SPACE CYBERSECURITY WEEKLY WATCH

Week 4

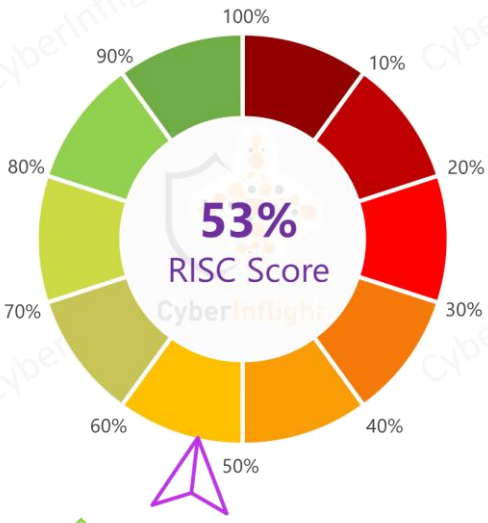
January 23 – 29, 2024

Timeframe : Weekly
# of articles identified : 26
Est. time to read : 40 minutes

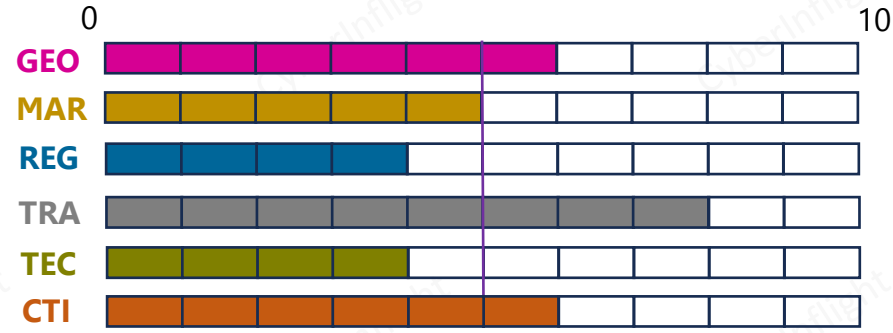
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

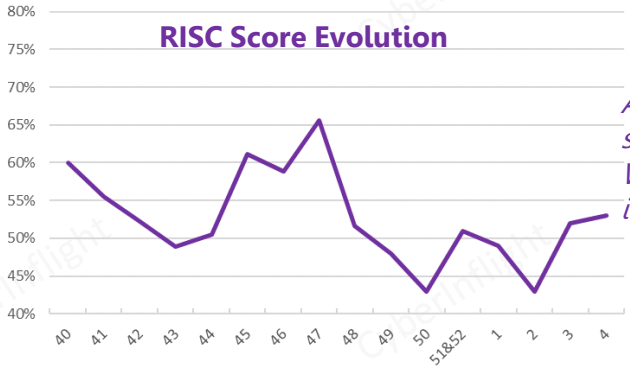
- GEOPOLITIC
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- TECHNOLOGY
- THREAT INTELLIGENCE
- IMPORTANT NEWS

Overview & RISC Score



Increase from last week (from 52% to 53%)





After a period of decline since the start of 2024, W3 & W4 show an increase.

This week's RISC Score is 53%. This week, South Korea announced a significant uptick in attempts of cyberattacks by foreign sources, mainly accusing China and North Korea. Also, Ukraine's military intelligence agency (HUR) announced that "Volunteer patriot" hackers of the BO Team launched a cyberattack against the Russian Far Eastern Research Center of Space Hydrometeorology "Planeta," destroying its database and expensive equipment. On the market front, a partnership between EUSPA and Qualinx to develop a consumer-grade, low-power GNSS receiver for the agency's GNSS authentication service. On the technology front, EUSPA and the European Commission have published an updated version of the Galileo OSNMA Internet Data Distribution (IDD) Interface Control Document (ICD) and the Certificate Practice and Certificate Practice Standards (CS/CPS). Last but not least, ESA announced the Space Systems Security challenge as part of its 3S conference, to be held on May 27-28, 2024.

GEOPOLITIC

Seoul's spy agency accuses China of major cyber attacks

South Korean spy agency on Wednesday reported a significant uptick in attempts of cyber attacks by foreign sources last year, waged mainly by North Korea and China. Chinese attacks tended to inflict more severe damage than North Korean ones, despite the latter being more frequent. **#SouthKorea #China**

Link: https://m.koreaherald.com/view.php?ud=20240124000731

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

Qualinx Partners with EUSPA to Advance GNSS Development

Qualinx, is partnering with the European Union Agency for the Space Programme (EUSPA) under the Fundamental Elements EU R&D funding mechanism to develop a consumer-grade, low-power GNSS receiver for the agency's GNSS authentication service. **#EUSPA #Qualinx**

Link: https://hardwarebee.com/electronic-breaking-news/qualinx-partners-with-euspa-to-advance-gnss-development/

REGULATION

[redacted]

TRAINING & EDUCATION

CYSAT – Startup Corner

CyberInflight will be present at this year's CYSAT 2024, in the Startup Corner! There are still places available to join us!
#CYSAT #CyberInflight
Link: https://www.linkedin.com/posts/alexandravaillant_cysat-cybersecurity-for-the-space-industry-activity-7153383815300677632-A_Qf?utm_source=share&utm_medium=member_desktop

Space Systems Security Challenge

ESA is happy to announce that in the context of 2024 Security for Space Systems (3S) conference, a hands-on security challenge is organised focusing on the security of space systems. This challenge stands out as the first of its kind to comprehensively cover all layers from RF communication to onboard data handling systems security in a space context.
#3SChallenge #ESA
Link: https://atpi.eventsair.com/24a06---3s2024/space-systems-security-challenge

TECHNOLOGY

EUSPA and the European Commission have published an updated version of the Galileo Open Service Navigation Message Authentication OSNMA IDD ICD and the CS/CPS

The publication of an updated version of the Galileo OSNMA Internet Data Distribution (IDD) Interface Control Document (ICD) and the Certificate Practice and Certificate Practice Standards (CS/CPS), together with the OSNMA operational cryptographic material, will allow users and receiver manufacturers to finalize the implementation of the OSNMA protocol in advance of the OSNMA Initial Service provision phase. **#Galileo #OSNMA**
Link: https://www.gsc-europa.eu/news/updated-documentation-and-cryptographic-material-in-preparation-for-the-galileo-osnma-initial

THREAT INTELLIGENCE

Military intelligence: Cyberattack on Russian scientific research center deals 'devastating' damage

"Volunteer patriot" hackers of the BO Team launched a cyberattack against the Russian Far Eastern Research Center of Space Hydrometeorology "Planeta," destroying its database and expensive equipment, Ukraine's military intelligence agency (HUR) said on Jan. 24. **#Cyberattack #Russia**

Link: https://kyivindependent.com/military-intelligence-cyber-attack-on-russian-space-hydrometeorology-research-center-deals-devastating-consequences/

CyberInflight is a Market Intelligence company dedicated to the topic of Space Cybersecurity. The company provides strategic market and research reports, bespoke consulting, market watch & OSINT researches and cybersecurity awareness training.
Contact us at: research@cyberinflight.com