# Operational Threat & Risk Information Sharing and Analytics

*TEAM* ***Threat***

OMG®
WE SET THE STANDARD®

ISE

ORACLE

IBM

demandware
move faster, grow faster

Model Driven Solutions
Where Business Meets Technology

U.S. Department of Defense
DEFENSE SECURITY SERVICE

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

CAL OES

KDM Analytics

FUJITSU

RSA INTELLIGENCE DRIVEN SECURITY

NIST

LOCKHEED MARTIN

# Introduction

Topic:

Operational threat and risk conceptual model and mappings

Presenter:

Cory Casanave, Model Driven Solutions

Cory-c@modeldriven.com

Organization:

Object Management Group

www.omg.org

Resources:

www.threatrisk.org

Government Sponsor

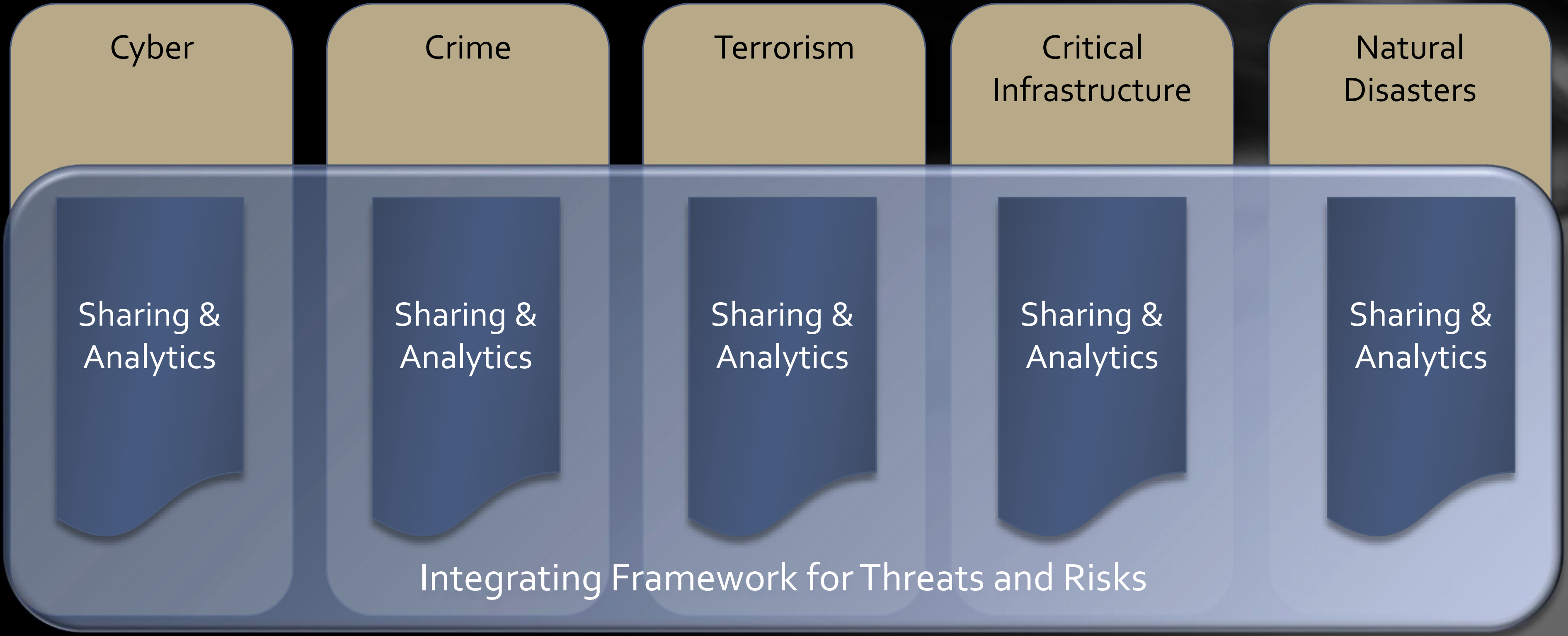
Information Sharing Environment

www.ise.gov

# Problem Space

- There is a critical need to understand and mitigate threats and risks – to “connect the dots”.
- The Landscape of threats is changing
  - Multiple attack vectors, cyber/physical and other
  - Advanced threats utilize multiple vulnerabilities
- There are multiple communities addressing the same threats
  - Cyber/physical, emergency management, safety, defense, etc.
- No comprehensive consistent semantic framework
  - Existing systems provide insular treatment of threat/risk relationships
  - Comprehensive system would allow system-of-systems interoperability (private/private, public/private)

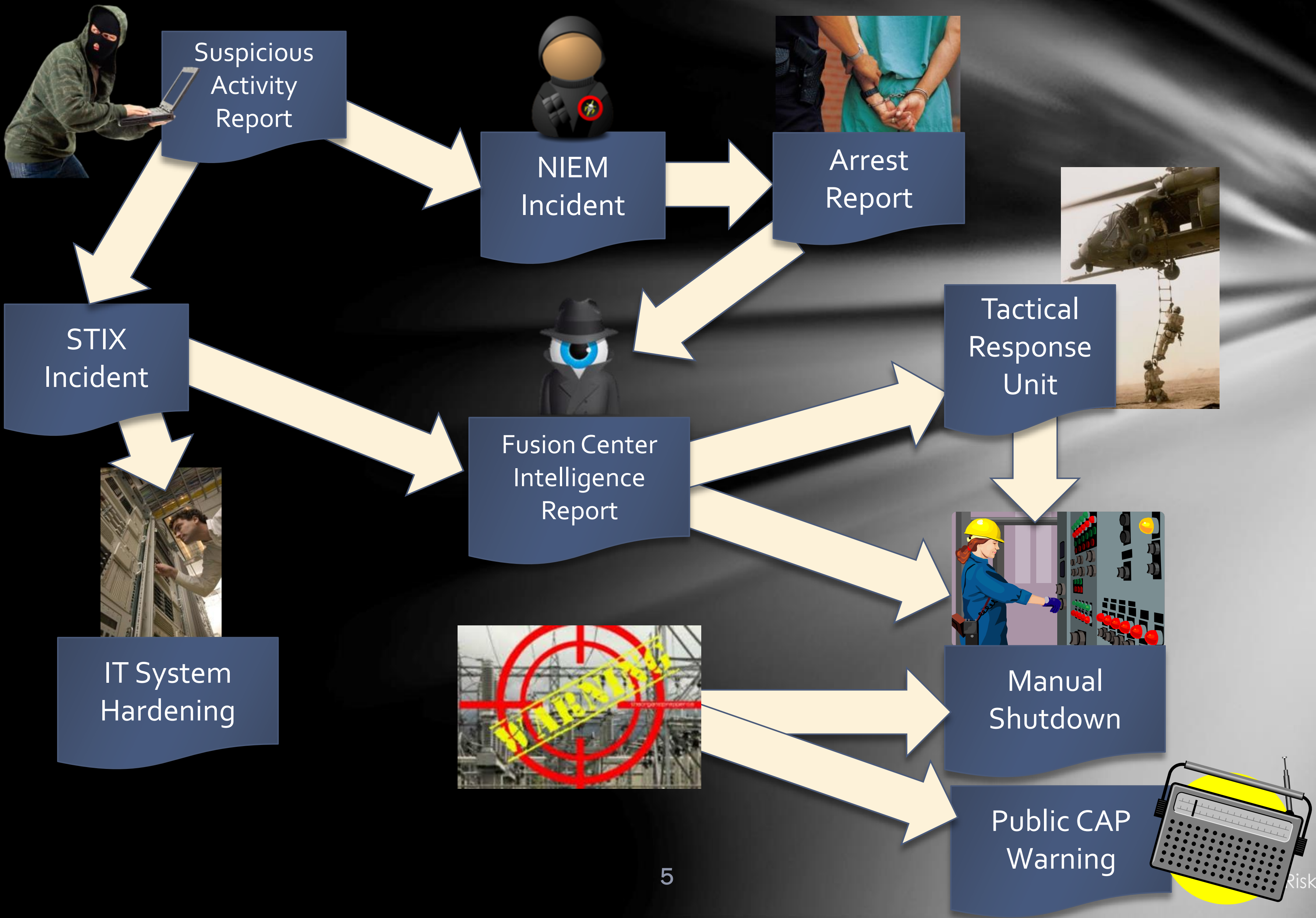
# What we need is an integrating framework that supports automated data mapping



An integrating framework that helps us deal with all aspects of a risk or incident

A federation of risk and threat information sharing and analytics capabilities

# Example Information Flows



Suspicious Activity Report

NIEM Incident

Arrest Report

STIX Incident

Fusion Center Intelligence Report

Tactical Response Unit

IT System Hardening

Manual Shutdown

Public CAP Warning

# Primary classes of use cases

Transformation from one information sharing data format to another

- Example: STIX Cyber Event to NIEM to a CAP Alert

Analytics of information federated from multiple sources

- Examples:
  - Fusion center “connects the dots” between a stolen laptop (from NIEM) and a cyber incident (From STIX)
  - Bio hazard detected by automated  instruments and collaborated by local health care professionals

