance directly. We also consider the type of events that are being shared and methods used to help sites gain confidence in sharing information of their own.

A recent focus of the Working Group has been on people, processes, tools and data needed for operational security, trying to answer some important questions such as how to engage people, how to communicate in a clear manner, how to deploy tools and technologies in tandem for effective defences, as well as how to have processes in place to ensure a consistent approach to handling and preventing security incidents.

Another area of work is around the use of pDNSSOC, a lightweight "80% SOC" solution focused on correlating DNS logs with Threat Intelligence. Having been specifically designed to be low impact to the deploying sites, pDNSSOC at the minimum requires a sensor to be installed in the DNS infrastructure of the site with an external centre performing the correlation and alerting activities.

In addition, we report on the outcomes of a recent WLCG Security Operations Centres Working Group workshop and hackathon which took place in December 2024. We will also present recent developments in the community, including both updates on deployment of security tools as well as progress in the sharing of threat intelligence in different contexts.

Primary author: CROOKS, David (UKRI STFC)

Co-author: VALSAN, Liviu (CERN)

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

Session Classification: Network, Security, Infrastructure & Operations I

Track Classification: Track 7: Network, Security, Infrastructure & Operations