AI & CYBERSECURITY NEWSLETTER

NOVEMBER 2021

Highlights

DOJ Attacks Back at REvil – Arrests and Seizure of $6.1M Ransom AND Knocks Them Offline

Expected Themes for 2021 PrivSec Global Virtual Cyberconference November 30-Dec 1

Accepting Nominations for 2022 Cybersecurity Leaders

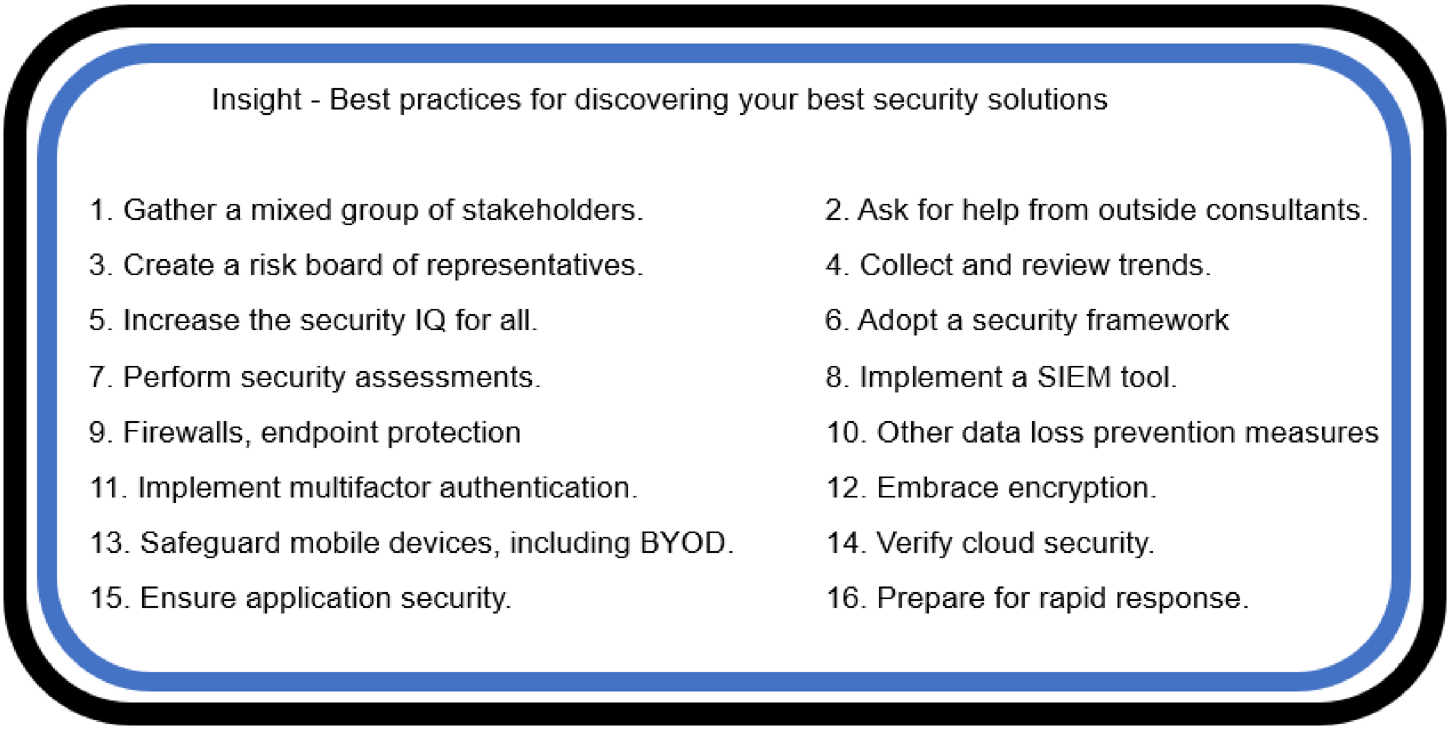
Muon Space Satellites to Create Meaningful Data Repository to Combat Climate Change

Poll Results for "Cloud Service Providers: Is Public Cloud, Private Datacenter, or Hybrid Right for You"

G2M Webinar Schedule and Upcoming Conferences

The U.S. $1T infrastructure bill includes $2B for cybersecurity and focuses on transportation, energy, water districts, state, and local governments. It includes $100M for the Department of Homeland Security (DHS) and its Cybersecurity and Infrastructure Security Agency (CISA) to help companies prevent and address cyberattacks. Some of the funds are designated as follows – $1B for state and local grants to improve cybersecurity and critical infrastructure, $550M for electrical grid cyber and physical security efforts, $157K for DHS research. Ransomware Task Force recommendations include requiring companies to disclose if they pay ransom to resolve a cyberattack.

