UML Modeling and Profiles for Threat Modeling

Gerald Beuchelt

December 2013

# Motivation

To enable advanced threat information sharing a couple of protocols such as OpenIOC, RID, or STIX/TAXII have emerged over the last few years. Each of these protocols comes with a data model suited for their respective use cases. While these protocols are well suited for their respective purpose and must be enabled to evolve independently, they are addressing their respective audiences only. To enable sharing across different platforms and federate sharing, a threat meta model is needed to enable consistent mapping across ecosystem boundaries.

With threat actors getting more sophisticated, it is important to not only be able to capture ‘tactical’ data such as threat signatures, but also be able to describe complex contextual information such as threat actor profiles, intent and motivation, strategies, etc., and relate such higher-order data to specific threat signatures, TTPs, and incident descriptions. An example of such a description could be a ‘threat use case diagram’ like this:



Figure 1: Notional platform independent threat and actor model

Note that figure is purely notional – a real profile would leverage the existing modeling work done by STIX, NIEM, OpenIOC, CORAS (see e.g. [2]), and i\*.

Such a high level description can be useful in a number of applications:

* Semantic interoperability across different threat sharing ecosystems
* Development of identification/attribution systems that correlate threat indicators and TTPs with specific threat actors or threat actor classes
* Standardization of forensic analysis tools for cyber investigations
* Dynamic policy evaluation, enabling Risk or Threat Intelligence-based access control
* Risk analysis and security posture planning, supported by knowledge about the actor motivation and the specific threat indicators associated with them.

Note that this project is not intended to replace or incorporate existing threat sharing mechanisms, but instead should focus on enabling semantic interoperability and federation of existing standards.

# Goals

To arrive at a comprehensive project scope that allows for delivery of usable artifacts in a timely manner, a phase-based approach is implemented. The first phase will focus on consolidating existing protocols and models and establishment of an initial set of semantics that can work across these different approaches.

The second phase will broaden the existing models to fully include comprehensive social modeling and introduce social behavior elements into the architecture. It may also introduce a comprehensive meta-model or General Threat PIM that can capture all aspects of threat modeling.

A third phase will extend the threat modeling to include non-cyber threats and develop an approach to include countermeasure modeling and mapping of countermeasures to threats, TTPs, and strategies.

It should be noted that this activity should not interfere with the natural evolution of existing protocols: the goal is to be able to map between existing and emerging threat sharing systems in a consistent manner. In addition, a common meta model will also allow guiding the future development and enhancements of protocols.

## Phase 1 – Model and Protocol Interoperability

### Incorporation of Other Modeling Approaches

Provide a Cyber Domain PIM and mappings to threat-specific languages (in the form of platform specific models – PSM) for cyber risk assessments that aligns the UML Profile for NIEM with existing work done by CORAS and STIX. In addition, existing data models and protocols, including STIX/TAXII, OpenIOC, NIEM, etc. should be integrated into the overall profile.

A number of threat modeling approaches have been developed in the last few years:

