Space Automated Threat Intelligence Sharing (SATIS) Technical Committee

This is the final charter. It has been submitted to and accepted by OASIS Open on August 22, 2024.

The comment period for this document has closed. If you wish to still provide feedback to project leaders, you may do so. Anyone may post comments directly on this document or by emailing comments to OASIS-charter-discuss@ConnectedCommunity.org

If you'd like to participate in this TC please contact join@oasis-open.org.

Details on TC membership are here.

Section 1: TC Charter

1.a. TC Name

Space Automated Threat Intelligence Sharing (SATIS)

1.b. Statement of Purpose

This charter establishes the north star for space CTI to evolve from the collection and analysis of information towards the contextualization and operationalization of space sector threat information at both the organizational and communal levels.

This means the evolution related to how we approach the unique threats to satellites, ground stations, and other space infrastructure, including the adversary's tactics, techniques, and procedures (TTPs), with a better view into their goals and adversarial objectives. The intended outcome is for space organizations to have an enhanced tool that can be used to better predict, prevent, and respond to cyber threats specific to space.

1.c. Business Benefits

1. Information Sharing

- Sharing information within the space community
- Modeling peer-to-peer, hub and spoke, and source subscriber approaches to avoid a “one approach fits all” mentality

2. Architectural Flexibility

- Space technology agnostic approach that supports the encapsulation of threats regardless of vendor technology
- Create the ability to “infer” architecture as part of the threat contextualization

3. Standardized Representations

- Establish or extend existing formats for key components of space cyber threat intelligence:
    - Campaigns
    - Threat actors
    - Incidents
    - Tactics, techniques, and procedures (TTPs)
    - Indicators
    - Exploit targets
    - Observables
    - Courses of action

4. Support for Space, Network, and Security Operators

- Determine how to map all threats facing space operators to existing frameworks such as MITRE ATT&CK, Space Attacks Research and Threat Analysis (SPARTA), and STIX.
    - Correlate essential elements of information (EEIs) to STIX Domain Objects (SDOs)
    - Data ingest requirements
    - Taxonomy for space-specific infrastructure and technology

1.d. Scope

Traditional Cybersecurity Threat Intelligence (CTI) continues to bring tremendous value to the global cyber defense community. The convergence of cyber enabled technology with space platforms indicates the need to evolve a space specific CTI extension as part of the STIX standard. In addition, the international space community needs to start working towards a CTI approach for machine-to-machine sharing of signals-based attacks as part of the journey to manage organizational as well as communal threat reduction. The work done in

this technical committee will enhance the bi-directional sharing of threat-related information via machine-to-machine transport methods, including TAXII.

Contextualizing space sector specific threats with existing CTI standards will also require the articulation of ground segment, user segment, link segment, launch segment and space segment operational concepts within an actionable data model. This segment level articulation of threat context will greatly assist the mission of space focused watch centers aligned in some form of ISAC community relationship. To facilitate the associated activities, Space ISAC will ensure that each segment has industry representation.

Exchanging critical cyber threat information among international space community trusted partners is critical. We need a holistic understanding of threats to defend against them in an effective manner. This is why a focus on information sharing will be a big part of the CTI for Space extension. This group will work to identify the proper transport methods for threat intelligence that align with the needs and capabilities of space operators.

Depending on the type of environment, space operators may not be aware of all existing threats to their infrastructure. There is a noted difference in detection capabilities and data frameworks between Network Operations Centers (NOC), Security Operations Centers (SOC) and Space Operation Centers (SOC). Using a standardized framework, operators can ingest information more efficiently and expedite courses of action to secure their entire attack surface.

As cyber threats continue to converge the various attack vectors for space, it is more crucial to identify coordinating events and external factors for the space industry. These factors can include but are not limited to electronic warfare (EW), geopolitical conflicts, space domain awareness (SDA), space weather forecasts, and satellite movements. A standardized framework for information sharing helps to capture these disparate elements.

1.e. Deliverables

The main deliverable of this TC will be a STIX framework for space-specific cyber threat intelligence, which will include an extension of the existing STIX framework to include indicators related to non-cyber attacks on space systems, specifically radio frequency interference.

The work being done in this technical committee will directly support information sharing and analysis initiatives for the Space ISAC Watch Center in the following ways:

1. Machine to Machine (M2M) Sharing with Industry Members and Government Partners:

    a. Space ISAC operates a threat intelligence platform (TIP) intended for automated sharing of indicators of compromise (IOCs) and other threat information to member and partner distributions. The platform assists analysts

in data collection/analysis and disseminates information to subscribers via a series of STIX-formatted collections.

