Threat Actor Context Technical Committee Meeting

TAC-TC January 21, 2020
Agenda

• Welcome
  • Introductions

• Quick Review of Purpose & Scope
  • Clarification of the TAC-TC Scope
    • Why are we thinking about Threat Actor Context?
      • The value proposition – (better resiliency decisions & faster incident response)
      • The delivered work product – (a documented knowledge framework)
  • Progressing, Not Regressing (additive)
    • Threat Actor Characteristics
    • Semantic Interoperability

• Path Forward
  • Call for Proposals?

• Ambiguity Recognition & Resolution Discussion
  • STIX 2.1 Grouping
  • Industry Ambiguous Terms Discussion
    • Threat
    • Mitigation
Statement of Purpose

Our purpose is to resolve ambiguity in the context of TA across different sources and solutions, to support organizing what is known, and to share information about Threat Actors and the STIX Domain Objects (SDOs) related to them, such as Intrusion Sets, Campaigns, and Indicators. In this context “Threat Actor” can be, but not necessarily limited to an individual, an organization, a criminal syndicate, a nation-state or other type of adversarial entity.

To resolve ambiguity, we will establish a common knowledge framework that enables semantic interoperability of threat actor contextual information. We believe this may involve enhancements that run across the strategic, operational, and tactical intelligence levels for use by public and private sector entities defending networks and endpoints. The TC will establish one or more Open Repositories under the OASIS rules, and each OASIS Member and non-Member will be eligible to contribute only after signing either an Entity Contributor License Agreement (CLA) or an Individual CLA per OASIS rules at https://www.oasis-open.org/resources/open-repositories/faq.
The purpose of this TC is to create a knowledge framework that enables semantic interoperability of threat actor contextual information. In other words, the purpose of the TAC TC is to help the community have coherent conversations in the STIX language. (This does not exclude the possibility of TAC been used standalone or integrated also into other CTI standards or solutions)

The scope of this TC’s efforts will include:

- Hosting one or multiple OASIS Open Repositories of Threat Actor information in STIX 2.x format. The intent is to facilitate schema alignment.
  - Facilitating disparate contributors to submit contributions of Threat Actor information that is aligned with the repository schema is within the scope of this TC.
  - Mechanisms to allow for data marking and other associated metadata to describe the source of the contribution are considered within scope.
- Validation, confirmation, curation, or quality control of the contributors’ assertions into the repository is not within the scope of this TC.
- Defining and documenting concepts that provide best practices and guidelines to remove ambiguity from STIX documents produced by different authors (e.g. Intrusion Set naming conventions)
- Identify appropriate extensions that are needed to operationalize STIX 2.x threat information including but not limited to:
  - Strategic Context
  - Operational Context
  - Tactical Context
  - Motivational Context
- Providing algorithms to align schema is an aspirational activity of this TC.

The base data model for the TAC data store would stem from the STIX 2.x Threat Actor SDO, the Campaign SDO, the Intrusion Set SDO and the Indicator SDO (including patterning) at a minimum. This will provide a uniform interface for integration of schema and content from multiple credible sources.
The Scope: Resolve ambiguity via creation of a standard for expressing Threat Actor Context that facilitates semantic interoperability and enables human and AI analysis.

- Solution providers and government agencies are expressing Threat Actor Context today.
  - A de facto standard is not readily apparent. There is no consensus among solution providers.
- There are multiple good frameworks available from OASIS, NIST, DHS, NSA, ODNI, and others.
  - Making these disparate frameworks semantically interoperable is of high value.
- Transition to practice by validating via Open Repositories.
  - Validation of the contributors’ assertions into the repositories is NOT within scope.
For Example:

NIST SP 800-30 Appendix D

- There are many different types of Threat Sources.
- So many characteristics that are applicable to a Threat Actor.

<table>
<thead>
<tr>
<th>Type of Threat Source</th>
<th>Description</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADVERSARIAL</td>
<td>Individuals, groups, organizations, or states that seek to exploit the organization’s dependence on cyber resources (i.e., Information in electronic form, Information and communications technologies, and the communications and information-handling capabilities provided by those technologies).</td>
<td>Capability, Intent, Targeting</td>
</tr>
<tr>
<td>ACCIDENTAL</td>
<td>Errors or errors due to incorrect use.</td>
<td>Range of effects</td>
</tr>
<tr>
<td>STRUCTURAL</td>
<td>Failure or errors for equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.</td>
<td>Range of effects</td>
</tr>
<tr>
<td>ENVIRONMENTAL</td>
<td>Natural or man-made disaster which the organization depends on which the organization depends, but which are outside the control of the organization. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).</td>
<td>Range of effects</td>
</tr>
</tbody>
</table>

- User
- Privileged User/Administrator

- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
  - Environmental Controls
    - Temperature/Humidity Controls
    - Power Supply
  - Software
    - Operating System
    - Networking
    - General-Purpose Application
    - Mission-Specific Application

- Fire
- Flood/Tsunami
- Windstorm/Tornado
- Hurricane
- Earthquake
- Bombing
- Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
- Telecommunications
- Electrical Power
Progressing, not Regressing

• We should be adding to current STIX representation choices, not removing or limiting representation choices.

• When we as humans analyze the status of things, we make our analytic assumptions on the context of the situation. We as humans can interpret word values of an open vocabulary and add the knowledge that we have. Unfortunately, computers need more than values from an open vocabulary to be able to “make sense” of the situation.

