SPACE-ISAC | CYWARE™ | Case Study

Space-ISAC Uses Cyware to Power Collective Defense for the Global Space Sector

The global space industry faces an unprecedented convergence of cyber and physical risks spanning IT security, ground/OT systems, and space/mission telemetry. To safeguard this interconnected ecosystem, Space-ISAC has embraced the SPARTA framework, a structured approach to space cyber threat modeling and assessment, as a foundation for building collective defense. Aligned with this framework, Space-ISAC's mission is to enable trusted, timely cyber threat sharing and coordinated response across its members.

To operationalize this at the necessary speed and scale, Space-ISAC implemented a Cyware-powered environment that serves as both a secure intelligence-sharing hub and an enabler of automated SecOps across member organizations. This approach not only strengthens mission assurance but also provides a repeatable blueprint for peers to follow, improving resilience and advancing the collective defense posture of the global space sector.

S - Structure: Context and Mission

The mission of Space-ISAC is to protect the global space ecosystem by fostering trusted, timely cyber threat sharing and coordinated response among its members. To fulfill this mission at the necessary speed and scale, Space-ISAC has operationalized a Cyware-powered environment that serves as both a secure intelligence-sharing hub and a promoter of an automated SecOps model for its member organizations.

P - Problem: Cyber-Physical Silos and Slow Collaboration

Space organizations face a unique and complex threat landscape where signals across three distinct domains often live in silos.

- **IT Security:** Traditional security operations, including SIEM, EDR/NDR, and identity management.
- **Ground/OT Systems:** Mission-critical operational technology like Telemetry, Tracking, and Command (TT&C) and mission control.
- **Space/Mission Telemetry:** In-orbit data such as RF interference and Space Situational Awareness (SSA) information.

Before adopting Cyware, the manual and decentralized nature of cross-organizational collaboration led to slow responses and a lack of shared awareness. Analysts and mission operators worked in parallel, delaying the crucial correlation of cyber indicators with operational anomalies. This resulted in analyst overload, high alert volume, and a struggle to keep up with the threat landscape.

A - Action: What We Implemented

Space-ISAC adopted Cyware's Intel Exchange, Orchestrate, and Collaborate solutions to address these challenges head-on. The implementation focused on two key pillars: a collective defense hub and an automated SecOps model for member organizations.

- **Collective Defense via the ISAC Hub:** The platform serves as a secure, role-based threat-intel sharing hub. It ingests and disseminates indicators, TTPs, advisories, STIX/TAXII collections. This allows for automated dissemination, with members subscribing to relevant feeds that flow directly into their security tools. A dedicated Watch Center normalizes, deduplicates, scores, and tags incoming intelligence with key context, such as mission, asset, supplier, and geography.
- **Automated SecOps:** Inside member organizations, the platform ingests data from a variety of sources—including IT, OT, and mission telemetry—to create a unified view. This data integration layer and correlation engine fuses cyber Indicators of Compromise (IoCs) with operational anomalies, such as an unusual uplink attempt paired with an identity anomaly, to improve detection quality. SOAR playbooks then automate a wide range of actions, including blocking/quarantining, revoking credentials, restricting uplink ACLs, opening incident response tickets, and notifying both mission operators and the ISAC channel.
- **Cross-Ecosystem Collaboration:** Cyware facilitated secure, inter-member workflows for joint investigations and "flight-control style" incident coordination. This bi-directional communication ensures that insights and actions are shared in near-real-time, fostering a more connected and responsive community. The platform also supports structured content and playbooks designed to align with sector best practices and emerging space CTI standards.

R - Results: Measurable Improvements in Mission Assurance

The implementation of Cyware has led to significant improvements in efficiency, collaboration, and overall security posture for Space-ISAC and its members.

- **Time-to-Share Indicators:** The time from a Watch Center alert to member dissemination has been reduced from 4-8 hours to just 5-30 minutes.
- **Mean Time to Detect (MTTD):** By correlating data across IT, OT, and mission telemetry, MTTD has decreased from 60-90 minutes to a remarkable 20-30 minutes.
- **Mean Time to Respond (MTTR):** Automated SOAR playbooks have cut the average response time from 4-8 hours down to 30-60 minutes.
- **Auto-Dissemination Coverage:** Between 60-80% of critical alerts are now automatically disseminated to subscribed members in near-real-time.
- **Analyst Efficiency:** The platform has saved an estimated 80-100 analyst hours per month by reducing duplicate alerts and enabling automation.

> With Cyware, we've moved from siloed data to fused intelligence. Our members can now anticipate and neutralize threats before they impact missions. It's a paradigm shift from reactive defense to proactive mission assurance.

T - Takeaways: Lessons for Other Organizations

Space-ISAC's journey with Cyware has provided valuable insights for other organizations looking to adopt a similar model:

- **Start small and scale:** Begin with a manageable number of high-value use cases and expand from there, rather than trying to solve everything at once.
- **Focus on data quality:** Treat deduplication and scoring as a primary objective. Reducing alert fatigue directly improves analyst efficiency and morale.
- **Pre-agree on rules:** Establishing redaction rules and sharing protocols beforehand ensures that real-time sharing can happen quickly during an active incident.
- **Socialize wins:** Regularly measuring and publicizing key metrics like MTTD/MTTR improvements, automated actions, and analyst hours saved helps to maintain buy-in from both leadership and the community.

A - Application: A Repeatable Blueprint

The blueprint for success is clear and can be replicated by others in the industry. It involves a 90-day rollout plan:

- **Days 0-15:** Discover & Prioritize: Inventory feeds across all domains (IT, OT, telemetry) and select high-value use cases for correlation.
- **Days 16-45:** Connect & Normalize: Stand up the platform, connect to feeds, normalize data to standards like STIX 2.x, and enrich with external context.
- **Days 46-75:** Correlate & Automate: Author cross-domain correlation rules and implement SOAR playbooks for automated response.
- **Days 76-90:** Operate & Prove Value: Go live, measure key metrics like MTTD/MTTR, and socialize the wins to maintain buy-in.

Prospects for a Collaborative Future

With the initial success and proven value, Space-ISAC members are now empowered to act on threats, not just receive fragmented information. The foundation is set for further automation and maturity. This partnership has allowed the space community to shift from a reactive to a proactive security stance, mapping cyber findings directly to their operational impact and ensuring mission continuity.

About Cyware

Cyware is leading the industry in Operationalized Threat Intelligence and Collective Defense, helping security teams transform threat intelligence from fragmented data points to actionable, real-time decisions. We unify threat intelligence management, intel sharing and collaboration, as well as hyper-orchestration and automation—eliminating silos and enabling organizations to outmanoeuvre adversaries faster and more effectively.

Learn More

Request a Demo Today