> *"Security is always excessive until it's not enough."*
> Robbie Sinclair, Head of Security, Country Energy, New South Wales, Australia"



Insight - Best practices for discovering your best security solutions

1. Gather a mixed group of stakeholders.
2. Ask for help from outside consultants.
3. Create a risk board of representatives.
4. Collect and review trends.
5. Increase the security IQ for all.
6. Adopt a security framework
7. Perform security assessments.
8. Implement a SIEM tool.
9. Firewalls, endpoint protection
10. Other data loss prevention measures
11. Implement multifactor authentication.
12. Embrace encryption.
13. Safeguard mobile devices, including BYOD.
14. Verify cloud security.
15. Ensure application security.
16. Prepare for rapid response.

DOJ Attacks Back Against REvil – Arrests and Seizure of $6.1M Ransom AND Knocks Them Offline

Department of Justice officials announced the arrests of five members of the ransomware criminal enterprise, REvil. REvil has been tied to over 7k ransomware attacks and hundreds of millions in ransoms, including the attack on meat supplier JBS and Miami-based technology company Kaseya. JBS paid $11M in ransom but Kaseya refused to negotiate with the cybercriminals. The arrests were part of an international investigation, Operation GoldDust, involving law enforcement agencies from 17 countries. Members of REvil were identified through wiretapping and seizure of REvil infrastructure – and, exploiting REvil tactics against its members.

Officials recovered $6.1M worth of cryptocurrency previously owned by Polyanin, who has also been indicted but not arrested (with extradition from Russia unlikely). Law enforcement agents recognize that seizure of millions squarely smacks REvil and serves as a deterrent to other attackers.

Working with the FBI, Romanian firm Bitdefender in September released a free decryptor for all REvil attacks that occurred before July 13.

"Since mid-September this year, the Sodinokibi/REvil decryptor has helped more than 1,400 companies in 83 countries recover their files and save over $550 million in unpaid ransom."

Bogdan Botezatu, Director of Threat Research, Bitdefender.

Tom Kellermann, Head of Cybersecurity Strategy at VMWare and an adviser to the U.S. Secret Service on cybercrime investigations, said, "The FBI, in conjunction with Cyber Command, the Secret Service and like-minded countries, have truly engaged in significant disruptive actions against these groups."“REvil was top of the list.” Kellermann credited this success as deriving from the determination by U.S. Deputy Attorney General Lisa Monaco that ransomware attacks on critical infrastructure should be treated as a national security issue akin to terrorism.

President Biden commented on the investigation, "We are bringing the full strength of the federal government to disrupt malicious cyber activity and actors, bolster resilience at home, address the abuse of virtual currency to launder ransom payments, and leverage international cooperation to disrupt the ransomware ecosystem and address safe harbors for ransomware criminals."

REvil may have been scamming some affiliates. Earlier this year, malware reverse-engineering specialists on the Russian-language Exploit cybercrime forum analyzed REvil samples and reported finding a backdoor that could be used by administrators to decrypt systems and files encrypted using the malware. Apparently, REvil's developers gave themselves a backdoor so they could negotiate directly with victims yet pretend to the responsible affiliate the victim had declined to pay.

Law enforcement and intelligence cyber specialists were able to hack REvil's computer network infrastructure, obtaining control of at least some of their servers. A leadership figure known as "0_neday," who had helped restart the group's operations after an earlier shutdown, said REvil's servers had been hacked by an unnamed party. "The server was compromised, and they were looking for me," 0_neday wrote on a cybercrime forum last weekend and first spotted by security firm Recorded Future. "Good luck, everyone; I'm off."

When gang member 0_neday and others restored those websites from a backup last month, he unknowingly restarted some internal systems that were already controlled by law enforcement.

