MITIGATING THREATS TO SPACE SYSTEMS: AN OVERVIEW OF SPACE ISAC WATCH CENTER

HOLISTIC APPROACH

The Watch Center takes a holistic approach to identify and report threats to space systems. It incorporates monitoring activity of satellite links, reporting anomalous maneuvers in earth orbits, and correlating these findings with terrestrial cyber activity observed through open sources and from community contributions.

THREAT LEVEL FRAMEWORK

Space ISAC implements a Threat Level Framework for assessing, determining, and disseminating the current threat level to members. This framework enables the Watch Center to provide real-time threat intelligence to members, helping them to take proactive measures to secure their systems. The framework is comprised of four tiers ranging from 'normal' to 'severe'. Each level contains a definition, criteria for change, and mitigation techniques for members.

OPERATIONAL SCOPE

The Watch Center's operational scope encompasses all threats and hazards affecting the global space community. It considers all segments of the space sector for information sharing: Link Segment, Space Segment, Launch Segment, Ground Segment, and User Segment. The Watch Center is divided into cells that focus on each of these segments, while having the ability to correlate as part of the greater mission of the Watch Center.

ANOMALY DETECTION AND CORRELATION

Watch Center analysts monitor data feeds and visualizations, detect anomalies, correlate this information with other data sources, and draft reports for members. The goal of the Watch Center is to produce products that inform members of threats across all segments of the space domain.

TRAFFIC LIGHT PROTOCOL (TLP)

Space ISAC utilizes the Traffic Light Protocol (TLP) designations published by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to ensure that sensitive information is shared with the appropriate audience. TLP is a mechanism to control how unclassified information is shared among a variety of entities within the Space ISAC community and is essential for operations of all ISACs.

DISSEMINATION OF ALERTS AND ADVISORIES

Space ISAC routinely disseminates alerts and advisories from trusted members and partners that detail the current adversary activity ranging from unsophisticated hackers, advanced persistent threats (APT), or nation-state actors. Space ISAC correlates this information in daily, weekly, and monthly reports that mention cyber threats, incidents, and vulnerabilities to critical systems.

REPOSITORY OF KNOWN THREAT ACTORS

Space ISAC maintains a list of priorities for information sharing, as well as a repository of known threat actors to aid in the process of identifying potential threats and vulnerabilities. Our weekly Open Source Cyber Analysis Report (OSCAR) presents a weekly snapshot of new threat actors reported and threat actor activity.

TRUSTED ENVIRONMENT

Space ISAC offers members a trusted environment to communicate about threats without risking tipping off the adversary.

VIRTUAL AND PHYSICAL SUPPORT

The Watch Center can support 10 analysts physically, with additional support virtually. Cloud architecture allows us the ability to host analysts from around the world from our 17 founding and platinum members.