SEMI-AUTOMATED CYBER THREAT INTELLIGENCE (ACT)

NG-SOC 2019
August 26th
Siri Bromander

mnemonic

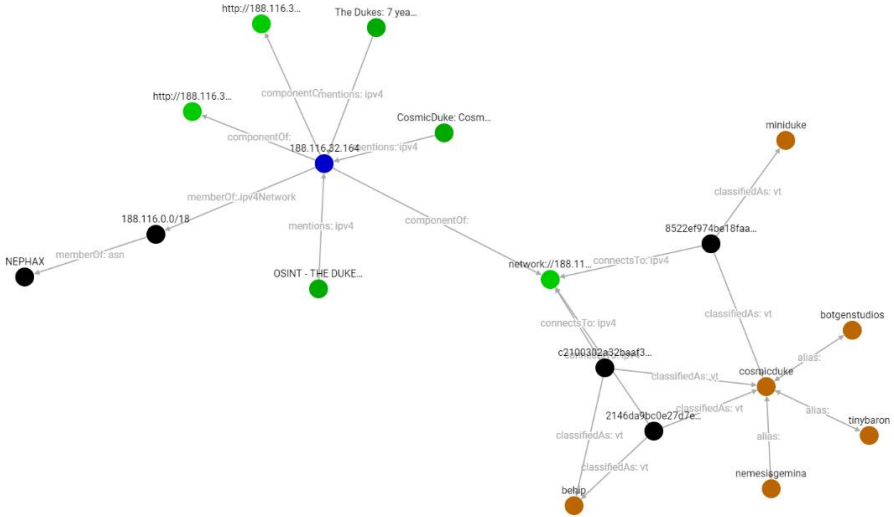
Goal

To collect and organize our knowledge of threats to make it useful

Data and Information

Data

Information



mnemonic

Semi-Automated Cyber Threat Intelligence (ACT)

The main objective of the research project is to develop a platform for cyber threat intelligence to uncover cyberattacks, cyber espionage and sabotage.

The project will result in new methods for data enrichment and data analysis to enable identification of threat agents, their motives, resources and attack methodologies.

In addition, the project will develop new methods, work processes and mechanisms for the generation and distribution of threat intelligence and countermeasures, to stop ongoing and prevent future attacks.

NSM

Nordic Financial CERT

Kraft CERT

UiO : Universitetet i Oslo

NTNU Norwegian University of Science and Technology

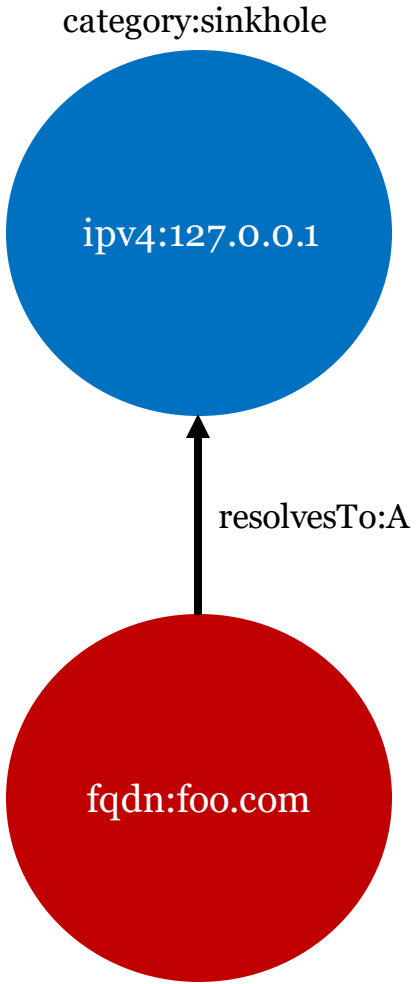
telenor

mnemonic

DATA MODEL

Data Model

- Objects
  - Global
  - Example: IP address
- Facts
  - Connected to one or two objects
  - Immutable
  - Timestamped
  - Owner
  - Role-based and explicit access control
  - Backed by evidence and comments



Current OSINT Sources

Import:

