G2M RESEARCH

AI & CYBERSECURITY NEWSLETTER

APRIL 2021

Highlights

Fusion Centers: Social Media, Blue Leaks, & Suspicious Activity Reporting; 2 Views - ACLU versus NSA

Speaking of Mark Zuckerberg… Signal versus WhatsApp

Sometimes It Does Not Pay To Be #1 – Acer Hit With Highest Ransomware Demand to Date - $50M

Some of our most substantive discussions happen in our narrow topic webinars. Consider attending both – a broad topic for a big picture look at successful approaches and some narrow subjects that dig deep into processes and solutions.

Our March webinar with Panasas, NGD Systems, Weka, and NetApp was an especially substantive, deep dive discussion. The webinar is available on our website and YouTube but I am attaching the slides here because of the depth and breadth of material - very informative. The session included a presentation by Dr. Andrew Bartko regarding the use of AI to monitor COVID-19 markers in wastewater at UCSD.

We are expanding our webinar schedule to include a webinar on cybersecurity, Tuesday, April 27 at 9:00am – "How to Take a 360 Degree View of Your Organization's Cybersecurity."

If you are interested in sponsoring a webinar but don't see a topic that quite fits your needs, we can modify topics or add topics to meet your objectives.

Cheers! Mike Heumann

“How to Take a 360 Degree View of Your Organization’s Cybersecurity”

Tuesday, April 27
9:00am

SecurityScorecard

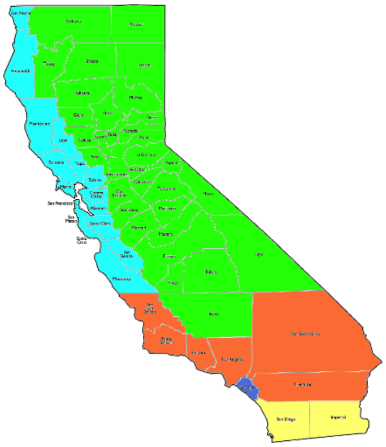
Fusion Centers:

Social Media, Blue Leaks, & Suspicious Activity Reporting

2 Views – ACLU versus NSA

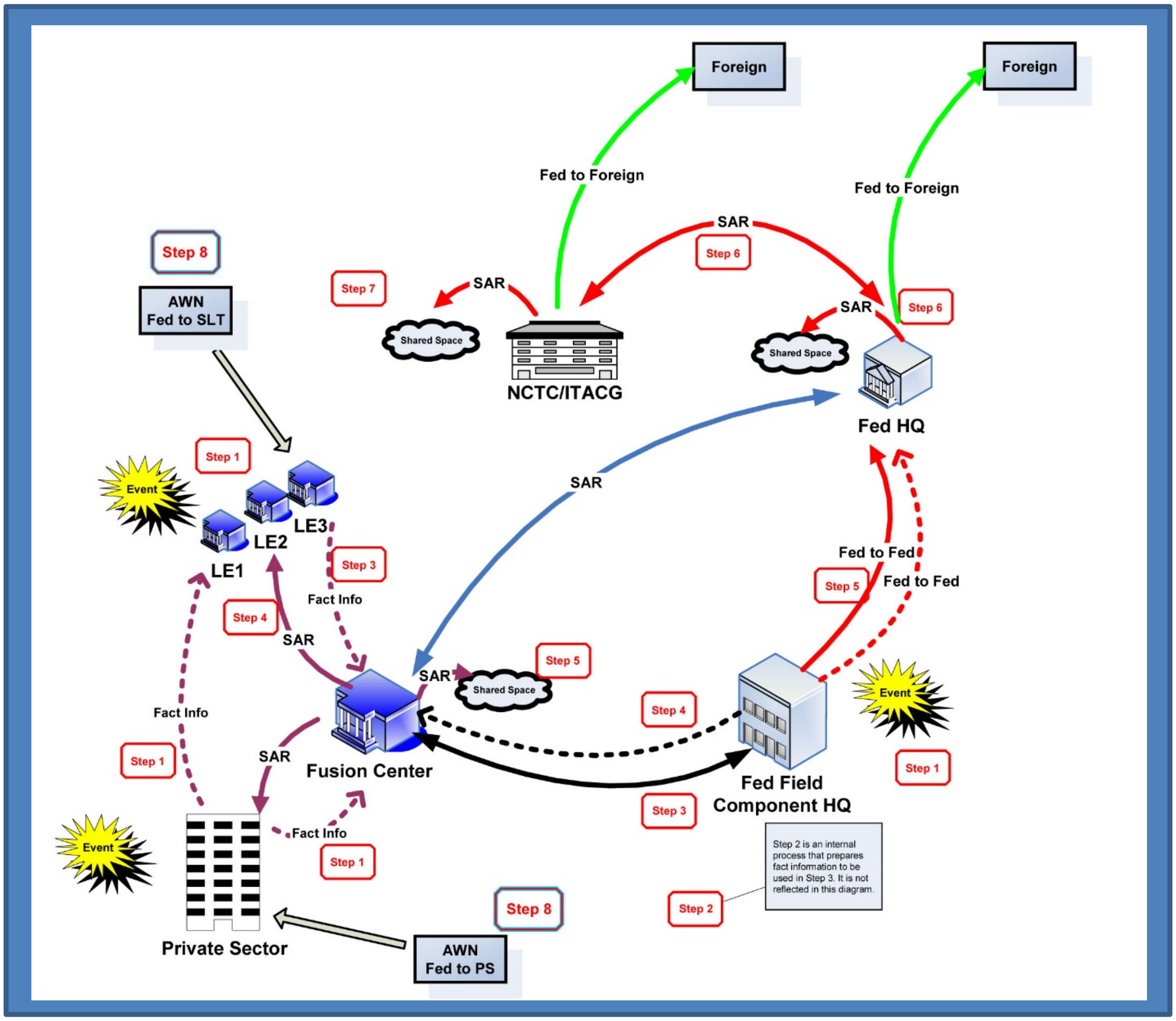
Where there is collection of data, there is always the prospect of great use and/or bad abuse.

