SPACE CYBERSECURITY WEEKLY WATCH

Week 11

March 12 - 18, 2024

Timeframe : Weekly

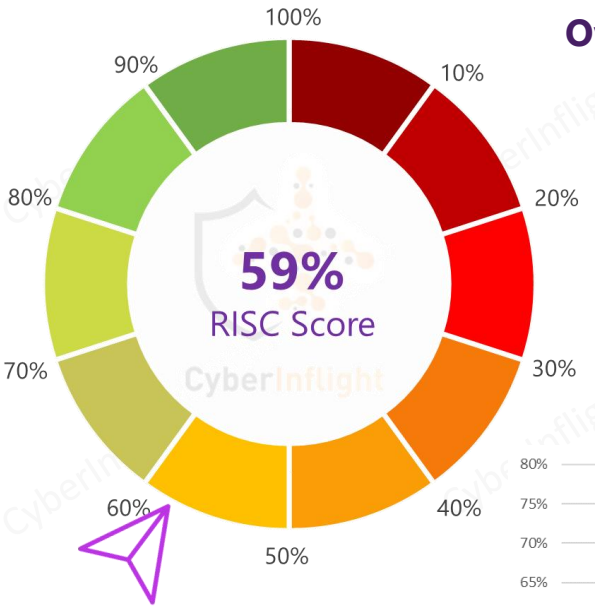
# of articles identified : 45

Est. time to read : 90 minutes

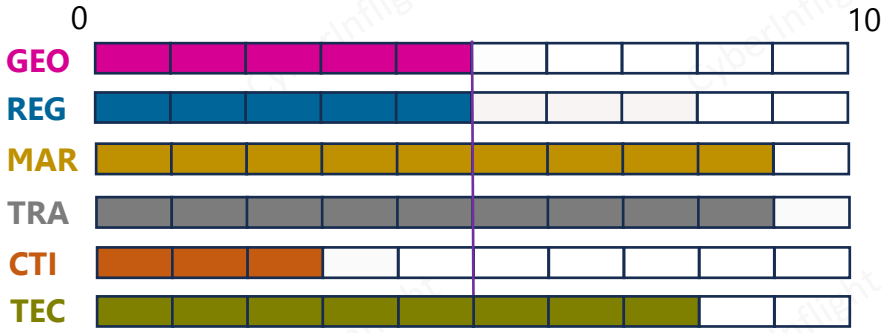
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

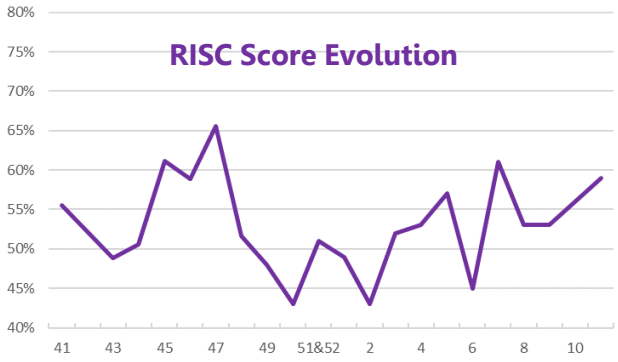
- GEOPOLITIC
- REGULATION
- MARKET INTELLIGENCE
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- TECHNOLOGY
- IMPORTANT NEWS

Overview & RISC Score



Increase from last week (from 56% to 59%)





After a rising period since the start of 2024, W6 has shown a decrease, W7 has shown an increase followed by a decrease for W8. Since W9 there has been an increase every week.

This week's RISC score is 59%. This week, an article was published about the US Space Force focusing on defensive cyber operations. In fact, earlier this year, 12 Guardians from the Peterson SFB moved away from base IT support to focus on defensive cyber operations. In addition, Australia's Cyber and Infrastructure Security Centre (CISC) released updated guidance to strengthen cybersecurity measures for Systems of National Significance (SoNS). On the market front, Science Applications International Corp. (SAIC) reported winning a $444 million contract to modernize launch instrumentation and information systems at U.S. Space Force launch sites in Florida and California. In addition, the EU conducted the Space Threat Response Architecture (STRA-X-24) exercise at the European External Action Service headquarters in Brussels from March 4-13. This week, Russia is also believed to have jammed the satellite signal of an RAF aircraft carrying British Defense Secretary Grant Shapps. Defense sources called it a "wildly irresponsible" act of electronic warfare. Finally, Fleet Space Technologies, a leading Australian space company, announced the successful demonstration of satellite-based push-to-talk (PTT) capabilities for the Australian Defence Force - Joint Capabilities Group as part of their ASCEND2LEO program. This achievement represents a significant leap forward in tactical communications capabilities.

