Space Information Sharing and Analysis Center

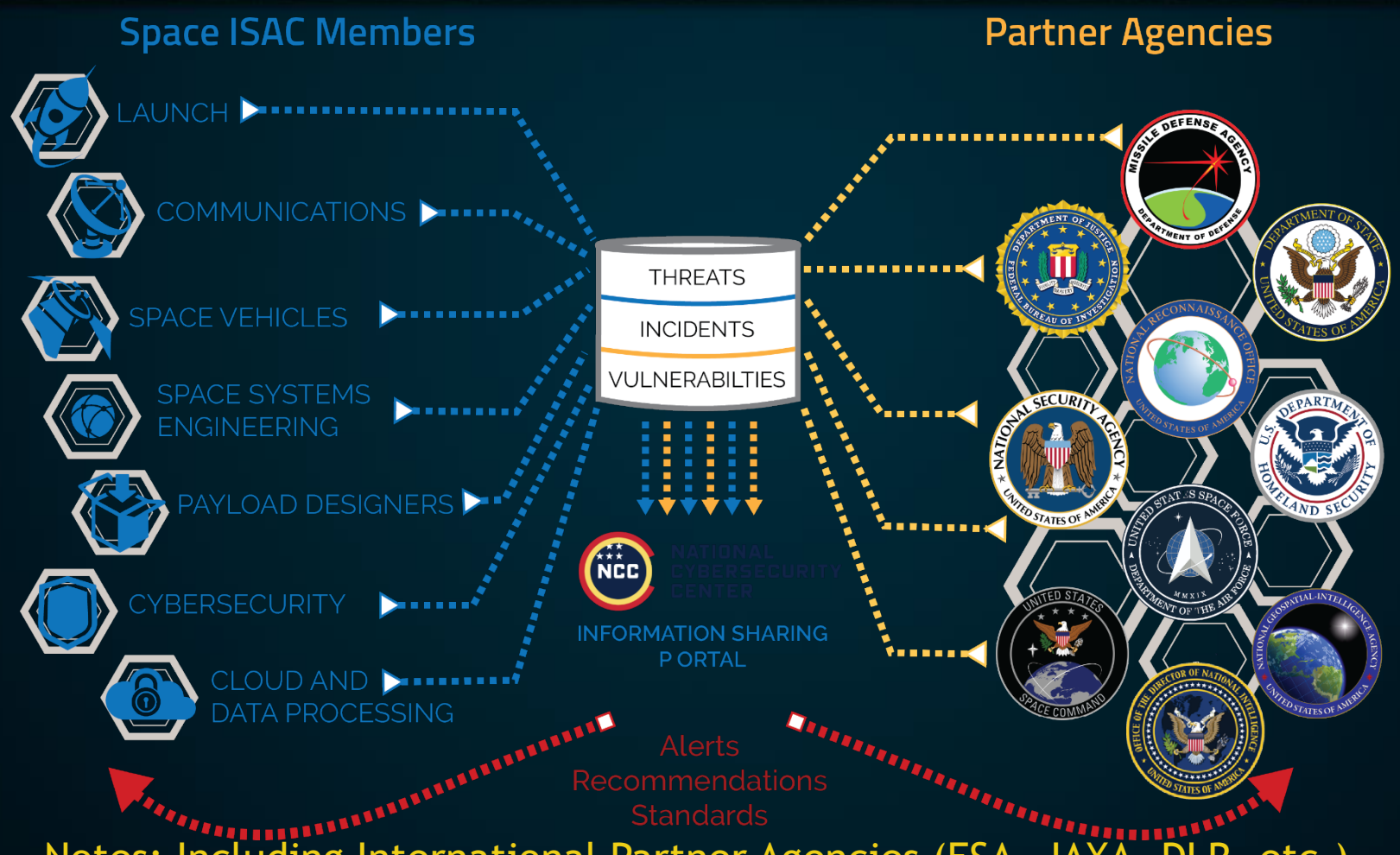
Threats to Remote Sensing Satellites ACCRES Briefing

Erin Miller, Executive Director, Space ISAC Ph. 303-596-4370, email: erin@s-isac.org

MISSION

The Mission of Space ISAC is to facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information.