And, much of the data culled has been packaged and delivered directly from the individual user, via social posts about getting vaccinated, vacation plans, new purchases, 10 year challenge photos (assisting in AI facial recognition), attendance at protests, and check-ins at every restaurant, workout, and airport - complete with selfies, food photos, and Fitbit results.



The Orange County Intelligence Assessment Center (OCIAC) monitors, stores, and analyzes massive amounts of internet communications including social media. Recent data analysis led OCIAC to identify seven members of The Base, a violent neo-Nazi white supremacist group, resulting in arrests in four states on charges including conspiracy to murder a Barstow couple and plans to overthrow the US government.

After 9/11, intelligence hubs were created to share anti-terrorism intelligence between local, state, and federal law enforcement agencies. The scope of these 80 fusion centers, each created independently, has expanded in scope to “detecting, deterring, disrupting, preventing, and mitigating the impact of drug activity, active shooters, transnational organized crime, cybercrimes, acts of terrorism, and other manmade and natural disasters” and are designed to “continuously collect data.”



Step 2 is an internal process that prepares fact information to be used in Step 3. It is not reflected in this diagram.

Fusion centers gained attention recently after Black Lives Matters protests. A massive data leak, called “the Blue Leaks”, of over a million files of highly sensitive FBI, law enforcement, and fusion center files, was published online, including 24 years of data stolen from 251 law enforcement websites. The data showed close monitoring of protests and BLM organizers. In Milwaukee, protestors identified from videos posted on social media received tickets in the mail for breaking curfew during the protests. Inspector Formolo explained that any social medial information accessed by Milwaukee’s Virtual Investigations Unit (VIU) is all open-source material, “Our guys are just pretty good at knowing how to go about connecting dots and stuff. That why we call it ‘social network analysis.’”

The Blue Leaks include personal information for police officers, such as name, rank, agency, email, home address, and cell phone number. Some files include ACH routing numbers, international bank account numbers, and other financial data. There are reasonable concerns that individual officers could be harmed as a result of the data breach.

Ilia Lolochenko, Founder and CEO of ImmuniWeb security company, expressed his concerns regarding publication of this largest hack of US law enforcement agencies, “The eventual outcome of this leak will likely have disastrous effects for many innocent people. First, it will likely inflict irreparable reputational, financial and even physical harm to suspects and people charged with crimes who later were acquitted in a court of law.”

