

## RF EMI to STIX Notional Mapping

Updated:

- 06/26/2025 - with additional use cases to begin mapping towards & building in CTIX. /HF
- 07/08/2025 - with SMOS anomaly cross reference (Use Case #5) and proof of concept cross walk after generating the relationship diagram in CTIX. //HF

### Introduction:

The purpose of this document is to annotate mapping RF EMI events to the STIX 2.1 framework through a series of publicly available and member submitted reports. The desired information elements are listed below. Each example report has had all available items extracted and mapped to the existing STIX 2.1 framework. **Highlighted** items did not intuitively map to existing STIX Domain Objects (SDOs) and may constitute the creation of unique SDOs and/or attributes. The majority of these data points were aggregated into the “description” attribute.

All data received from member organizations has been obfuscated in accordance with Space ISAC Operating Rules.

### Consolidated Reporting Components:

This chart maps the assumed reporting elements for RF EMI events and assesses the ability to map them to current STIX 2.1 representations. This exercise operates under the assumption that all elements can be mapped, whether as an SDO or attribute. Many of these items were included in the “description” attribute of various SDOs as a catch all. Items highlighted in red constitute data elements that did not have a strong, straightforward mapping.

Reporting Element	Data	STIX 2.1 Mapping	Revised Terminology
Aerospace SPARTA TTP	SDO	Attack Pattern	
<b>Anomaly Details</b>	SDO	Intrusion Set	Incident
<b>Anomaly Type Capture</b>	Attribute	Intrusion Set > Description	Incident > Description
<b>Any additional anomalies captured</b>	Attribute	Intrusion Set > Description	
Associated Ground Station at Point of Impact or Anomaly	SDO	Infrastructure	
<b>Exhibited Anomaly Capture (Narrative)</b>	Attribute	Intrusion Set > Description	Incident > Description
<b>Exhibited Anomaly Payload Impact</b>	Attribute	Incident > Description	Incident > Impact_refs
<b>Frequency Band Impacted</b>	Attribute	Incident > Description	
GPS time, ECEF position and velocity	Attribute	Incident > Description	
MITRE ATT&CK TTP	SDO	Attack Pattern	
MITRE D3FEND	SDO	Course of Action	

MITRE FIGHT TTP	SDO	Attack Pattern	
NORAD ID	SDO	Identity	
Orbit (LEO, SSO, HEO, MEO, GEO)	Attribute	Identity > Description	Location > Description
Orbital Altitude at Point of Anomaly Capture	Attribute	Incident > Description	Incident > event_refs
Polarization	Attribute	Incident > Description	
Post Event Status of Satellite	Attribute	Incident > Description	
Sensor Field of View	Attribute	Incident > Description	
Sensor Pointing Angle(s) During Anomaly	Attribute	Incident > Description	
Terrestrial Lat/Long (SSO and LEO)	SDO	Location	
TLE Before & TLE After	Attribute	Incident > Description	
Uplink or Downlink Impacted	SDO	Infrastructure	
UTC Correlated Event Start/Stop (Provides Duration)	Attribute	Intrusion Set > First Seen/Last Seen	Event . start_time, end_time

## Notional Reporting Format

- Title:
- Summary:
- Anomaly Details:
  - Type
  - Date
  - Start Time
  - Stop Time
  - Beam Format
  - Pulse Duration/Time Between Pulses
  - Laser Color
  - Wavelength Frequency
- Satellite/Sensor Details
  - Satellite Constellation
  - Satellite(s) Affected
  - Satellite Location at Anomaly Start
  - Satellite Location at Anomaly End
  - Sensor Wavelength/Frequency Operating Range
  - Sensor Pointing Angle(s) During Anomaly
  - Sensor Field of View
  - Sensor Effect
  - Post Event Status of Satellite
  - Event Association

## Use Case #1

**TITLE:** RF Anomaly incident Report ID:00001

**SUMMARY:**

Polaris 99 (NORAD ID 12345) experienced RFI while collecting over Belarus. Diagnostics lead us to believe this event was not internally generated by Cave of the Winds. Graphics are below and attached.

NOTE 1: Resources are being generated and all files will be pushed to the relevant S3 bucket.

NOTE 2: This collection was not for a USG tasking.

