Contribution ID: **21** Type: **Oral Presentation**

Building an Open Source Security Operations Center at Nikhef

Wednesday, 24 March 2021 13:30 (30 minutes)

Centralizing (and visualizing) what is happening at a compute site enjoys ongoing effort from both industry and the community. An established example is include the ELK stack, importing, storing and visualizing logs, while more recently traffic analysis has gotten more and more attention - especially from WLCG.

At Nikhef, we have attempted to create a reasonable, recreatable SOC design based on output of the WLCG SOC WG. After experiments with an IBM POWER8 (S822L) system and various network setups, we landed on an AMD 64-core system that handles 100Gbit, potentially 200Gbit pending experimentation.

The result is a small cluster of Open Source software that receives between 40 and 80 million syslog messages per day, and around 600 and 750 million traffic logs from Zeek. Much of this cluster is set up using Ansible and is intended to be released to the community.

During this talk, we will discuss our SOC setup, and discuss some practical findings with regards to a high-performing setup.

Primary author: ROORDA, Jouke (Nikhef)

Presenter: ROORDA, Jouke (Nikhef)

Session Classification: Network, Security, Infrastructure & Operations Session

Track Classification: Network, Security, Infrastructure & Operations