Fusion Centers are owned and operated by state and local entities with support from federal partners in the form of training, security clearances, and Homeland Security grants. In early 2012, the Foreign Intelligence Surveillance Court approved sharing raw NSA data with the National Counterterrorism Center (NCTC) which oversees the intelligence community, including the Department of Homeland Security, FBI, and federal fusion center partners.

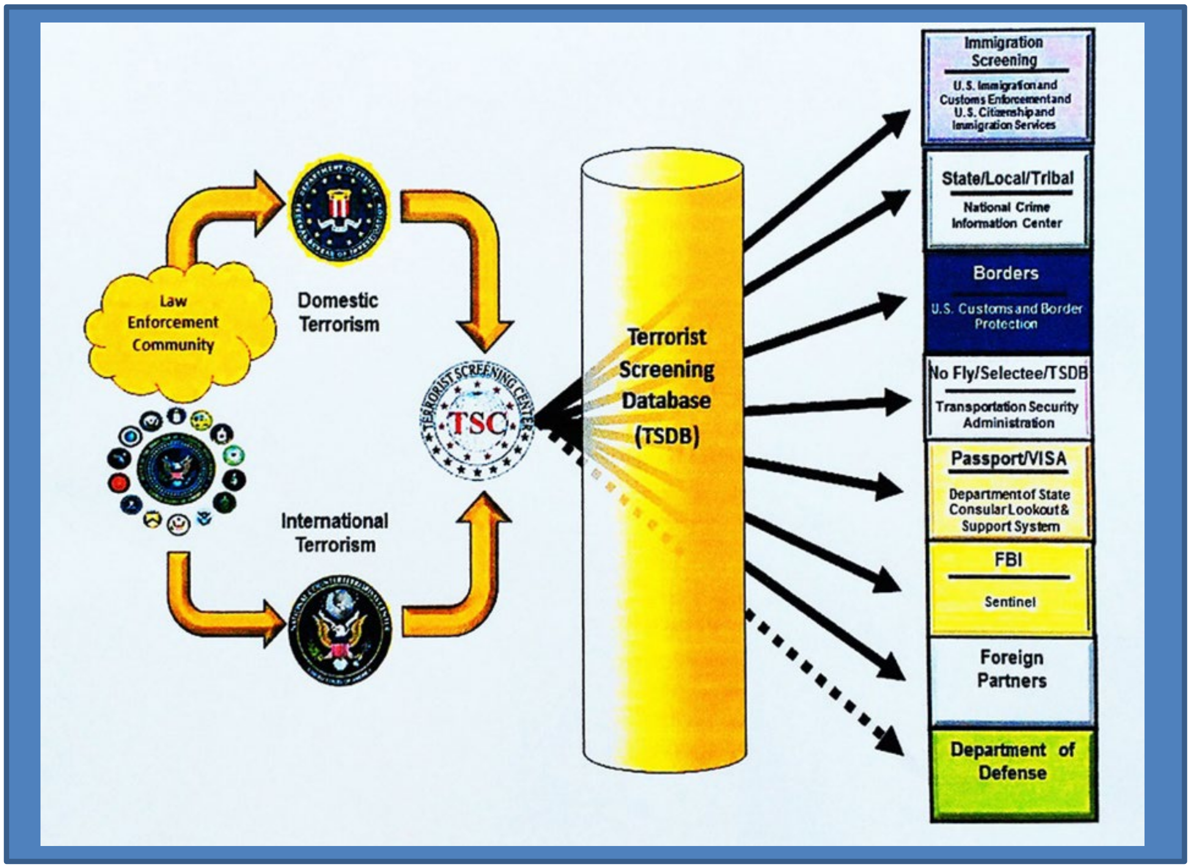
Excerpt, 3 Ways to Improve Fusion Center Intelligence for Local Agencies:

“Data has a shelf life and must remain complete and timely. Incomplete data sets can cause certain criminal activities to be underrepresented, which can lead to law enforcement agencies either over- or underestimating threats and ineffectively allocating resources. Data must also be fresh and relevant; agencies can’t afford to rely on outdated information, especially when dealing with rapidly unfolding events. Yet keeping data for historical learning and longitudinal studies its also important.”

