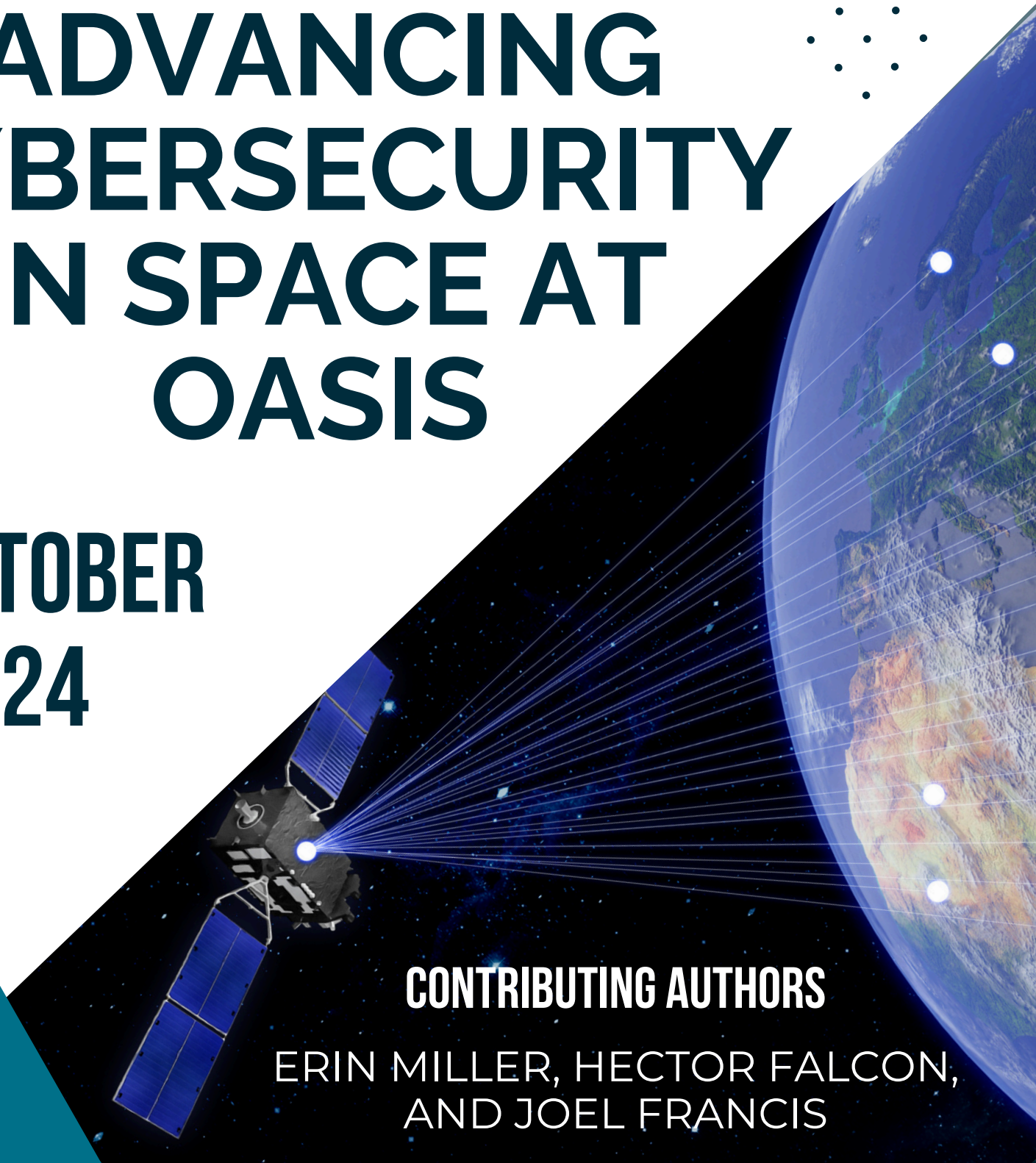
Space ISAC & OASIS

ADVANCING CYBERSECURITY IN SPACE AT OASIS

OCTOBER 2024



CONTRIBUTING AUTHORS

ERIN MILLER, HECTOR FALCON, AND JOEL FRANCIS

Blog Post: Advancing Cybersecurity in Space at OASIS
Publish Date: Wednesday, 02 October
Authors: Erin Miller, Hector Falcon, and Joel Francis

Advancing Cybersecurity in Space at OASIS

As space operations become increasingly complex, the need for effective threat intelligence sharing is more crucial than ever. The increase in data transmission across space networks brings both opportunities and heightened risks, as cyber threats increasingly target critical space infrastructure. Protecting these assets demands a coordinated and proactive approach to threat intelligence sharing. To address this, the OASIS global standards body is working with Space ISAC to form the Space Automated Threat Intelligence Sharing (SATIS) Technical Committee (TC). The group will formally launch on Oct 9, but initial members include NSA, Northrup Grumman, Cyware, MITRE, Peraton, and Carnegie Mellon University. SATIS will build on existing frameworks like Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII) to help secure space operations against evolving threats.

