1. Name of the TC

Threat Actor Context (TAC) Technical Committee
2. Statement of Purpose

The TAC TC aims to resolve ambiguity and enable interoperability across different threat-intelligence-relevant information sources and technological solutions to support organizing what is known about threat actors and their activities

The work of the TAC TC is also aligned with the scope of the CTI TC to create information representations and protocols that address the need to model, analyze, and share cyber threat intelligence in cyber-relevant time. The TAC focuses on the expansion of the representations of the adversaries.

To resolve ambiguity TAC will establish a common knowledge framework that enables semantic interoperability of threat actor contextual information and will involve representation enhancements that run across the strategic, operational, and tactical intelligence levels for use by public and private sector entities defending networks and endpoints. TAC will establish one or more Open Repositories under the OASIS rules. <https://www.oasis-open.org/resources/open-repositories/faq>.

Business Benefits

Organizations that currently share Cyber Threat Intelligence (CTI) are confronted with multiple schemas and share through multiple tools. This limits an organization's ability to strategically correlate and analyze attack data, which could lead to a better understanding of their adversary's goals, capabilities, and trends in targeting and techniques.

TAC TC seeks to provide semantic extensions for the STIX 2.x data model thereby allowing for semantic graph representation for the CTI community.

Semantic interoperability is the ability of computer systems to exchange data unambiguously. This enables machine computable logic, inferencing, knowledge discovery, and data federation between information systems.

We are defining terms about Threat Actors to provide semantic interoperability between the variety of systems contributing threat intelligence. This is a significant benefit to existing open sources such as MITRE’s ATT&CK and MISP Galaxy by strengthening their abilities to corroborate and cross-reference with other repositories.

The deliverables of this TC will be a benefit to the users of threat intelligence provided by sources which use different standards or knowledge representations. This enhances the usability of STIX by providing a bridge to other representations. Contributors, including both open source and proprietary, would be able to share the content descriptions and assertions regarding specific Threat Actors, Campaigns and Intrusion Sets and other SDOs. Users would gain access to a high-quality, harmonized data set that enables organizations to conduct a "competitive analysis" of their adversaries in order to react more quickly to and possibly anticipate changes in the adversary activities. This would benefit decision-making for risk management as well as resource allocation.

The TAC Open Repository TC would allow for both OASIS Members and non-Members to contribute subject to the CLA terms and conditions.
3. Scope of Work
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 and other emerging representations.

The scope of this TC’s efforts will include:
	* 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 need 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.
	* 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 metadata to describe the source of the contribution are considered within scope (e.g., data markings, etc).
	* Validation, confirmation, curation, or quality control of the contributors’ assertions into the repository is not within the scope of this TC.
4. 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.
5. Deliverables

	* Ontology Specification Repository
		+ Formal Ontology Implementation
			- OWL Representation of the STIX 2.x Specification
				1. STIX Semantic Expression Ontology Documentary
			- OWL Representation of the TAC Ontology
		+ Specification Documentation
			- TAC Ontology Specification Document
			- STIX Semantic Expression Ontology Document
	* Additional types, vocabularies, taxonomies, and ontologies that extend the STIX 2.x standard, such as, but not limited to:
		+ Threat Actor subtypes
		+ Industry Sectors
		+ Motivation & Motive
		+ Temporality

The above will have corresponding Committee Notes as per the following graphic.

* + Committee Note on Open Repository User Manuals
		- As Contributors
		- As Consumers



Other working and living documents will be generated by the TC to facilitate the creation of the Specification and Committee Notes.

1. IPR Mode
This TC will operate under the [Non-Assertion IPR mode](https://www.oasis-open.org/policies-guidelines/ipr#Non-Assertion-Mode) as defined in Section 10.3 of the [OASIS IPR Policy document](https://www.oasis-open.org/policies-guidelines/ipr).
2. Audience
The OASIS Members of the TAC TC seek to:
	* shape the dialogue on the context of adversaries
	* advance the representation used for the context
	* contribute to the Open Repositories

1. The Contributors and Consumers of the TAC Open Repository will be:
	* government agencies protecting their information assets
	* Not-for-Profit and Non-Governmental Organizations (NGOs) protecting their information assets
	* companies protecting their information assets
	* academic institutions and think tanks conducting research on threat actors, campaigns and intrusion sets
	* students conducting research on patterns of behavior of threat actors
2. Language

The primary language of the TAC TC will be English.