SPACE CYBERSECURITY WEEKLY WATCH

Week 39

September 24 - 30, 2024

Timeframe : Weekly

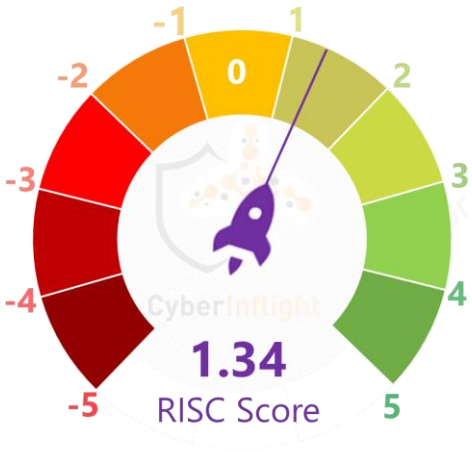
# of articles identified : 22

Est. time to read : 60 minutes

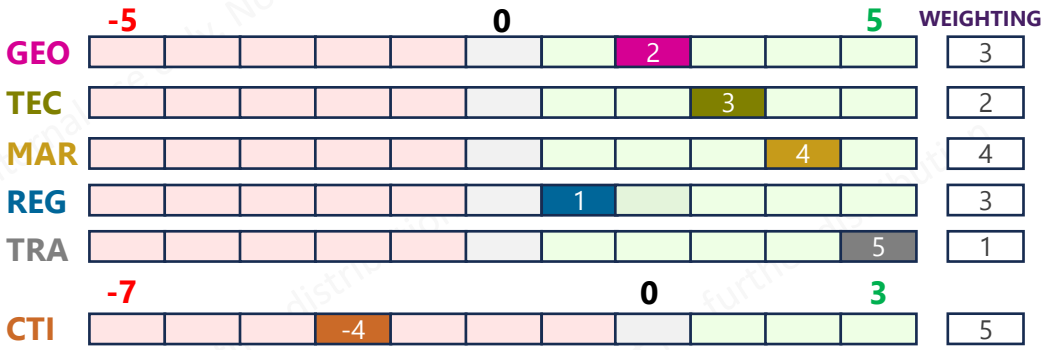
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

- GEOPOLITICS
- TECHNOLOGY
- MARKET INTELLIGENCE
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

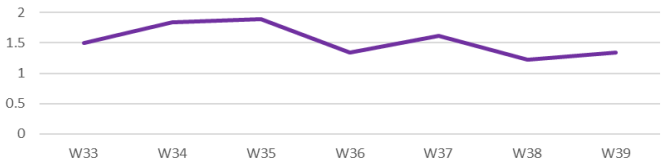
RISC Score Assesment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score Evolution



This week's RISC score is 1.34, an increase from last week, mainly due to reduced threats and positive technological innovation news in the ecosystem.

On the geopolitical front, UK, US, and Canada have entered into a trilateral agreement to jointly address the increasing cyber threats posed to critical national infrastructures. By leveraging artificial intelligence, the three nations aim to create more robust, adaptive defense systems capable of countering sophisticated cyberattacks. This collaboration reflects a growing trend in multinational cybersecurity efforts, especially in response to escalating geopolitical tensions. On the technological side, the US Air Force, under its Defense Experimentation Using the Commercial Space Internet (DEUCSI) program, is pushing forward secure SATCOM solutions with an emphasis on advanced AESA and RFIC technologies. This initiative seeks to leverage commercial satellite communications to enhance defense capabilities while maintaining data security. On the market front, the French Space Command has expressed strong support for the European Union's proposed IRIS² multi-orbit secure communications network, designed to provide both GEO and LEO-based satellite services. The network is a key part of Europe's strategy to enhance the security of its space assets while ensuring that critical communications remain uninterrupted. On the regulatory front, CyberOps Pty has expanded its Space Cyber Framework, designed to address the unique cybersecurity challenges in the space domain. This framework offers a comprehensive approach to securing space assets, from satellites to ground control stations. It includes best practices, threat assessment methodologies, and incident response strategies tailored to the space industry. On the threat intel side, NASA faces security breach, hacker claims to breach system twice. Lastly, PNT resilience takes center stage at IPSEC 2024 with discussions revolved around how PNT resilience underpins key sectors such as defense, telecommunications, and energy.

