SPACE CYBERSECURITY WEEKLY WATCH

Week 20

May 14 - 20, 2024

Timeframe : Weekly

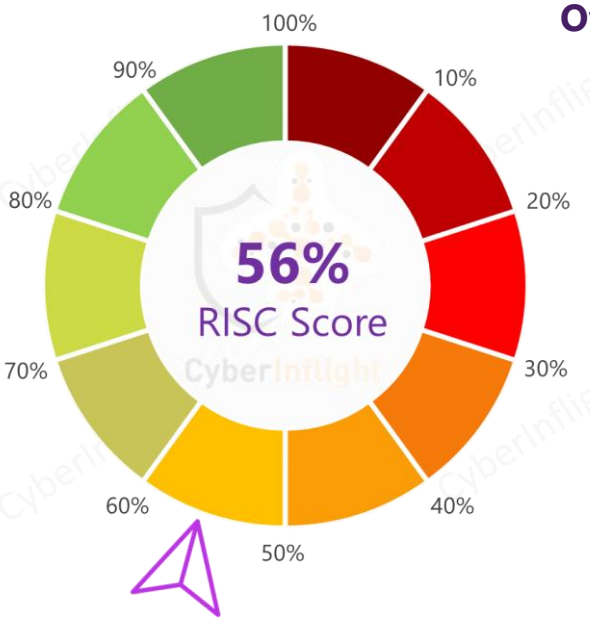
# of articles identified : 27

Est. time to read : 45 minutes

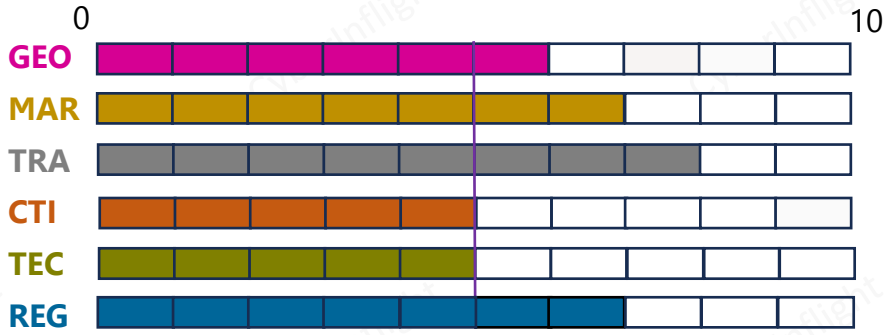
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

Overview & RISC Score



A 1% decrease from last week



RISC Score Evolution

This W20 shows a slight decrease from last week's RISC Score level. The tendency still remains constant, except for W17 which showed the highest score level of the year.

This week's RISC score is 56%. This week, France remains undecided about an offer from US Space Command to take part in Operation Olympic Defender, the US-led initiative to strengthen defense and deter hostility in space. In addition, the Federal Office for Information Security (BSI) unveils its cybersecurity framework for space applications. The office identified actions and goals to implement suitable measures for designing cybersecurity for space infrastructures. On the market front, Governor of Maryland and State of South Australian Premier signed a Memorandum of Understanding between Maryland & South Australia to collaborate in cybersecurity, outer space and high technology. In addition, China has emerged as a global leader in tackling critical infrastructure issues through its groundbreaking QKD technology, demonstrated by its quantum satellite program. On the technology front, SEALSQ announced that its post-quantum semiconductors solutions are designed to provide a reliable foundation for secure computing and transaction verification. The company stands at the forefront of integrating quantum computing and IoT, offering a unique and trusted cybersecurity platform. Finally, the Ukrainian military's Starlink terminals went down on the first day of the Russian offensive in Kharkiv Oblast on May 10th . They were jammed by Russian electronic warfare systems.

GEOPOLITIC

[redacted]

France undecided on US offer to join 'Olympic Defender' space effort

France remains undecided about an offer from US Space Command to take part in Operation Olympic Defender, the US-led initiative to strengthen defense and deter hostility in space – but says that if it does join up, it will not be turning over operational control of its military space capabilities to its US allies. **#France #OlympicDefender**

Link: https://breakingdefense.com/2024/05/france-undecided-on-us-offer-to-join-olympic-defender-space-effort/

[redacted]

REGULATORY

[redacted]

The Federal Office for Information Security (BSI) unveils its cybersecurity framework for space applications

Satellite applications have become an integral part of everyday life. Space-based systems are also highly relevant for sovereign task. The BSI is responsible for strengthening the information security of such satellite systems and ensuring the availability of services via integral, authentic communications. The office identified actions and goals to implement suitable measures for designing cybersecurity for space infrastructures. The document is for now only available in German, but the English version is to be released soon. **#BSI #SpaceCybersecurity**

Link: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/IT-Sicherheit-in-Luft-und-Raumfahrt/it-sicherheit-in-luft-und-raumfahrt_node.html

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

[redacted]

Maryland and South Australia officials sign Memorandum of Understanding to collaborate in cybersecurity, outer space and high tech

Governor Wes Moore and State of South Australian Premier, Peter Malinauskas, signed a Memorandum of Understanding between Maryland and South Australia to collaborate in cybersecurity, outer space and high tech. also there: Australian Ambassador Kevin Rudd, MD Sec. Commerce Kevin Anderson. **#SouthAustralia #Maryland**

Link: https://x.com/SenatorSusanLee/status/1792360166127755674

[redacted]

[redacted]

TRAINING & EDUCATION

[redacted]

TRAINING & EDUCATION

China's quantum satellites: paving the way for a global unhackable ground and space network infrastructure

In an era of escalating cyber threats and the increasing vulnerability of critical infrastructures, the need for secure communication systems has never been more critical. As cyber warfare targets essential information systems, nations are compelled to fortify their communication channels against potential breaches. Compounding this challenge is the looming threat of quantum computers, capable of rendering conventional cryptographic methods obsolete. China has emerged as a global leader in tackling these issues through its groundbreaking QKD technology, notably demonstrated by its quantum satellite program. **#QuantumSatellites #SpaceSecurity**

Link: https://idstch.com/cyber/chinas-quantum-satellites-paving-the-way-for-a-global-unhackable-ground-and-space-network-infrastructure/

[redacted]

TECHNOLOGY

SEALQ quantum computing and IoT: a transformative synergy with next-generation root of trust IoT

Leader in semiconductor, PKI and Post-Quantum technology development, SEALSQ, announced that its post-quantum semiconductors solutions are designed to provide a reliable foundation for secure computing and transaction verification in a world threatened by quantum computing capabilities. SEALSQ stands at the forefront of integrating quantum computing and IoT, offering a unique and trusted cybersecurity platform. It offers innovative solutions able to ensure the security and integrity of digital interactions and transactions across various industries including fintech, healthcare, automotive, defense and space research. **#SEALQ #QuantumComputing**

Link: https://www.globenewswire.com/news-release/2024/05/14/2881407/0/en/SEALQ-Quantum-Computing-and-IoT-A-Transformative-Synergy-with-Next-Generation-Root-of-Trust-IoT.html

[redacted]

THREAT INTELLIGENCE

[redacted]

[redacted]

[redacted]

Ukrainian military's Starlink terminals went down at beginning of Russian offensive in Kharkiv Oblast

The Ukrainian military's Starlink terminals went down on the first day of the Russian offensive in Kharkiv Oblast on May 10th. They were jammed by Russian electronic warfare systems. **#Ukraine #Starlink**

Link: https://www.pravda.com.ua/eng/news/2024/05/17/7456272/

[redacted]

[redacted]

[redacted]

[redacted]