“The REvil ransomware gang restored the infrastructure from the backups under the assumption that they had not been compromised,” Oleg Skulkin, Head of Digital Forsenics and Incident Response Team, Group-IB. “Ironically, the gang's own favorite tactic of compromising the backups was turned against them.”

PrivSec Global Virtual Cyberconference November 30-December 1

PRIVSEC GLOBAL
A GRC WORLD FORUMS LIVESTREAM EXPERIENCE

This year's PrivSec Global, virtual cybersecurity event, is scheduled for November 30-December 1. Ten key themes from last year's event include the following and are expected to be part of this year's conversation.

1) World events, such as the pandemic, provide a smorgasbord of opportunities for cybercrime. Accordingly, speakers highlighted the importance of international cooperation in defending against such attacks.
2) The rush to work from home and hybrid workplaces create vulnerabilities that need to be addressed, especially as these work models are expected to continue for the long-term.
3) There are risks and opportunities for businesses holding large amounts of unstructured data.
4) The need for cross-disciplinary connectness between privacy and security as part of corporate culture.
5) The importance of considering employee needs and motivation as companies increase reliance on machine learning.
6) The shift to cloud requires new approaches to risk, with trust more crucial than ever.
7) International data transfers are becoming a major concern.
8) There is strong support for a US federal privacy law
9) There is a cyber skills gap – in both education and culture.

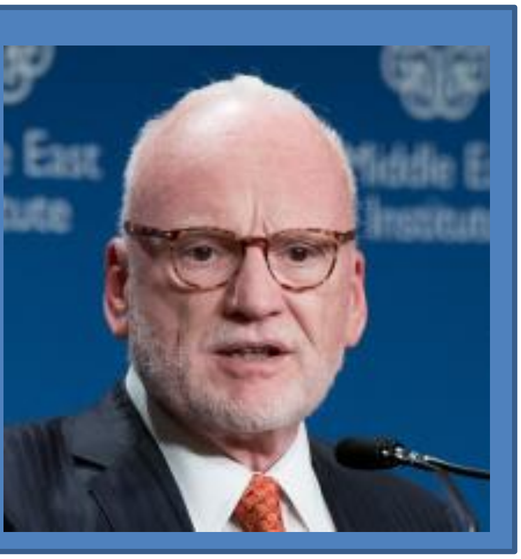
As Marcin Szczepanik, Head of Information and Data Security at Essar Oil UK, explains:

"From my experience, it's often about educating the business and HR what is a BIG deal about cyber and why cyber skills cannot be simply compared to any other engineering skills that they have had for 30 years. Also, it takes time to develop culture, awareness, and attractive environment for cyber talent. Let's face it, if the organization does not encourage transparency and privacy, you can't expect people to be driven to deliver state of the art cyber security posture. Also, how do you keep your staff to work for you if they don't feel that C-Level drive for cyber. And, finally, sourcing cyber talent is not easy either. Sometimes HR does not necessarily have experience in that friend and not many recruiters with relevant experience. It's all about determination of the individuals leading the infosec and privacy posture in your organization and the organization appreciating their often invisible work and dedication."

10) There is a strong desire for better training of workforces in data protection, privacy, and security.

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked."

Richard Clarke, Good Harbor Security Risk Management, CEO and former White House Cybersecurity Advisor



Accepting Nominations for 2022 Cybersecurity Leaders

SECURITY

Here is your opportunity to highlight those people making an impact in the industry.

Security and its partner for the Top Cybersecurity Leaders list, (ISC)^2, are looking for enterprise information security executives, who have made and continue to make significant contributions in the cybersecurity space to their organizations and/or the enterprise-level information security profession.

> We want leaders that are not only mitigating risk within their organizations and furthering the profession of cybersecurity, but those that are innovative, forward-thinkers and thought-leaders in the industry. The goal of the program is to highlight cybersecurity professionals who are making a difference in their organization and/or in the industry as a whole. Entrants and nominees do not need to be members of (ISC)^2 to apply to this program.

Nominations will be considered based on the overall positive impact that their work has had on their shareholders, organizations, colleagues and the general public.

This year's Top Cybersecurity Leaders will be honored in the March 2022 eMagazine of *Security* magazine and online.

Nominations are due by December 01, 2021. Send questions to *Security* Associate Editor Maria Henriquez at henriquezm@bnpmedia.com.