Space ISAC Communities



Notes: Including International Partner Agencies (ESA, JAXA, DLR, etc.)

Executive Summary

Space ISAC is taking a multi-decade approach to commercial, international and government collaboration.

- National Cybersecurity Center is the Executive, Operational and Administrative function for Space ISAC.

Space ISAC members are leaders in the security for space community.

- Not recreating a new powerbase, we're leveraging an existing one.
- Formed to bring together members that represent across defense, IC, commercial and international critical infrastructure.

Space ISAC is not a political organization; we're operational. Solving problems for analysts and operators across the globe.

- Through public-private partnership infrastructure that exists today, we're building a Space ISAC HQ location that will serve the space community for the long-game.
- Conducting threat sharing, notifications of incidents of compromise, and alerts in a high-trust environment.

Security for space protects humanity and raises the posture of the entire sector.

- Value of space to humans on Earth shows up in our food supply chain, jobs, access to healthcare, education, communications, aviation, emergency services, transportation, and financial services.

Founding Board Members

Space ISAC Task Forces

CMMC Task Force

- *Cybersecurity Maturity Model Certification* is based on three levels, implemented to shore up supply chain
- this group is focused on building compliance with CMMC

Exercise Task Force

- led 2 exercises in 2021 • currently developing Ground Station ZTA scenario for 2022

SPD-5 Task Force

- formed in response to *Space Policy Directive 5* • focused on developing security standards

Space ISAC Summit Task Force

- Planning and development of Annual *Value of Space Summit* • 3rd consecutive VOSS this year

Space ISAC Communities of Interest

Small Satellite Community of Interest

- comprised of satellite owners/operators
- facilitates quarterly community calls

Blockchain Community of Interest

- explores blockchain applications for the space industry
- created by Space ISAC Members

Artificial Intelligence / Machine Learning Community of Interest

- focused on applying AI/ML technology to space
- created by Space ISAC Members

Workforce and Development Community of Interest

- focused on building out education portfolio for cybersecurity for space

Space ISAC Working Groups

Information Sharing Working Group

• developing quarterly white papers • responsible for direction and oversight for Space ISAC Watch Center

Analyst Working Group

• first line of defense for the Space ISAC Watch Center • meets monthly to brief threats to space systems

Supply Chain Risk Management Working Group

• focused on gaining visibility into space industry supply chain • goal to promote trusted supplier network

Space ISAC Current Capabilities

Member Portal

- Daily, Weekly, and Monthly **Reports**
- Regular alerts provide **Situational Awareness** to members
- Timely analysis of **Incidents and Threats**
- Bi-directional sharing for **Member Submitted Data**

Threat Intelligence Platform

- **Intel Collections** curated by Space ISAC
- **Integrated Feeds** from government and commercial sources
- Advanced automation **ingests** intel packages and **identifies** actionable indicators

Actionable Intelligence

- Routine **Threat Briefings** held monthly*
- Intel reports **Track Adversary Activity** and **Inform** the sector of **Vulnerabilities**
- Dissemination of actionable information strengthens **Operational Collaboration**

Intelligence Deliverables

Routine Information Products

20 Weekly Reports

500+ Daily Reports

- **Open-Source Cyber Analysis Report (OSCAR): January 2022 – Present**
  - Detailed report providing insight and trends on emerging cyber threats to the space sector.
- **Secure Space Daily Summary: January 2021 – Present**
  - Comprehensive daily product intended to provide situational awareness to members and partners

Incident/Event Analysis

- In depth advisories and briefings disseminated to members

SolarWinds
December 2020

- Led briefing to members
- Focused reporting period beginning in Dec. 2020
- Disclosed names of victims, indicators, and mitigations

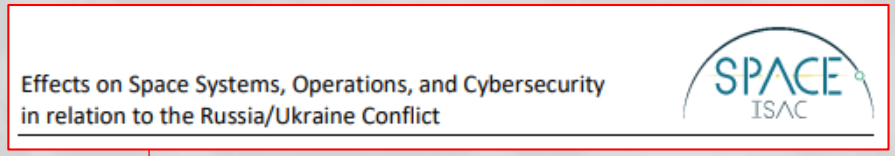
CVE-2021-44228 (Log4j)
December 2021

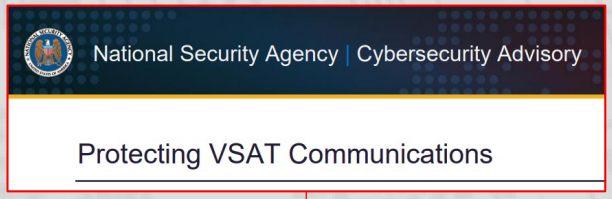
- First disclosed to members on Dec. 9, 2021
- Released advisory derived from member submissions
- Briefed **Analyst Working Group** on effects to space systems

