Contribution ID: **115** Type: **Lecture**

Intrusion detection with SOC: threat intelligence, monitoring, integration and processes

Tuesday 21 June 2022 16:00 (1 hour)

- indicators of compromise (IoCs), threat intelligence sharing, TLP protocol
- tools and technologies: MISP, Zeek, OpenSearch etc.
- deploying a Security Operation Center
- security incidents: detecting and alerting

Summary

Presenter: CROOKS, David (UKRI STFC)

Track Classification: Track 2: Detection