- APTNotes
  - https://github.com/aptnotes/data
- APT & CyberCriminal Campaign Collection
  - https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections
- RSS Feeds
  - Infosec blogs
- MISP (circl.lu feed)
- MITRE ATT&CK

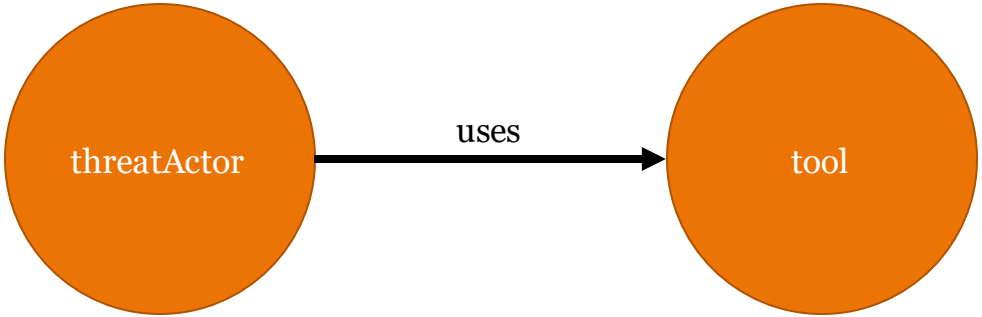
Enrich:

- mnemonic PassiveDNS
  - https://passivedns.mnemonic.no/
- Shadowserver IP-BGP
  - https://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP
- VirusTotal

