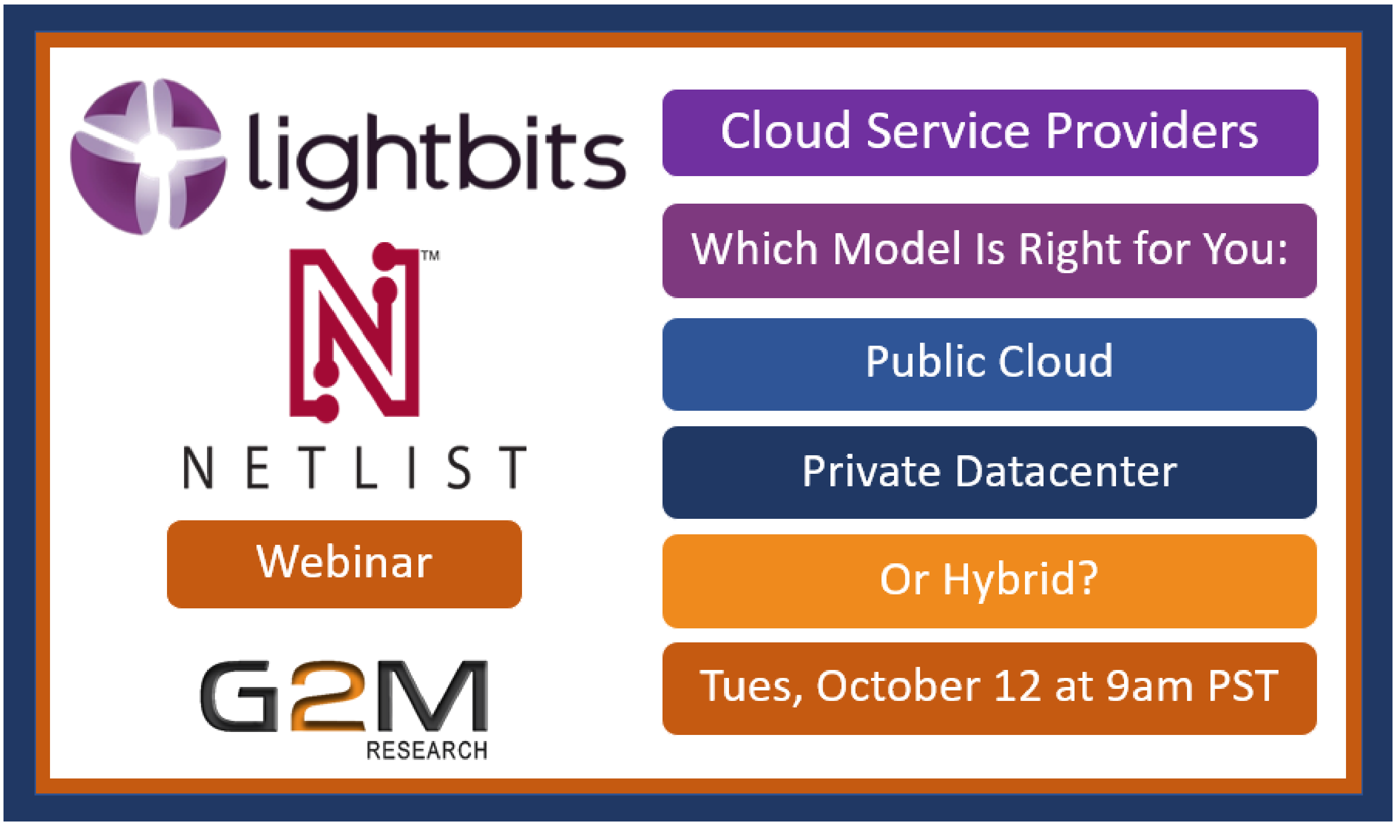
Highlights

- Most Expensive Take-Out: $5.9M Ransomware Attack on Food Supply
- Japan is Done “Playing Nice” with China; Goes on Offensive Against Cyber Attacks
- Winner: Port of Houston; Loser: Wannabe Hackers
- Influx of Conti Ransomware & Disgruntled Affiliate Publishes Conti Gang IP Addresses
- Amazon’s $1500 Robotic Dog, Astro
- Poll Results: “Advanced SSDs – PCIe Gen4, U.3, and New Form Factors”