Cave of the Winds CollectID / Product Reference # is XXXXXXXX

Image IDs are: N/A

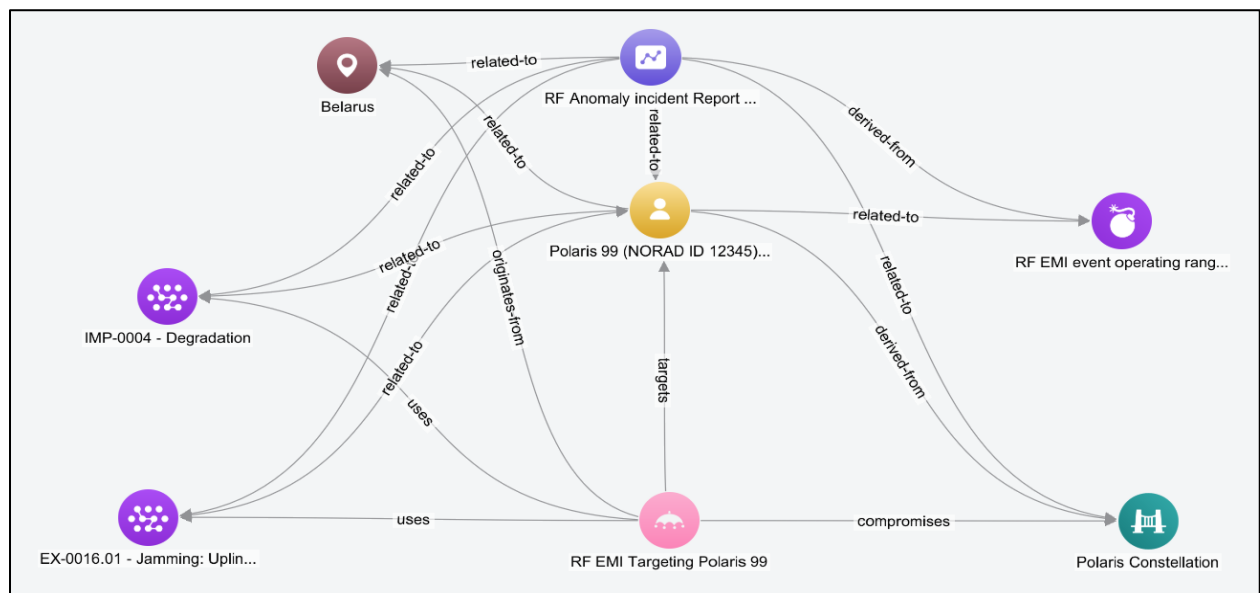
**ANOMALY DETAILS:**

- a. *TYPE (i.e., EMI, Laser, Kinetic)* EMI
- b. *DATE* 2025-01-05
- c. *START TIME* 10:07:31.11476802 GPS
- d. *STOP TIME* 10:07:46.48721785 GPS
- e. *BEAM FORMAT (i.e. pulsed or continuous for laser)* N/A
- f. *PULSE DURATION/TIME BETWEEN PULSES (for laser)* N/A
- g. *LASER COLOR (e.g. green, white for laser)* N/A
- h. *WAVELENGTH/FREQUENCY* 9.5 GHz to 9.8 GHz

**SATELLITE/SENSOR DETAILS**

- a. *SATELLITE CONSTELLATION:* **Polaris**
- b. *SATELLITE AFFECTED:* **Polaris 99**
- c. *SATELLITE LOCATION AT ANOMALY START* (GPS time, ECEF position and velocity)  
"time": "2025-01-05T10:07:30.399842000",  
"position": [ 3709827.938272481, 1288361.3591651241, 5750563.833813384],  
"velocity": [ 6423.807568044799, 17.29518894077, -4132.467078238404]
- d. *SATELLITE LOCATION AT ANOMALY END* (GPS time, ECEF position and velocity)  
"time": "2025-01-05T10:07:45.599837000",  
"position": [3806963.475189205, 1288342.0567631586, 5686969.5297837695],  
"velocity": [6356.893226540573, -19.81006932685573, -4235.022542210345]
- e. *SENSOR WAVELENGTH/FREQUENCY OPERATING RANGE* 9.5 GHz to 9.8 GHz
- f. *SENSOR POINTING ANGLE(S) DURING ANOMALY* (GPS time, quaternion)  
"time": "2025-01-05T10:07:37.999846000",  
"attitude": [-0.29905150969579747, -0.9130912460025813, 0.07774590286074551, 0.26606041655950646]
- g. *SENSOR FIELD OF VIEW* 0.7 deg
- h. *SENSOR EFFECT (e.g. temporary impairment of sensor, permanent damage)* None
- i. *POST EVENT STATUS OF SATELLITE* Operational
- j. *EVENT ASSOCIATION (linked to OPSCAP and/or SYSCAP change)* N/A

- **TITLE** → Report
  - Description: Full report (Summary, Anomaly Details, Satellite/Sensor Details)
- **SATELLITE AFFECTED** → Identity
- **SATELLITE CONSTELLATION** → Infrastructure
- **ANOMALY DETAILS** → Intrusion Set
  - Description: *TYPE, DATE, BEAM FORMAT, PULSE DURATION, WAVELENGTH/FREQUENCY*
- **SATELLITE/SENSOR DETAILS** → Incident
  - Description: Satellite Affected, Location at Anomaly Start/End, Sensor Wavelength/Frequency Operating Range,
- Attack Pattern: Contains Sparta TTPs
- **SATELLITE LOCATION** → Location



## Use Case #2: RFI Guatemala

**TITLE:** RF Anomaly Incident Report ID000002

**SUMMARY:**

Polaris 98 (NORAD ID 123456) experienced RFI while collecting over Central America. Diagnostics lead us to believe this event was not internally generated by Cave of the Winds. Graphics are below and attached.