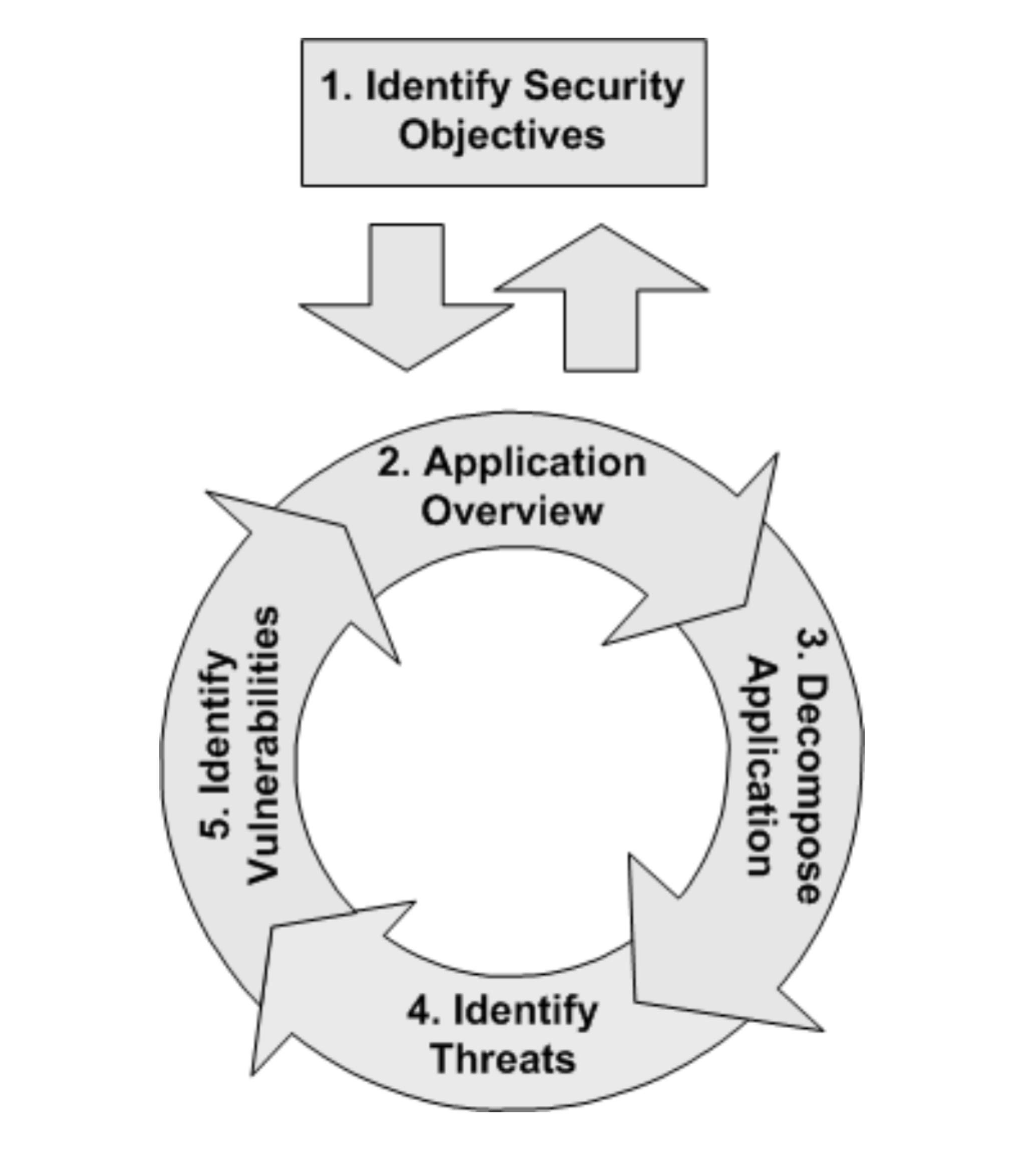
* Threat categories – STRIDE
  + Spoofing
  + Tampering
  + Repudiation
  + Information Disclosure
  + Denial of Service (Ddos)
  + Elevation of privilege
* Modeling life cycle (Application Centric)
  + Identify Security Objectives/Asset Identification
  + Architecture Documentation
  + Application Decomposition
  + Threat Identification
  + Vulnerability Identification

Figure : Threat Modeling Approach (see [3])

* + Threat Rating

### NIEM Aligned Cyber Domain PIM for STIX

A possible concrete artifact for the first phase could be a Cyber Domain PIM that profiles and models STIX information exchange using the NIEM profile. This would allow synchronization between these different models, and prepare a general mapping strategy for cross-protocol/meta-model mapping using an actual example. As a result, the Cyber Domain PIM would then provide two PSMs: one for STIX and one for NIEM:



Figure 3: Initial Cyber Domain PIM with STIX and NIEM

## Phase 2 – Social and Behavioral Modeling

### Social and Behavioral Modeling

Also, a crucial goal is to integrate social work such as the i\* framework that can describe social aspects and strategy, intent, and motivation, and allow the attribution of observed vulnerability exploitations to active campaigns. Specifically, a final meta-model would allow the combination of STIX (see Figure ??) and OpenIOC indicators with knowledge contained in a CORAS diagram (Figure ??), and ultimately with the characterization of a threat actor described in the security extensions of the i\* model (Figure ??)

