UiO : Department of Informatics
University of Oslo

Siri Bromander, Dr. Audun Jøsang, Dr. Martin Eian

Semantic Cyberthreat Modelling

Our research projects

- Oslo Analytics
- ACT
- TOCSA

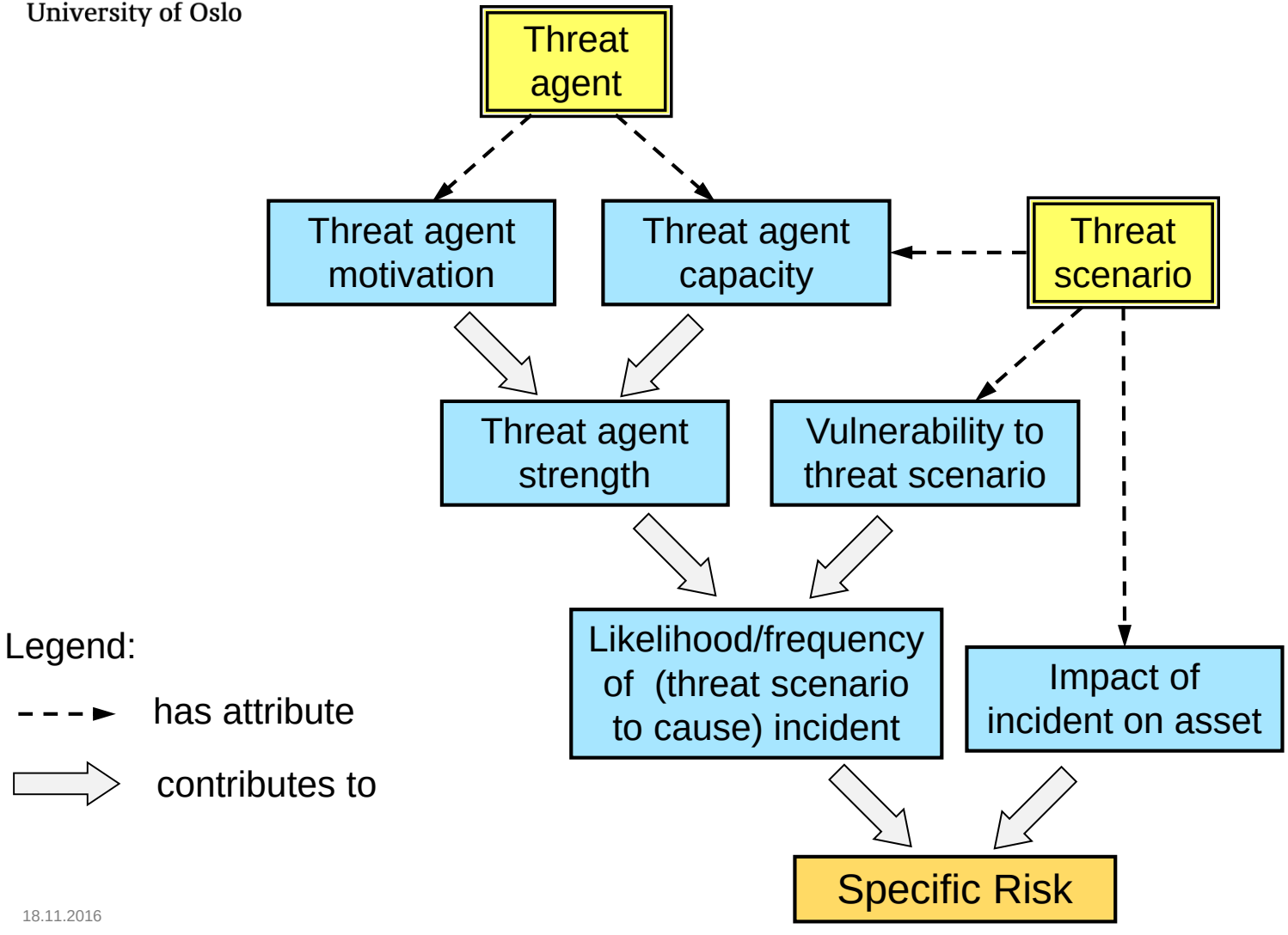
The ACT-project will develop new algorithms and a new platform for cyber threat intelligence

Oslo Analytics develops advanced analytical methods based on big data analysis, subjective logic and Bayesian modelling to gain a deep situational awareness and understanding of security incidents

TOCSA will develop models and tools based on ontologies for fully and semi-automated classification and discovery of cyberthreats.

Semantic Cyberthreat Modelling

- Difficult – if possible – to decide on countermeasures when having less to little knowledge of the threat actor.
- To utilize computer capasity to analyse the complex and large datasets we have, we need to classify and structure the data that can give us information and knowledge.