# Approach

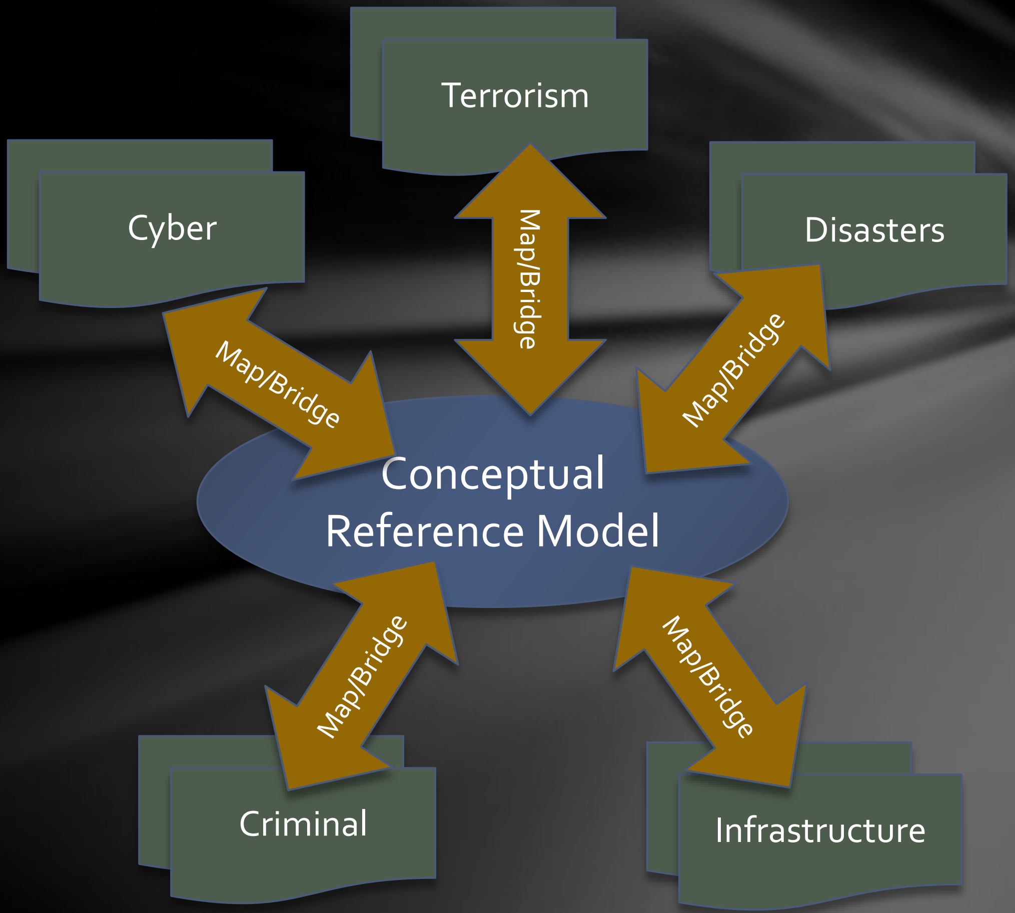
Highlight O(N) vs. O(N^2)

Construct a conceptual reference model informed by existing schema, research and best practices

- This conceptual model is independent of specific data structures, technologies and terminologies

Define mapping models between the conceptual model and purpose/technology schema

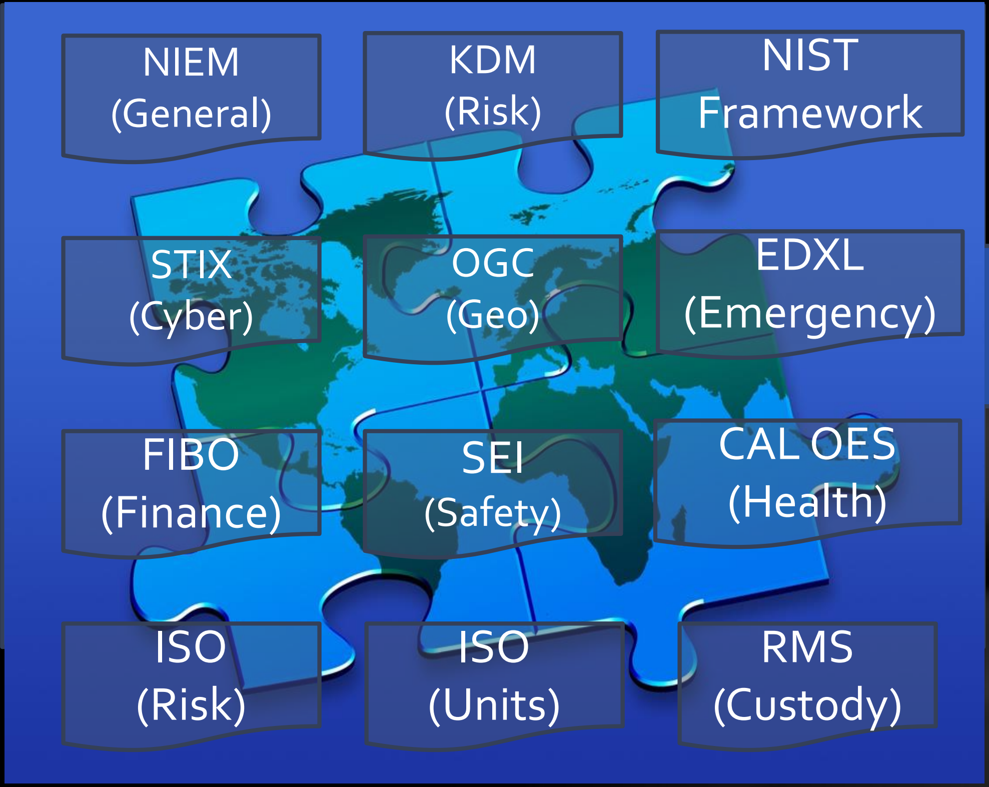
Make both models sufficiently precise that they can drive automated bridging between any mapped schema



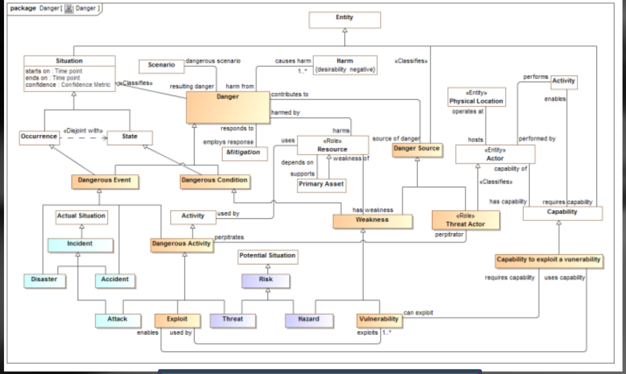
# Precepts

- The purpose/organizational/technology specific schema will not (should not) go away
- A "one size fits all" solution will not work
  - There will be no one technology
  - There will be no one terminology or language
  - There will be no one data structure for threats and risks
- Our focus is <u>federation</u>
  - Understanding the concepts behind the schema
  - Mapping them to/through a common conceptual model
  - Enabling interoperability by bridging between the specific schema
  - Supporting integration and coordination of mitigation and response capabilities

# Conceptual Model Inputs



## Conceptual Reference Model



MAP

STIX, NIEM, EDXL, Others

*There is still more to do to fully integrate the above and we anticipate more inputs and use cases*

# Realization

*This "conceptual reference model" orientation is really quite different from defining a model or ontology for a specific purpose or application!*

# Mappings included

STIX – Structured Threat Information Exchange, for Cyber threat information. (Moving to Oasis "CTI")

NIEM – National Information Exchange Model – For justice, public safety and other domains.

Risk Model – A concrete risk model for data interchange is included and mapped as none currently exists as a standard.

NIST 800-53 – Security and Privacy Controls for information systems. This is not a data mapping but shows how the concepts support the controls.

Note: More mappings are anticipated as the initiative unfolds. Some may be published but not standardized.

# Ontological Challenges

Past present and future all are of interest and important to the semantics of the data. "Temporal aspects" of all relationships and situations is important. Not understanding these temporal aspects could result in error.

- The threat/risk model incorporates temporal aspects into the core of the ontology and language. All situations and relationships are temporal. In OWL and other FOL based languages this requires reification.

Provenance of every "fact" is crucial to trust.

- Due to the reification, metadata can be attached to every assertion.

Different communities and systems use different ways to represent the same thing or occurrence in the world.

- The threat/risk model is a model of a real (or possible) world, not data. These concepts provide a pivot point between different data representations that are then **mapped**.

What something is and the roles it takes in various situation gets conflated.

- "Role" is a "first class" concept – something or someone may play different roles at the same or different times

# Pivoting Through a Reference Model

Data representations (Schema & Instances)