Russian Invasion of Ukraine
February 2022

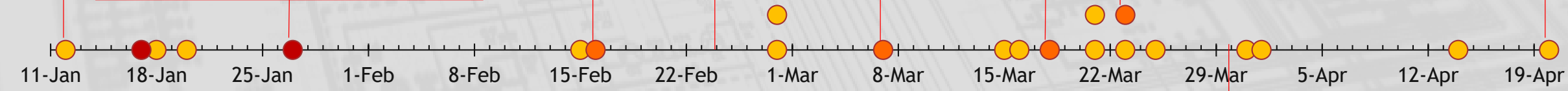
- First disclosed to members on Feb. 24, 2022
- Reporting on attacks specific to space systems
- Briefed timeline to **Analyst Working Group**

Space ISAC Reporting Timeline – Russian Invasion of Ukraine





February 24:
Russian Invasion of Ukraine



01.01.2022 - 4.20.2022

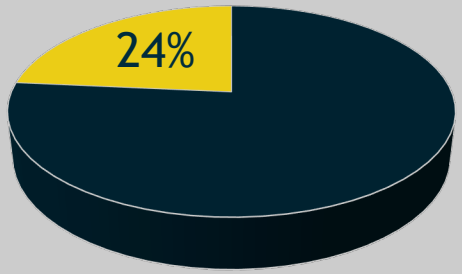
85 Total alerts sent

20 Alerts Related to Russian threat activity

6 Related to targeting space systems

4 alerts correlating Russian threats to space systems

Space ISAC Alerts



March 30, 2022
Space ISAC/ODNI Classified Briefing

- Coordinated briefing to industry regarding Russian threats to Space system
- Provided one-time read-on to members of space industry with need-to-know

Watch Center Vision

- Watch Center Initial Operating Capability is planned for Q3-Q4 2022
- *The Space ISAC Watch Center will fuse disparate data sources to create a complete picture of ground and space, allowing analysts to track adversary activity across segments.*
- Space ISAC Analysts need data sets and analysis tools providing
  - Single picture of ground and space for collective defense of the global space community (commercial, international, defense, startups, 4th & 5th tier suppliers)
  - Ability to track adversaries through ground and space and increase commercial sector security

Watch Center
Initial Operating Capability

Initial Operating Capability is intended to

- Converge on the cyber and physical threats to the space domain
- Fuse data from disparate sources
- Leverage Azure Machine Learning & Data Science products to provide analytics/events of interest to the community Display visualizations for analysts
- Offer Space ISAC analysts from public and private sector access to Watch Center

Space Threats Taxonomy

Watch Center Use Cases vs Specific Threats to Space Segments

Threats Observed by Segment

Link Segment	Space Segment	Ground Segment	Launch Segment	User Segment
C2 Intrusion	GPS Interference	Attacks to IC/OT Systems	C2 Intrusion	Loss of Network Connection
Malware/Ransomware	Satellite Spoofing/Jamming	Supply Chain Attacks	Denial of Service	Compromised Banking Transactions
Denial of Service	Space Debris	Malware/Ransomware	Remote Code Execution	Supply Chain Disturbances
Remote Code Execution	Space Weather Interference	Remote Code Execution	GPS Jamming	GPS Interference
Man in the Middle Attacks	Anomalous Behavior	Terminal Hacking	Insider Threat	
Signal Spoofing/Jamming	Satellite Maneuvers			

Watch Center IOC Use Cases

Purposeful RF Interference	**Nation State Actors**	**Ground Entry Point (GEP) Intrusion**	**Satellite Maneuver Alerts**	**Cyber Threat Intel Enrichment**

RFI: Categories of Risks, Threats, and Vulnerabilities to Commercial Remote Sensing Satellites

1. Payload

- What vulnerabilities exist in payload components?
- What TTPs could threat actors use to target satellite payloads?
- What is the business risk associated with hosted payloads?
- What specific technologies are used to mitigate threats?