Cave of the Winds CollectID / Product Reference # is XXXXXXXXX

Image IDs are: N/A

**ANOMALY DETAILS:**








- a. TYPE (i.e., EMI, Laser, Kinetic) EMI
- b. DATE 2024-1-03
- c. START TIME 06:39:52.03561945 GPS
- d. STOP TIME 06:40:00.80927561 GPS
- e. BEAM FORMAT (i.e. pulsed or continuous for laser) N/A
- f. PULSE DURATION/TIME BETWEEN PULSES (for laser) N/A
- g. LASER COLOR (e.g. green, white for laser) N/A
- h. WAVEL ENGTG/FREQUENCY 9.3 GHz to 9.9 GHz

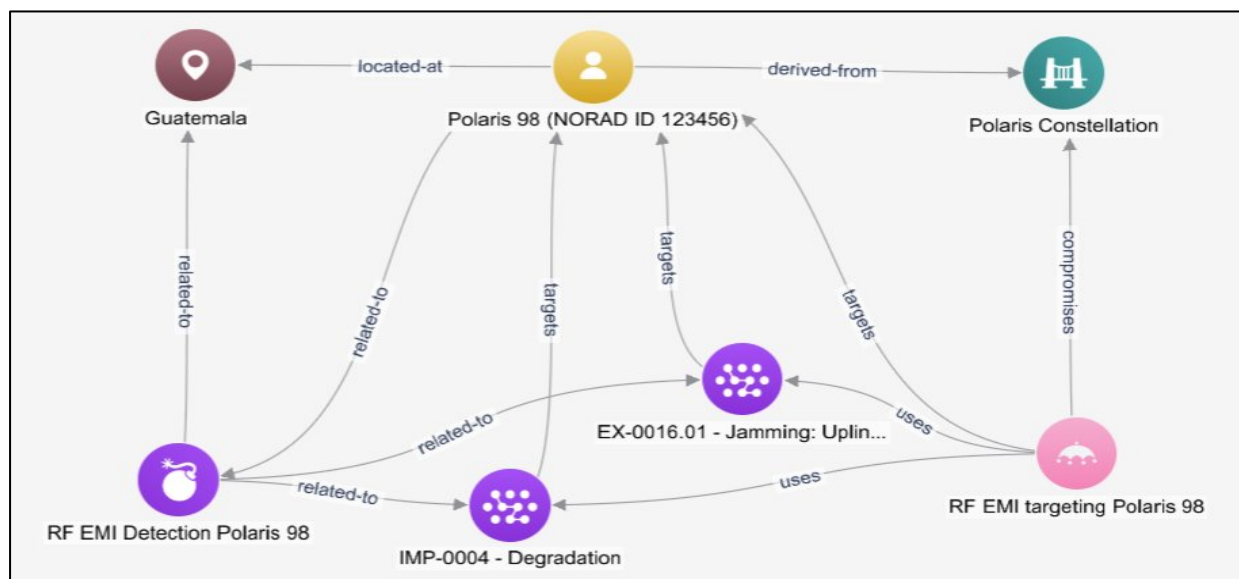
**SATELLITE/SENSOR DETAILS:**

- a. SATELLITE CONSTELLATION Polaris
- b. SATELLITE AFFECTED Polaris 98
- c. Obfuscated NORAD ID: 123456
- d. SATELLITE LOCATION AT ANOMALY START
  - "time": "2025-01-03T06:39:22.000002727",
  - "position": [ 35721.651126396486, -6612933.6401067935, 2318864.225620057 ],
  - "velocity": [ 4337.369714770672, -1908.1717687760465, -5483.343840638025 ] }
- d. SATELLITE LOCATION AT ANOMALY END
  - "time": "2025-01-03T06:40:30.400010500",
  - "position": [ 331438.1855352285, -6726973.6048504, 1937843.002420463 ],
  - "velocity": [ 4306.238510747472, -1424.781865541579, -5652.596710630712 ] }
- e. SENSOR WAVELENGTH/FREQUENCY OPERATING RANGE 9.3 GHz to 9.9 GHz
- f. SENSOR POINTING ANGLE(S) DURING ANOMALY
  - { "time": "2025-01-03T06:39:56.200006614",
  - "attitude": [ 0.39333012840960485, 0.8133741436690773, -0.28264880646878093, -0.3222166416446697 ] }
- g. SENSOR FIELD OF VIEW 0.7 deg
- h. SENSOR EFFECT (e.g. temporary impairment of sensor, permanent damage) None
- i. POST EVENT STATUS OF SATELLITE Operational
- j. EVENT ASSOCIATION (linked to OPSCAP and/or SYSCAP change) N/A