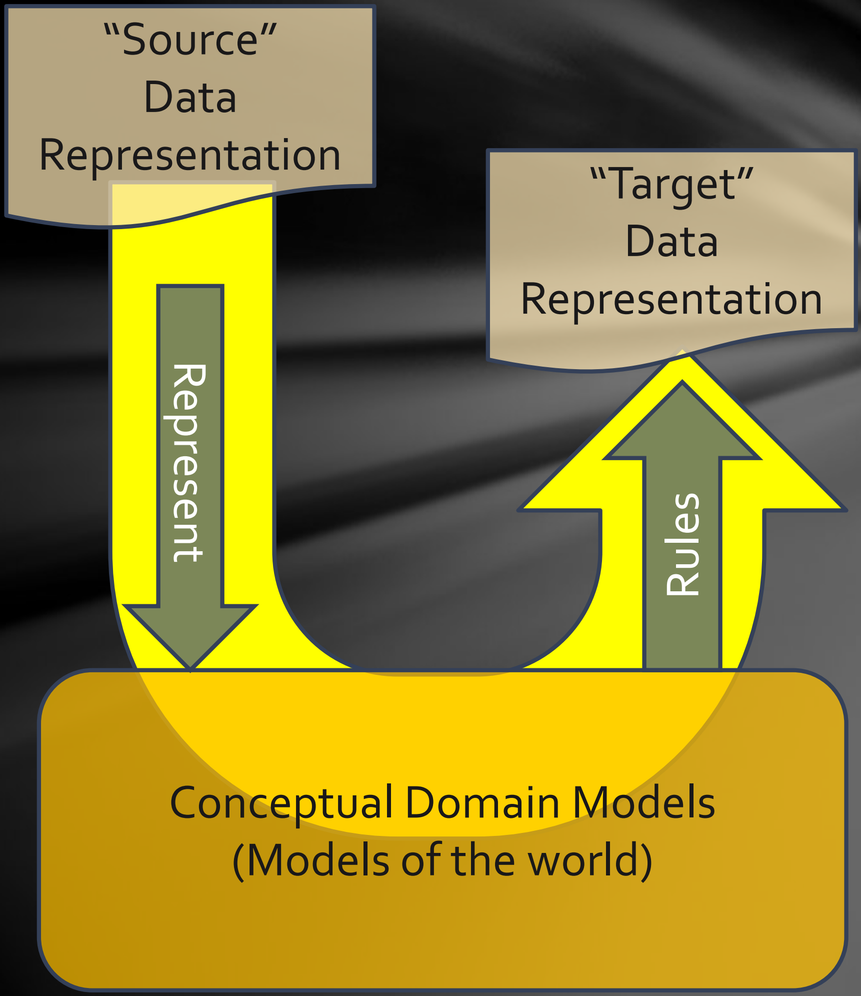
- Model data for a purpose using a technology
- "Instances" are data structures (e.g. SQL tables or XML documents) – "facts" about the things in the world from some perspective

Conceptual Reference Models

- A conception of the world by a group of stakeholders – less purpose specific
- "Instances" are things in the world – so can't be in models

Using abstraction, we can have multiple representations of facts about the world in different data structures and technologies

Rules define how domain concepts can be represented in a particular form – rules can be simple and generic or heavyweight and specific, depending on the representation.


"Source" Data Representation
"Target" Data Representation
Represent
Rules
Conceptual Domain Models (Models of the world)

# Kinds of models

## Conceptual Reference Models

- Defines the terms and concepts of the threat & risk domain as a semantic model. Conceptual models can also be transformed to ontologies.

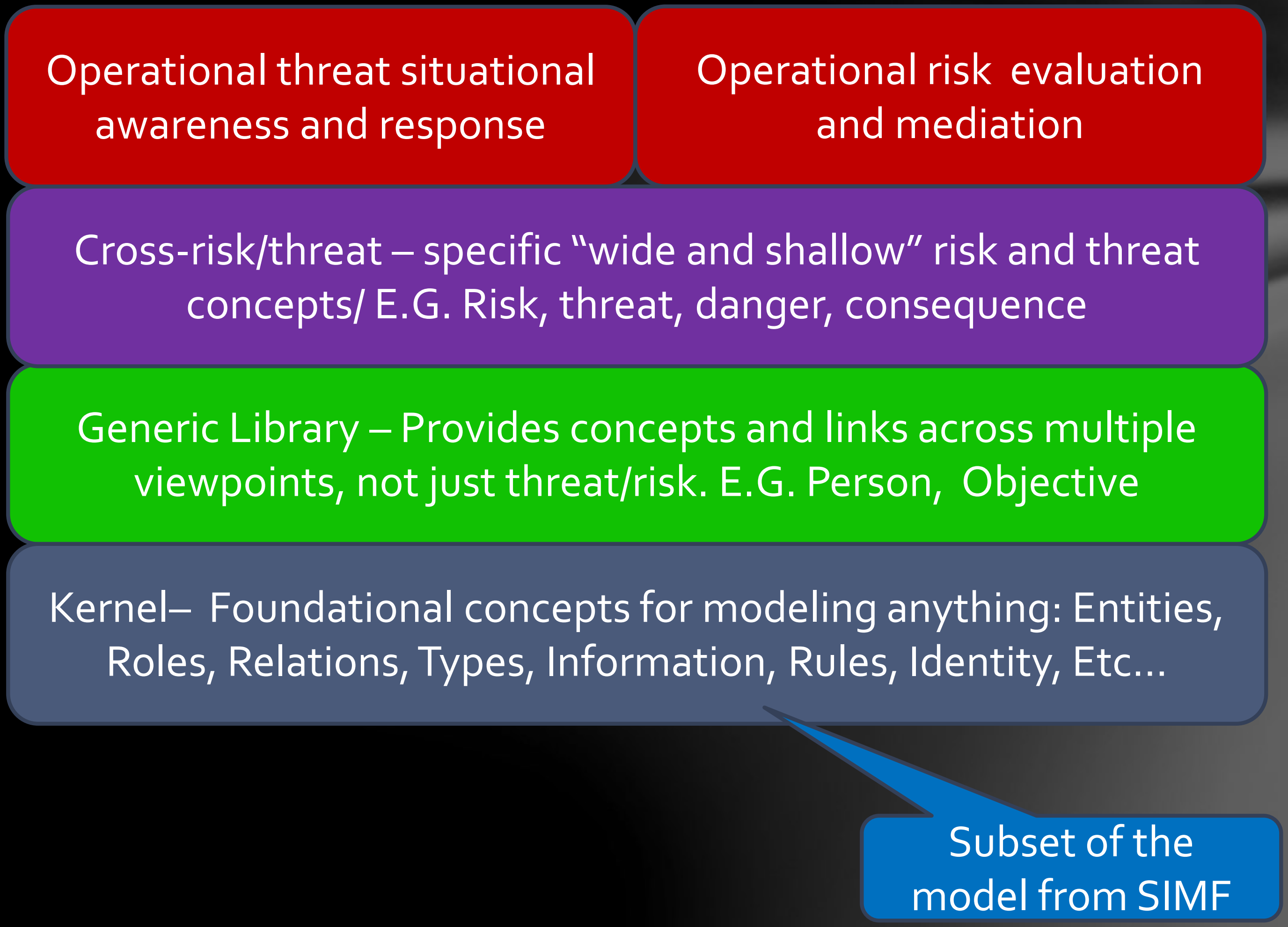
## Data models

- Represents specific logical or physical data schema for a specific purpose – more concrete and structured.
- Data models are a direct representation of some kind of schema, e.g. XML Schema, SQL Schema or RDF Schema.

## Mappings

- Mappings relate a data model to one or more conceptual models to provide for automated transformation and federation of information in these deferent formats.
- The conceptual models become the "pivot point" between multiple data representations of the same and related concepts.

# Conceptual Model Layering



Operational threat situational awareness and response

Operational risk evaluation and mediation

Cross-risk/threat – specific “wide and shallow” risk and threat concepts/ E.G. Risk, threat, danger, consequence

Generic Library – Provides concepts and links across multiple viewpoints, not just threat/risk. E.G. Person, Objective

Kernel– Foundational concepts for modeling anything: Entities, Roles, Relations, Types, Information, Rules, Identity, Etc…