2. Ground Segment

- What security vulnerabilities exist in ground station networks?
- How might a threat actor move laterally through ground station networks?
- What is the business risk associated with ground station as a service (GSaaS) models?

3. Space Vehicles/Orbital

- What the likelihood and impact of space environment variables?
- What security measures are implemented in the satellite bus?
- How are satellite owners/operators notified of significant maneuvers?

4. Link/Transmission

- What vulnerabilities exist in satellite uplinks/downlinks?
- How is sensor data maintained, verified and/or validated?
- How might a threat actor spoof satellite data?

RFI: Categories of Risks, Threats, and Vulnerabilities to Commercial Remote Sensing Satellites

1. Payload
   - Physical interference of optical sensors with directed energy or light
   - High powered directed energy to damage power and processing units
   - Adversary gaining access to command/control via network or device hacking
2. Ground Segment
   - Spoofing/jamming of TT&C to send malicious commands
   - Supply chain tampering to infect software or hardware with backdoors
   - Leveraging commercial VSATs to gain network access to send malicious commands
3. Space Vehicles/Orbital
   - Space debris and orbital objects damaging assets
   - Perceived cost for onboard encryption technology/services
4. Link/Transmission
   - Jamming/denial of bandwidth
   - Spoofing uplink – both waveform modulation and data
   - Spoofing downlink – spacecraft can easily mimic real signals or terrestrial emitters

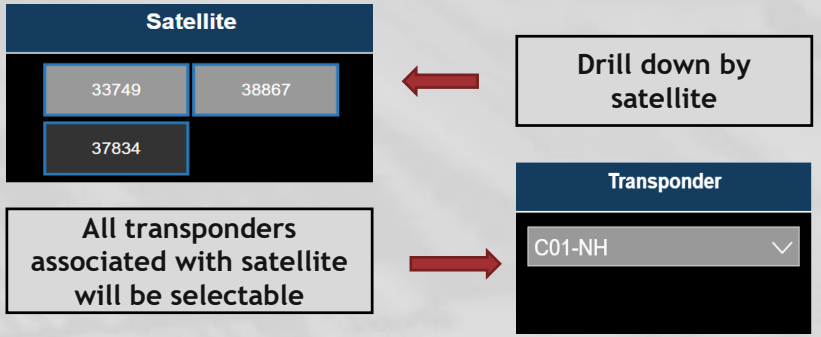
RF EMI Use Case

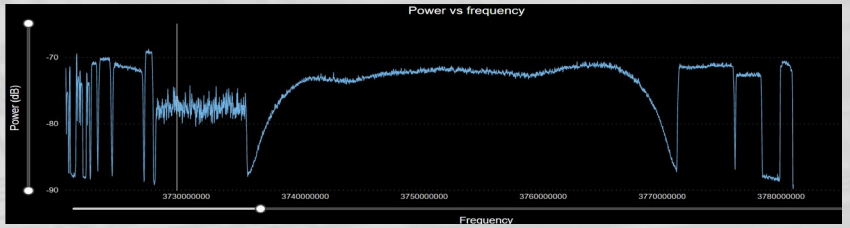
Scenario Development | Use Case Created | Identify Data Source(s) | Visualization and Implementation | Analyst Template Design

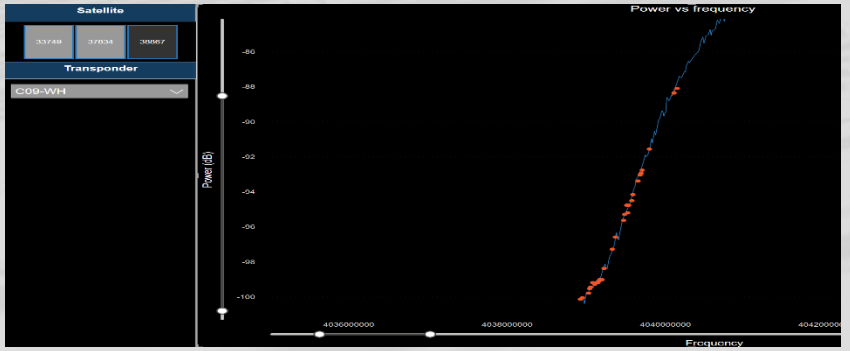
Threat Scenario: Radio Frequency Electromagnetic Interference is observed in a satellite's downlink

