Contribution ID: **62** Type: **Oral Presentation**

Incident Detection

Monday, 22 March 2021 09:00 (1h 30m)

A typical situation security teams encounter is to find out whether they are possibly a victim of an ongoing security incident spreading in, or across infrastructures.

To decide whether your resources are affected by the incident you basically face two problems:
• How to share sensitive information, like Indicators of Compromise (IoCs).
• How to efficiently use the available information (IoCs).

In particular the problem of matching reported IoCs to the available data can be very time consuming. Starting from low level parsing of central syslog data of the monitored systems, to matching patterns in network flows need to be automated as far as possible.

The WLCG SOC WG activity addresses both challenges Resource Center (RC) security teams are facing in their daily life.
The framework developed there was presented at earlier Security Workshops at ISGC and at other conferences. After an introduction to the SOC, the focus will be on deployment of the framework and a demonstration how the SOC can help to share threat intelligence (for example) IoCs detected by a partner RC, and consequently give an answer to the question if your RC is also a victim to the same attack.

Presenters: Dr CROOKS, David (UKRI STFC); ROORDA, Jouke (Nikhef); Dr GABRIEL, Sven (Nikhef/EGI)

Session Classification: Security Workshop