Subset of the model from SIMF

# Conceptual Model Packages

**Core Concepts**

Foundation

Identifiers

Information

Patterns

Process

Quantities and Units

Rules

Situations

Timeframe

**Generic Concepts**

Ability

Actors

Assessment

Control

Credentials

Enterprise

Entity Kinds

Intent

Location

Observation

Organization

Person

Prediction

Resources

Systems

**Threat and Risk Specific Concepts**

Campaign

Course of Action

Cyber

Danger Categories

Incident

Indicator

Kill Chain

Mitigation

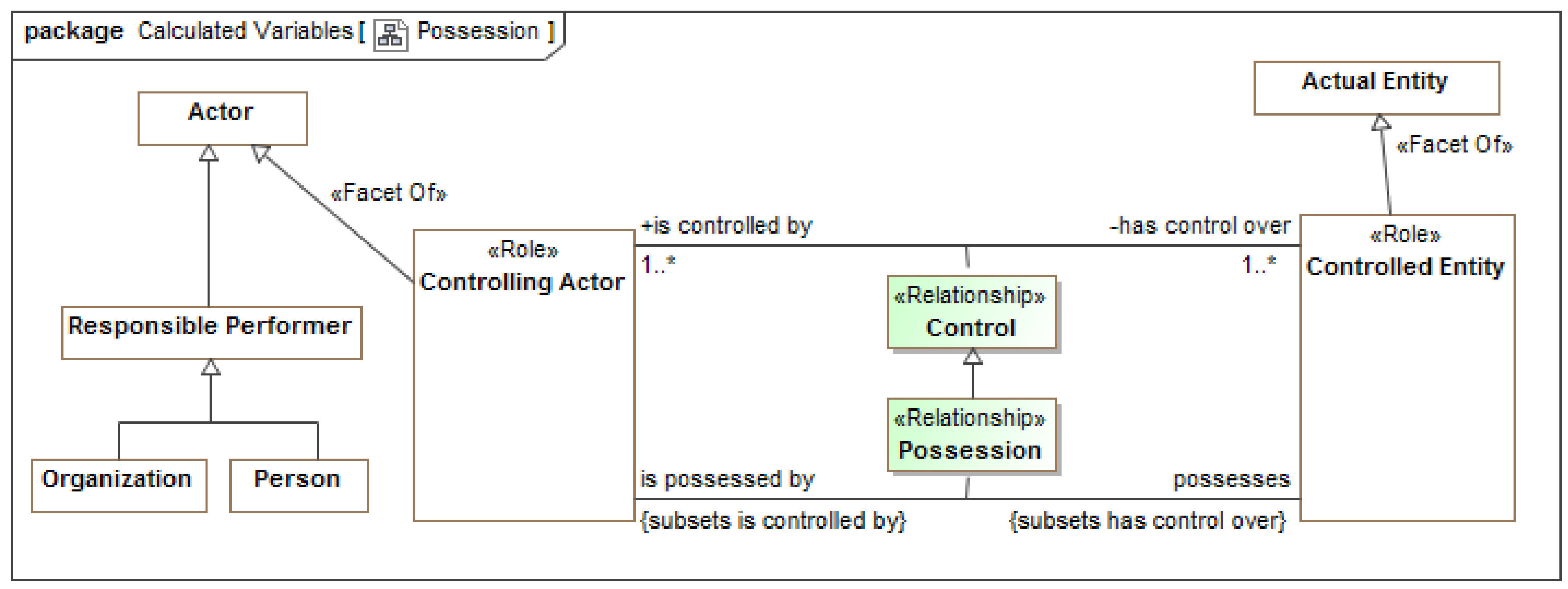
Risk Treatment

Threat

Undesirable Situations

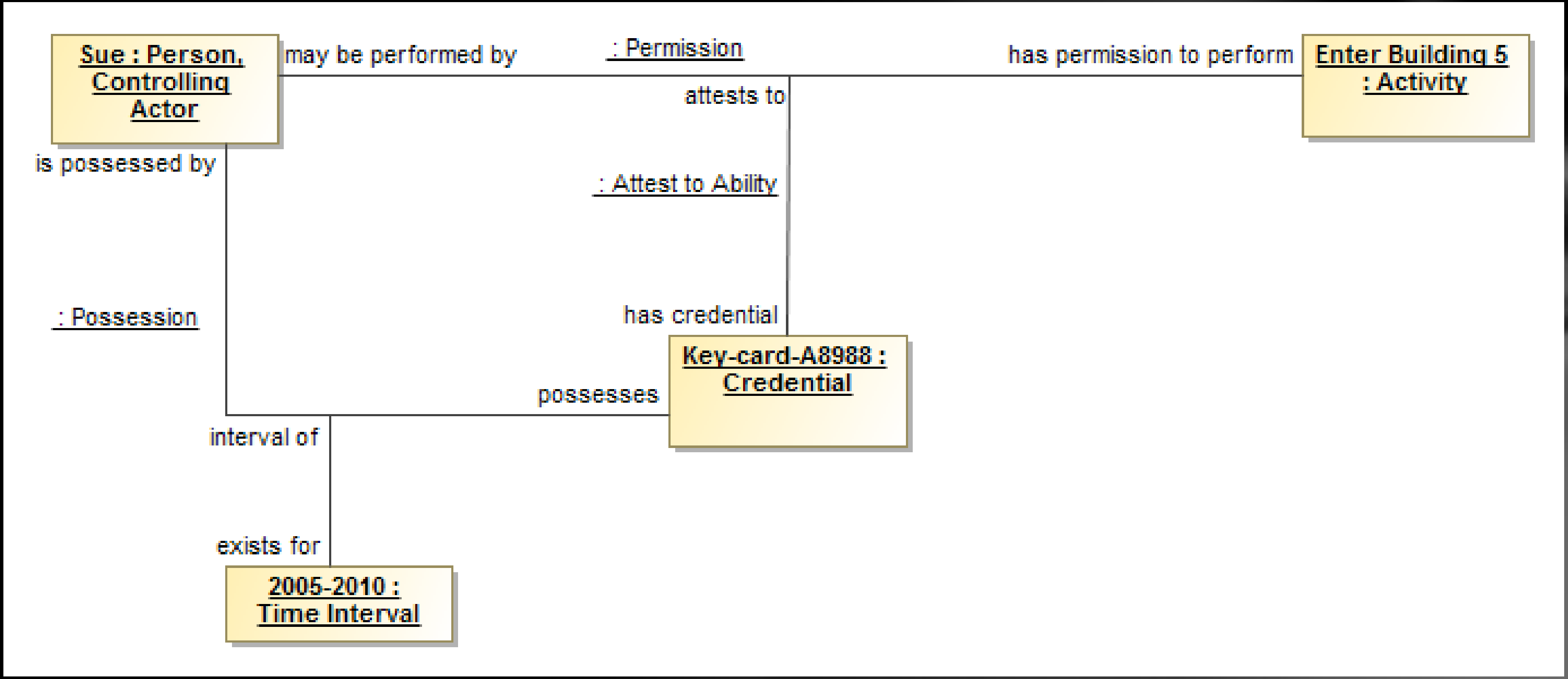
Vulnerability

# Example of Modeling Style



- Control Possession relationships are "first class" – have a timeframe, can be part of cause and effect, etc.
- "Controlling Actor" is a role – people and organizations can play this role
- Both entity classes and relationships form hierarchies
- There are multiple ways "data structures" could be arranged to represent this information or a subset of it – that is the subject of mappings.

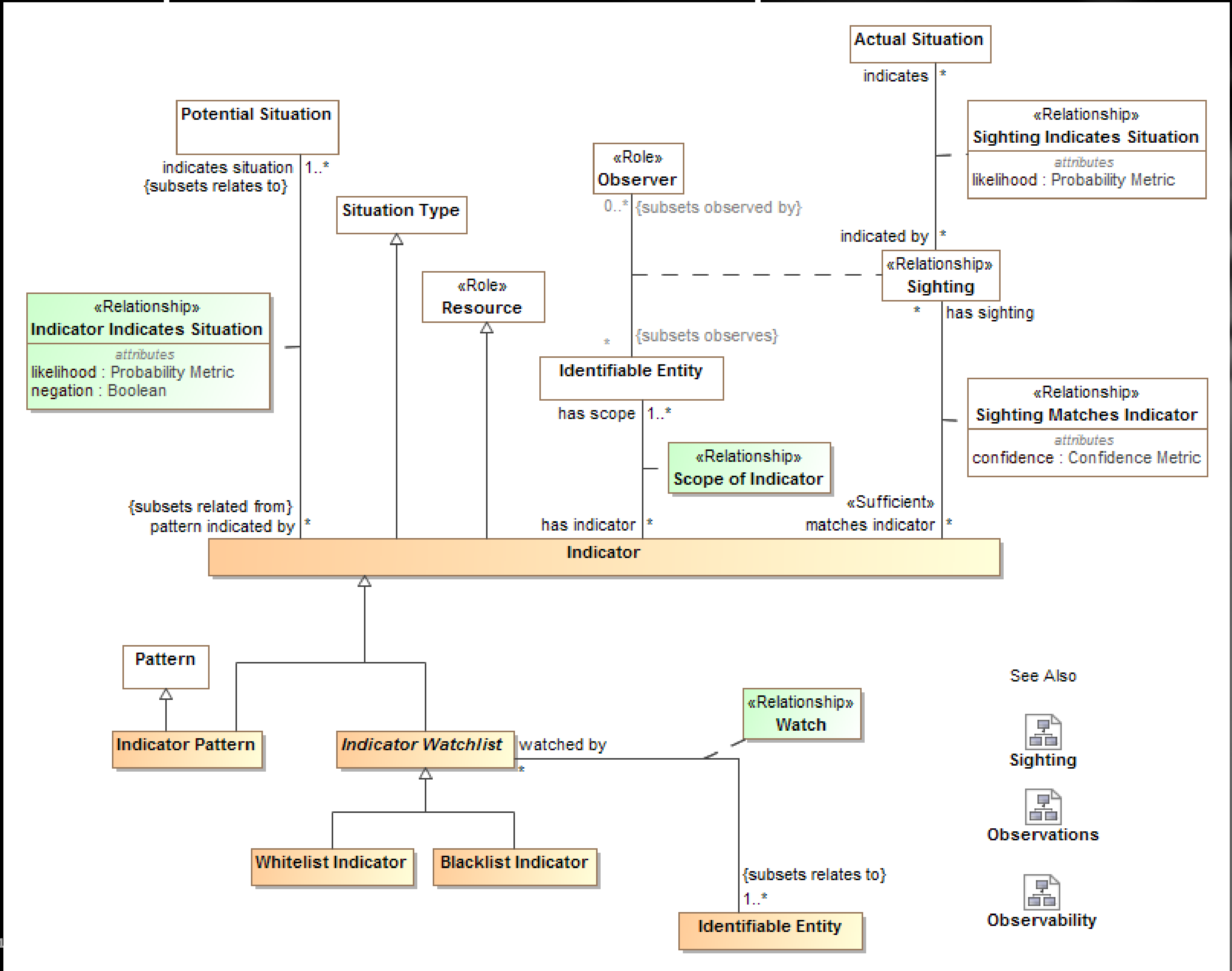
# Example Instances


Sue : Person, Controlling Actor
may be performed by
: Permission
has permission to perform
Enter Building 5 : Activity
attests to
is possessed by
: Attest to Ability
: Possession
has credential
Key-card-A8988 : Credential
possesses
interval of
exists for
2005-2010 : Time Interval

In the time interval from 2005-2010 Sue <possesses>“Key-card-A8988” that <attests to> the permission: Sue <has permission to perform> “Enter Building 5”.

Note: Note the best notation; this is intended to validate the model using UML.

# Example of more threat-specific module



Actual Situation

indicates *

«Relationship»
Sighting Indicates Situation
attributes
likelihood : Probability Metric

indicated by *

Potential Situation

indicates situation 1..*
{subsets relates to}

«Role»
Observer

0..* {subsets observed by}

Situation Type

«Relationship»
Sighting

* has sighting

«Role»
Resource

«Relationship»
Indicator Indicates Situation
attributes
likelihood : Probability Metric
negation : Boolean

* {subsets observes}

Identifiable Entity

has scope 1..*

«Relationship»
Sighting Matches Indicator
attributes
confidence : Confidence Metric

«Relationship»
Scope of Indicator

{subsets related from}
pattern indicated by *

has indicator *

«Sufficient»
matches indicator *

Indicator

Pattern

Indicator Pattern

Indicator Watchlist

watched by
*

«Relationship»
Watch

Whitelist Indicator

Blacklist Indicator

{subsets relates to}
1..*

Identifiable Entity

See Also

Sighting

Observations

Observability

# Model/Ontology/Vocabulary Representation

Operational Threat/Risk uses the in-progress “Semantic Information Modeling for Federation” (SIMF) specification, being developed in the OMG.