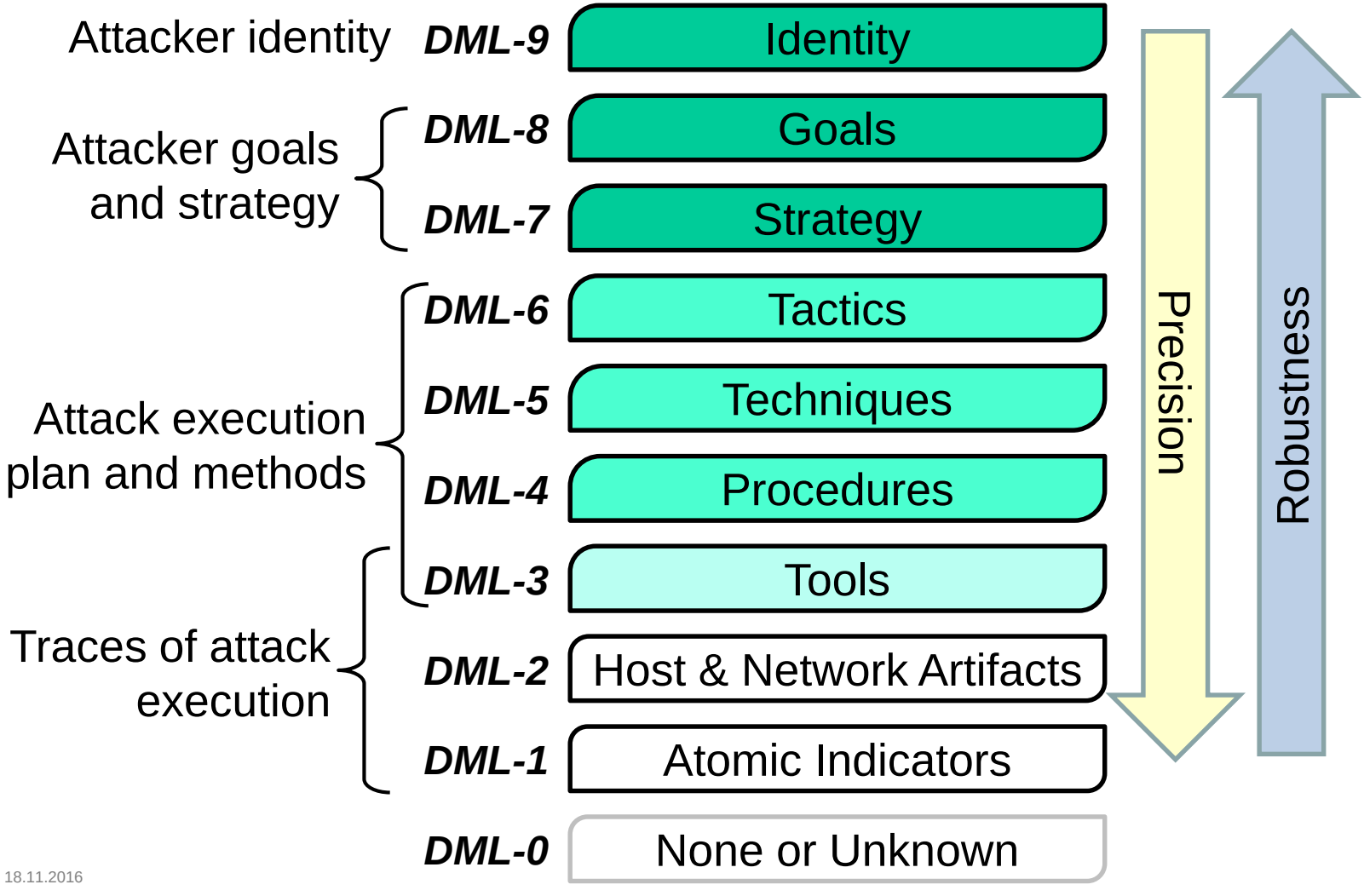

Threat agent
Threat agent motivation
Threat agent capacity
Threat scenario
Threat agent strength
Vulnerability to threat scenario
Likelihood/frequency of (threat scenario to cause) incident
Impact of incident on asset
Specific Risk
Legend:
has attribute
contributes to