To maximize efficiencies, improve services, and advance technology, industries look more and more to artificial intelligence, particularly machine learning. Interconnectivity, and resource management are integral to optimizing the utility of this data. Our essential services and those interrelated infrastructures are vulnerable to cybersecurity attack because they are data-rich environments and the value of the maintaining essential services – hospitals and electrical grids - makes them desirable targets for ransom demands. This newsletter looks at some of those vulnerabilities.

Our G2M Multi-Vendor Webinar Series 2022 schedule is available at the end of our newsletter and on our www.g2minc.com website. We have some exciting topics coming up. We also provide a list, with links, of upcoming conferences, although most continue to be virtual.

Cheers! Mike Heumann



Most Expensive Take-Out: $5.9M Ransomware Attack on Food Supply

Darkside and REvil ransomware groups spawned BlackMatter, an evil ransomware group claiming to have inherited the best features of its parent organizations. BlackMatter attacked NEW Cooperative Inc., shut down its operations, and demanded $5.9M ransom.

NEW Cooperative, Inc is a member-owned farmer cooperative with 60 operating locations throughout north, central and western Iowa. They have been in business since 1973 and generate over $424M annual revenue. NEW Cooperative Inc, operates grain storage elevators, buys crops from farmers, sells chemicals, and owns technology platforms for farmers that provide agronomic advice to maximize harvest. Their software provides for management of 40% of grain production and 11 million animals feed schedules. The company created temporary workarounds to receive grain and distribute feed.

That same week, Crystal Valley Farm Coop announced it the target of a ransomware attack which disrupted company operations, including disabling payment systems using major credit cards, though local cards continued to work. Crystal Valley Farm Coop is a Minnesota farm supply and grain marketing cooperative which serves 2500 farmers and livestock producers. They operate eight grain elevators with the capacity to store 25 million bushels. No public information has been provided to say whether or not this was another BlackMatter attack and how much ransom was demanded.

Currently, there is a global shortage of truck drivers making delivery reliability challenging. In the agricultural industry, delivery delays equate to wasted crops. Cyberattacks obviously wreak havoc on production and delivery times. And, these attacks are hitting as growers near their Autumn harvest. NEW Cooperative has said they will not pay any ransom.

The workarounds by NEW Cooperative is a positive takeaway according to cybersecurity expert, Jacobson. *"The companies need to go into the assumption, play the what-if game. What if this happened to us? What has to come back alive and how are we going to make that happen? If it's bringing out note cards and number two pencils and clipboards, then that's what it is. It may be being able to run things manually."*

Doug Jacobson, Professor, Iowa State University
Owner, Palisade Systems

Japan is Done “Playing Nice” with China; Goes on the Offensive Against Cyber Attacks

To be fair, Japan is on the offensive against China, Russia, and North Korea, saying all three are main threats to its cybersecurity because they undertake hostile activities in the area. China considers its inclusion in Japan’s national cybersecurity strategy as based on unfounded threats. But, Japan says China is stealing sensitive defense and advance technology information. They do add that Russia is suspected of leading hostile operations for political or military purposes. Not reduced just to words, the Japanese include “tough countermeasures using every effective means and capability available” as the approach going forward.

Police Chief Mitsuhiro Matsumoto officially identified Chinese hacker group, Tick, as responsible for cyberattacks on Japan. And, Tokyo Metropolitan Police Department filed a case against a Chinese systems engineer for attacks targeting the Japan Aerospace Exploration Agency and 200 Japanese companies and research institutions. Based on a fake ID used by the engineer to register a web server in Japan for attacks against JAXA, police believe the China’s People’s Liberation Army was involved in the attacks.