SIMF defines a foundational semantic conceptual model for the modeling language as well as a UML (Unified Modeling Language) profile.

The UML Profile is what has been shown, using the “Cameo Concept Modeler” from Nomagic.

Based on the (draft) specification, CCM is able to generate OWL for the threat/risk model. Other implementation technologies could be generated as well.

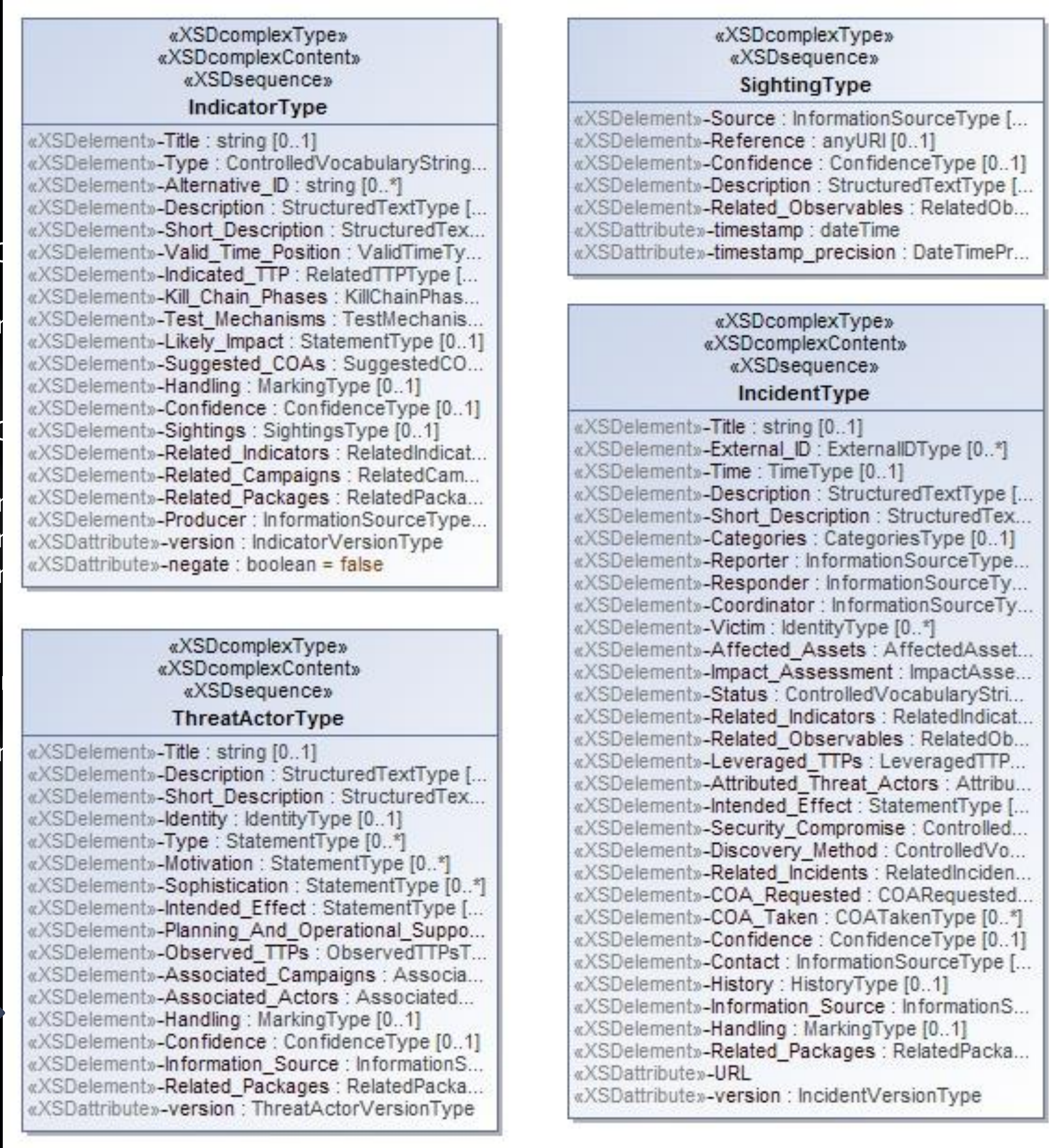
# Data Mappings

*STIX & NIEM*

# Representing the STIX physical model

```
se="stixCommon:IndicatorBaseType">
s:sequence>
            <xs:element name="Title" type="xs:string" minC
                        <xs:annotation>
                                    <xs:documentatior
                        </xs:annotation>
            </xs:element>
            <xs:element name="Type" type="stixCommon:C
                        <xs:annotation>
                                    <xs:documentatior
                                    <xs:documentatior
                                    <xs:documentatior
                        </xs:annotation>
            </xs:element>
            <xs:element name="Alternative_ID" type="xs:st
                        <xs:annotation>
                                    <xs:documentatior
```

XML Schema is reverse engineered into UML. Next version of STIX will have native UML model.



«XSDcomplexType»
«XSDcomplexContent»
«XSDsequence»
**IndicatorType**

«XSDelement»-Title : string [0..1]
«XSDelement»-Type : ControlledVocabularyString...
«XSDelement»-Alternative_ID : string [0..*]
«XSDelement»-Description : StructuredTextType [...
«XSDelement»-Short_Description : StructuredTex...
«XSDelement»-Valid_Time_Position : ValidTimeTy...
«XSDelement»-Indicated_TTP : RelatedTTPType [...
«XSDelement»-Kill_Chain_Phases : KillChainPhas...
«XSDelement»-Test_Mechanisms : TestMechanis...
«XSDelement»-Likely_Impact : StatementType [0..1]
«XSDelement»-Suggested_COAs : SuggestedCO...
«XSDelement»-Handling : MarkingType [0..1]
«XSDelement»-Confidence : ConfidenceType [0..1]
«XSDelement»-Sightings : SightingsType [0..1]
«XSDelement»-Related_Indicators : RelatedIndicat...
«XSDelement»-Related_Campaigns : RelatedCam...
«XSDelement»-Related_Packages : RelatedPacka...
«XSDelement»-Producer : InformationSourceType...
«XSDattribute»-version : IndicatorVersionType
«XSDattribute»-negate : boolean = false

«XSDcomplexType»
«XSDsequence»
**SightingType**

«XSDelement»-Source : InformationSourceType [...
«XSDelement»-Reference : anyURI [0..1]
«XSDelement»-Confidence : ConfidenceType [0..1]
«XSDelement»-Description : StructuredTextType [...
«XSDelement»-Related_Observables : RelatedOb...
«XSDattribute»-timestamp : dateTime
«XSDattribute»-timestamp_precision : DateTimePr...

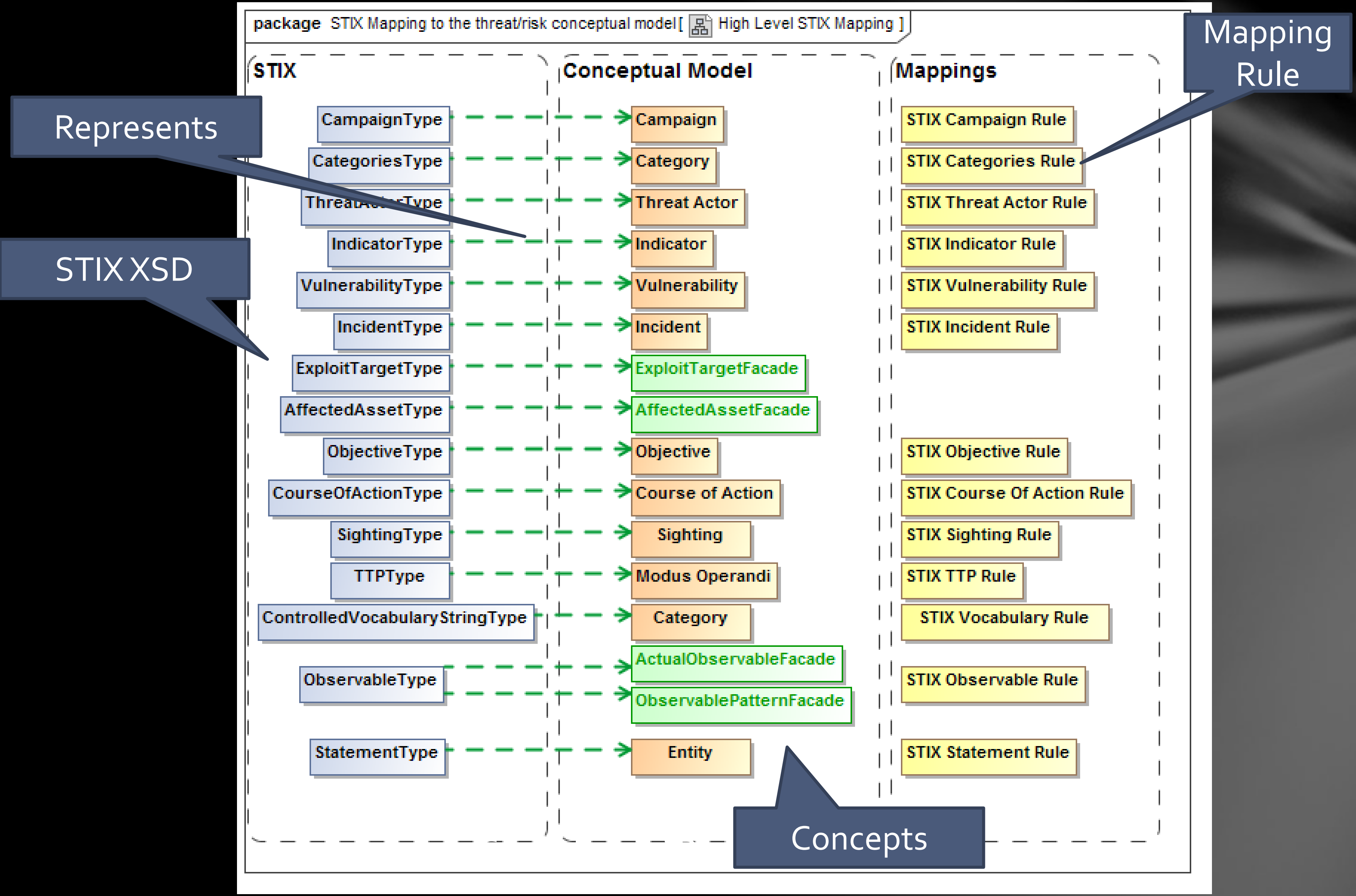
«XSDcomplexType»
«XSDcomplexContent»
«XSDsequence»
**ThreatActorType**