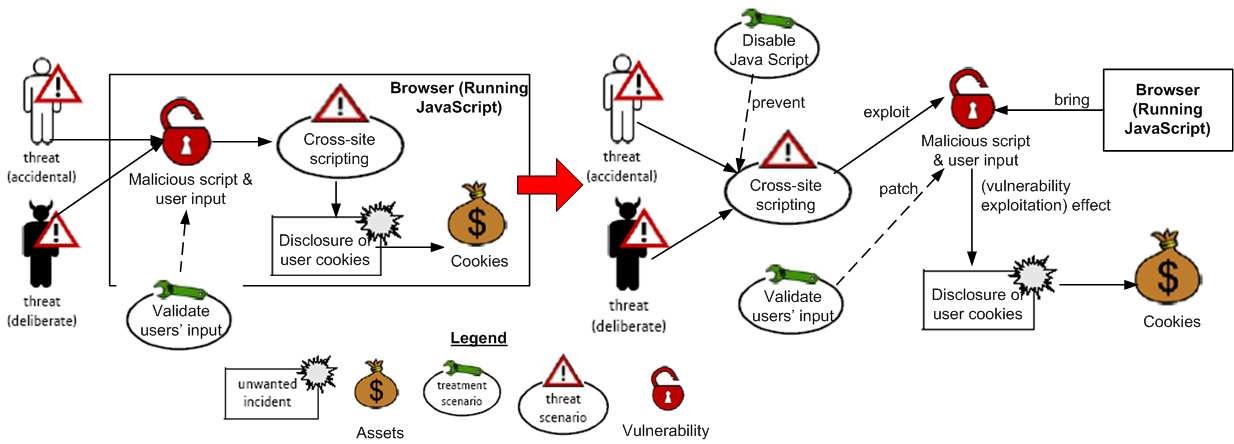


Figure 4: CORAS-based threat model (taken from [1])

Specifically, STIX already has a ThreatActor type (Figure ??) that should be aligned with the NIEM types from phase 1 and the CORAS threat actor work.

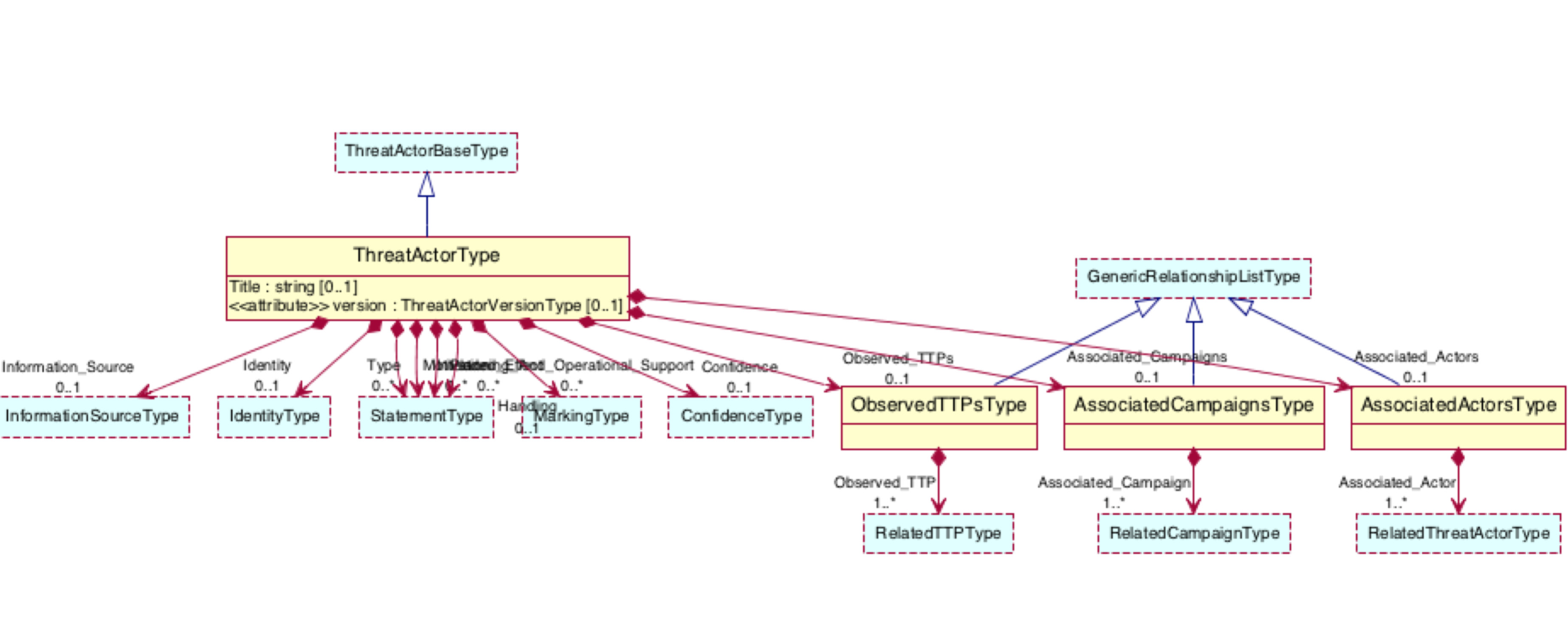


Figure 5: STIX ThreatActorType UML Representation

Guidance for social and behavioral modeling of complex concepts such as the Threat Actor, campaigns, strategy, motivation and intent, etc. may be gained from the i\* Framework[[1]](#footnote-1). Specifically, some of the Tropos research has already highlighted an approach to develop an actor-based security ontology:

* Anti-goals, which define scenarios where no software is faulty, but external factor prevent proper operation (see [5])
* Security Attack Scenario modeling, partially capturing the connection of intent, actor, and TTPs (see Figure ?? and [6]). This could be combined with the broader characterizations of actors as possible within the i\* framework.



