RSA 2026 Submission Guidelines

--DRAFT CTI/SATIS/DAD-CDM Proposal --

Session Title

Expanding STIX: AI-Enhanced Threat Intelligence for Space and Deception Defense

(Limit 75 characters, *including spaces*.)
Your session title should clearly indicate the topic of your presentation. Your title should pique the interest of the Program Committee and, subsequently, your audience.

Session Details

Limited to 2500 characters. Submitted:

This panel addresses the critical gap in cyber threat intelligence: sharing machine-readable threat data beyond traditional IT networks. Cyber threats now target space systems and information environments at an unprecedented scale. Japan's space agency suffered multiple cyberattacks in 2024, while researchers identified 124 space sector attacks related to Ukraine's war. Deepfake attacks surged 1,400% in 2025, costing businesses $500,000 per incident. Traditional STIX objects cannot model these emerging threat vectors.

****Main Points:** Our panel demonstrates STIX extensions from two active OASIS standardization efforts. We show how space-domain objects model satellite command hijacking, RF interference patterns, and orbital threats. We present Channel, Media Outlet, and Narrative objects that track AI-generated disinformation campaigns across platforms, plus integration challenges and solutions.**

****What Makes This Different:** This is the first public demonstration of production-ready STIX extensions for space and deception domains. Unlike other CTI sessions focusing on traditional network threats, we address threats that didn't exist five years ago but now threaten critical infrastructure daily. Our panelists work directly with these standards, showing actual JSON objects, relationship mappings, and detection patterns.**

Live Demonstrations: Three scenarios. First, modeling satellite constellation attacks using SATIS objects showing threat actor attribution, affected orbital assets, and cascading ground impacts. Second, tracking deepfake campaigns using DAD-CDM objects connecting AI-generated content across social platforms to attribution networks. Third, cross-domain correlation reveals how space communication disruptions facilitate disinformation campaigns.

Case Studies: The Viasat incident provides our space threat baseline—Russian actors compromised ground infrastructure disabling satellite modems across Ukraine and surrounding countries. Our SATIS objects can model this attack pattern for automated detection. For FIMI threats, we examine the 2024 KnowBe4 incident where North Korean actors used AI-enhanced photos to pass remote job interviews.

Takeaways: STIX schema files for space and deception domains compatible with existing TIP systems; implementation guides for OpenCTI, MISP, and commercial TIP systems; detection rule templates for identifying space-targeted malware and AI-generated content.

This panel addresses the most pressing gap in cyber threat intelligence: how to share machine-readable threat data for domains beyond traditional IT networks. Cyber threats now target space systems and information environments at unprecedented scale. Japan's space agency suffered a series of cyberattacks throughout 2024, while researchers identified 124 cyberattacks against the space sector related to the war in Ukraine. Deepfake attacks surged 1,400% in 2025, costing businesses $500,000 on average per incident. Traditional STIX objects cannot model these new threat vectors.

Main Points We Will Cover: Our panel will demonstrate STIX extensions from two active OASIS standardization efforts. We will show how new space-domain objects model satellite command hijacking, RF interference patterns, and orbital threats. We will present Channel, Media Outlet, and Narrative objects that track AI-generated disinformation campaigns across platforms. We will demonstrate integration challenges and solutions for these new domains.

What Makes This Session Different: This is the first public demonstration of production-ready STIX extensions for space and deception domains. Other CTI sessions focus on traditional network threats. We address threats that did not exist five years ago but now threaten critical infrastructure daily. Our panelists work with these standards. They will show actual JSON objects, relationship mappings, and detection patterns that work in real environments today.

Live Demonstrations: We will demo three specific scenarios. First, modeling a satellite constellation attack using SATIS objects to show threat actor attribution, affected orbital assets, and cascading ground impacts. Second, tracking a deepfake campaign using DAD-CDM objects to connect AI-generated content across social platforms to attribution networks. Third, cross-domain correlation showing how space communication disruption enables disinformation campaigns to spread without fact-checking infrastructure.

Current Case Studies: The Viasat incident provides our space threat baseline. Russian actors compromised ground infrastructure to disable satellite modems across Ukraine and surrounding countries. Our SATIS objects can model this attack pattern for automated detection. For FIMI threats, we will examine the 2024 KnowBe4 incident where North Korean actors used AI-enhanced photos to pass remote job interviews for sensitive positions. DAD-CDM objects can track these identity manipulation techniques.

Actionable Takeaways: Attendees will receive three practical deliverables. First, STIX schema files for both space and deception domains that work with existing TIP platforms. Second, implementation guides showing integration steps for OpenCTI, MISP, and commercial threat intelligence platforms. Third, detection rule templates that security teams can deploy immediately to identify space-targeted malware and AI-generated content in their environments.

Panel Expertise: Our panel will include technical contributors from the SATIS and DAD-CDM OASIS committees, along with practitioners who have implemented STIX extensions in operational environments. The moderator will have extensive experience in CTI standardization and OASIS technical committee work.