## STIX 2.1 Proof of Concept

- **TITLE** → Report
  - Description: Full report (Summary, Anomaly Details, Satellite/Sensor Details)
- **SATELLITE AFFECTED** → Identity
- **SATELLITE CONSTELLATION** → Infrastructure
- **ANOMALY DETAILS** → Intrusion Set
  - Description: *TYPE, DATE, BEAM FORMAT, PULSE DURATION, WAVELENGTH/FREQUENCY*
- **SATELLITE/SENSOR DETAILS** → Incident
  - Description: Satellite Affected, Location at Anomaly Start/End, Sensor Wavelength/Frequency Operating Range,
- Attack Pattern: Contains Sparta TTPs
- **SATELLITE LOCATION** → Location

Relations		
	Attack Pattern	2
	Identity	1
	Incident	1
	Infrastructure	1
	Intrusion Set	1
	Location	1
	Report	1



## Use Case 3: RFI in GEO

### **TITLE: RFI in GEO (MESA Verde RF EMI)**

Summary: Between **2 Mar '25 and 8 Mar '25**, Hydra satellites #1 – 3 experienced **RF EMI related anomalies concurrent with downlink jamming resulting in a degradation** while interfacing with the following latitudes and longitudinal areas. Elements below were validated as being impactful upon downlinks geolocated to and around these regions and not related to internal functions of the **Mesa Verde** satellite owner/operator systems or payloads. Graphics and visuals not provided.

### **ANOMALY DETAILS:**

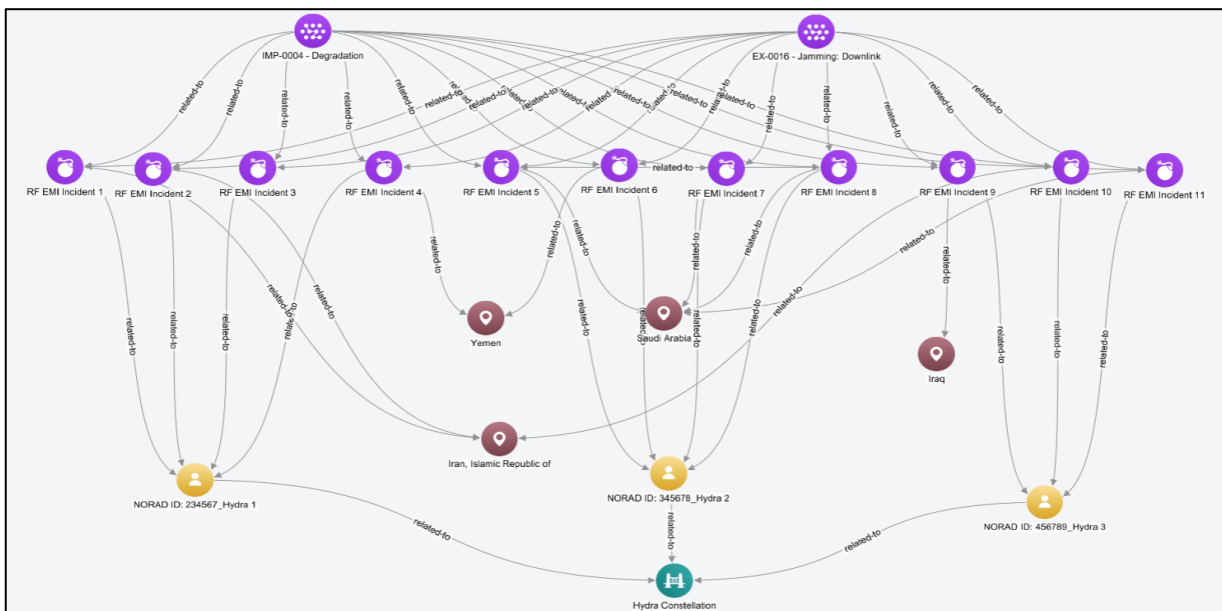
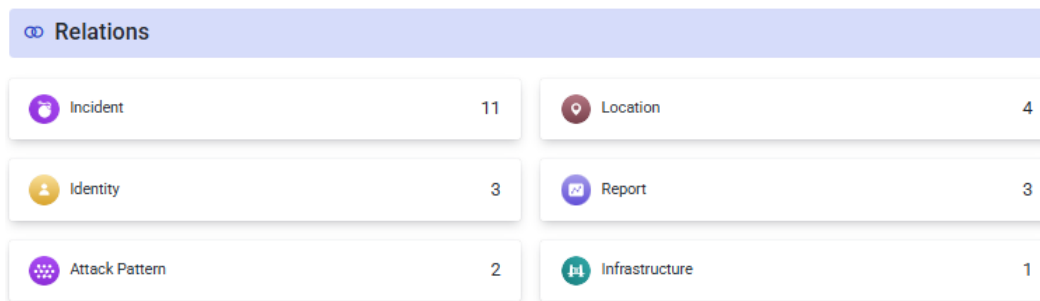
- a. Regions of Interference Correlation w/Fair Accuracy to Downlinks: Lat / Long
  - NORAD ID: 234567, Hydra 1 (**Identity**)
  - RF EMI **Incident 1**: 33.398438 46.286224
  - RF EMI **Incident 2**: 28.432617 51.75424
  - RF EMI **Incident 3**: 23.15918 51.563412
  - RF EMI **Incident 4**: 17.138672 47.901614
  - NORAD ID: 345678, Hydra 2 (**Identity**)
  - RF EMI **Incident 5**: 22.280273 49.410973
  - RF EMI **Incident 6**: 17.358398 49.15297
  - RF EMI **Incident 7**: 20.566406 46.073231
  - RF EMI **Incident 8**: 23.730469 43.739352
  - NORAD ID: 456789, Hydra 3 (**Identity**)
  - RF EMI **Incident 9**: 30.629883 46.377254
  - RF EMI **Incident 10**: 33.398438 46.286224
  - RF EMI **Incident 11**: 22.412109 47.960502