GEOPOLITIC

[redacted]

[redacted]

Guardians Of The Digital Frontier : USSF Focusing On Defensive Cyber Operations

Earlier this year, 12 Guardians from Peterson SFB shifted away from base IT support to focus on defensive cyber operations. All 12 Guardians were reassigned from working with the Defense Red Switch Network. "This was driven by the Chief of Space Operations' vision to get all Cyber Guardians and operations into defensive cyber operations roles, instead of the base operations support IT role," said U.S. Space Force Master Sgt. Matthew Crafton, 21st Communications Squadron test control flight chief. **#SpaceForce #CyberWarfare**

Link: https://www.petersonschriever.spaceforce.mil/Newsroom/News/Display/Article/3705037/guardians-of-the-digital-frontier-ussf-focusing-on-defensive-cyber-operations/

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

REGULATION

Australia's CISC Releases Updated Cybersecurity Guidance For Systems of National Significance

Australia's Cyber and Infrastructure Security Centre (CISC) released on Monday updated guidance materials aimed at bolstering cyber security measures for Systems of National Significance (SoNS), which represent the country's most critical infrastructure assets. The comprehensive guidance includes specific instructions for SoNS on fulfilling the Incident Response Planning obligation and detailed guidelines for meeting the Cyber Security Exercise obligation.

#Australia #CriticalInfrastructure

Link: https://industrialcyber.co/threats-attacks/australias-cisc-releases-updated-cybersecurity-guidance-for-systems-of-national-significance/

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

[redacted]

Data Systems At Space Force Sites To Get $444M Modernization Under SAIC Contract

Science Applications International Corp. (SAIC) reports landing a contract worth $444 million to modernize the launch instrumentation and information systems at U.S. Space Force launch sites in Florida and California. Under the terms of the contested Digital Transformation, Acquisition, Modernization and Modification (DTAMM) contract from the U.S. Space Force's Space Systems Command, SAIC is tasked with modernizing old-style space launch range instrumentation and processes to support an accelerated cadence of space missions. **#USSF #SAIC**

Link: https://militaryembedded.com/cyber/cybersecurity/data-systems-at-space-force-sites-to-get-444-million-modernization-under-saic-contract

[redacted]

[redacted]

[redacted]

MARKET & COMPETITION

Why Taiwan Is Building A Satellite Network Without Elon Musk

In Taiwan, the government is racing to do what no country or even company has been able to: build an alternative to Starlink, the satellite internet service operated by Elon Musk's rocket company, SpaceX. Officials in Taiwan face constant reminders that its communication infrastructure must be able to withstand a crisis. The island democracy sits 80 miles from China, where leaders have vowed to use force if needed to assert claims that Taiwan is part of its territory.

#Taiwan #Investment

Link: https://dnyuz.com/2024/03/14/why-taiwan-is-building-a-satellite-network-without-elon-musk/

Arabsat And Anexia Sign MoU To Support Development of Private Cloud Services And GPU Services For Innovative Projects

The Arab Satellite Communications Organization (Arabsat), the main provider of satellite services in the Arab region, signed a memorandum of understanding with Anexia to enhance the cooperation in the fields of satellite communications, private cloud services, and GPU technology services, and provide integrated solutions to customers by taking advantage of the capabilities of both parties, and sharing common interests. **#Arabsat #Anexia**

Link: https://spacewatch.global/2024/3/arabsat-and-anexia-sign-mou-to-support-development-of-private-cloud-services-and-gpu-services-for-innovative-projects/

SpaceX Inked $1.8Bn Deal With US Intelligence Agency To Create A Network Of Spy Satellites, Report Says

SpaceX's substantial ties to US national security are deeper than previously known, according to a new Reuters report. The astronautics company inked a $1.8 billion deal in 2021 with an American intelligence agency to create a network of spy satellites, the outlet reported, citing five sources familiar with the terms of the program. **#SpaceX #SpySatellite**

Link: https://www.businessinsider.com/spacex-contract-network-spy-satellites-us-intelligence-report-2024-3?r=US&IR=T