China argues the strategy as “baseless slander” against both Russia and China. And, Chinese Foreign Ministry spokesperson Wang Wenbin argued, “Groundless speculations should be avoided. As a matter of fact, the US is the biggest empire of hacking and tapping as we all know. China firmly rejects any organization or country throwing mud at China under the pretext of cyber security or using the issues to serve their political purposes.”

Police Chief Matsumoto said he has evidence, including witness testimony.

A press release by Press Secretary Yoshida Tomoyuki, includes the following:

1. Security of cyberspace is extremely important to ensure peace and prosperity of the international community including Japan, and it was reaffirmed at the recent G7 Leaders’ Summit held in the United Kingdom.
2. Against this backdrop, on July 19th (local time), the United Kingdom, the United States and other countries issued public statements including on a group conducting cyberattacks known as APT40 which the Chinese government is behind, and an indictment charging four members of APT40 has been issued in the United States. Japan also assesses that it is highly likely that the

Chinese government is behind APT40 and has been paying close attention with deep concern to these attacks by APT40 and others which threaten the security of cyberspace. Japan strongly supports the public statements by the United Kingdom, the United States and other countries which express the determination to uphold the rules-based international order in cyberspace.

3. Japan recently made the announcement on cyberattacks in which it is highly likely that an Advanced Persistent Threat group called Tick, which the Unit 61419 of the Chinese People's Liberation Army is behind, was involved. Japan further confirmed that Japanese companies were also targeted in the aforementioned case by the group known as APT40.
4. Malicious cyber activities that could potentially undermine the foundation of democracy embodied by free, fair and secure cyberspace cannot be condoned. The Government of Japan considers it to be a matter of strong concern from the national security viewpoint, firmly condemns and will take strict measures against these activities.
5. Japan will continue to closely cooperate with the international community including the G7 countries and make efforts in order to develop free, fair and secure cyberspace.