### **SATELLITE/SENSOR DETAILS:**

- a) Constellation: Hydra (**Part of Identity**)
- b) Attack Patterns Denoted:
- c) Downlink Jamming: EX-0016 (**Attack Pattern**)
- d) Signal Degradation: IMP-0004 (**Attack Pattern**)
- e) Satellites Affected: 3x Obfuscated NORAD IDs (**234567, 345678 & 456789, Part of Identity**)
- f) TYPE (i.e., EMI, Laser, Kinetic) EMI (**Jamming**)
- g) Initial Start Date: 2024-03-02
- h) START TIME/Date: 00:00:00 UTC/2 March 2025
- i) STOP TIME/Date: 23:59:59 UTC/8 March 2025
- j) BEAM FORMAT (i.e. pulsed or continuous for laser) N/A
- k) PULSE DURATION/TIME BETWEEN PULSES (for laser) N/A
- l) LASER COLOR (e.g. green, white for laser) N/A
- m) WAVELENGTH/FREQUENCY: not disclosed

## STIX 2.1 Proof of Concept

- **TITLE** → Report
  - Description: Full report (Summary, Anomaly Details, Satellite/Sensor Details)
  - Report bundle includes all 11 incidents reported
- **SATELLITE AFFECTED** → 3x Identity objects
  - Includes: *Constellation designation, Satellites Affected*
- **SATELLITE CONSTELLATION** → Infrastructure
- **ANOMALY DETAILS** → 11x Incident objects
- **SATELLITE/SENSOR DETAILS** → 11x Incident objects
  - Description: *TYPE, DATE, BEAM FORMAT, PULSE DURATION, WAVELENGTH/FREQUENCY, Regions of interference correlation*
  - Description: Satellite Affected, Location at Anomaly Start/End, Sensor Wavelength/Frequency Operating Range,
- **TYPE**: Attack Pattern: Contains Sparta TTPs
- **SATELLITE LOCATION** → 4x Location objects





## Use Case #4:

The Cybersecurity and Infrastructure Security Agency (CISA) has been working with government and industry partners to increase resilience to GPS disruptions that could impact critical infrastructure operations. The national Position, Navigation and Timing (PNT) ecosystem heavily relies on GPS as the primary source of position navigation and timing. The event below illustrates how PNT users should understand the impacts to operations should GPS be unavailable.

In January 2022, a GPS interference event occurred over a thirty-three (33) hour period in the vicinity of Denver International Airport due to a transmitter errantly broadcasting in the GPS frequency. Interference was first detected by aircraft pilots and communicated to Federal Aviation Administration (FAA) Air Traffic Control Facilities. Due to the significant number of reports, the FAA issued a Notice to Air Missions warning of the GPS interference.