GEOPOLITICS

UK, US, and Canada unite on cybersecurity & AI for national defense

UK, US, and Canada have entered into a trilateral agreement to jointly address the increasing cyber threats posed to critical national infrastructures. By leveraging artificial intelligence, the three nations aim to create more robust, adaptive defense systems capable of countering sophisticated cyberattacks. This collaboration reflects a growing trend in multinational cybersecurity efforts, especially in response to escalating geopolitical tensions. The initiative also focuses on intelligence sharing and strengthening military ties through the application of emerging technologies.
#CriticalInfra #AI
Link: https://ukdefencejournal.org.uk/uk-us-and-canada-join-forces-on-cybersecurity-and-ai/

TECHNOLOGY

USAF drives secure SATCOM through DEUCSI program

US Air Force, under its Defense Experimentation Using the Commercial Space Internet (DEUCSI) program, is pushing forward secure SATCOM solutions with an emphasis on advanced AESA and RFIC technologies. This initiative seeks to leverage commercial satellite communications to enhance defense capabilities while maintaining data security. As reliance on satellite communication grows, ensuring resilient and protected communication channels has become a strategic priority for the USAF in the evolving defense landscape. **#USAF #SecureSATCOM**
Link: https://news.satnews.com/2024/09/25/viasat-awarded-u-s-a-f-deucsi-contract-for-phased-array-antenna-tech-development/

MARKET & COMPETITION

French Space Command backs EU's IRIS² secure comms network

The French Space Command has expressed strong support for the European Union's proposed IRIS² multi-orbit secure communications network, designed to provide both GEO and LEO-based satellite services. The network is a key part of Europe's strategy to enhance the security of its space assets while ensuring that critical communications remain uninterrupted. This development is also in response to growing geopolitical challenges and the need for Europe to remain competitive in space communications. **#IRIS2 # SATCOM**

Link: https://www.spaceintelreport.com/french-space-command-on-eus-proposed-iris2-multi-orbit-secure-comms-network-and-leo-and-geo-based-space-sentries/

Mitsubishi Heavy Industries joins space ISAC to strengthen cyber defense

Mitsubishi Heavy Industries (MHI) has officially joined the Space Information Sharing and Analysis Center (ISAC) to enhance its cybersecurity posture for space systems. By becoming part of Space ISAC, MHI aims to share intelligence, collaborate on threat assessments, and improve resilience against cyber threats targeting space infrastructure. The move aligns with MHI's strategic focus on developing secure space technologies for both defense and commercial applications, making this partnership crucial in the growing global space cybersecurity market. **#SpaceISAC #CyberDefense**

Link: https://www.satellitetoday.com/cybersecurity/2024/09/27/mitsubishi-heavy-industries-joins-space-isac/

TRAINING & EDUCATION

[redacted]

PNT resilience takes center stage at IPSEC 2024

Critical infrastructure resilience and security are the focal points of the IPSEC 2024 conference, with experts emphasizing the importance of positioning, navigation, and timing (PNT) systems. Discussions revolved around how PNT resilience underpins key sectors such as defense, telecommunications, and energy. Attendees explored innovations in PNT security technologies and shared insights into mitigating the growing threats to these essential systems from cyberattacks and disruptions. **#PNTResilience #IPSEC**

Link: https://spaceanddefense.io/navigating-pnt-for-critical-infrastructure-resilience-and-security-ipsec-2024-speaker-interview/?utm_source=rss&utm_medium=rss&utm_campaign=navigating-pnt-for-critical-infrastructure-resilience-and-security-ipsec-2024-speaker-interview

[redacted]

[redacted]

REGULATION

CyberOps Unveils Space Cybersecurity Framework to Secure Future Space Missions

CyberOps Pty has introduced its Space Cyber Framework, designed to address the unique cybersecurity challenges in the space domain. This framework offers a comprehensive approach to securing space assets, from satellites to ground control stations. It includes best practices, threat assessment methodologies, and incident response strategies tailored to the space industry. As space missions become more complex and reliant on digital technologies, such frameworks are critical to safeguarding the security and integrity of space operations. **#SpaceCyberFramework #CyberOps**

Link https://www.linkedin.com/posts/cyberops_spacecyber-infosec-activity-7246384683762999297-2P5f/?utm_source=share&utm_medium=member_desktop

THREAT INTELLIGENCE

NASA Faces Security Breach, Hacker Claims to Breach System Twice

A hacker has claimed to have breached NASA's systems twice, exposing potential vulnerabilities in the space agency's cybersecurity defenses. NASA, responding swiftly, into the matter while maintaining that no critical systems were compromised. The incident raises concerns about the launched an investigation cyber resilience of agencies managing space infrastructure, highlighting the importance of ethical hacking and proactive vulnerability management. As space becomes increasingly digitized, securing these systems is paramount to avoiding catastrophic disruptions.
#NASA #SystemVulnerability

Link: https://www.timesnownews.com/technology-science/hacker-claims-to-breach-nasas-system-twice-heres-how-the-space-agency-reacted-article-113756443

[redacted]