Additional Context: Data will demonstrate both inadvertent and purposeful RF EMI. Data is consumed by the analyst dashboard and produces visualizations. Space ISAC will notify members of satellite position, frequency, and nature of the experienced RF RMI

Data Set(s): RF EMI, indicators, and warnings data available in Unified Data Library (UDL), derived from Kratos Global Sensor Network (KGSN)







Satellite Maneuver Alerts

Scenario Development | Use Case Created | Identify Data Source(s) | Visualization and Implementation | Analyst Template Design

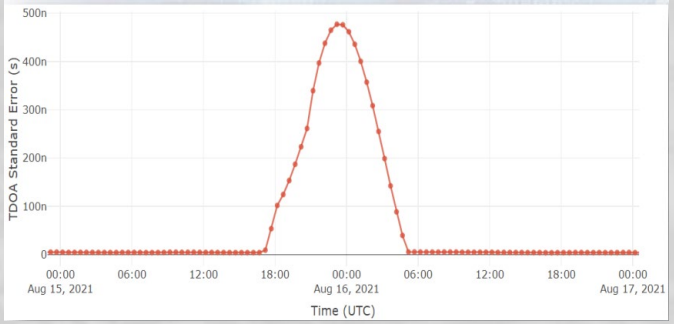
Threat Scenario: A significant maneuver is observed in a satellite

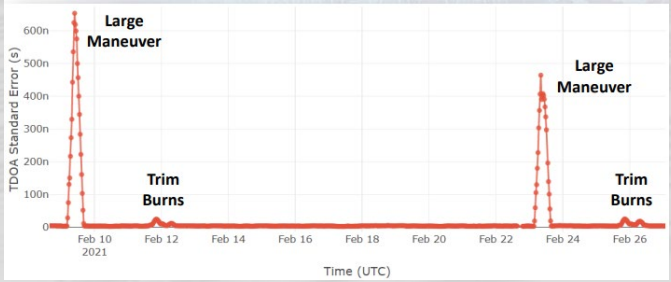
Additional Context: Time difference of arrival and frequency difference of arrival data is used to map state vectors of satellite position. Space ISAC will alert members of significant maneuvers observed in data visualizations

Data Set(s): TDOA/FDOA and State Vectors data available in Unified Data Library (UDL) derived from Kratos Global Sensor Network (KGSN)