«XSDelement»-Title : string [0..1]
«XSDelement»-Description : StructuredTextType [...
«XSDelement»-Short_Description : StructuredTex...
«XSDelement»-Identity : IdentityType [0..1]
«XSDelement»-Type : StatementType [0..*]
«XSDelement»-Motivation : StatementType [0..*]
«XSDelement»-Sophistication : StatementType [0..*]
«XSDelement»-Intended_Effect : StatementType [...
«XSDelement»-Planning_And_Operational_Suppo...
«XSDelement»-Observed_TTPs : ObservedTTPsT...
«XSDelement»-Associated_Campaigns : Associa...
«XSDelement»-Associated_Actors : Associated...
«XSDelement»-Handling : MarkingType [0..1]
«XSDelement»-Confidence : ConfidenceType [0..1]
«XSDelement»-Information_Source : InformationS...
«XSDelement»-Related_Packages : RelatedPacka...
«XSDattribute»-version : ThreatActorVersionType

«XSDcomplexType»
«XSDcomplexContent»
«XSDsequence»
**IncidentType**

«XSDelement»-Title : string [0..1]
«XSDelement»-External_ID : ExternalIDType [0..*]
«XSDelement»-Time : TimeType [0..1]
«XSDelement»-Description : StructuredTextType [...
«XSDelement»-Short_Description : StructuredTex...
«XSDelement»-Categories : CategoriesType [0..1]
«XSDelement»-Reporter : InformationSourceType...
«XSDelement»-Responder : InformationSourceTy...
«XSDelement»-Coordinator : InformationSourceTy...
«XSDelement»-Victim : IdentityType [0..*]
«XSDelement»-Affected_Assets : AffectedAsset...
«XSDelement»-Impact_Assessment : ImpactAsse...
«XSDelement»-Status : ControlledVocabularyStri...
«XSDelement»-Related_Indicators : RelatedIndicat...
«XSDelement»-Related_Observables : RelatedOb...
«XSDelement»-Leveraged_TTPs : LeveragedTTP...
«XSDelement»-Attributed_Threat_Actors : Attribu...
«XSDelement»-Intended_Effect : StatementType [...
«XSDelement»-Security_Compromise : Controlled...
«XSDelement»-Discovery_Method : ControlledVo...
«XSDelement»-Related_Incidents : RelatedInciden...
«XSDelement»-COA_Requested : COARequested...
«XSDelement»-COA_Taken : COATakenType [0..*]
«XSDelement»-Confidence : ConfidenceType [0..1]
«XSDelement»-Contact : InformationSourceType [...
«XSDelement»-History : HistoryType [0..1]
«XSDelement»-Information_Source : InformationS...
«XSDelement»-Handling : MarkingType [0..1]
«XSDelement»-Related_Packages : RelatedPacka...
«XSDattribute»-URL
«XSDattribute»-version : IncidentVersionType

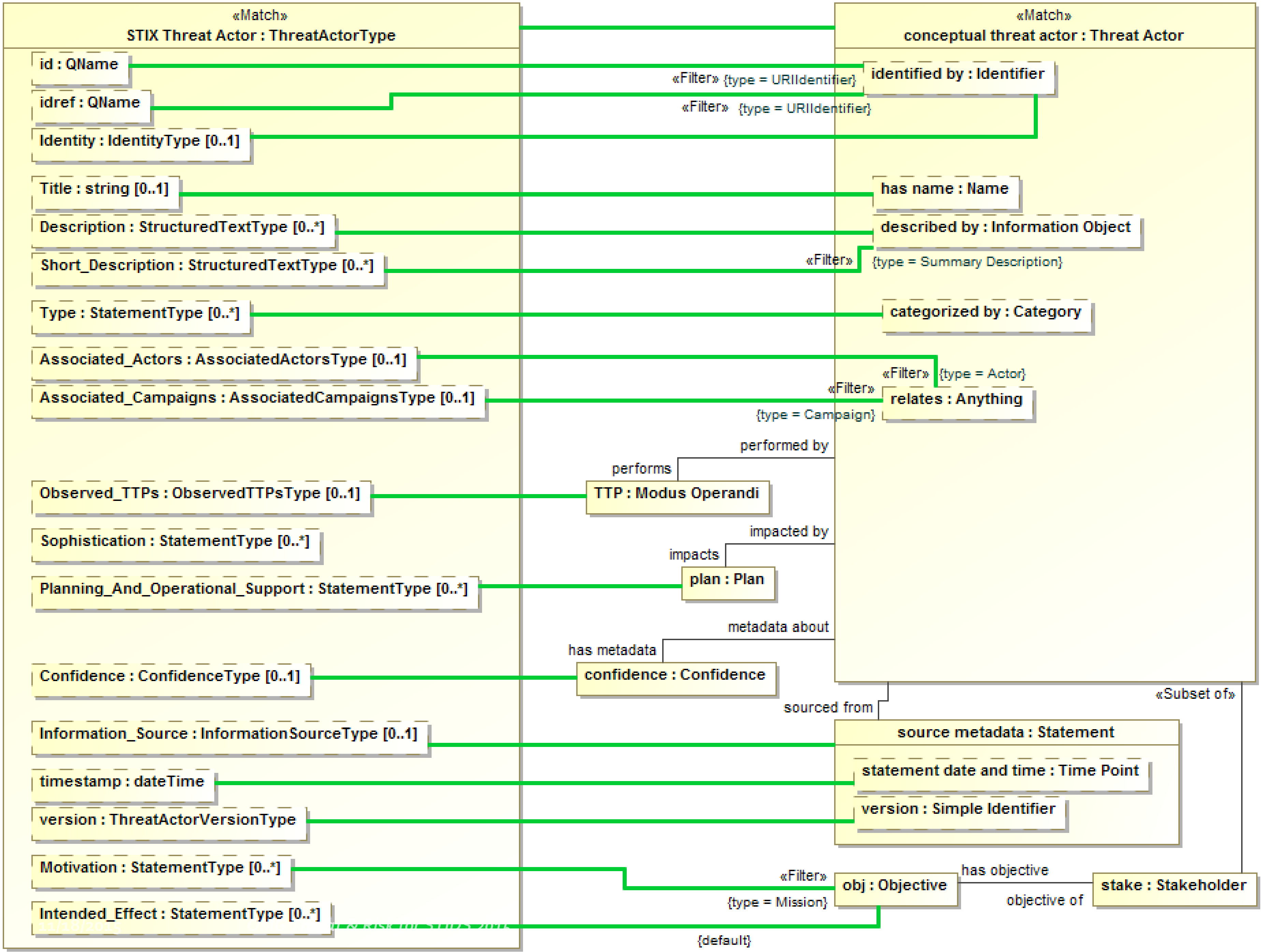
# XML Element represents concept



package STIX Mapping to the threat/risk conceptual model [ High Level STIX Mapping ]

| STIX | Conceptual Model | Mappings |
|---|---|---|
| CampaignType | Campaign | STIX Campaign Rule |
| CategoriesType | Category | STIX Categories Rule |
| ThreatActorType | Threat Actor | STIX Threat Actor Rule |
| IndicatorType | Indicator | STIX Indicator Rule |
| VulnerabilityType | Vulnerability | STIX Vulnerability Rule |
| IncidentType | Incident | STIX Incident Rule |
| ExploitTargetType | ExploitTargetFacade | |
| AffectedAssetType | AffectedAssetFacade | |
| ObjectiveType | Objective | STIX Objective Rule |
| CourseOfActionType | Course of Action | STIX Course Of Action Rule |
| SightingType | Sighting | STIX Sighting Rule |
| TTPType | Modus Operandi | STIX TTP Rule |
| ControlledVocabularyStringType | Category | STIX Vocabulary Rule |
| ObservableType | ActualObservableFacade<br>ObservablePatternFacade | STIX Observable Rule |
| StatementType | Entity | STIX Statement Rule |

