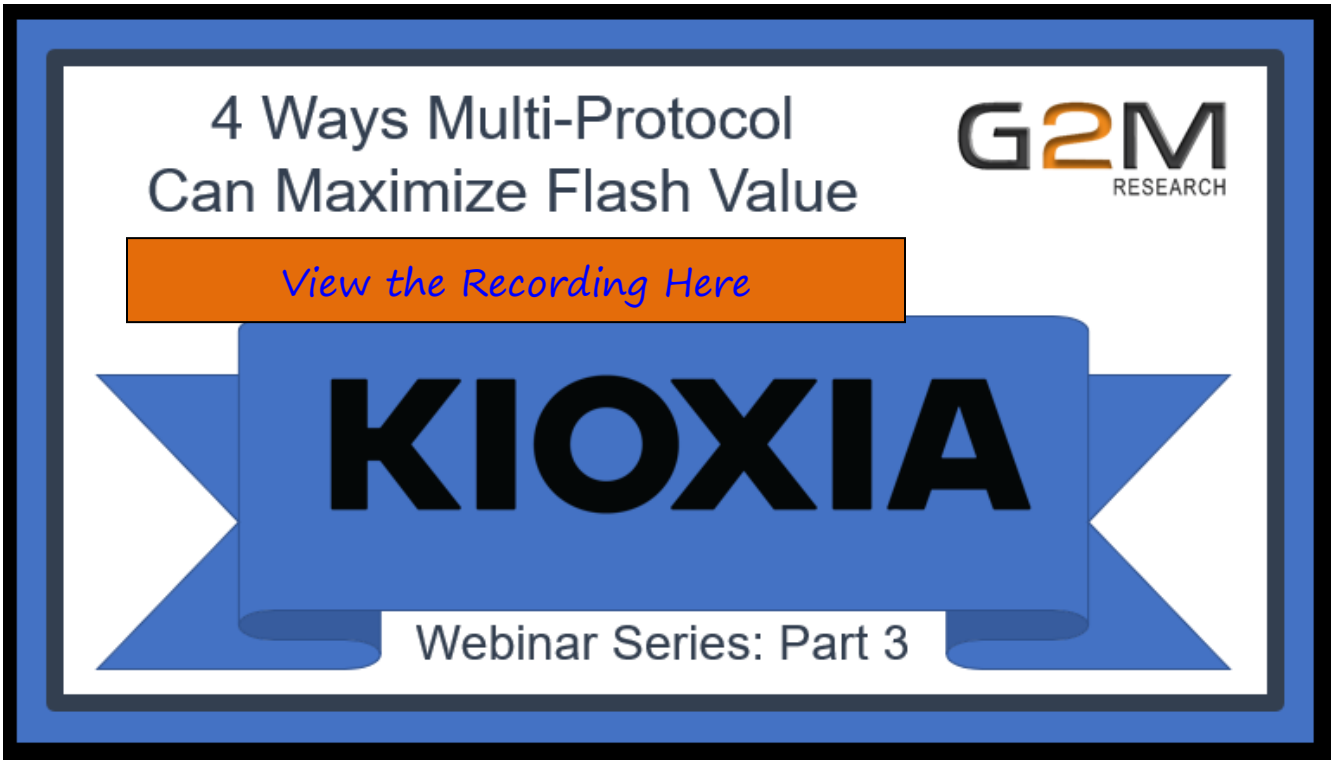
Highlights

"The thing that personally keeps me up at night as a cybersecurity professional are these supply chain attacks - you're talking about impacting tens of thousands and hundreds of thousands of companies and organizations around the world from a single hack."

"By some estimates, cybercrime is expected to globally cost up to $6 trillion annually. Losses of this scale put the incentives for innovation and investment at risk and will be more profitable than the global trade of all major illegal drugs combined."