Origins of SATIS

The concept for SATIS emerged from a successful experience with Space ISAC's automated machine-to-machine sharing of cyber-related indicators through a proprietary threat intelligence platform. Building on this success, SATIS aims to bring these capabilities to the broader space domain, addressing the urgent need for timely and precise information sharing.

Utilizing STIX and TAXII

At the core of the SATIS initiative are STIX and TAXII, which are both OASIS standards. STIX is a widely used language format for exchanging cyber threat intelligence (CTI) and communicating threat intelligence in a machine-readable format. It enables organizations to share critical information about cyber threats efficiently. By extending STIX to accommodate space-specific threats, SATIS aims to create a robust taxonomy that includes elements such as adversaries' tactics, techniques, and procedures (TTPs), as well as incidents and indicators of compromise. In parallel, the SATIS TC will enhance the bi-directional sharing of threat data through machine-to-machine methods, including TAXII, to ensure secure and seamless information exchange.

Key Objectives

The SATIS TC will focus on several key objectives to enhance cybersecurity in the space sector, including:

- Encouraging a collaborative approach to threat intelligence sharing among space organizations through various effective communication models,
- Promoting architectural flexibility by adopting a technology-agnostic approach that encapsulates threats across different vendors and platforms,
- Developing or extending standardized formats for key components of space cyber threat intelligence, facilitating clearer communication and understanding among stakeholders, and
- Mapping threats to existing cybersecurity frameworks, providing essential support for space operators, and enabling them to effectively respond to and manage cyber threats.

The Collaborative Future of Space Cybersecurity

Exchanging critical cyber threat information among international space community trusted partners is critical and will require collaboration among stakeholders. The SATIS TC is actively seeking input and participation from a diverse range of stakeholders to refine the framework and address the evolving threats in space. Whether you're a customer, vendor, or solution provider, your involvement is crucial.

To help shape the future of threat intelligence sharing in space and participate from the start, we invite you to join the SATIS TC. View the project's final charter and the call for participation. Contact join@oasis-open.org for more information.

About the author(s):

Erin Miller

Ms. Erin M. Miller is the Executive Director of the Space Information Sharing and Analysis Center (Space ISAC). Space ISAC serves as the primary focal point for the global space industry for "all threats and all hazards." Stood up at the direction of the White House in 2019, Erin led the Space ISAC to open its operational Watch Center, alongside its Cyber Malware and Analysis Vulnerability Laboratory in Colorado Springs, CO, USA. Under Erin's leadership, Space ISAC's headquarters facility is already serving several countries to achieve its mission of security and resilience for the global space industry. Each year Space ISAC puts on the Value of Space Summit (VOSS), co-hosted with The Aerospace Corporation at the University of Colorado Colorado Springs.

Hector Falcon
Hector Falcon is the Cyber, Space & Intelligence Principal Integrator at Space ISAC. He holds an Associate degree in Electronic Systems Technology from the Community College of the Air Force, a Bachelor of Science in Business & Information Systems Technology, and a Master of Science in Information Technology & Strategy. A 26-year veteran of the United States Air Force and United States Space Force, Hector's expertise includes radio, signals, cyber, intelligence, space, and adversarial multi-domain concepts. His goal is to leverage his diverse experience to advance multi-domain strategies and enhance understanding in the field of strategic competition.

Joel Francis
Joel has leveraged his background in technical writing and information design in the commercial threat intelligence field and enjoys building unique insights on the threat landscape for the space industry. Through his work at the Space ISAC, Joel communicates with space subject matter experts from across the world to track threats to space systems and facilitate information sharing across the space sector. As the lead of the Space ISAC's Watch Center, Joel tracks trends and significant activity regarding threats to the space community. Joel received his bachelor's degree in Professional and Technical Writing at the University of Colorado Colorado Springs and has helped to co-author several publications on behalf of Space ISAC.