Contribution ID: **2** Type: **not specified**

Cyber Threat Intelligence Workshop

Tuesday, 9 April 2024 09:00 (3h 30m)

This workshop will unpack initiatives and ideas emerging from the CTI subtask of WP8 T3. NREN participants will present their use cases for threat intelligence and journeys towards realising them; from collecting, validating, correlating with flow data and acting on indicators. We will also present aspects of our planned R&E Security Intelligence Hub - an ISAC-like virtual organisation facilitating the exchange of threat intel within and beyond the GÉANT community. Come join us and share your thoughts!

The following use cases will be presented:

- SURF: Modern flow analysis: nfdump2clickhouse experiences
- HEAnet: Threat Intel Visualised
- CYNET: Secure Collaboration & Intelligence Information Sharing Platform (SCIISP)
- DeiC: pDNSSOC: Leveraging MISP indicators via a pDNS-based infrastructure as a poor man's SOC
- SUNET: C2-scanner
- PSNC: Malware analysis services for CTI
- GÉANT: CTI and the R&E Security Intelligence Hub: Plans for GN5 projects and beyond

Note: all presentations are TLP:GREEN (limited disclosure [community only])

Presenter: MOOI, Roderick (GÉANT)