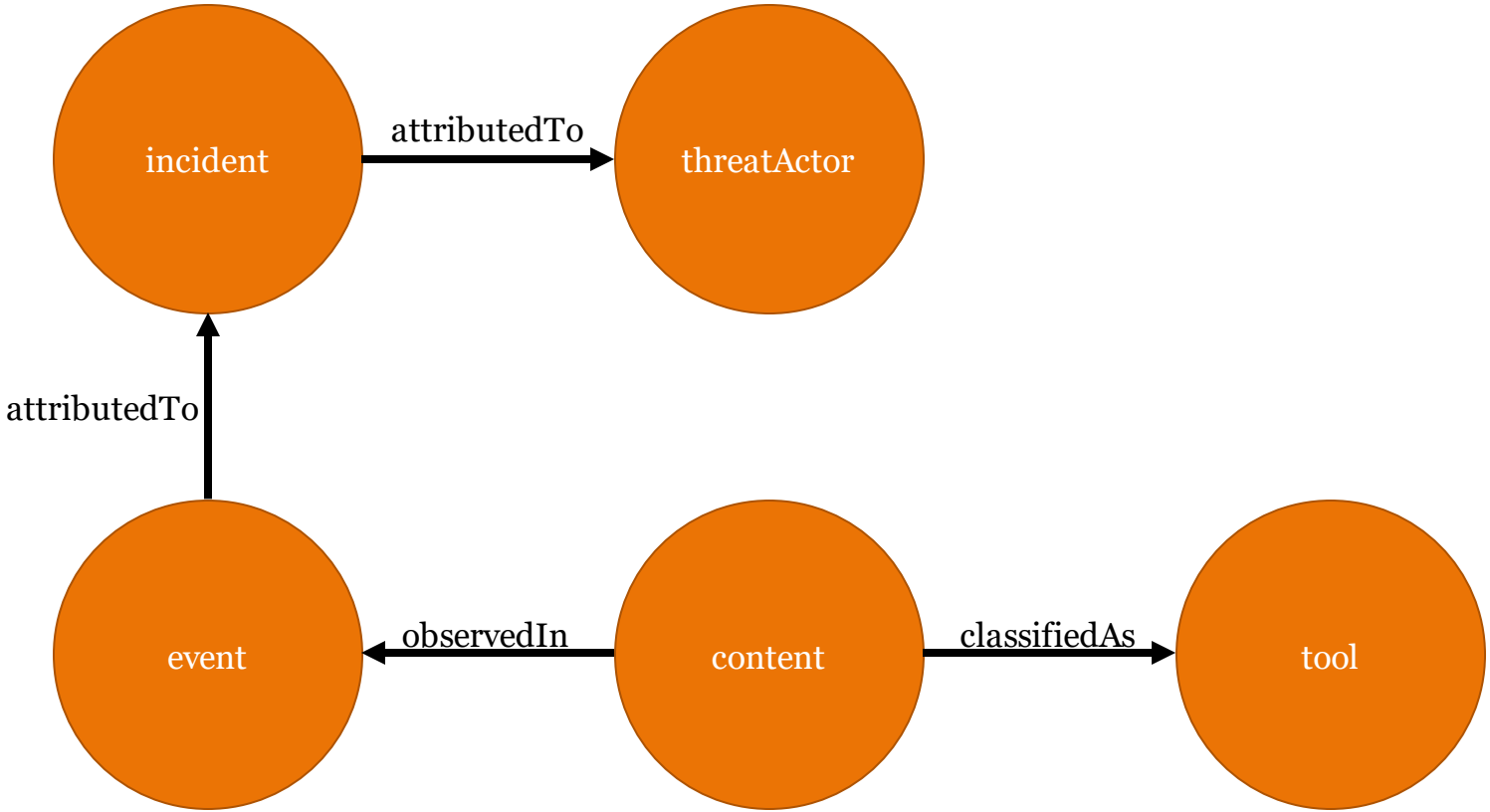
Problem

- Multiple ways to represent the same information

Example: Threat actor uses tool

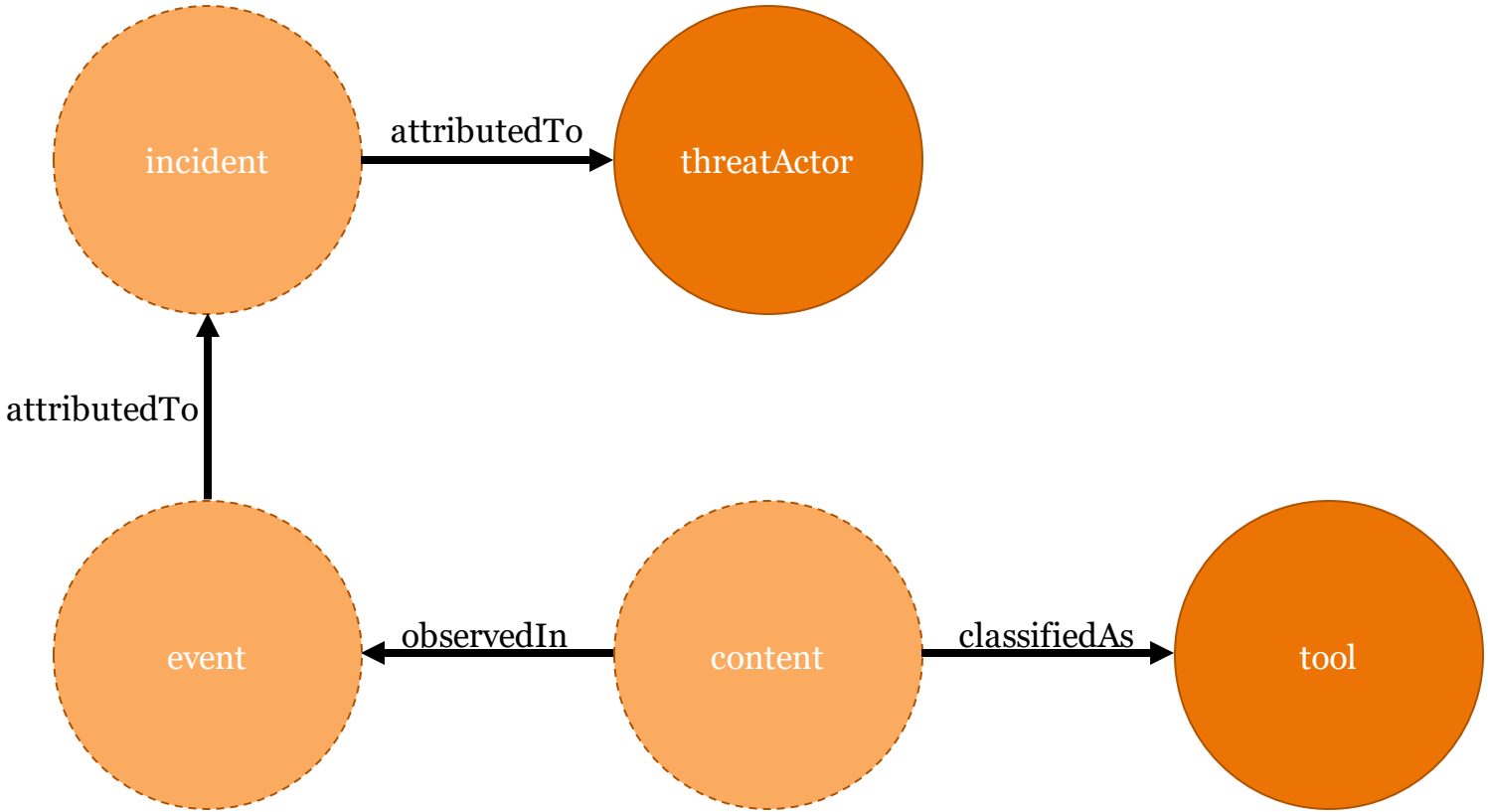


Example: Threat actor uses tool



mnemonic

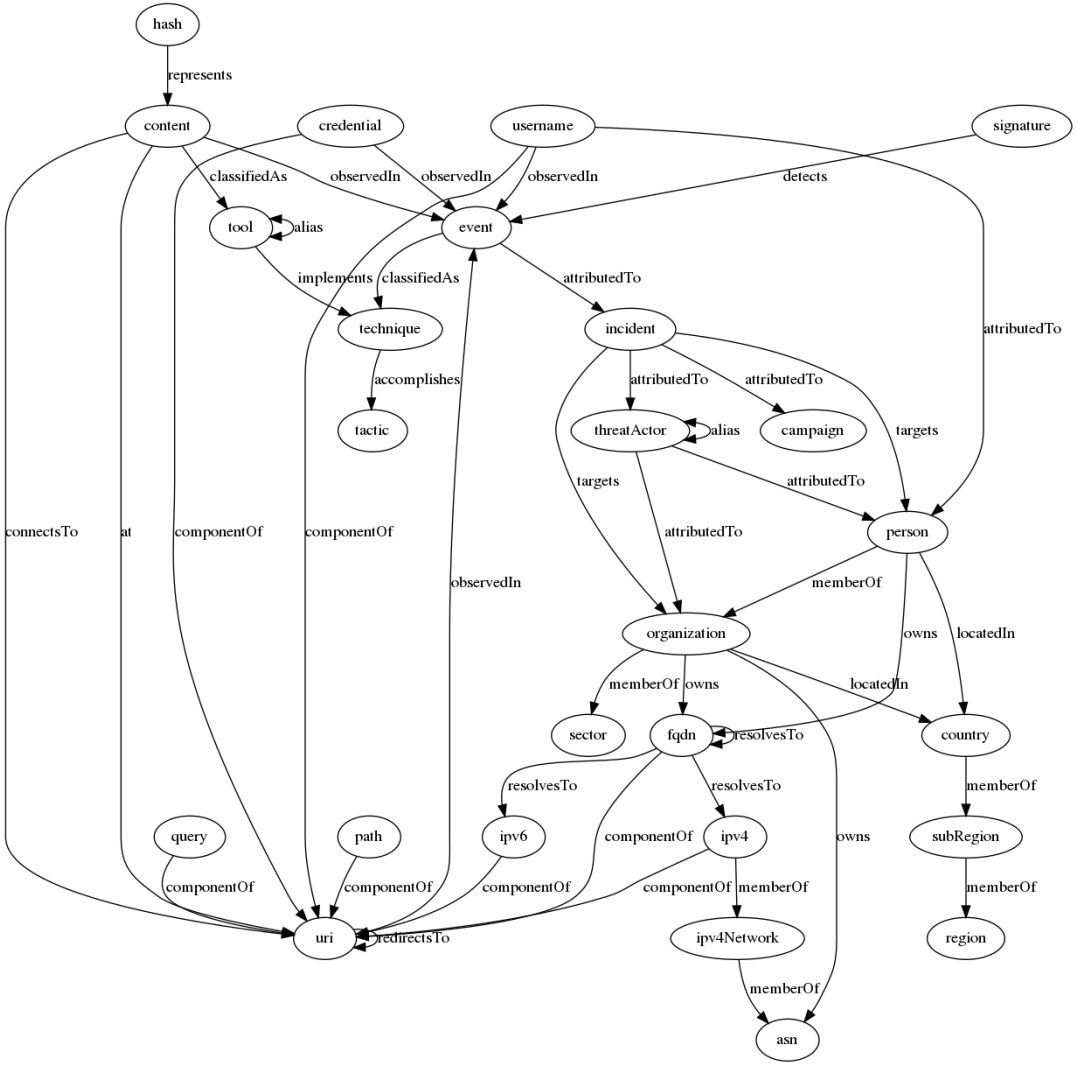
Example: Threat actor uses tool



mnemonic

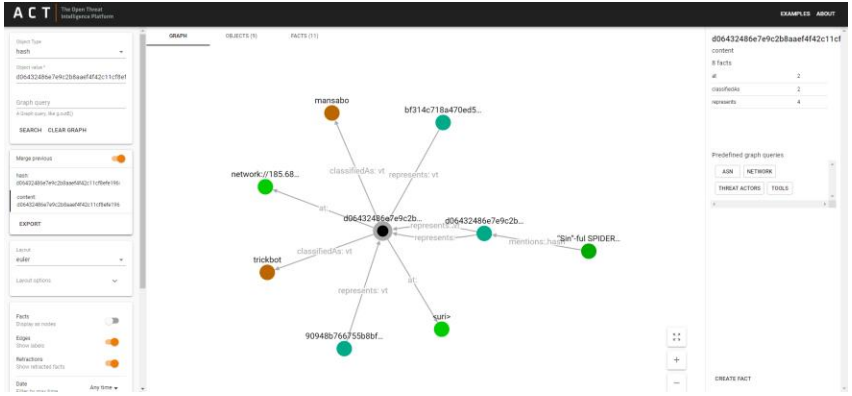
Data Model

- Objects
  - Global
  - Example: IP address
- Facts
  - Connected to one or two objects
  - Immutable
  - Timestamped
  - Owner
  - Role-based and explicit access control
  - Backed by evidence and comments
- Placeholders



THE ACT PLATFORM

mnemonic



Backend

REST API

GUI

Apache TinkerPop

Cassandra

elasticsearch

ACT Core

mnemonic

Threat Intelligence Platform - Summary

- Github repositories
  - https://github.com/mnemonic-no/act (installation docs)
  - https://github.com/mnemonic-no/act-api-python
  - https://github.com/mnemonic-no/act-bootstrap
  - https://github.com/mnemonic-no/act-frontend
  - https://github.com/mnemonic-no/act-platform
  - https://github.com/mnemonic-no/act-scio
  - https://github.com/mnemonic-no/act-splunk
  - https://github.com/mnemonic-no/act-triggers
  - https://github.com/mnemonic-no/act-workers
  - License: ISC (BSD compatible)
- Public AWS instance
  - https://act-eu1.mnemonic.no

ACT continued

- New information sources
- Information sharing
- Trust and confidence
- GUI improvements