Why This Matters Now: China conducted 68 space launches in 2024, setting a new annual record. Russian GPS jamming affects Norwegian aviation practically every day, with GPS interference reported 44 days in just the first two months of 2024. Iran deployed AI-generated content and fake online personas to target US voters during the 2024 election. Traditional cybersecurity frameworks cannot address these threats. STIX extensions provide the common language that defense communities need to share threat data at machine speed and scale.

This session will:

Attendees will:
Master domain-specific STIX extensions for space and information warfare

Understand AI-enhanced threat intelligence sharing frameworks

Learn to model space and narrative-based threats using extended STIX objects

Discover integration paths for existing STIX platforms

Help shape future cyber, space, and information warfare defense

(Limit 2,500 characters, *including spaces*.)
Describe your session here. This is the most important part of your submission for Program Committee review—please be thorough and specific to increase your chance of acceptance by differentiating your submission from others. (Note: bullets not supported)

Some ideas for what to include:

- What are the main points you plan to cover?
- What is new/different/profound about what you'll be covering?
- Will you be demoing something—what and why?
- Do you have some current examples/case studies that help illustrate the points you'll be making? What are they and how do they fit it?
- What actionable takeaways will attendees have? Our Program Committee wants to understand the impact your session will have and tangible actions attendees of your session will be motivated to take.

Specifics are key in this part of your submission—this should not read like a marketing brochure—the voice and expertise of the presenter is extremely important here.

This part of your submission will not be published anywhere—this is all about helping the Program Committee understand the depth of your submission and your unique expertise to deliver.

Key Takeaways

Master STIX extensions for space cybersecurity and AI-powered deception threats

Understand Channel, Narrative, and space-specific objects for threat modeling

Address adaptation challenges in non-traditional threat domains requiring real-time AI correlation

Shape STIX development across cyber, space, and information warfare domains

Session Classification
--**Level:** Advanced (STIX practitioners, CTI architects, domain integration professionals)
--**Format:** Technical Presentation

Target Audience
--STIX implementers and integration engineers
--Cyber threat intelligence analysts addressing space or misinformation threats
--Standards technologists extending CTI models
--Security architects exploring intelligence interoperability

Abstract
STIX development accelerates with OASIS SATIS for space threat intelligence and DAD-CDM for AI-powered deception campaigns. This session demonstrates object innovations, cross-domain correlations, and real-world implementation of STIX extensions addressing satellite vulnerabilities and synthetic media threats.

(Limit 400 characters, *including spaces*.)

In a few sentences, explain what your session will cover (Note: bullets not supported). This abstract will be included in our marketing materials, website, and Mobile Experience. *NOTE: How long is 400 characters? This paragraph is 264 characters, including spaces.*

Session Format—Please choose one of the following:

- Individual Speaker—One speaker only.
- Co-Speakers—This format has two speakers.

- Panel Discussion—This is a session with a Moderator (Panel Leader) and up to three Panelists. The Moderator is responsible for facilitating the panel discussion and is the main contact for the RSAC™ Conference Speaker Manager. Panel participants should represent diverse points of view and background.

Will this presentation be seen elsewhere within 45 days before or after Conference?

- Yes
- No

Submitter's Comments

To be inserted by submitter

This session addresses RSA 2026's most critical new threat vectors: space domain security and AI-enhanced information warfare. Both SATIS and DAD-CDM represent active OASIS standardization efforts with immediate practical impact for threat intelligence programs.

(Limit 400 characters, *including spaces*.)

Is there anything else you want to tell the Program Committee? Please include that detail using the field below.

Session Profiling Information

The following information will help ensure that the attendees clearly understand if they have the appropriate experience to get the most benefit from your session.

Session Classification—Please choose one of the following:

- **Advanced**—Focused on advanced principles and concepts, geared toward attendees with deep subject knowledge and 15 or more years of experience. Little/no time is spent on defining terms and background. These sessions should contain demonstrations, line code, advanced architecture discussions, tools that can be shared, or similar level of content.
- **Intermediate**—Focused on principles and concepts that would appeal to attendees with more than 5 years of experience. Little, if any, time is spent on definitional terms and concepts. Contains instructive demos, management tools, deep process discussions, or similar level of content.
- **General**—This classification is used for compelling strategic sessions and introductions to new technology.

Should your session be designated as a "Technical" session?

- Yes
- No

Potential Speakers:

Moderator and Panelists (info needed for each):

Session Role: Moderator or Panelist

First Name

Middle Initial (optional)

Last Name

Company/Organization

Job Title

Address, City, State/Province, Country, Postal Code

Primary email address (must be unique)

Primary Telephone

Mobile Telephone

Biography (less than 800 characters (not words), including spaces) (bullets are not supported)

Optional Videos if you haven't spoken at RSAC in the past. A great way for speakers who are new to Conference to illustrate their speaking skills, command of English, as well as give an indication of their expertise.