Winner: Port of Houston

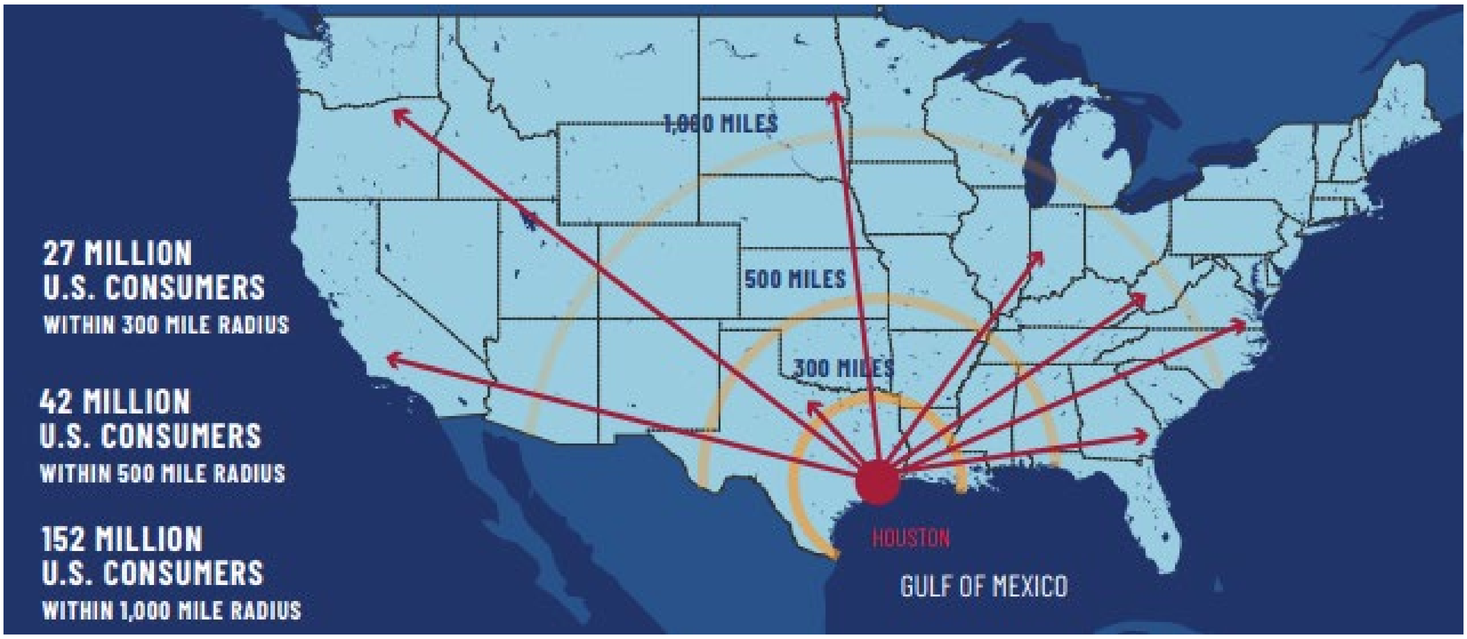
Loser: Wannabe Hackers

The Port of Houston used it Facilities Security Plan to successfully block a cybersecurity attack. Hackers exploited a vulnerability in password management software and installed malicious code. However, the breach was detected and these hackers were unable to cause any disruption to systems and services and no operational data was compromised. Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly attributes the attack to a "nation-state actor."

The Maritime Transportation System includes 95,000 miles of coastline, 361 ports, and over 25,000 miles of waterways and intermodal landside connections. CISA identified six port facility cyberattack risk areas: 1) facility access – disruption of serves used to direct cargo, 2) terminal headquarters – data breaches of sensitive client and caro information, 3) ransomware – including manipulation and destruction of data, 4) operational technology systems – interruption of communications used to control physical processes such as pumps and cargo handling equipment, 5) positioning, navigation, and timing – could result in accidents, damage to infrastructure, release of hazardous materials, 6) vessel – impacts to interconnectivity between vessels and facilities.

Recent notable port attacks include a July 2017 cyber attack on A.P. Moller Maersk, a Danish integrated shipping company and largest container shipping line and vessel operator in the world since 1996. The attack called "Peyta" reached shipping and ports, affected 17 hacked terminals around the world, and resulted in a loss of $200-300M. In July 2018 Cosco Shipping-affiliated terminal at the Port of Long Beach had a ransomware attack. The Barcelona Port Authority and the Port of San Diego both were attacked in September 2018.

Ninety percent of overseas trade enters or leaves the United States by ship. The twenty five mile Port of Houston complex handles 69% of Gulf Coast container traffic and is the largest port in Texas with 96% market share in containers, handling around 247 million tons of cargo each year. The Port of Houston owns and operates eight public terminals to serve domestic and international customers and includes a constellation of 6,500 acres of properties.



Influx of Conti Ransomware & Disgruntled Affiliate Publishes Conti Gang IP Addresses

