**BENOIT HAMELIN**, Tutte Institute for Mathematics and Computing
*Representation of cyber defense telemetry for exploration tasks*

Cyber defense of networks relies on the acquisition of large quantities of system telemetry, providing visibility into events that reveal intrusions. We present here a simple methodology for building a representation of salient objects that enables identifying *interesting* activity through an explorative lens. This approach organizes anomalies along similarity axes, while emphasizing features that distinguish objects from others. The methodology leverages labelling of routine activity, providing factual documentation of the baseline of systems as observed by sensors. Anomalous objects, among which lie traces of intrusions, are thus expressed through a vocabulary of modes of normal behaviour they are similar to, facilitating their interpretation.