Muon Space Satellites to Create Meaningful Data Repository to Combat Climate Change

Muon Space will launch a fleet of satellites designed to analyze Earth's atmosphere, land, and water in fine detail using measurements from its own equipment and publicly available satellite data. Muon's satellites will use thermal infrared sensors, infrared spectroscopy, and low-frequency radar to gather data and apply its algorithms to existing image databases and calculating soil moisture levels, snow depth, and standing water in various locations. Their integrated remote sensing platform is expected to provide accuracy and integration of data to more effectively combat climate climate.

Early customers such as Tomorrow.io and Google are partnering with Muon to develop new mission-critical geophysical datasets, which have already resulted in catch businesses polluting protected areas. "In areas like agriculture where there are some bogus things going on, you can see something like waste discharge very clearly with these approaches," Jonny Dyer, CEO and cofounder of Muon Space, says. "When we look back in 20 years, it's going to be obvious that the only way markets can develop around this stuff and regulators can feel comfortable is if this is real and you have good data."

Muon's founders are veterans of the space industry. Jonny Dyer was the chief engineer of Skybox Imaging, a startup that created techniques to make satellites smaller and cheaper, purchased by Google in 2014. Dan McCleese, is the former chief scientist at NASA's Jet Propulsion Laboratory. Muon Space raised $10 million in seed funding led by Costanoa Ventures with participation from Space Capital, Congruent VC, Ubiquity Ventures, South Park Commons, and Climactic VC.

We at Muon Space believe partnering with the scientific community is a critical part of advancing the commercialization and the applicability of new space to climate.

Dan McCleese
Chief Scientist, Muon Space

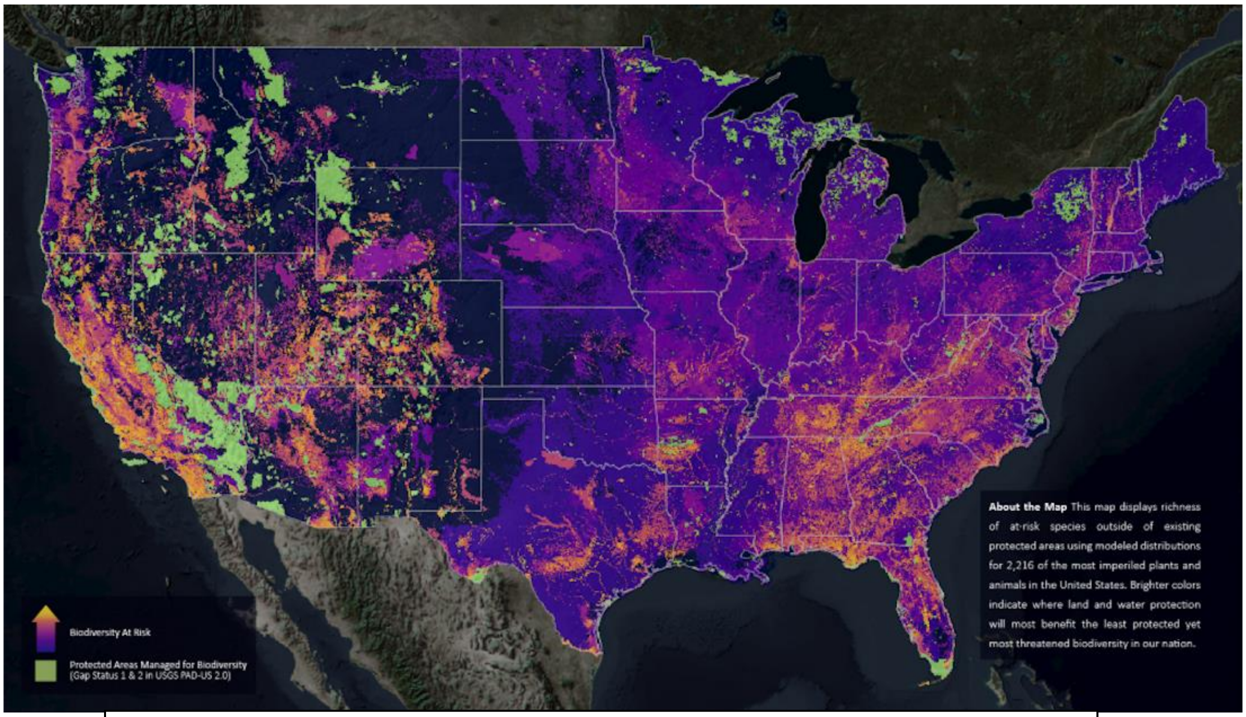
Historically, governments have openly shared much of the data gathered from their satellites. But working with the information has been tough. Much of their systems' technology predates any planning for the modern era of cloud computing and AI-based data analysis.