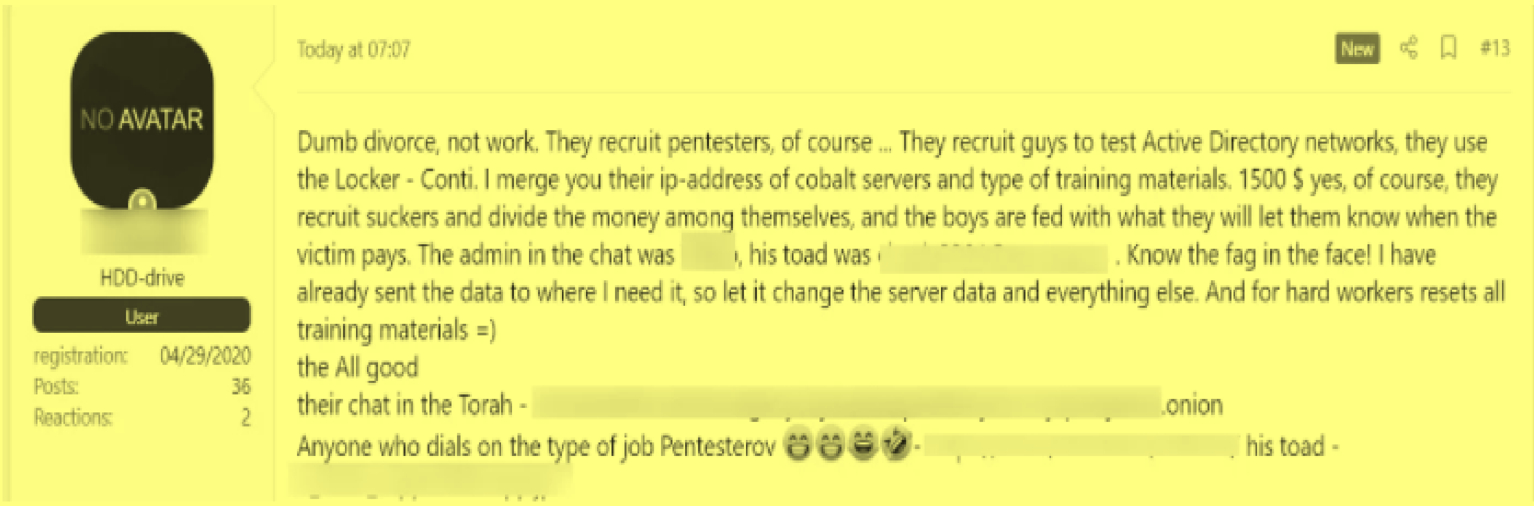
The FBI and Cybersecurity and Infrastructure Security Agency (CISA) issued an alert regarding the influx of Conti ransomware, citing over 400 attacks on U.S. and international organizations.

Conti ransomware gangs have largely targeted organizations where IT outages can have devastating consequences including hospitals, 911 dispatch carriers, and law enforcement agencies. They have made ransom demands for as much as $25M and they do not always return data after being paid. One of the biggest leaks by Conti was of 3 GB of data from Advantech, a chip manufacturer.

The FBI and CISA caution that Conti actors gain initial access to networks through spear phishing campaigns using targeted emails that contain malicious attachments or links, stealing remote desktop protocol credentials, phone calls, fake software promoted as search engine optimization, and other vulnerabilities in external assets. Conti hackers run a getuid payload then a more aggressive payload, and Kerberos attacks for triggers the Admin hash to conduct brute force attacks. They employ tools already available on the victim network and add tools to escalate privileges. After stealing and encrypting data, the hackers demand the victim pay a ransom for release of the encrypted data and threated the victim with public release of data if the ransom is not paid.

Recommended mitigations include multi-factor authentication, network segmentation and filter traffic, scan for vulnerabilities, keep software updated, remove unnecessary applications and apply controls, implement endpoint and detection response tools, limit access to resources over the network, especially by restricting RDP, secure user accounts, and, in the case of infection, use the ransomware response checklist, scan your backups with antivirus to see that it is free of malware, and report the incident immediately.