Tactics: Command and Control, Execution, Impair Process Control

Techniques: Command-Line Interface, Execution through API, Scripting





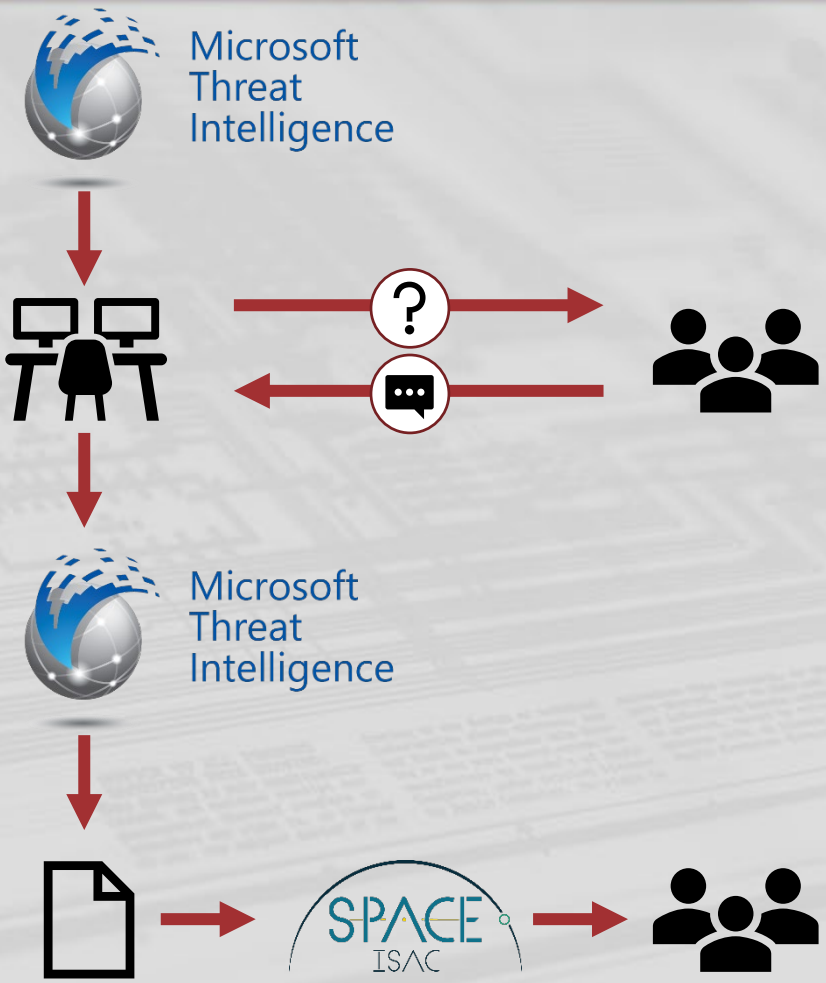
Nation State Actors

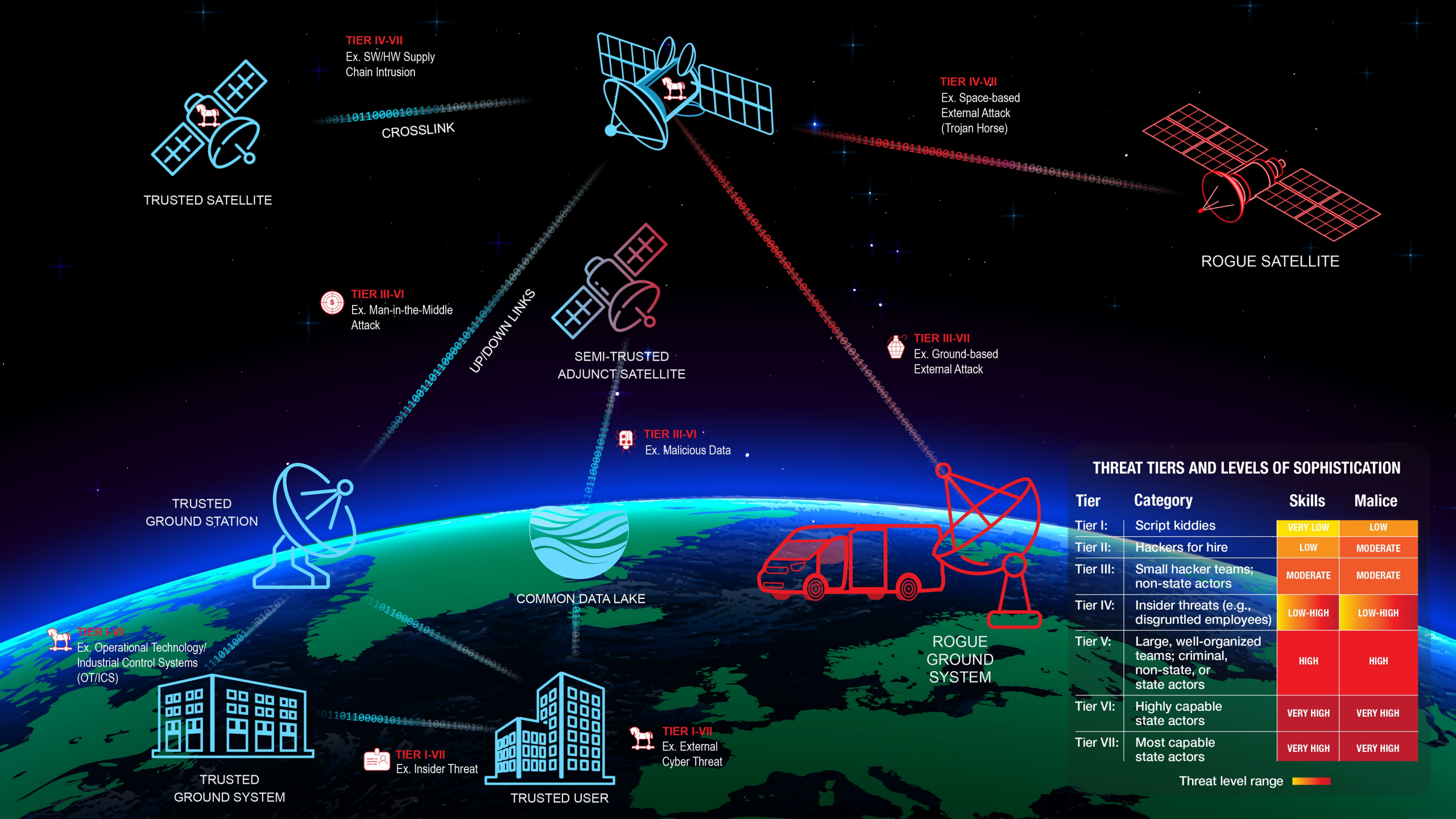
Scenario Development | Use Case Created | Identify Data Source(s) | Visualization and Implementation | Analyst Template Design