Gretchen Stewart, Chief Data Scientist, Intel Public Sector
Juan Colon, Advisory Industry Consultant, SAS Institute

The ACLU has expressed concerns that “[t]here appears to be at least some conscious effort to circumvent public oversight by obscuring who is really in charge of these fusion centers and what laws apply to them” finding that federal authorities reap the benefits of working with the centers but avoid responsibility. And, because some state have stronger privacy or open-records laws than the federal government, fusion centers can manipulate who owns the records or where they are officially held to avoid stricter privacy protections. “Since no two fusion centers are alike, it is difficult to make generalized statements about them. Clearly not all fusion centers are engaging in improper intelligence activities and not all fusion center operations raise civil liverties or privacy concerns. But some do, and the lack of a proper legal framework to regulate their activities is troublesome.”

The National Security Agency (NSA) has strategic partnerships with 80 major global corporations including AT&T, DXC, HP, Qwest, Motorola, Cisco, Qualcomm, IBM, Oracle, Intel, Microsoft, and Verizon to provide hardware, network infrastructure, application software, and operating system support. The NSA collects data from internet searches, websites visited, emails sent and received, social media activity, blogging, videos watched and/or uploaded, photos viewed and/or uploaded, cell phone apps and GPS, phone call records, text messages, Skype calls, online purchases, credit card transactions, financial information, legal documents, travel documents, health records, cable shows watched and/or recorded, commuter toll roads, electronic bus and subway passes, Smart passes, facial recognition data from surveillance cameras, educational records, arrest records, driver’s license, and DNA.


Law Enforcement Community
Domestic Terrorism
International Terrorism
TSC
Terrorist Screening Database (TSDB)
Immigration Screening
U.S. Immigration and Customs Enforcement and U.S. Citizenship and Immigration Services
State/Local/Tribal
National Crime Information Center
Borders
U.S. Customs and Border Protection
No Fly/Selectee/TSDB
Transportation Security Administration
Passport/VISA
Department of State Consular Lookout & Support System
FBI
Sentinel
Foreign Partners
Department of Defense

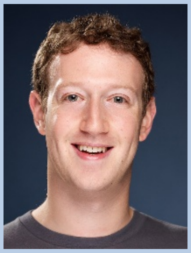
Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), led by the US Department of Justice, Department of Homeland Security, FBI, and state and local law enforcement agencies, collects and processes fusion center data including from tips provided by citizens. These tips are used to initiate investigations. The reportable behaviors listed in the National SAR standards include taking photos of buildings "in a manner that would arouse suspicion in a reasonable person." The problem may lie in the fact that some people are more reasonable than others.

SAR reporting has had great success in financial crimes including bank fraud and money laundering. In one case, investigators were able to uncover a fraudulent investment scheme in southern California that robbed hundreds of investors, mostly Filipino immigrants, of over $25M. Alternatively, some of reported activities include middle eastern males purchasing pallets of water and Chinese nationals taking photos of the Folsom Dam. Notably, there have been numerous cases reported of people reporting criminal activity against blacks, where video and witness testimony clearly demonstrate otherwise, including a woman trying to prevent a black man from entering his own condominium.

The ACLU concerns about fusion centers center around privacy, racial and ethnic profiling, and SAR abuses. In the view of the NSA, "If you have nothing to hide, you have nothing to fear." The truth probably lies somewhere in between the two.

But, bottom line, at least this time, you cannot blame it entirely on Mark Zuckerberg.

Speaking of Mark Zuckerberg… Signal versus WhatsApp



Well, this is fun news. A hack reveals that Mark Zuckerberg uses his competitor's product, Signal, despite owning WhatsApp. A 2019 Facebook hack of 533M user's personal information found that Mark Zuckerberg prefers using the secure application, Signal. The Facebook leak is one of the biggest leaks in history, including phone numbers, emails, photos, and data from over 106 countries for 533M users.