TRAINING & EDUCATION

Enhancing Space Cybersecurity: Securing Space Systems From Cyber Threats

Attend this conference of the ISSA Conferences 2024, in San Francisco, on May 1, 2024. Representatives from ONCD, NSpC, DoD, NASA, and Space ISAC will discuss public and private sector efforts to address risks and best practices for industry to consider. **#Awareness #Conference**

Link:https://www.rsaconference.com/usa/agenda/session/Enhancing%20Space%20Cybersecurity%20Securing%20Space%20Systems%20From%20Cyber%20Threats

Space Lasers : Next Leap In Global Communications

Space lasers are transforming the world. Not the far-off future of science fiction, but the universe of how data and communications flow today — everywhere from deep space missions to countless applications here on earth, including consumer internet services, military operations, and banking transactions. Lasers can transmit vast amounts of data over great distances at the speed of light, 100 times faster than previously possible in space. **#Lasers #Technology**

Link: https://industrytoday.com/space-lasers-next-leap-in-global-communications/

Epic CTF : Space Grand Challenge

Join us for a cosmic episode of Simply Cyber Live as we delve into the cosmos of cybersecurity! Our special guest, Henry Danielson, Adjunct Professor at CalPoly, will be our guide through the interstellar world of cyber challenges with the Space Grand Challenge. What is the Space Grand Challenge? It is an international competition open to middle and high school students from across the globe! Teams from all over the world will compete in a gamified satellite cybercrime scenario to help solve Mission Kobayashi 2.45-0. Learn more about this exciting CTF opportunity available from CalPoly and how you can participate this April. **#CTF #Competition**

Link: https://www.youtube.com/watch?v=HOBOTQE2Y0

Former NASA Chief Knowledge Officer Says Cyber Complacency Is Dangerous

The three-day national Australian Cyber Conference in March, organized by the Australian Information Security Association (AISA), is set to feature some of the "greatest minds in cyber" from across the globe. Dr Hoffman, former NASA chief knowledge officer, is one such speaker, and plans to urge Australian decision-makers to do better when it comes to cyber security. **#NASA #Awareness**

Link: https://the-riotact.com/former-nasa-chief-knowledge-officer-says-cyber-complacency-is-dangerous/190210

TRAINING & EDUCATION

Space : EU Carries Out Space Threat Response Architecture 2024 Exercise (STRA-X-24)

From 4 to 13 March, the EU carried out the Space Threat Response Architecture (STRA-X-24) exercise in the European External Action Service Headquarters in Brussels. The exercise tested the EU´s response capacity to a situation in which EU space assets are subject of an attack targeting space services which are essential for governments, businesses, and citizens. **#EU #Exercise**

Link: https://www.eeas.europa.eu/eeas/space-eu-carries-out-space-threat-response-architecture-2024-exercise-stra-x-24_en

THREAT INTELLIGENCE

[redacted]

[redacted]

Russia Suspected of Jamming GPS Signal On Aircraft Carrying Grant Shapps

Russia is believed to have jammed the satellite signal on an RAF aircraft carrying Grant Shapps, UK Secretaty of State for Defence, according to government sources. Shapps was travelling from Poland to the UK when jamming interferences happened. It is understood that the GPS signal was interfered with for about 30 minutes while the plane flew close to Russia's Baltic exclave of Kaliningrad. Mobile phones could no longer connect to the internet and the aircraft was forced to use alternative methods to determine its location, the source said. Defence sources called it a "wildly irresponsible" act of electronic warfare. **#UK #Jamming**

Link: https://www.theguardian.com/politics/2024/mar/14/russia-suspected-of-jamming-gps-signal-on-aircraft-carrying-grant-shapps

[redacted]

[redacted]

[redacted]

[redacted]

TECHNOLOGY

Fleet Space's Centauri Becomes Earth's Smallest Voice-Capable Satellite After In-Orbit Software Update

Fleet Space Technologies, a leading Australian space exploration company, announced the successful demonstration of satellite-enabled Push-to-Talk (PTT) capabilities for the Australian Defence Force - Joint Capabilities Group as part of their ASCEND2LEO program. This achievement signifies a major leap forward in tactical communications capabilities.
#Australia #PTT

Link: https://fleetspace.com/news/fleet-spaces-centauri-becomes-earths-smallest-voice-capable-satellite-after-in-orbit-software-update

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