CTI Sharing Module

Nassos Bountioukos

CyberAlytics Limited

n.bountioukos@cyberalytics.com

CyberSecDome

Cyberalytics

Main Utility

- **IoC Sharing between Domes**
  New threats will be shared between all Domes
- **Machine Learning based report generation**
  Will use LLM techniques and query public IOC repositories to generate reports for each incident
- **Enrichment of future incidents**
  - The information that will be shared between the Domes will help to enrich future incidents
- **Privacy aware sharing**
  - The TLP protocol will be used for the labelling of the Assets to ensure that private information will not be exchanged

TAXII and STIX

TAXII Protocol
- **An open-source protocol** that helps share information about cyber threats

STIX Standard
- Enables CTI sharing in a **consistent** and **machine-readable** manner

CTI Module