Figure 6: Modification Attack Scenario in SI\* (from [6])

The Si\* (Secure i\*) working groups have developed a modeling tool (STS Tool) that may prove useful in the necessary analysis of this aspect of the Threat Modeling project.

### Meta-Model Development Based on Existing Work

With the phase 1 work in place, the Cyber Domain PIM can then be extended by other PSMs (including IODef, OpenIOC, etc.) to enable comprehensive interoperability across different systems (see Figure ??). With a sufficiently broad model in the Cyber Domain PIM, users of the respective PSMs will better understand the limitations of the existing protocols and models and deploy additional technologies to address gaps in their environments.



Figure 7: Complete Cyber PIM/PSM ecosystem

## Phase 3 – Non-Cyber and Countermeasure Modeling

A third phase will look at broadening the Cyber Domain PIM and the associated Threat Meta Model to extend to non-cyber related threats. This phase is not well defined at this time, but the goal will be to allow for threat sharing across cyber, physical, and other domains. This will require more research into current threat sharing practices with other stakeholders.

Similar to the goal for the Cyber Domain PIM, such an extension into non-cyber domains is not intended to replace or incorporate existing threat sharing mechanisms, but instead should focus on enabling semantic interoperability and federation of existing standards.

Finally, a third phase may also look into the modeling of specific countermeasures that can be used to respond to threats: with such a model, a threat sharing environment can start implementing not only ‘wire-speed’ threat sharing and heighten share situational awareness, but also assist in automated deployment of specific countermeasures to mitigate the threats thus shared.

# Strategy

Identify existing elements and technologies that can be leveraged into developing a comprehensive model. Specifically, we should take a look at the following projects and stakeholders:

* Threat ontology by CMU
* STIX and TAXII, OpenIOC, RID, CAP, etc.
* ThreadConnect, Mandiant, and similar online tools
* Organizations that have experience in threat intelligence sharing
* Government programs, such as NIEM, DHS HSIN, HSP, Infragard, etc.

# Deliverables

## Phase 1

* Cyber Domain Platform Independent Model (PIM) for Threat Modeling – this PIM needs to incorporate the concepts found in existing modeling approach and specifically allow the conceptual characterization and relationships of
  + Threat actors, groups, organization
  + Motivation, intent, strategies, including social modeling aspects
  + Campaigns, constituents
  + Tactics, techniques, and procedures
  + Vulnerabilities, threats, and corresponding indicators/signatures
* Platform Specific Models (PSM) representing existing approaches including STIX, OpenIOC, NIEM, etc.
  + The existing relationship between modeling systems (such as STIX and OpenIOC) must be preserved, and – essentially – become a result of the conceptual modeling approach
  + Any NIEM representation of threat sharing will need to be consistent with the existing NIEM PIM [4], and re-use existing data models from the applicable NIEM domains

## Phase 2

Comprehensive UML meta-model and specific profiles for threat modeling that can be used to build:

* Threat Sharing Meta-Model to describe elements need to build the PIM
* Extension of the Cyber Domain PIM to include rich social and behavioral aspects of complex elements such as Threat Actors, Campaigns, Stratgy, Motivation and Intent, etc.

In addition, implementation guidance should include :

* Mappings to eventing protocols such as CAP or IODef
* Transport bindings (PIM and PSM layer), such as TAXII for STIX
* Non-normative guidance on integration approaches of existing security solutions and threat-sharing initiatives

## Phase 3

* Extension of the Cyber Domain PIM and the Threat Meta Model to non-cyber domains, including law enforcement, defense, counter terrorism, counter narco-trafficking, etc.
* Extension of the model to include a comprehensive countermeasure model to assist automatic deployments of specific threats.

## Notional Timeline



# References

[1] E. Yu, et al., “A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations”,

[2] H. Dahl, et al., “Structured Semantics for the CORAS Security Risk Modelling Language”,

[3] M. Knobloch, “Threat Modeling”, <https://www.owasp.org/images/c/cf/OWASP-BeNeLux_2010_ThreatModeling.pdf>

[4] OMG, “UML Profile for NIEM (Beta 1)”, dtc-12-07-09

[5] V.E.S. Souza, et al., “Monitoring and Diagnosing Malicious Attacks with Autonomic Software”, 10.1007/978-3-642-04840-1\_9

[6] P. Giorgini, et al., “Towards the Development of Secure Information Systems: Security Reference Diagrams and Security Attack Scenarios.” See http://klase.fbk.eu/papers/MGM-CAiSE04.pdf

1. See e.g. here: <http://www.cs.toronto.edu/km/istar/#RelatedPublications>   
    or here: <http://istar.rwth-aachen.de/> [↑](#footnote-ref-1)