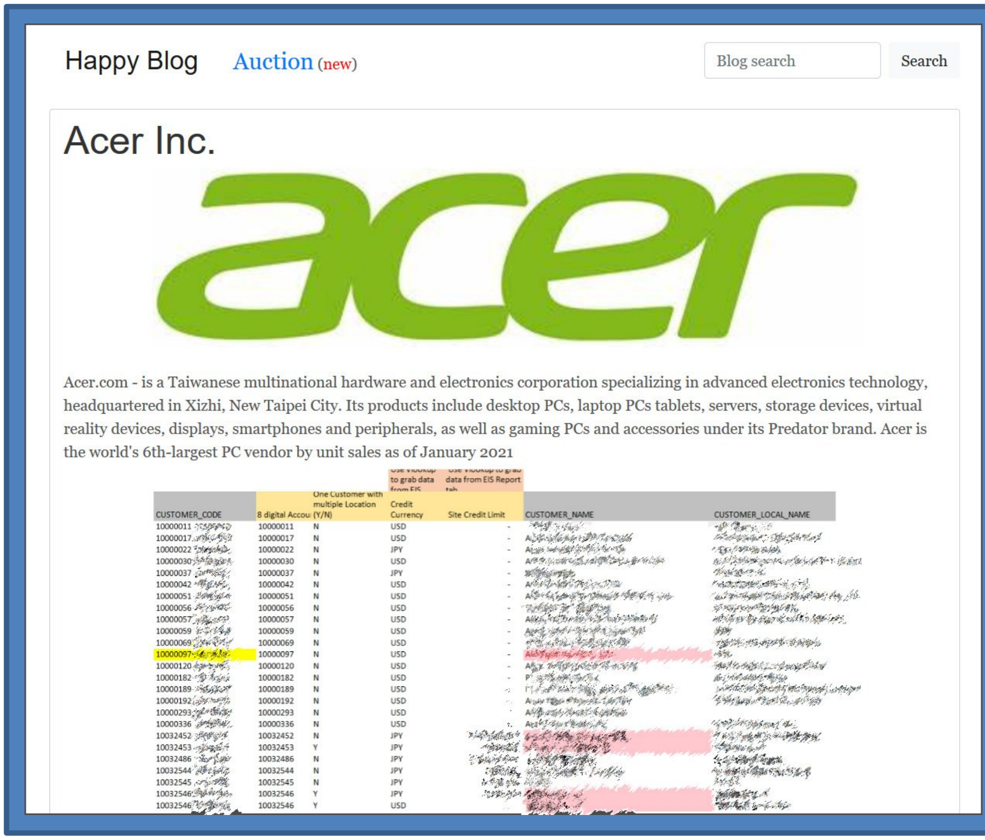
After the news broke of Zuckerberg's supposed use of Signal, the company retweeted a link to the story writing: "With the May 15th WhatsApp Terms of Service acceptance deadline fast approaching, Mark leads by example." Gotcha. Do as I do, not as I sell/own.

Sometimes It Does Not Pay to Be #1 – Acer Hit With Highest Ransomware Demand to Date - $50M

Hackers gained access to Acer via a Microsoft Exchange vulnerability and has demanded $50M in ransomware. The group behind the attack is REvil, which is believed to be an offshoot of hackers, GandCrab. REvil gang ransomware demands vary greatly, based on the annual revenue of the hacked company. Taiwanese electronics and computer maker, Acer, has 7k employees and earned over $7.8B in 2019. The ransomware demand was set to increase to $100M after March 28. There is no available news whether Acer paid the demand or is in negotiations with the cybercriminals.

"Acer routinely monitors its IT systems, and most cyberattacks are well defensed. Companies like us are constantly under attack, and we have reported recent abnormal situations observed to the relevant law enforcement and data protection authorities in multiple countries."

"We have been continuously enhancing our cybersecurity infrastructure to protect business continuity and our information integrity. We urge all companies and organizations to adhere to cybersecurity disciplines and best practices and be vigilant to any network activity abnormalities." - Acer.



Acer Inc.

Acer.com - is a Taiwanese multinational hardware and electronics corporation specializing in advanced electronics technology, headquartered in Xizhi, New Taipei City. Its products include desktop PCs, laptop PCs tablets, servers, storage devices, virtual reality devices, displays, smartphones and peripherals, as well as gaming PCs and accessories under its Predator brand. Acer is the world's 6th-largest PC vendor by unit sales as of January 2021

