

# Trust Groups and the use of Threat Intelligence in the Research Community

*Tuesday, 25 August 2020 14:30 (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.

In this context, the WLCG Security Operations Centre Working Group has been working to establish a threat intelligence sharing trust group in the academic research community.

The purpose of this group would enable members to easily exchange Indicators of Compromise (IoCs) of ongoing security incidents and allow them to use this information to secure their own infrastructures. In addition, this capability would enhance the ability of participating organisations to better respond to security incidents spanning multiple sites within the community.

The mandate of the working group includes the exploration of both the technical and social aspects of forming such a trust group. The technological means of sharing 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 hosting at CERN, which leverages existing trust partnerships. In addition, MISP allows for a number of methods to access intelligence data, including synchronising events to peer instances as well as direct access via a REST API.

The type of intelligence being shared in this trust group is often most applicable at the campus or institution level; an important part of the work of establishing the group is investigating ways of sharing the relevant intelligence with the hosting institutions.

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.

In addition, we report on the outcomes of a recent workshop focussing on threat intelligence which took place in Nikhef in October 2019, which addressed many of these issues, as well as including a validation of a reference workflow incorporating threat intelligence. This workflow includes a technology stack previously reported on at ISGC 2018.

Finally, we report on the status of ongoing work to establish the necessary rules of engagement for sites taking part in this trust group.

**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