CosmicGuard

CYBERSECURITY

Safeguarding Space Mission Ground Segments

Welcome to the future of space mission cybersecurity. At GMV, we understand that the success of space missions' hinges on the security and integrity of operational ground systems. Introducing ***CosmicGuard***, a groundbreaking cybersecurity solution designed to protect against advanced threats and ensure the continuity of your missions.

CosmicGuard is an all-in-one cybersecurity solution, transparent, multi-operating system, compact, with a very low footprint. It monitors processes, scans connections, ensures file integrity, protects operating system start-up, and manages the use of hardware devices—protecting critical aspects of operational ground systems.

marketing.TIC@gmv.com

gmv.com

CYBERSECURITY SOLUTION FOR OPERATIONAL GROUND SYSTEMS

How does it work?

CosmicGuard ensures that only legitimate operations are allowed on operational ground systems. For unknown or suspicious operations, ***CosmicGuard*** blocks them, and sends an alert in real-time to a centralized console where the user can take immediate action.

CosmicGuard reports to CERT/CSIRT all security events, such as changes in the integrity of a critical resource or whitelisted process and any security policy violation.

The basic pillars of ***CosmicGuard*** are:

- **Transparent:** Assures security preserving normal operations and guaranteeing availability.
- **Multi-Operating System:** Compatible with Windows and Linux operating systems.
- **Compact:** Security is controlled with a single component deployed in the endpoints.
- **Low Footprint:** Minimum use of resources, no need for endpoint hardware or OS upgrades.

Benefits

- **Adaptability:** Keeps up with evolving threats, adapting quickly to new risks.
- **Simplicity:** Streamlines cybersecurity management with a comprehensive solution.
- **Precision:** Minimizes false positives, improving operational efficiency.
- **Continuity:** Ensures mission success by protecting operational ground systems.

Protection against threats

- Detects **Operating System** component modifications.
- Handles a whitelist of trusted **processes**.
- Manages **hardware device** usage.
- Filters access requests, rejecting illegal **data** access.
- Includes an application-level firewall to protect **communications**.
- Protects the **operating system start-up** and recovery mode/safeboot options.
- Manages security from a centralized server to command security policies and monitor incidents in real time.