FURTHER WORK

SOCCRATES project

mnemonic

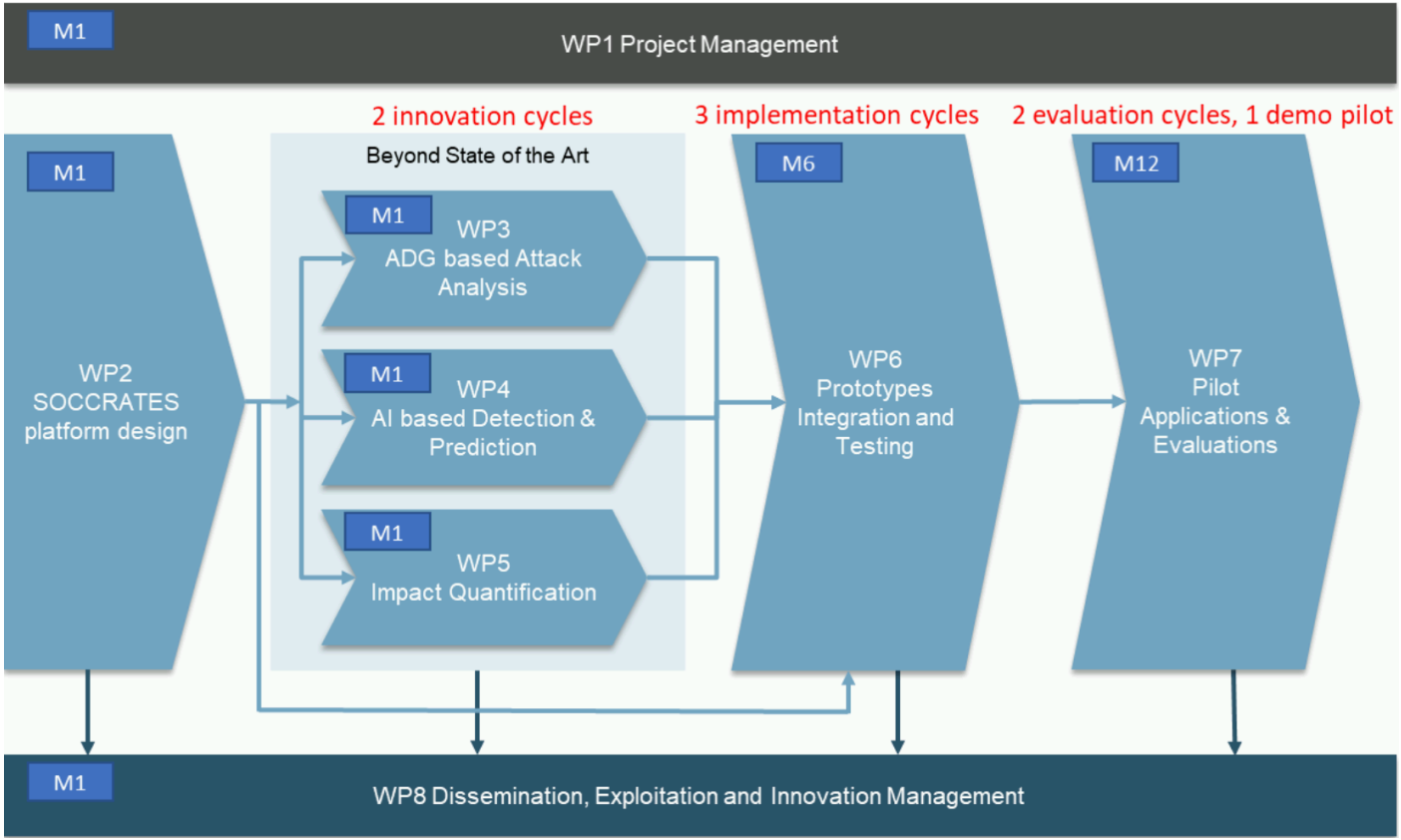
SOCCRATES

SOC & CSIRT Response to Attacks & Threats based on attack defence graphs Evaluation Systems (SOCCRATES)

The SOCCRATES project proposes to develop a new security platform for Security Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs), that will significantly improve an organisation's capability to quickly and effectively detect and respond to new cyber threats and ongoing attacks.