Commercial small satellite constellations offer a scalable, more cost-effective compliment to the large government systems but are not capable of the precise, scientific geophysical measurements needed for climate change applications. It's no longer enough for systems like these to count every tree on the Earth's surface; now they aim to measure each one's health, size, and species to compute their total biomass and ability to pull carbon dioxide out of the air.

Muon's goal is to build a single application to help companies do things like monitor the efficacy of their reforestation programs and allow regulators to prove which farmers are polluting certain rivers. "We think that over the next 10 years there's going to have to be a huge reckoning in terms of transparency around things like carbon credits and that we're going to need better data to adapt to climate changes," says Jonny Dyer. "We need to move from images of the planet to fundamental geophysical measurements."

Muon seeks to "fundamentally transform humanity's ability to address climate change and its impacts by deploying the world's most powerful scientific remote sensing satellite constellations."

Climate models disagree – often dramatically – and feedback mechanisms between parts of the biosphere (e.g. the impact of soil moisture on crop production) are still poorly modeled with incomplete, inconsistent data sets. Government bodies have been working to modernize their tech, but private industry tends to outpace their efforts.


Biodiversity At Risk
Protected Areas Managed for Biodiversity (Gap Status 1 & 2 in USGS PAD-US 2.0)

About the Map This map displays richness of at-risk species outside of existing protected areas using modeled distributions for 2,216 of the most imperiled plants and animals in the United States. Brighter colors indicate where land and water protection will most benefit the least protected yet most threatened biodiversity in our nation.

NatureServe's map on biodiversity shows that 90 percent of Americans live within 30 miles of an area of high biodiversity importance.

Microsoft, Google, and Amazon.com have built systems that gather public climate data. Microsoft Corp. plans to be carbon-negative by 2030, one of the most ambitious corporate climate pledges to date. “We are the largest participant in the carbon removal market today,” says Lucas Joppa, Microsoft’s chief environmental officer. “How in the world are we ever going to monitor and validate the removal that we paid for in any sort of scalable way? The answer lies in remote sensing.” Microsoft’s Planetary Computer is one of the biggest repositories of climate-related data. Joppa warns that many problems still exist around working with satellite data, including basic, painstaking work such as pulling subpar images from databases and finding the right algorithms to simplify complex scientific measurements. “This is not easy, and it’s not cheap if you want to extract meaningful information,” he says.

Joe Hamman, a research scientist at the National Center for Atmospheric Research, says technological innovations could prove a distraction at a time of extreme urgency for climate-related work because of the piecemeal approach. “I don’t want to downplay what people are trying to do, but there are marginal benefits on many of these things,” he says. “There are fundamental challenges that we face with the climate that don’t go away because we have a new satellite or a clever way of doing accounting.” Muon Space provides a comprehensive, more accurate methodology to meet these climate objectives.

“As inhabitants of Earth, we are deeply passionate about facing these challenges head-on. As engineers and scientists, we see a clear opportunity to realize the promise of New Space to revolutionize our visibility into Earth’s Systems. As people, we are all at a place in our lives where we can’t imagine a better field to dedicate our time and energy to.” Jonny Dyer, Muen Space, CEO. *“There are rare moments in life when the stars align — moments where there is a confluence of people, passion, and opportunity that fit together perfectly.* “Creating Muon feels like one of those rare, stars-aligned moments.”

Poll Results for Cloud Service Providers: Is Public Cloud, Private Datacenter, or Hybrid Right For You?

with Sponsors Lightbits and Netlist

What do you see as the greatest tradeoff between on-premises storage, cloud storage, and a hybrid model (check one):

Overall Cost:	13%
Cost Predictability:	25%
Performance:	21%
Performance Predictability:	13%
Security/Data Privacy:	17%
Other Concerns:	0%
No concerns/no opinion:	13%

What are the biggest impacts of maintaining an on-premises datacenter as a cloud services provider (check all that apply):

CapEx costs:	45%
Staffing costs and expertise:	36%
Security concerns:	27%
Coordinating datasets across multiple datacenters:	32%
Don’t know/no opinion:	27%

G2M Research Multi-Vendor Webinar Series

Our November 9 webinar, sponsored by Weka, KIOXIA, and NetApp, "The Explosion in Radiometry,Cryo-EM, and other Imaging Technologies: Can Storage Keep Pace?" is available to view here, along with a copy of the slidedeck here.