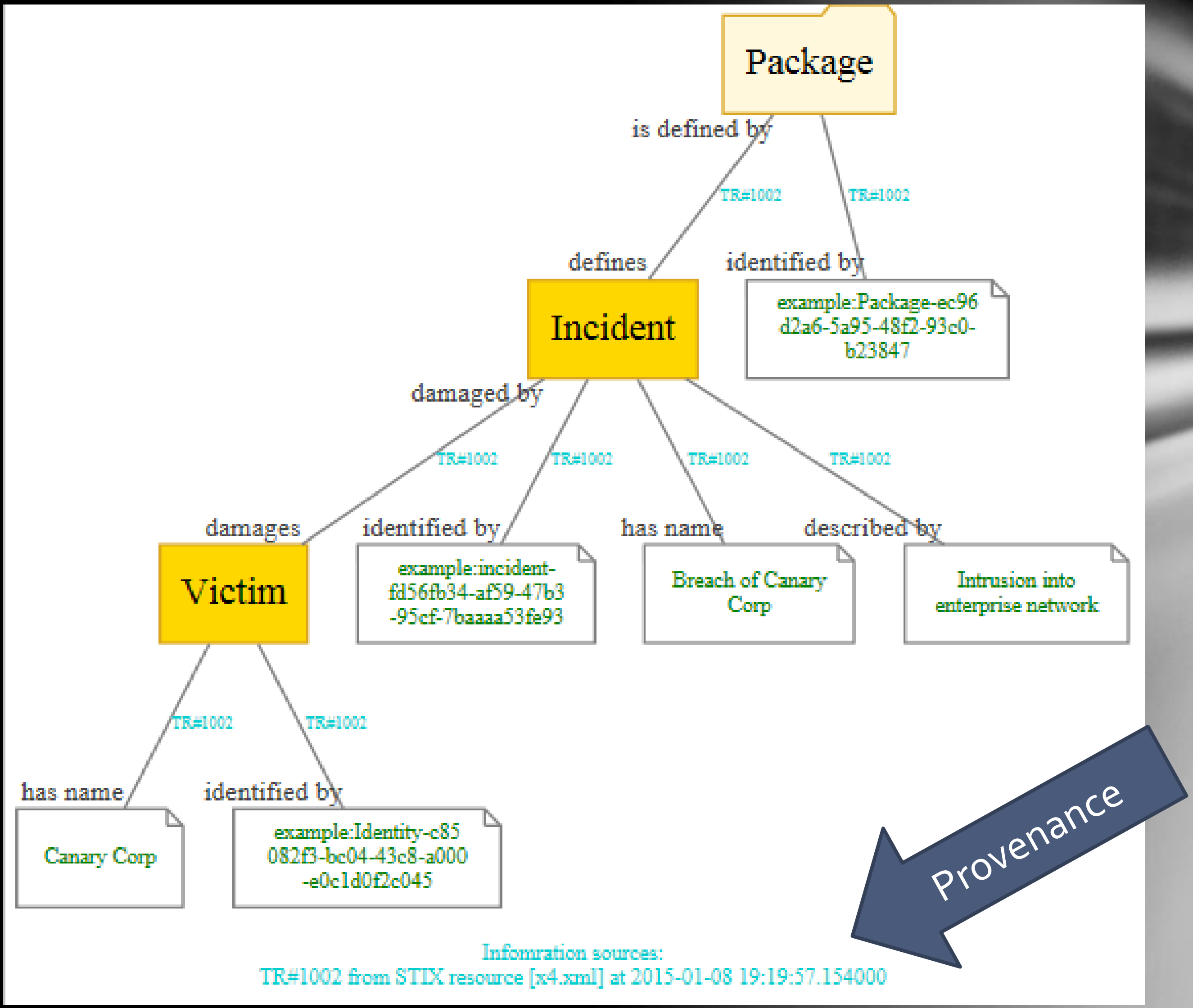
Rules specify mapping details


«Match»
STIX Threat Actor : ThreatActorType
id : QName
idref : QName
Identity : IdentityType [0..1]
Title : string [0..1]
Description : StructuredTextType [0..*]
Short_Description : StructuredTextType [0..*]
Type : StatementType [0..*]
Associated_Actors : AssociatedActorsType [0..1]
Associated_Campaigns : AssociatedCampaignsType [0..1]
Observed_TTPs : ObservedTTPsType [0..1]
Sophistication : StatementType [0..*]
Planning_And_Operational_Support : StatementType [0..*]
Confidence : ConfidenceType [0..1]
Information_Source : InformationSourceType [0..1]
timestamp : dateTime
version : ThreatActorVersionType
Motivation : StatementType [0..*]
Intended_Effect : StatementType [0..*]
«Match»
conceptual threat actor : Threat Actor
identified by : Identifier
«Filter» {type = URIIdentifier}
«Filter» {type = URIIdentifier}
has name : Name
described by : Information Object
«Filter» {type = Summary Description}
categorized by : Category
«Filter» {type = Actor}
«Filter»
relates : Anything
{type = Campaign}
performed by
performs
TTP : Modus Operandi
impacted by
impacts
plan : Plan
metadata about
has metadata
confidence : Confidence
sourced from
«Subset of»
source metadata : Statement
statement date and time : Time Point
version : Simple Identifier
«Filter»
{type = Mission}
obj : Objective
has objective
objective of
stake : Stakeholder
{default}

# Example STIX source data

```
<stix:Incident id="example:incident-fd56fb34-af59-47b3-95cf-7baaaa53fe93" timestamp="2014-08-28T16:42:52.859547+00:00"
xsi:type='incident:IncidentType' version="1.1.1">
        <incident:Title>Breach of Canary Corp</incident:Title>
        <incident:Time>
                <incident:Incident_Discovery precision="second">2013-01-13T00:00:00</incident:Incident_Discovery>
        </incident:Time>
        <incident:Description>Intrusion into enterprise network</incident:Description>
        <incident:Reporter>
                <stixCommon:Description>The person who reported it</stixCommon:Description>
                <stixCommon:Identity id="example:Identity-5db269cf-e603-4df9-ae8c-51ff295abfaa">
                        <stixCommon:Name>Sample Investigations, LLC</stixCommon:Name>
                </stixCommon:Identity>
        <stixCommon:Time>
                <cyboxCommon:Produced_Time>2014-03-11T00:00:00</cyboxCommon:Produced_Time>
        </stixCommon:Time>
        </incident:Reporter>
        <incident:Victim id="example:Identity-c85082f3-bc04-43c8-a000-e0c1d0f2c045">
        <stixCommon:Name>Canary Corp</stixCommon:Name>
    </incident:Victim>
        <incident:Impact_Assessment>
        <incident:Effects>
                <incident:Effect xsi:type="stixVocabs:IncidentEffectVocab-1.0">Financial Loss</incident:Effect>
        </incident:Effects>
    </incident:Impact_Assessment>
        <incident:Confidence timestamp="2014-08-28T16:42:52.859570+00:00">
        <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">High</stixCommon:Value>
    </incident:Confidence>
</stix:Incident>
```