Cybersecurity experts learned more regarding the Conti group operations after a gang affiliate leaked inside information because he was not paid as much as promised for his efforts. The angry contractor provided IP addresses for group's Cobalt Strike command-and-control servers and a 113MB archive including cybercrime tools and training materials after being paid only $1500 while, he says, the gang made millions. Affiliates are promised 20-30% of the ransom. The hacker shared the following anonymous post including "they recruit suckers and divide the money among themselves, and the boys are fed with what they will let them know when the victim pays.."



registration: 04/29/2020
Posts: 36
Reactions: 2

Today at 07:07

Dumb divorce, not work. They recruit pentesters, of course ... They recruit guys to test Active Directory networks, they use the Locker - Conti. I merge you their ip-address of cobalt servers and type of training materials. 1500 $ yes, of course, they recruit suckers and divide the money among themselves, and the boys are fed with what they will let them know when the victim pays. The admin in the chat was [redacted], his toad was [redacted] . Know the fag in the face! I have already sent the data to where I need it, so let it change the server data and everything else. And for hard workers resets all training materials =)
the All good
their chat in the Torah - [redacted].onion
Anyone who dials on the type of job Pentesterov 😆😆😄🤪 - [redacted] his toad - [redacted]

Forum post from disgruntled affiliate

Amazon’s $1500 Robotic Dog, Astro

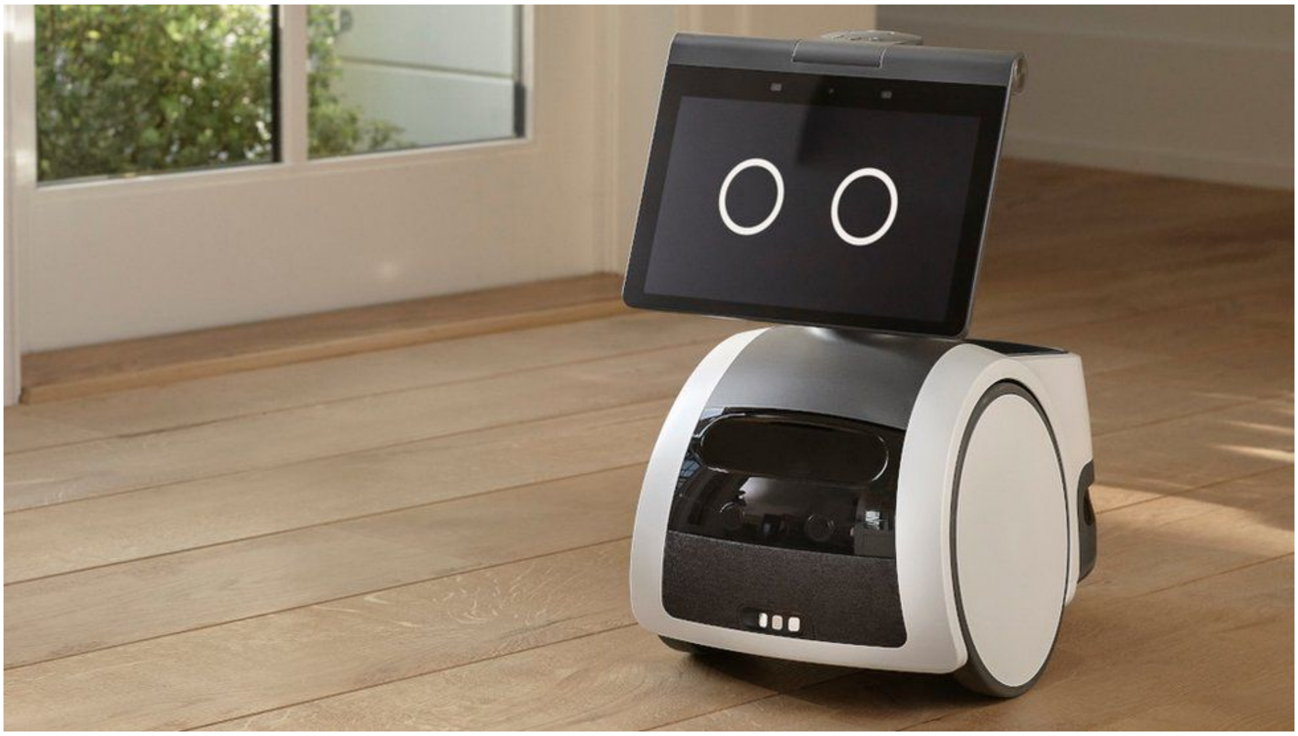
amazon Prime

Steven Levy, Wired, gives his analysis of Amazon’s robotic dog, Astro. And, it is hysterical. Here is an excerpt.