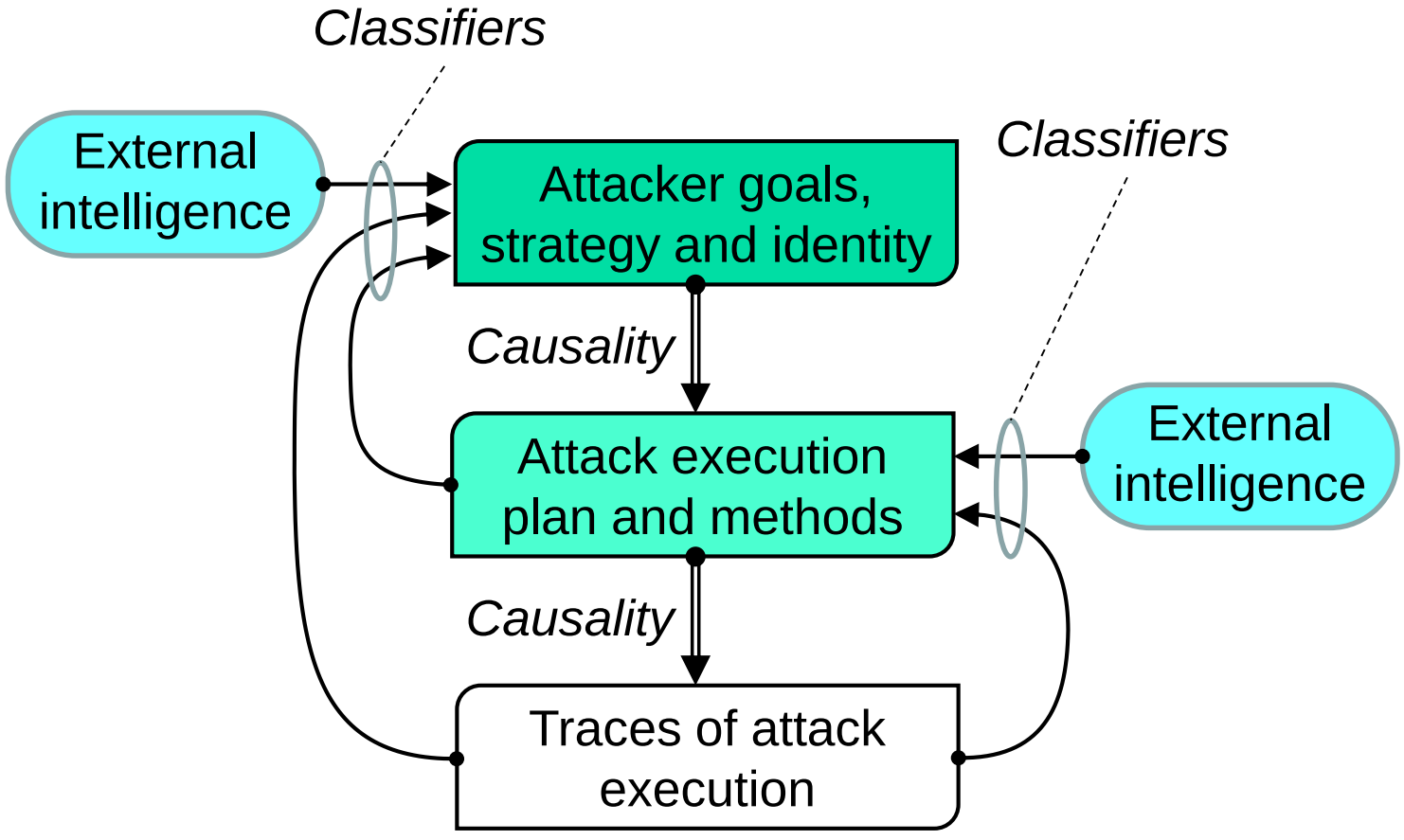
Use cases

1. Incident response
2. Information sharing
3. Intrusion detection

Stillion's Detection Maturity Level Model

- Defining levels of maturity where each level focus on what the IR team is capable of detecting/doing.


Attacker identity
DML-9
Identity
Attacker goals and strategy
DML-8
Goals
DML-7
Strategy
Attack execution plan and methods
DML-6
Tactics
DML-5
Techniques
DML-4
Procedures
DML-3
Tools
Traces of attack execution
DML-2
Host & Network Artifacts
DML-1
Atomic Indicators
DML-0
None or Unknown
Precision
Robustness


Classifiers
External intelligence
Attacker goals, strategy and identity
Classifiers
Causality
Attack execution plan and methods
External intelligence
Causality
Traces of attack execution

Semantic Feature Extraction: «Goal»

- «Replicate Acme Company's Super Awesome Product Foo in 2 years or less" → {"Replicate", "Product"}
- Mandiant's APT1 report→ {"Replicate", "Product"}, {"Replicate", "Manufacturing process"}, {"Obtain", "Business plan"}, {"Obtain","Policy position"}
- →{Action, Object}

Related work

- ATT&CK
- CAPEC
- Intel Threat Library
- STIX (+TAXII, MAEC, CybOX)

Example applications of semantic cyberthreat models

1. Incident response: graph database
2. Information Requests: quick graph query
3. Intrusion detection: automated signature creation

1) Execution of **net.exe** with **time** as the first argument and **victim system** as the second argument
2) Timestamp returned by the command in step 1
3) Execution of **at.exe** with **victim system** as the first argument and ((timestamp from step 2) + 1 minute) as the second argument

1) Evidence collection
2) Analysis of evidence
3) Identification of new indicators, artifacts, tools and TTPs
4) Threat agent attribution

Conclusion

Semantic modelling of threats is a promising approach for automated threat and attack detection at multiple levels of abstraction. A semantic model of threats will enable security analysts to work faster and more efficiently in terms of identifying threat agents and take advantage of previous experience and gathered intelligence when handling incidents caused by known or unknown threat agents. The task of extracting semantic features for all levels of abstraction in our suggested extended DML model is an undertaking of daunting proportions. In order to make this task manageable the reuse of related standards and taxonomies is required.

Questions?