



Contribution ID: 60

Type: **not specified**

Tool options and choices

Wednesday 6 November 2024 16:00 (30 minutes)

Zeek, MISP, pDNSSOC, Elasticsearch, Opensearch, Elastiflow, ElastiAlert, other information sources, other tools?

Advantages, capabilities, limitations, concerns....

Let's discuss

Presenters: Dr CROOKS, David (UKRI STFC); LUEDERS, Stefan (CERN)

Session Classification: SOC Hackathon