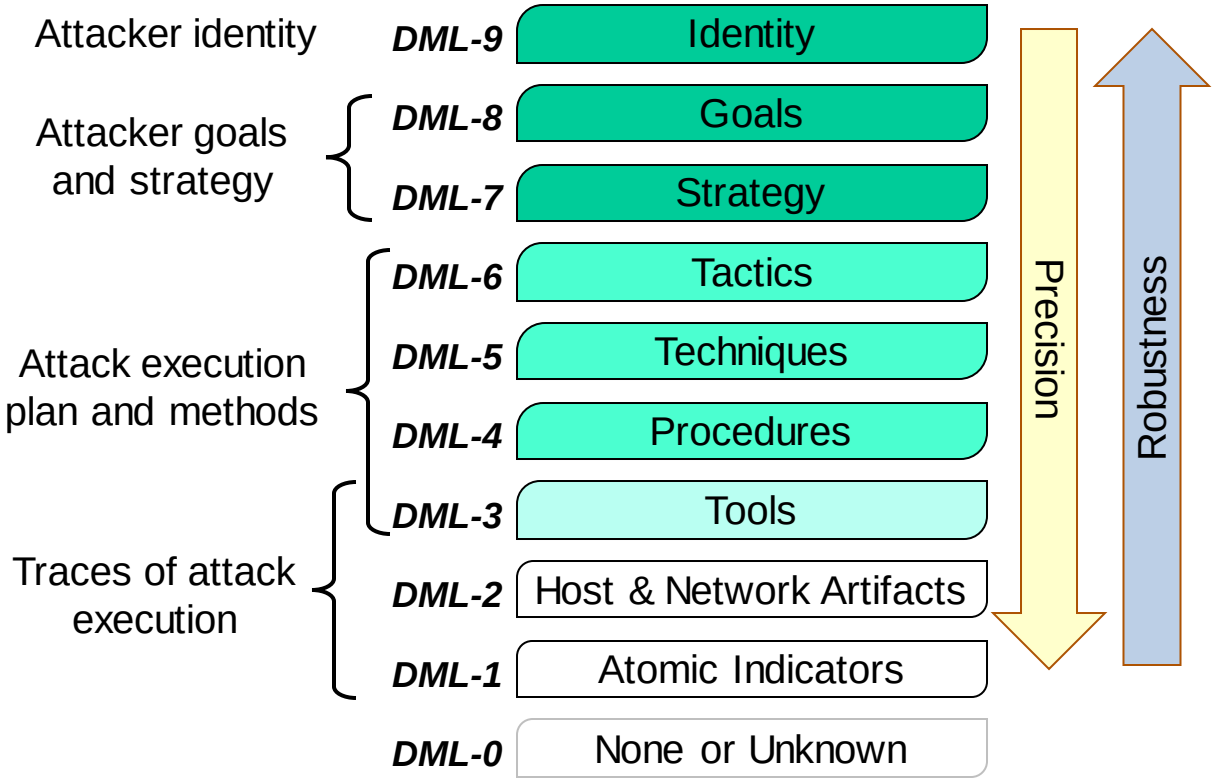
The platform aims to provide several innovative components for automated infrastructure modelling, attack detection, cyber threat intelligence utilization, threat trend prediction, automated analysis using attack defence graphs and business impact modelling to aid human analysis and decision making on response actions, and enable the execution of defensive actions at machine-speed.

SOCCRATES



mnemonic

SOCCRATES: Modelling tactical CTI



http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html

SOCCRATES – mnemonic's contribution

Tactical threat intelligence describes how an adversary operates: their Tactics, Techniques and Procedures (TTPs). The MITRE ATT&CK framework defines a taxonomy of tactics and techniques, but no such taxonomy exists for procedures. The taxonomy of tactics and techniques does not provide enough detail to model adversary behaviour in an attack-defence graph. MITRE has published Adversary Emulation Plans (AEPs) that could be used as input to an ADG-based system; however, these AEPs are created manually, which makes large-scale generation of AEPs infeasible. In this task, a machine-readable definition of adversary procedures will be developed to enable automatic generation of AEPs. The ACT platform –technology from MNM – will be extended to include the formal procedure definition and implementation of the method for generation of AEPs from procedure descriptions. The AEPs will be used as input to ADG-based systems (WP3) to enhance the capability with modelling the most likely attack behaviour.

SOCCRATES – mnemonic's contribution

- Formal definition of «Procedures»
- Automate the creation of Adversary Emulation Plans
- →Predict likely adversary behaviour