Threat Modeling and Sharing

Summary

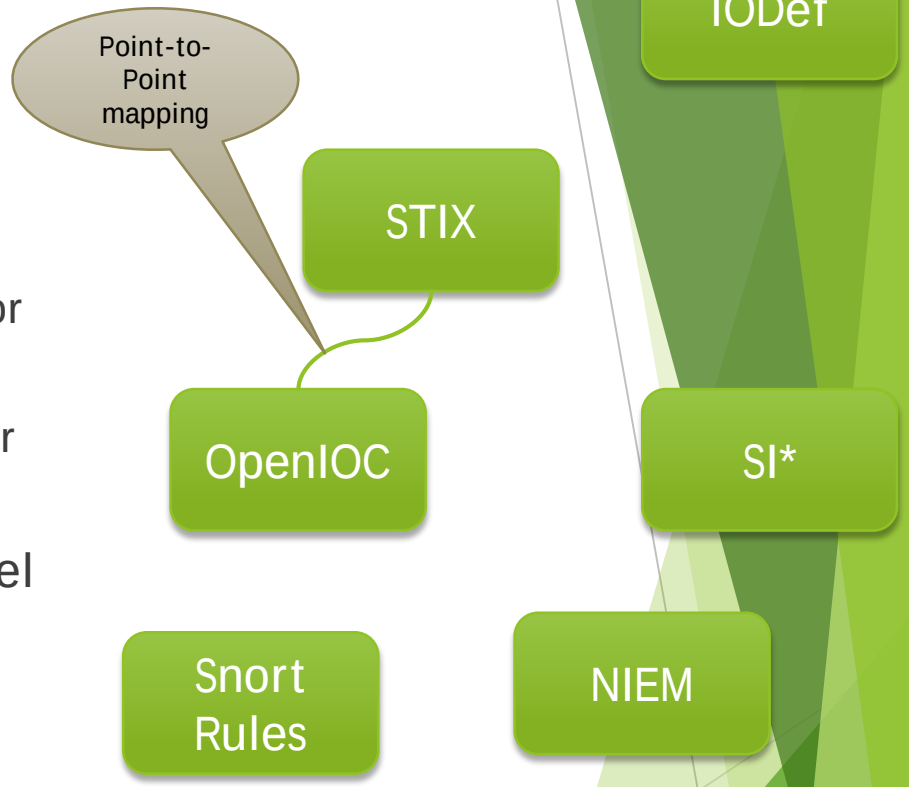
- Proposal to kick off Threat Modeling project
  - Multi-phase approach
  - Initially: create Cyber Domain PIM and STIX PSM with UML Profile for NIEM
  - Expand to other PSM, create Threat Meta Model
  - Expand to non-cyber domains
- Community focused
  - Leverage existing work (STIX, OpenIOC, IODef, SI*, etc.)
  - Connect to stakeholder within OMG and external

Motivation

- Threat information sharing critical enabler for ‘wire-speed’ defense of complex systems
- Information sharing requires shared concepts for subject area
  - NIEM is used by US federal, state, and local government, as well as internationally
  - STIX is being adopted by a large number of users
  - Snort rules are common for IDS
- Multiple protocols, languages, and models used throughout industry today, but:
  - Re-use of existing protocols for threat exchange (e.g. IODef)
  - Focus on threat indicators/signature and classification (e.g. STIX, OpenIOC)
- Desire to have traceability from indicators to threat actors and their motivation/intent
  - Leverage existing work performed by social modeling and behavior groups, e.g. SI*
- Some integration with other enterprise systems, but no comprehensive approach

Motivation – Clarification

- This is NOT to concentrate threat sharing and modeling at OMG
  - No desire to 'take over' from successful approaches such as STIX or OpenIOC
  - Collaboration with non-OMG member will be critical for success
- Focus on development of meta-model and semantic interoperability for
  - broadening view on, and
  - identifying specific areas of improvement
- Leverage strength of MDA to threat sharing



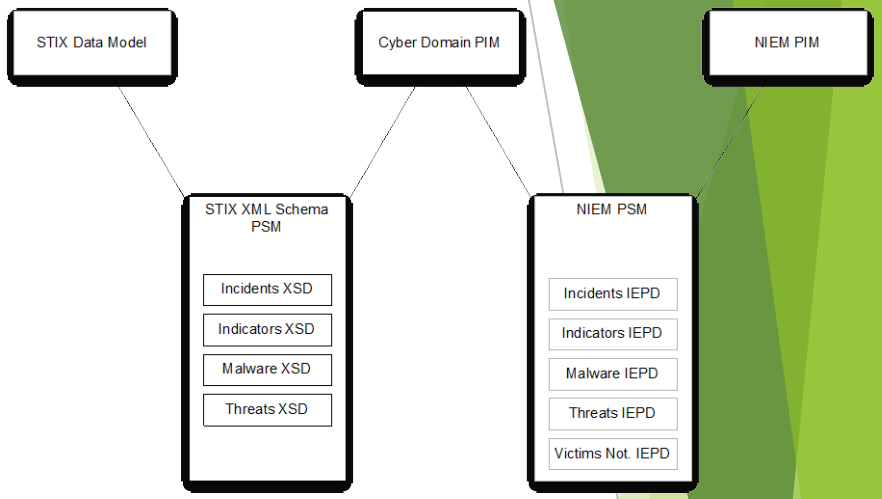
Threat Models Today are – at best – ad hoc coordinated