2. Cross Cell/Segment Correlation

    a. The Space ISAC Watch Center is made up of five Cells: Coordination, All-Source, Terrestrial, Signals, and Space. Each cell has their own designated activities, and the latter four correspond to segments of the space attack surface. Watch Center analysts correlate information across cells to determine impacts present in multiple segments.

3. Tracking Adversary Activity Throughout All Space Segments

    a. Finished deliverables of the Watch Center assess threat indicators from all segments of the space attack surface and seek to correlate these indicators across segments, whenever appropriate.

4. Support for Space Operators

    a. The Space ISAC community is comprised of a variety of different operating environments to include security operations center and space operation centers (SOC) and network operations centers (NOC). Analysts from Space ISAC member companies may ingest different data types, ranging from cyber threat intelligence (CTI), radio frequency (RF) signatures, satellite telemetry, space weather forecasts, and more. Expanding the STIX framework for these additional data types will directly support the automated sharing of actionable information to all operators in the space environment.

5. Determine how to map all threats facing space operators to existing frameworks such as MITRE ATT&CK, Space Attacks Research and Threat Analysis (SPARTA), and STIX.

- Correlate essential elements of information (EEIs) to STIX Domain Objects (SDOs)
- Data ingest requirements
- Taxonomy for space-specific infrastructure and technology (e.g., infrastructure-type-ov expansion)
- Physical-observable objects and properties with examples

1.f. IPR Mode

Non-Assertion

1.g. Audience

Space industry producers; Space industry communities of interest, Space industry regulators, Space Operators and Industry representatives to include:

- Space Operations Centers

- Network Operations Centers
- Security Operations Centers

1.h. Language

English

1.i.(Optional References for Section 1)

The Space ISAC operates a Watch Center to monitor and report all threats and all hazards information to the global space community. The Watch Center seeks to analyze, validate, and fuse information from disparate sources to track adversary activity through ground and space. It does so through the ingestion and correlation of data from publicly available information, information shared by government partners, and member submissions. The Watch Center correlates information using a set of industry-adopted frameworks, notably MITRE ATT&CK, Space Attack Research & Tactic Analysis (SPARTA) and STIX.

Section 2: Additional Information

2.a. Identification of Similar Work

OASIS Cyber Threat Intelligence TC

2.b. First TC Meeting

TBD - likely end of September

2.c. Ongoing Meeting Schedule

Bi-weekly to start. TC members will determine long-term cadence once the project is launched.

2.d. TC Proposers

- Erin Miller, erin@spaceisac.org, Space Information Sharing and Analysis Center (Space ISAC)
- Joel Francis, joel@spaceisac.org, Space Information Sharing and Analysis Center (Space ISAC)
- Hector Falcon, hector@spaceisac.org, Space Information Sharing and Analysis Center (Space ISAC)
- Timothy O'Neill, toneill@mitre.org, MITRE Corporation

- Theresa Suloway, tsuloway@mitre.org, MITRE Corporation
- Dan Wachtler, dan@darklight.ai, DarkLight, Inc.
- Paul Patrick, ppatrick@darklight.ai, DarkLight, Inc.
- Utkarsh Garg, utkarsh@cyware.com, Cyware Labs Inc
- Terrence Driscoll, terrence.driscoll@cyware.com , Cyware Labs Inc
- Laurie Tyzenhaus, latyzenhaus@cert.org, CERT
- Stefan Hagen, stefan@hagen.link, Individual
- Steve Relitz, Stephan.Relitz@peraton.com, Peraton

2.e. Primary Representatives' Support

I, Erin Miller, as OASIS primary representative for the Space ISAC, confirm our support for the SATIS TC and our participants listed above.

I, Doraiswamy (Raj) Rajagopal, as OASIS primary representative for MITRE Corporation., confirm our support for the SATIS TC and our participants listed above.

I, Paul Patrick, as OASIS primary representative for DarkLight, Inc., confirm our support for the SATIS TC and our participants listed above.

I, Sandi Noonan, as OASIS primary representative for Carnegie Mellon University, confirm our support for the SATISe TC and our CERT participants listed above.

I, Rikki Watlington, as OASIS primary representative for Peraton confirm our support for the SATIS TC and our participants listed above.

2.f. TC Convener

Erin Miller, erin@spaceisac.org, Space Information Sharing and Analysis Center (Space ISAC)

For more information, please see:

- TC Process