• The few open vocabularies associated with Threat Actor, Intrusion Set, Identity, and Grouping do not provide comprehensive machine readable or semantic interoperable context to allow an AI to reason.

• Hence, we need to extend our ability to express enough information in machine interpretable form. We need to be able to model the context of a Threat Actor, in addition to tagging the Threat Actor object with the proper open vocabulary.
Why Threat Actor Context?

• “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

— Sun Tzu, The Art of War
Threat Actor Context – Know Thy Enemy

Graph Modeling organizes what is known about the adversaries and cyber threats from sources such as threat intelligence and incident response.

Analytic Pivoting and other cyber “analytic tradecraft” used for sense-making, decision-making, and executing courses of action is facilitated by representing the Threat Actor Context as semantic interoperable graph models.
Questions about Threat Actors

- What Threat Actors should my enterprise be concerned about?
- What *motivates* them?
- What Strategic, Operational, Tactical, and Technical knowledge do we have about the Threat Actor?
- Are there *current world events* that influence the Threat Actor?
- Are they state sponsored, if so, what is the relationship between the Threat Actor and the Nation State?
- What is their level of sophistication?
- Who are their affiliates?
- Are there common characteristics of who they target?
- What industry or organizations do they commonly target?
- What is their infrastructure like?
- Do they have a command hierarchy?
- How many individuals make up this Threat Actor?
STIX 2.1 SDOs Capture Some Threat Actor Context

- Threat Actor
- Intrusion Set
- Campaigns
- Grouping
- Identity
- others
Ambiguity

• Although the STIX specification explicitly states that a Threat Actor is not an Intrusion Set, in practice, the Intrusion Set is often used to describe “properties orchestrated by a single threat actor”.

• Since there are multiple SDOs that capture partial information it introduces ambiguity.
STIX 2.1 Threat Actor Definition

- Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent. A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time.

- Threat Actors leverage their resources, and possibly the resources of an Intrusion Set, to conduct attacks and run Campaigns against targets.

- Threat Actors can be characterized by their motives, capabilities, goals, sophistication level, past activities, resources they have access to, and their role in the organization.
STIX 2.1 Intrusion Set Definition

- An Intrusion Set is a grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization. An Intrusion Set may capture multiple Campaigns or other activities that are all tied together by shared attributes indicating a commonly known or unknown Threat Actor. New activity can be attributed to an Intrusion Set even if the Threat Actors behind the attack are not known. Threat Actors can move from supporting one Intrusion Set to supporting another, or they may support multiple Intrusion Sets.

- Where a Campaign is a set of attacks over a period of time against a specific set of targets to achieve some objective, an Intrusion Set is the entire attack package and may be used over a very long period of time in multiple Campaigns to achieve potentially multiple purposes.

- While sometimes an Intrusion Set is not active, or changes focus, it is usually difficult to know if it has truly disappeared or ended. Analysts may have varying level of fidelity on attributing an Intrusion Set back to Threat Actors and may be able to only attribute it back to a nation state or perhaps back to an organization within that nation state.
STIX 2.1 Identity Definition

- Identities can represent actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, systems or groups (e.g., the finance sector).

- The Identity SDO can capture basic identifying information, contact information, and the sectors that the Identity belongs to. Identity is used in STIX to represent, among other things, targets of attacks, information sources, object creators, and threat actor identities.

<table>
<thead>
<tr>
<th>description (optional)</th>
<th>string</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A description that provides more details and context about the identity, potentially including its purpose and its key characteristics.</td>
</tr>
</tbody>
</table>
STIX 2.1 Grouping Definition

A Grouping object explicitly asserts that the referenced STIX Objects have a shared context, unlike a STIX Bundle (which explicitly conveys no context). A Grouping object should not be confused with an intelligence product, which should be conveyed via a STIX Report.

A STIX Grouping object might represent a set of data that, in time, given sufficient analysis, would mature to convey an incident or threat report as a STIX Report object. For example, a Grouping could be used to characterize an ongoing investigation into a security event or incident. A Grouping object could also be used to assert that the referenced STIX Objects are related to an ongoing analysis process, such as when a threat analyst is collaborating with others in their trust community to examine a series of Campaigns and Indicators. The Grouping SDO contains a list of references to SDOs, SCOs, and SROs, along with an explicit statement of the context shared by the content, a textual description, and the name of the grouping.
Open Vocabularies are a start...

- threat-actor-role-ov
  - agent
  - director
  - independent
  - infrastructure-architect
  - infrastructure-operator
  - malware-author
  - sponsor
**Grouping SDO for Threat Actor Context?**

A Grouping object can be used to hold a graph of all facts we know about an adversary’s Tools, Campaigns, Location, Infrastructure, etc.

Object Oriented Programming and ontology languages have the construct of subclassing. Would this be appropriate for some SDOs?
Missing Context Concepts?

• Behavior timelines of Threat Actor
  • Frequency of interactions
  • Time of most interactions
  • Order of execution of TTPs

• Cultural characteristics

• Relevant World Events (geopolitics)

• Typical Targets
  • Industry
  • Country
  • Political

• Social Media Interactions
  • Recruiting/Grooming
  • Geopolitical information
  • Social Networks

• Financial Information

• Technical Networks and Affiliations

All the above should be able to be described at a level of precision and be able to answer high-level questions such as, how a threat actor has evolved over time, their operations, and changes to their behavior with regards to strategic goals.
Call for Proposals?

• We have a stated Purpose
• We have a stated Scope
• We need a development plan

• Strategic, Operational, Tactical, Technical focused subcommittees?