Threat Scenario: Nation State Actor is observed targeting the space sector in a sophisticated campaign

Additional Context: Microsoft Threat Intelligence Center tracks nation state actors and notices an attributed China-based actor is conducting targeted attacks against VPN infrastructure of SATCOM providers. MSTIC sends RFI to Space ISAC with indicators to date, Space ISAC consolidates feedback, MYSTIC provides additional guidance to include threat hunting queries

Data Set(s): Microsoft Threat Intelligence Center (MSTIC)





THREAT TIERS AND LEVELS OF SOPHISTICATION

Tier	Category	Skills	Malice
Tier I:	Script kiddies	VERY LOW	LOW
Tier II:	Hackers for hire	LOW	MODERATE
Tier III:	Small hacker teams; non-state actors	MODERATE	MODERATE
Tier IV:	Insider threats (e.g., disgruntled employees)	LOW-HIGH	LOW-HIGH
Tier V:	Large, well-organized teams; criminal, non-state, or state actors	HIGH	HIGH
Tier VI:	Highly capable state actors	VERY HIGH	VERY HIGH
Tier VII:	Most capable state actors	VERY HIGH	VERY HIGH

Threat level range

Space System Cyber Vulnerabilities

Uplinks and Downlinks

- **Description:** The uplink of commanding and the downlink of telemetry, tracking, and products collected from our space vehicles
- **Common Attacks/ Vulnerabilities**
  - Communications systems jamming
  - Command injection
  - Data injection
  - Crypto bypass
  - Communications systems spoofing
  - Tapping of communications links
  - Replay attacks
- **Common Mitigation Methodologies**
  - NSA Type-I encryption
  - Authentication
  - Authenticated encryption
  - Secure protocols
  - Frequency bands
- **Policy Considerations**
  - Encryption and authentication policies
  - Policies mandating secure protocols and frequency bands
- **Seen in the wild?** Yes

Space System Cyber Vulnerabilities

Rogue Satellite

- **Description:** Rogue satellite on orbit manipulates SV through cyber means
- **Common Attacks/ Vulnerabilities**
  - Attacking the satellite's onboard computer, reconfiguring or modifying software leading to infiltration, exfiltration or denial of service
  - Manipulation of the bus controllers to affect satellite positioning or initiating de-orbiting
  - Collisions
  - Eavesdropping
- **Common Mitigation Methodologies**
  - CMD validation
  - Memory protection
  - Root of trust
  - Bus segmentation
  - Least privilege
- **Policy Considerations**
  - DiD policies
- **Seen in the wild?** Yes

Summary

Watch Center Capability - IOC Q1 2023 (Jan-Mar)

- Monitors threats to the commercial space sector
- Reporting directly to members and beyond
- Produce trends analysis and distribute broadly
- Connects with partners across the globe

Cyber Vuln Lab - Q1 2023

- Conduct hardware and software testing
- Uses digital twins to emulate the space systems architecture
- Sets a community expectation for cybersecurity for commercial space systems
- Connects with partner labs across the globe