Approach

- Multi-Phase Approach
  - Start with initial mapping of existing concepts (STIX Data Model <-> NIEM UML Profile
  - Develop meta-model for threat modeling and expand scope
  - Include non-cyber domains
- Include creation of Platform Independent Model (PIM) and Platform Specific Models (PSM) that represent STIX, OpenIOC
- Include social model of threat actors, campaigns, motivation
  - E.g. through leveraging SI* framework concepts
- Integrate with
  - NIEM 3.0
  - Common Alerting Protocol (CAP)
  - Other applicable systems
- Extend beyond cyber threat sharing
  - Non-cyber domain integration
  - Sharing of countermeasure for specific threats

Phase 1

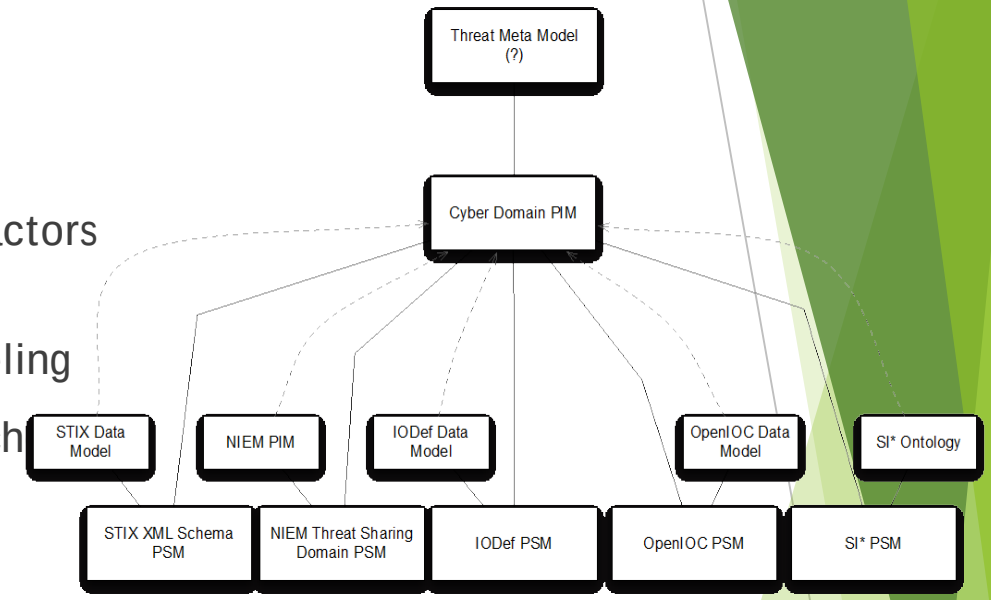
- Create “Cyber Domain PIM” utilizing UML Profile for NIEM to model STIX information exchange
  - NIEM profile exists today
  - STIX has currently richest model and broadest interest base



- Expected output: Specification that includes
  - Cyber Domain PIM
  - STIX PSM
- Rationale: fairly easy to achieve, concretization of a Cyber Domain PIM that can serve as basis for meta-model or semantic models for other platforms

Phase 2

- Richer social and behavioral modeling, e.g.:
  - Leverage of SI* framework concepts of modeling social actors and their behavior
  - Integration with CORAS modeling
  - Inclusion of XORCISM approach



- Expansion of Cyber Domain PIM, adding new PSMs, and/or development of Threat Meta-Model
  - OpenIOC, IODef, XORCISM, SI*, Snort Rules, etc.

Phase 3 (notional)

- Non-cyber domain modeling
  - Integration with existing threat models for law-enforcement, defense, emergency preparedness
  - Develop common threat ontology, based on threat meta-model
  - Provide cross-domain capabilities, e.g. for describing complex campaigns
  - Include domains such as Supply Chain Risk Management (SCRM), Digital Forensics (e.g. SCOX, DFXML), etc.
- Countermeasure modeling
  - Develop consistent model for countermeasures
  - Allow mapping of countermeasures to threat
  - Countermeasure sharing to facilitate automatic mitigation of known threats

Goals

- Enable conceptual interoperability of existing systems
  - Validate existing mappings (e.g. STIX/OpenIOC) and allow mapping of new PSMs (NIEM Threat Sharing PSM, SI*, XORCISM, etc.) to each other
- Enable simplified creation of automated threat sharing systems
  - Tools-supported code generation
  - Semantic interoperability through shared ontology
- Enable automatic threat mitigation
  - Include mitigation recommendations in modeling to enable wire-speed defense
- Improve attribution capabilities by including richer characterization of social domain in actor/campaign classification
  - Full traceability from observed indicators to social and individual motivation and intent

Notional Timeline

Prerequisites

- UML Profile for NIEM
- STIX Data Model

Phase 1

- RFC for Cyber Domain PIM and STIX PSM, based on UML Profile for NIEM and STIX Data Model

Phase 2

- Collaboration with other stakeholders (SI*, XORCISM, etc.)

- Development of expanded PIM and/or meta-model

- Platform specific models for other threat languages/ approaches

Phase 3

- Outreach to non-cyber stakeholders

- Model extensions to incorporate other domains

- Countermeasure modeling