Contribution ID: **14** Type: **Oral Presentation**

Building a minimum viable Security Operations Centre for the modern grid environment

Tuesday, 2 April 2019 16:00 (30 minutes)

The modern security landscape affecting grid and cloud sites is constantly evolving, with threats being seen from a range of avenues, including social engineering as well as more direct approaches. It is vital to build up operational security capabilities across the Worldwide LHC Computing Grid (WLCG) in order to improve the defense of the community as a whole. As reported at ISGC 2017 and 2018, the WLCG Security Operations Centres (SOC) Working Group (WG) has been working with sites across the WLCG to develop a model for a Security Operations Centre reference design.

We present the current status of a minimum viable SOC design applicable to a range of different WLCG sites, centered around a few key components.

The design uses the Zeek Intrusion Detection System for monitoring what is happening at the network level in strategic locations: for example at border between the local cluster and external networks, the border between different local network domains or at core infrastructure nodes. The Malware Information Sharing Platform (MISP) is used to share information regarding relevant security events and the associated Indicators of Compromise (IoCs). By feeding IoCs from MISP into Zeek we have a platform that allows the community to share threat intel that is immediately actionable across the entire grid.

The logs produced by Zeek are processed using the Elasticsearch, Logstash, Kibana (elastic) stack for real time indexing and visualisation. This provides sites with a powerful tool for incident response and network forensics. The alerts raised by Zeek are further aggregated, correlated and enriched by an advanced notification processing engine. This ensures that most false positives are automatically whitelisted while at the same time reducing the total number of raised alerts that need to be managed by the computer security team of each site. By enriching these alerts and adding context of what happened around the moment the malicious activity was detected, the time needed to handle these alerts is greatly reduced.

We present possible deployment strategies for all these components in a grid context as well as the integration between them. We also report on the current status of work on integrating other sources of data, in particular using netflow/sflow, into this model.

Lastly we discuss how making use of these SOC capabilities distributed across the participating sites can lead to increasing the operational security across the entire grid.

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

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

Session Classification: Networking, Security, Infrastructure & Operations

Track Classification: Network, Security, Infrastructure & Operations