Operators of systems from a wide range of critical infrastructure that rely on the GPS signal for uninterrupted PNT services also detected interference with (1) surface and rail traffic and (2) communications towers and services using GPS timing signals. Ground-based industry users of GPS/PNT services and others reported GPS interference to the United States Coast Guard Navigation Center (NAVCEN) and the Federal Communications Commission (FCC) Public Safety and Homeland Security Bureau.

Departments and agencies responsible for monitoring and coordinating response to GPS interference events implemented the established national coordination process. The FCC Enforcement Bureau deployed, located, and coordinated shut down of the emitter. No accidents or injuries occurred because of the GPS interference incident. However, several critical infrastructure sectors were degraded. Many systems that detected the event had resilient alternate timing built in for backup or fail-over timing and experienced minor or no degradation of services.

An investigation of the interference positively identified an emitter unintentionally transmitting a signal within the GPS L1 frequency. Some receivers within a line of sight of the transmitter experienced GPS signal disruption. The affected area on the ground covered approximately 50 nautical mile radius on the ground and spanned approximately 230 nautical miles in distance from the interfering transmitter at flight levels up to approximately 36,000 feet.

Improving interference detection and mitigation (IDM) of GPS signal interference is a priority of CISA. CISA is leading a federal government interagency after-action review of the event to (1) encourage owner/operator resilience by sharing best practices, (2) improve capabilities, processes, and procedures on reporting GPS interference and (3) encourage shared situational awareness with the goal of enhancing government and industry information sharing to further improve expediting IDM of interfering emissions, affecting GPS signals over the United States and its territories.

[CISA Insights GPS Interference Event](#)

## STIX 2.1 Proof of Concept

- **TITLE** → Report
  - Description: Full report (Summary, Anomaly Details)
- **ANOMALY DETAILS** → Incident
  - Details include: *START/STOP TIME, ANOMALY TYPE*
- **TYPE**: Attack Pattern: Contains Sparta TTPs