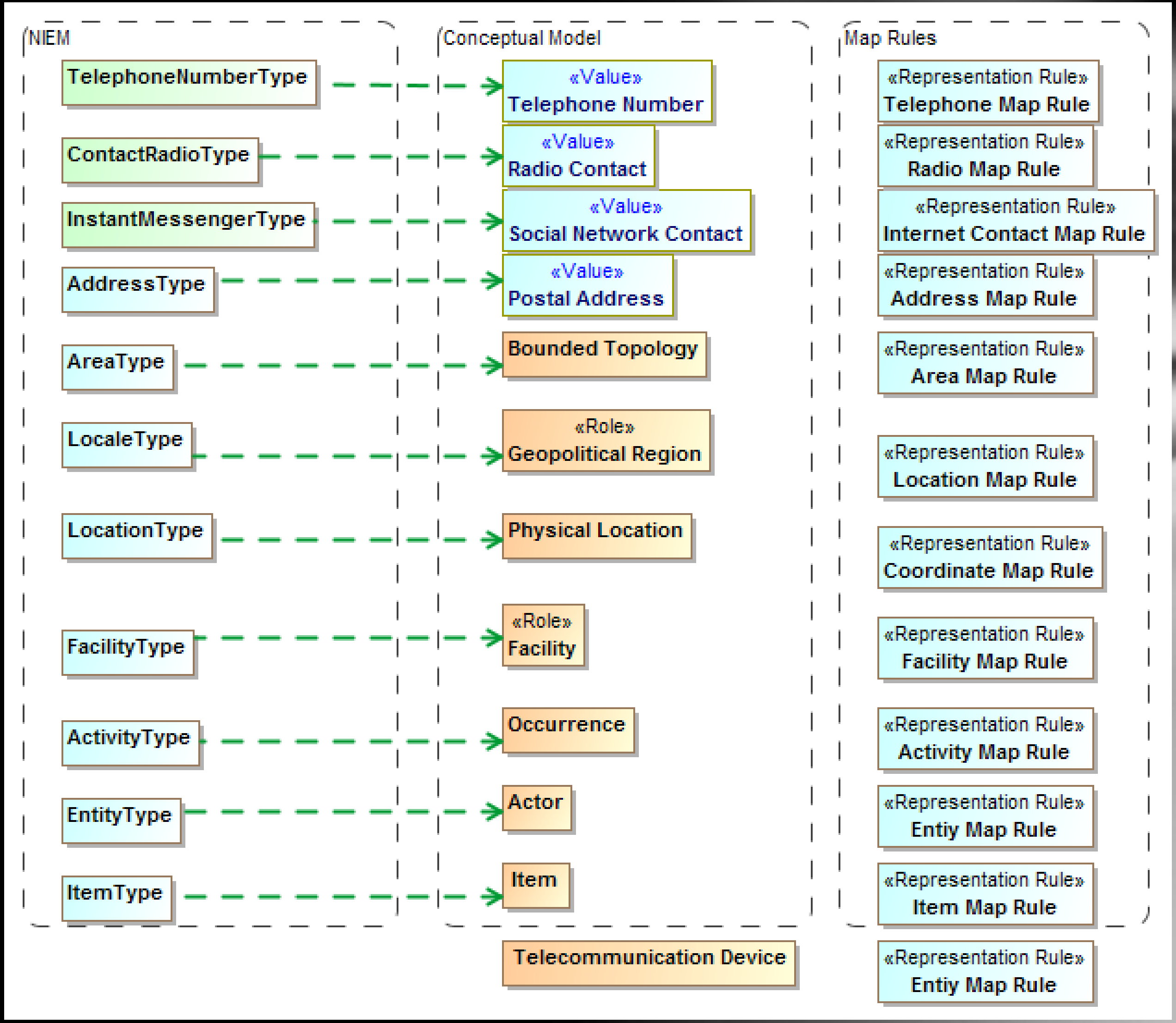
# Example of mapped data graph

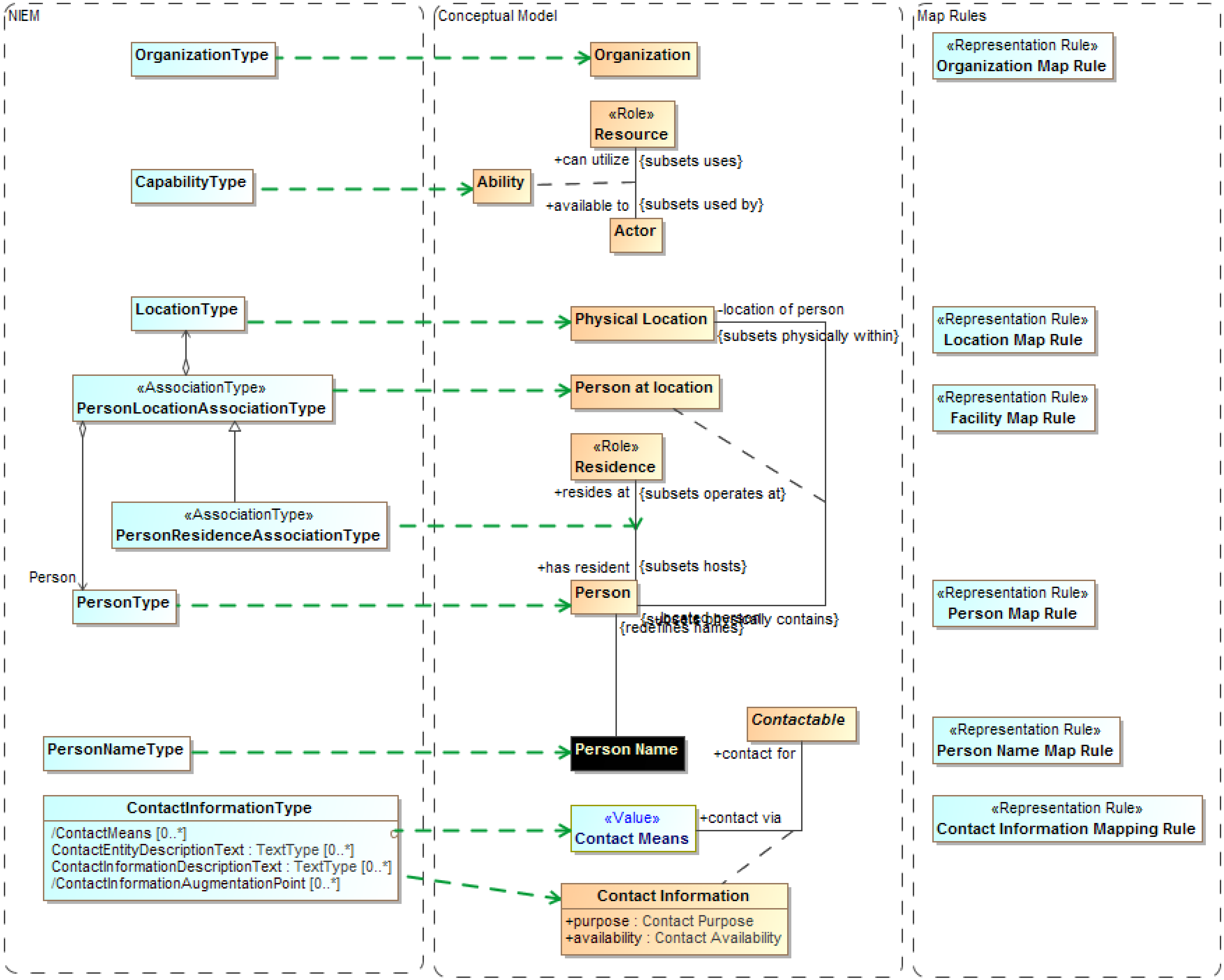


Infomration sources:
TR#1002 from STIX resource [x4.xml] at 2015-01-08 19:19:57.154000

Provenance

# NIEM Mapping summary (1)


NIEM
TelephoneNumberType
ContactRadioType
InstantMessengerType
AddressType
AreaType
LocaleType
LocationType
FacilityType
ActivityType
EntityType
ItemType
Conceptual Model
«Value» Telephone Number
«Value» Radio Contact
«Value» Social Network Contact
«Value» Postal Address
Bounded Topology
«Role» Geopolitical Region
Physical Location
«Role» Facility
Occurrence
Actor
Item
Telecommunication Device
Map Rules
«Representation Rule» Telephone Map Rule
«Representation Rule» Radio Map Rule
«Representation Rule» Internet Contact Map Rule
«Representation Rule» Address Map Rule
«Representation Rule» Area Map Rule
«Representation Rule» Location Map Rule
«Representation Rule» Coordinate Map Rule
«Representation Rule» Facility Map Rule
«Representation Rule» Activity Map Rule
«Representation Rule» Entiy Map Rule
«Representation Rule» Item Map Rule
«Representation Rule» Entiy Map Rule

NIEM
OrganizationType
CapabilityType
LocationType
«AssociationType»
PersonLocationAssociationType
«AssociationType»
PersonResidenceAssociationType
Person
PersonType
PersonNameType
ContactInformationType
/ContactMeans [0..*]
ContactEntityDescriptionText : TextType [0..*]
ContactInformationDescriptionText : TextType [0..*]
/ContactInformationAugmentationPoint [0..*]
Conceptual Model
Organization
«Role»
Resource
+can utilize
{subsets uses}
Ability
+available to
{subsets used by}
Actor
Physical Location
-location of person
{subsets physically within}
Person at location
«Role»
Residence
+resides at
{subsets operates at}
+has resident
{subsets hosts}
Person
{subsets physically contains}
located person
{redefines names}
Contactable
+contact for
Person Name
«Value»
Contact Means
+contact via
Contact Information
+purpose : Contact Purpose
+availability : Contact Availability
Map Rules
«Representation Rule»
Organization Map Rule
«Representation Rule»
Location Map Rule
«Representation Rule»
Facility Map Rule
«Representation Rule»
Person Map Rule
«Representation Rule»
Person Name Map Rule
«Representation Rule»
Contact Information Mapping Rule

# Result of mapping

*Two-way semantic “pivot” through conceptual reference models*

# The Process

*Building a community and standards to protect against threats and risks*

# Open Community Process

Our goal is to create and encourage

- Open standards for threat and risk information sharing
- A community of information providers, consumers, analysts and products

- The standards process is organized under the "Object Management Group" (www.omg.org)
- The community "home" is www.threatrisk.org

While not required by OMG process, the submission team publishes draft specifications to invite comment, engagement, community building and implementation. OMG Membership is encouraged but not required.

Stakeholders may contribute to the specification.

We are also exploring options for open source implementations

# Who Is OMG?

**Object Management Group (OMG):**

- Founded in 1989
- More than 470 member companies
- The largest and longest standing not-for-profit, open-membership consortium which develops and maintains computer industry specifications.
- Continuously evolving to remain current while retaining a position of thought leadership.

# Developing Standards

Standards are developed using OMG's mature, worldwide, open development process. With over 20 years of standards work, OMG's one-organization, one-vote policy ensures that every vendor and end-user, large and small, has an effective voice in the process.

Finance Healthcare Insurance Government

# OMG's Best-Known Successes

### Common Object Request Broker Architecture

- CORBA® remains the only language- and platform-neutral interoperability standard

### Unified Modeling Language

- UML® remains the world's only standardized modeling language

### Business Process Modeling Notation

- BPMN$^{TM}$ provides businesses with the capability of understanding their internal business procedures

### Common Warehouse Metamodel

- CWM$^{TM}$, the integration of the last two data warehousing initiatives

### Meta-Object Facility

- MOF$^{TM}$, the repository standard

### XML Metadata Interchange

- XMI®, the XML-UML standard

# Submitters and Contributors (Thus Far)

Model Driven Solutions division of Data Access Technologies

KDM Analytics, Inc.

International Business Machines, Inc.

RSA, The Security Division of EMC

Lockheed Martin, Inc.

Oracle Corporation

Fujitsu

TEAM THREAT

Information Sharing Environment (ise.gov)

Demandware

U.S. Air force

U.S. Defense Security Services

California Public Safety (http://www.Caloes.ca.gov)

U.S. National Information Sharing Model PMO (https://www.niem.gov/)

Duke Energy

NSA/UCDMO

NIST

INCOSE

Integrated Networking Technologies, Inc.

Tibco Software Inc.

Hitachi

NC4

Others pending approval

# Questions and Invitation

*Join us! Help us: Define the standard, validate it with your use cases, merge with other models,  implement it, fund it*