November 17, KIOXIA presented the second webinar in their four-part webinar series, "The Next Flash Revolution at Scale: Open Source Software + Software-Enabled Technology." Each webinar stands alone and collectively provides an overview of the innovation, direction, and leadership KIOXIA provides in this enterprise storage space. The video is available to view and a copy of the slidedeck is available here. KIOXIA webinar Part 1, "Why Flash Memory At Scale Should be Software-Defined" is available to view here along a copy of the slidedeck here.

Our webinar schedule is below. Click on the topics to get more information about that specific webinar. You can view all our webinars and access all the slide deck presentations. To sponsor any of our webinars, contact G2M for a prospectus.

Dec 14:	2021 Enterprise Storage Wrap-up Panel Discussion
Feb 1:	Storage Architectures for High-Performance Computing
Feb 15:	Cybersecurity: Zero Trust or Trust Your People
March 8:	Storage Architectures for AI & ML
March 29:	Storage Technologies for Datacenters in Space
April 26:	Effective Architectures for Edge Computing & Storage
May 24:	Data, Networking, & Storage Acceleration
June 21:	Scaling Storage Capacity & Bandwidth Effectively
July 19:	Hot Semiconductor Startups: Changing the Rules
Aug 23:	Advanced NVMe SSDs
Sept 13:	Public/Private Storage Architectures for CSPs
Oct 11:	Storage Fabrics for Mega-Datacenters
Nov 8:	Securing Cloud Datacenters Resources
Dec 13:	What was Hot (or Not) in 2022, and Predictions for 2023

Conferences

November 29- Dec 3	Amazon re:Invent, Vegas
November 30- Dec 1	PrivSec Global, Virtual
January 5-8	CES 2022, Vegas
Jan 11-13	FloCon 2022, Virtual
January 26-28	SNIA 2021 Annual Members Symposium, Virtual
January 27- Feb 5	Cyber Threat Intelligence Summit & Training, Bethesda
February 2-4	IT DEFENSE 2022, Berlin
February 7-10	RSA Conference, San Francisco & Virtual
February 7-11	Cisco Live, Amsterdam
February 8-11	ITExpo, Fort Lauderdale
February 14-15	Gartner Security & Risk Management Summit, Dubai
February 17-18	Deep Learning Hybrid Summit, San Fran & Virtual
February 28- March 3	MWC Barcelona
March 2-3	Big Data & AI World, London
March 2-3	Cloud Expo Europe, London
March 11-12	SXSW 2022, Austin
March 14-16	Gartner Identity & Access Management, Vegas
March 14-17	Gartner Data & Analytics Summit, Orlando
March 23-24	Paubox SECURE 2022, Vegas
March 28-31	Data Center World, Austin
April 19-21	ODSC East, Boston
April 23-27	NAB, Vegas

May 4-5	World Summit AI Americas, Montreal
May 9-11	Gartner Data & Analytics Summit, London
May 10-13	Black Hat Asia, Singapore
May 11-12	AI & Big Data Expo, Santa Clara
May 18-19	Gartner Digital Workplace Summit, London
June 7-10	Women in Tech Global Conference 2022, TBA & Virtual
June 12-16	Cisco Live, Vegas
June 14-16	Digital Enterprise Show, Malaga
June 21-22	Gartner Security & Risk Management Summit, Sydney
June 21-22	Gartner Digital Workplace Summit, San Diego
June 29- July1	Mobile World Congress, Shanghai
August 6-11	Black Hat USA, Vegas
August 11-14	DEF CON 30, Vegas
September 19-20	Industry of Things World, Berlin
September 28-29	IoT World, Santa Clara
October 5-6	Evolve, Vegas
November 18-19	Data Strategy & Insights (Forrester Research), Virtual
December 1-2	AI & Big Data Expo Global, London