### Relations



Attack Pattern

4



Identity

1



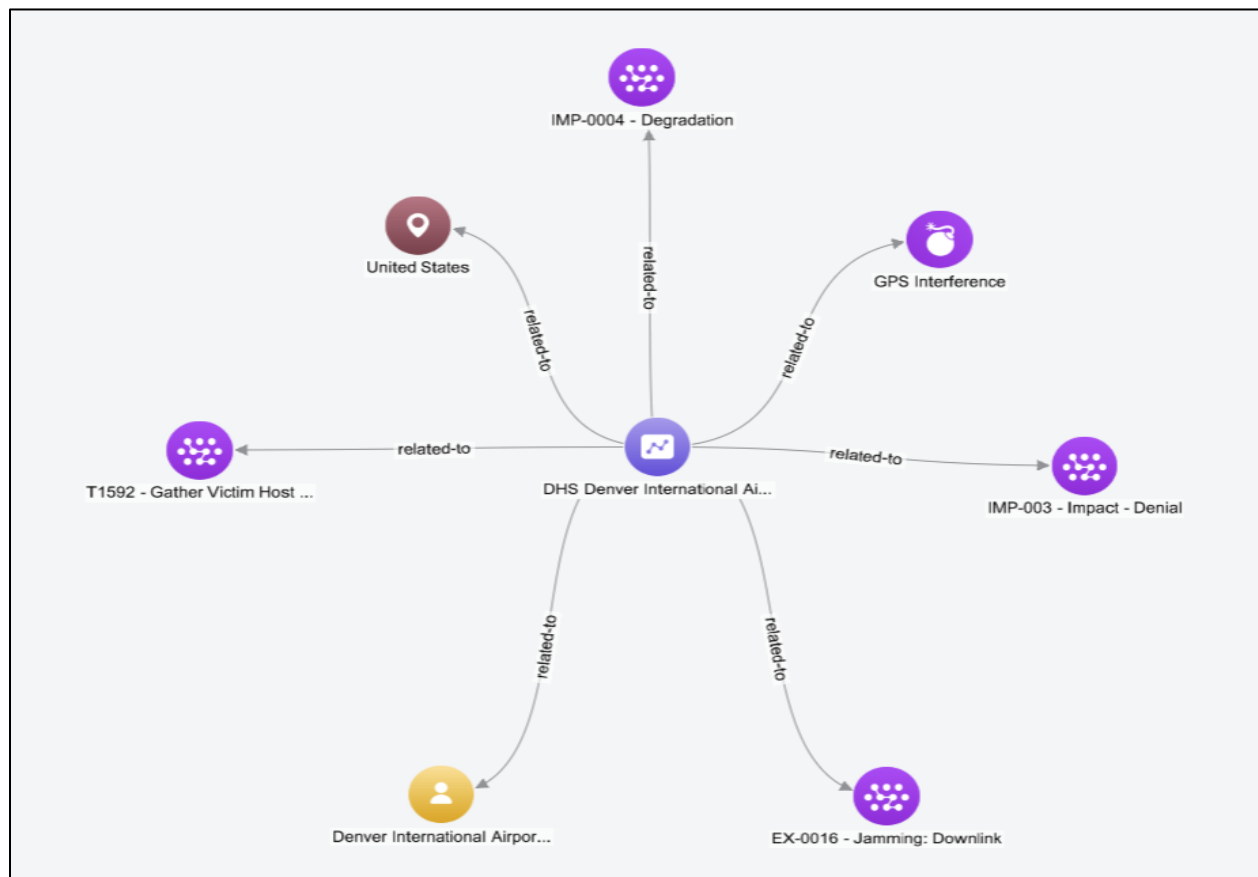
Incident

1



Location

1



## Use Case #5:

**TITLE:** SMOS Unknown Anomaly\_8 Mar 2025

### **SUMMARY:**

The Soil Moisture and Ocean Salinity (SMOS) satellite (NORAD ID #36036) during the week of 3 March to 10 March 2025, exhibited an anomaly that generated an unlocked condition on 2025-03-08 starting on 19:28:25 UTC (Julian day 067) over the Southern Atlantic Ocean, midway between Brazil and Saint Helena.

### **ANOMALY DETAILS:**

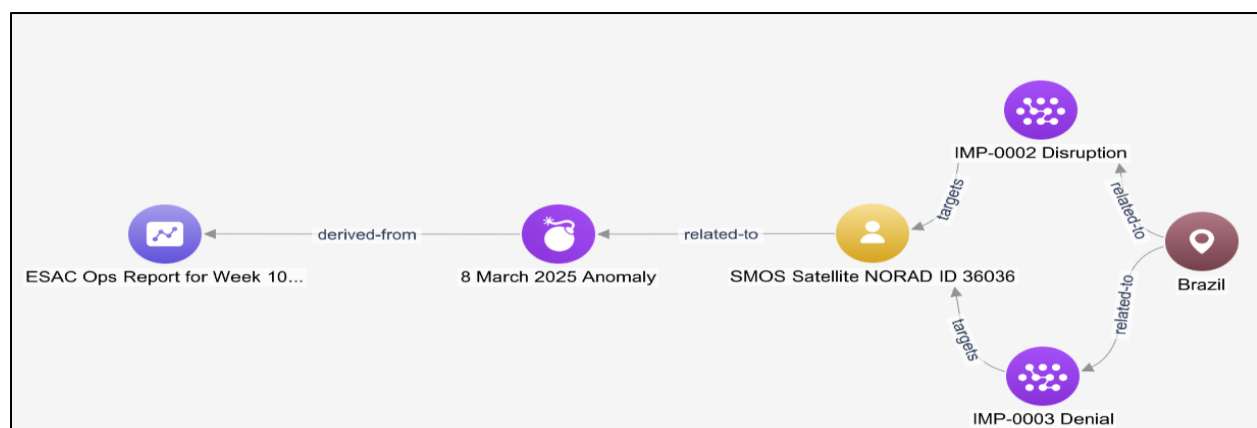
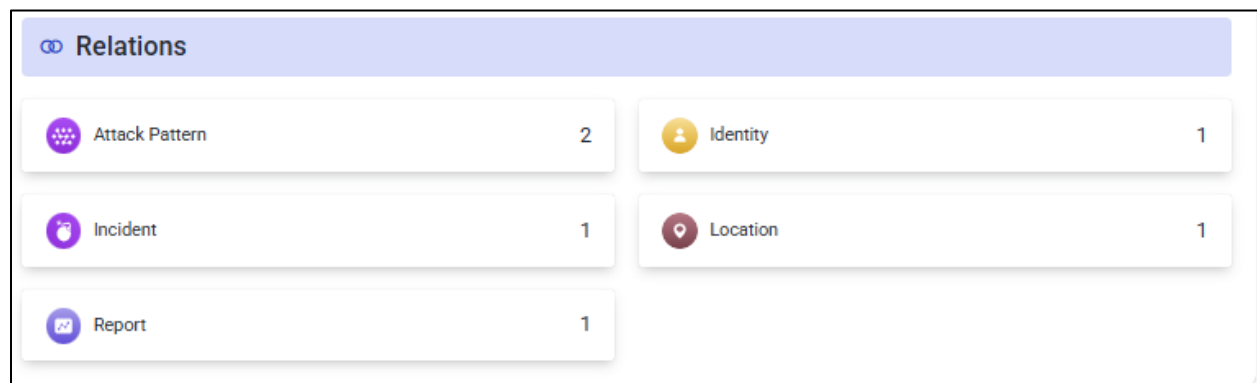
- b. *TYPE (i.e., EMI, Laser, Kinetic)* EMI
- c. *DATE* 2025-03-08
- d. *START TIME* 19:28:25 UTC
- e. *STOP TIME* 20:00:00 UTC
- f. *BEAM FORMAT (i.e. pulsed or continuous for laser)* N/A
- g. *PULSE DURATION/TIME BETWEEN PULSES (for laser)* N/A
- h. *LASER COLOR (e.g. green, white for laser)* N/A
- i. *WAVELENGTH/FREQUENCY* **L-Band (1.4 GHz)**