Astro, apparently named after the big, sloppy, non-robotic dog in The Jetsons*, is the bastard offspring of a video-conferencing device and a Roomba vacuum cleaner, although it doesn’t run Zoom and it won’t clean your floors. It can prowl around the house like a pint-sized mall cop, but unless you’re a drug kingpin looking to save on bodyguards, do you really need a constant robotic patrol of your living room?*

Astro can’t open the refrigerator door and it can’t grasp anything, but if a human being in the kitchen grabs a bottle and pops it open, they can bend down and put it in Astro’s cupholder and Astro could roll into the living room and deliver it to someone too lazy to move their ass off the sofa.

Oh, and it will cost $1,500. Subscribe for more.



“Advanced SSDs – PCIe Gen4, U.3, and New Form Factors”
with sponsors KIOXIA and Intel

When considering SSDs for your datacenter, what factors drive your selections? (check all that apply):

The recommendations of application software providers:	29%
The recommendations of/choices available from our server vendor(s):	31%
SSD performance:	69%
SSD advanced features:	24%
SSD capacity:	54%
Other:	10%

The upcoming U.3 specification will enable U.2 NVMe SSDs, SAS/SATA SSDs, & HDDs to fit into the same slot. How important is the ability interchange media types to your organization? (check one):

Very Important – We adjust our server configurations regularly:	20%
Important – It will allow us to update our servers and extend their life:	20%
Somewhat Important – It will provide us with more purchasing flexibility:	24%
Not that important – We can work with our current configurations:	7%
Not that important – We will transition to all-U.2 SSDs in the near future:	4%
Not that important – We will transition to EDSFF SSDs when available:	7%
No opinion:	18%

G2M Research Multi-Vendor Webinar Series

Our webinar schedule is below, including our schedule for 2022. Click on any of the topics to get more information about that specific webinar. You can view all our webinars and access all the slide deck presentations

Interested in sponsoring a webinar? Contact **G2M** for a prospectus.

We also help companies build custom webinars and webinar series as another highly effective approach to reach your target audience – before the webinar(s) with direct and social media marketing, during the webinar with a customized presentation and audience polls, and after the webinar with use of the recording and presentation materials for outreach. Join us for our KIOXIA series (dates and details soon).

Oct 12:	Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?
Nov 9:	The Explosion in Imagery from Radiometry, Cryo-EM, and Other Imaging Technologies: Can Storage Keep Pace?
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

Upcoming Conferences

October 8-9	THOTCON 2021
October 14	SecureWorldExpo
October 19-20	IAPP Privacy. Security. Risk. 2021
October 20-21	Counter-Insider Threat Symposium
October 20-21	DevSecCon London
October 20-22	Counter Insider Threat Symposium, Maryland
October 25-27	InfoSec World 2021
October 26-28	MWC Los Angeles
November 2-4	Microsoft Ignite, Virtual
November 8-11	Black Hat Europe, London
November 9-10	OCP Global Summit, San Jose
November 15-18	SC21, St Louis
November 29- Dec 3	Amazon re:Invent, Vegas
January 5-8	CES 2022, Vegas
January 26-28	SNIA 2021 Annual Members Symposium, Virtual
February 7-10	RSA Conference, San Francisco & Virtual
February 8-11	ITExpo, Fort Lauderdale
February 28- March 3	MWC Barcelona
March 2-3	Cloud Expo Europe, London
March 14-17	Gartner Data & Analytics Summit, Orlando
April 23-27	NAB, Vegas

G2M RESEARCH

Effective Marketing & Communications
with Quantifiable Results