			Use vlookup to grab data from EIS	Use vlookup to grab data from EIS Report tab		
CUSTOMER_CODE	8 digital Accou	One Customer with multiple Location (Y/N)	Credit Currency	Site Credit Limit	CUSTOMER_NAME	CUSTOMER_LOCAL_NAME
10000011 [redacted]	10000011	N	USD	-	[redacted]	[redacted]
10000017 [redacted]	10000017	N	USD	-	[redacted]	[redacted]
10000022 [redacted]	10000022	N	JPY	-	[redacted]	[redacted]
10000030 [redacted]	10000030	N	USD	-	[redacted]	[redacted]
10000037 [redacted]	10000037	N	JPY	-	[redacted]	[redacted]
10000042 [redacted]	10000042	N	USD	-	[redacted]	[redacted]
10000051 [redacted]	10000051	N	USD	-	[redacted]	[redacted]
10000056 [redacted]	10000056	N	USD	-	[redacted]	[redacted]
10000057 [redacted]	10000057	N	USD	-	[redacted]	[redacted]
10000059 [redacted]	10000059	N	USD	-	[redacted]	[redacted]
10000069 [redacted]	10000069	N	USD	-	[redacted]	[redacted]
10000097 [redacted]	10000097	N	USD	-	[redacted]	[redacted]
10000120 [redacted]	10000120	N	USD	-	[redacted]	[redacted]
10000182 [redacted]	10000182	N	USD	-	[redacted]	[redacted]
10000189 [redacted]	10000189	N	USD		[redacted]	[redacted]
10000192 [redacted]	10000192	N	USD		[redacted]	[redacted]
10000293 [redacted]	10000293	N	USD		[redacted]	
10000336 [redacted]	10000336	N	USD		[redacted]	[redacted]
10032452 [redacted]	10032452	N	JPY	[redacted]	[redacted]	[redacted]
10032453 [redacted]	10032453	Y	JPY	[redacted]	[redacted]	[redacted]
10032486 [redacted]	10032486	N	JPY	[redacted]	[redacted]	[redacted]
10032544 [redacted]	10032544	N	JPY	[redacted]	[redacted]	[redacted]
10032545 [redacted]	10032545	N	JPY	[redacted]	[redacted]	[redacted]
10032546 [redacted]	10032546	Y	JPY	[redacted]	[redacted]	[redacted]
10032546 [redacted]	10032546	Y	USD		[redacted]	[redacted]

The cybercriminals posted screenshots to prove they gained access and warned Acer "to not repeat the fate of the SolarWind."

AI & Cybersecurity Events – All Virtual

April 14	Denver Cyber Security Summit 2021
April 15	INTERFACE Alaska 2021
April 19-21	World Summit AI - Montreal
April 20-21	Data Connectors Chicago Cybersecurity Summit
April 22	SecureWorld Southeast 2021
April 27	IAPP Global Privacy Summit 2021
April 27	CyberNow Summit 2021
April 27-28	ISMG Virtual Cybersecurity Summit: Midwest
April 27	CypherCon 5.3
April 28-29	Gartner Identity & Access Management Summit
May 3	IEEE International Conference on Networking, Architecture & Storage
May 4	ISMG Virtual Cybersecurity Summit: Pacific Northwest
May 4-6	ISACA Conference North America 2021
May 4-6	Gartner Data & Analytics Summit
May 5	FutureCon Washington DC 2021

G2M Research Multi-Vendor Webinar Series

Our March webinar "One Year after COVID-10: How Did Storage Architectures Perform for Biotech AI Modeling & What Can We Learn From This?" was sponsored by Panasas, (Adam Marko, Andrew Bartko), NGD Systems (Scott Shadley), Weka (Greg Mazzu), and NetApp (Esteban Rubens). You can view the webinar here and a pdf of the slides here.

Our 2021 webinar schedule! Click on any of the topics to get more information about that specific webinar. Interested in Sponsoring a webinar? Contact G2M for a prospectus.

April 27:	How to Take a 360 Degree View of Your Organization's Cybersecurity
May 18:	Responsive and Efficient Storage Architectures for Social Media
June 15:	It's 2021 - Where Has NVMe-oF™ Progressed To?
July 13:	Computational Storage vs Virtualized Computation/Storage in the Datacenter: "And The Winner Is"?
Aug 17:	AI/ML Storage - Distributed vs Centralized Architectures
Sept 14:	Composable Infrastructure vs Hyper-Converged Infrastructure for Business Intelligence
Oct 12:	Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?
Nov 9:	The Radiometry Data Explosion: Can Storage Keep Pace?
Dec 14:	2021 Enterprise Storage Wrap-up Panel Discussion

G2M RESEARCH