### **SATELLITE/SENSOR DETAILS**

- b. *SATELLITE CONSTELLATION:* **N/A**
- c. *SATELLITE AFFECTED:* **SMOS NORAD ID 36036**
- d. *SATELLITE LOCATION AT ANOMALY START* (GPS time, ECEF position and velocity)  
**N/A**  
    "position": **N/A**  
    "velocity": **N/A**
- e. *SATELLITE LOCATION AT ANOMALY END* (GPS time, ECEF position and velocity)  
    "time": **N/A**  
    "position": **N/A**  
    "velocity": **N/A**
- f. *SENSOR WAVELENGTH/FREQUENCY OPERATING RANGE* **1.4 GHz**
- g. *SENSOR POINTING ANGLE(S) DURING ANOMALY* (GPS time, quaternion)  
    "time": **N/A**  
    "attitude": **~ 766 km**
- h. *SENSOR FIELD OF VIEW* **N/A**
- i. *SENSOR EFFECT (e.g. temporary impairment of sensor, permanent damage)* **Unlocked, out of parameter, not functional**
- j. *POST EVENT STATUS OF SATELLITE* **Operational**
- k. *EVENT ASSOCIATION (linked to OPSCAP and/or SYSCAP change)* N/A

## STIX 2.1 Proof of Concept

- **TITLE** → Report
  - Description: Full report (Summary, Anomaly Details, Satellite/Sensor Details)
    - URL: [SMOS FOS Report for Week 10, Year 2025](#)
    - Title: ESAC Ops Report for Week 10
- **8 March 2025 Anomaly** → Incident
- **SATELLITE AFFECTED** → Identity
  - SMOS Satellite NORAD ID 36036
- **SPARTA TTPs** → Attack Pattern
  - IMP-0002 Disruption
  - IMP-0003 Denial
- **SATELLITE LOCATION AT TIME OF ANOMALY** → Location
  - Brazil: - 17.75 Lat, 335.36 Long



## Consolidated Mapping of Identified Elements in Reporting Examples

This chart shows an overall representation of data elements that were extruded from each use case and does not factor in how they were mapped in the current STIX 2.1 format. Items marked as Y show elements that were identified in the corresponding use cases. Items marked as N show which were not present in the source report.

EElS	Use Case #1	Use Case #2	Use Case #3	Use Case #4	Use Case #5
NORAD ID	Y	Y	N	N	Y
UTC Event Start	Y	Y	Y	Y	Y
UTC Event Stop	Y	Y	Y	Y	Y
TLE Before Event	N	N	N	N	N
TLE After Event	N	N	N	N	N
GPS Time	Y	Y	Y	N	N
ECEF Position and Velocity	Y	Y	N	N	N
Orbital Altitude at Point of Anomaly	N	N	N	N	N
Terrestrial Lat and Long Correlation	Y	Y	Y	N	N
Orbit (LEO, SSO, HEO, MEO, GEO)	N	N	N	N	Y
Exhibited Anomaly Capture (Narrative)	Y	Y	Y	Y	Y
Exhibited Anomaly Payload Impact	Y	Y	Y	N	N
Uplink or Downlink Impacted	N	N	Y	N	N
Frequency Band Impacted	Y	Y	N	N	N
Additional Anomalies Captured	N	N	Y	N	N
Anomaly Type Capture (Interference, Jamming, Spoofing, Space WX)	Y	Y	Y	Y	Y
Aerospace SPARTA TTPs (as assigned by Owner/Operator)	N	N	N	N	N
Aerospace SPARTA TTPs (as assigned by Space ISAC WC)	Y	Y	Y	Y	Y
MITRE ATT&CK TTPs	N	N	N	N	N
MITRE D3FEND TTPs	N	N	N	N	N
MITRE FIGHT TTPs	N	N	N	N	N
Associated Ground Station at Point of Impact or Anomaly	N	N	N	N	N
Polarization	N	N	N	N	N
Sensor Field of View	Y	Y	N	N	N
Sensor Point Angle During Anomaly	Y	Y	N	N	N
Post Event Status of Satellite (Non-Operational vs Operational)	Y	Y	N	N	Y
<b>Total Number of Correlations</b>	<b>14</b>	<b>14</b>	<b>10</b>	<b>5</b>	