David Kennedy, founder of Binary Defense and TrustedSec and former marine who conducted cyber missions for the U.S. military and the National Security Agency



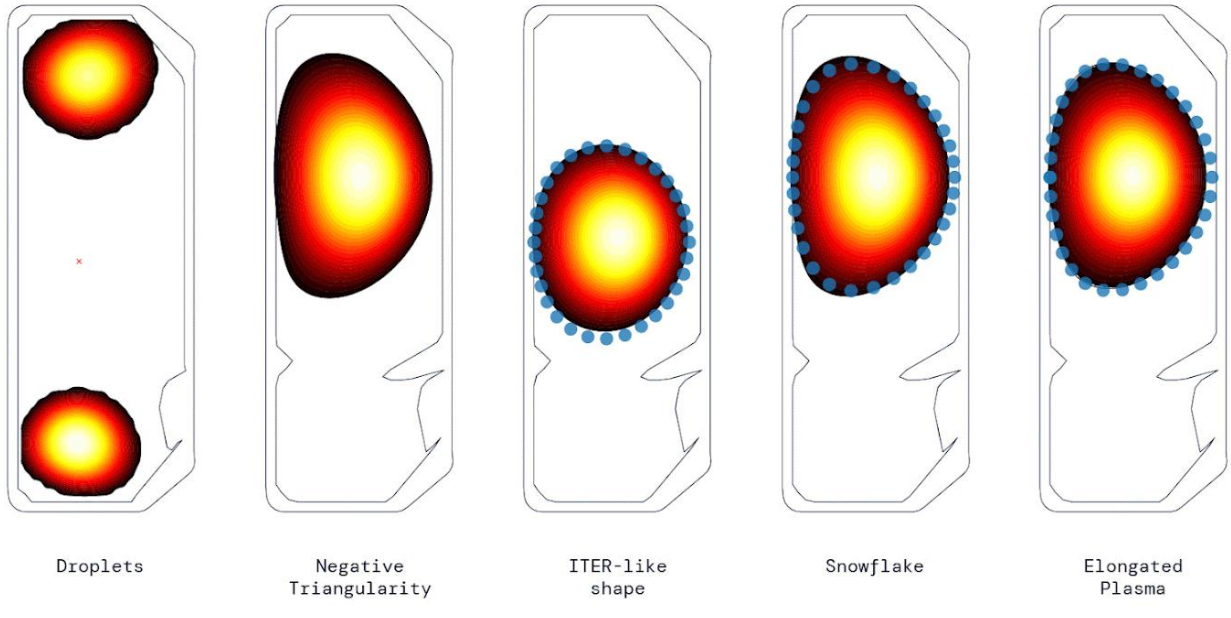
Just days after the FBI warned that BlackByte ransomware gang had hacked entities in three US critical infrastructure sectors (government facilities, financial, and food and agriculture), the group successfully gained access to San Francisco 49er servers. BlackByte claimed access to 2020 invoices with billing statements from the 49ers to partners including AT&T, Pepsi, and the City of Santa Clara and demanded ransom in exchange for not publishing the invoices.

BlackByte is a ransomware-as-a-service (RaaS) operation that allows affiliates to use its ransomware for a percentage of the proceeds. It is decentralized, with independent operators developing the malware, hacking into organizations or filling other roles. It's part of a trend of ransomware groups becoming increasing sophisticated. A report by the FBI and NSA explain that ransomware operators are even setting up an arbitration system to resolve payment disputes among themselves. Ransomware hackers remain in compromised networks for weeks as worm their way in. The BlackByte executable leaves a ransom note in all directories where encryption occurs. The ransom note includes the .onion site that contains instructions for paying the ransom and receiving a decryption key.

When BlackByte first began hacking sites, Trustwave security firm released a decryption tool for victims to unlock files for free instead of paying ransom to have the files unlocked. BlackByte updated the ransomware to overcome that flaw. Red Canary's analysis determined that BlackByte hacks some victims by exploiting ProxyShell, a series of vulnerabilities in Microsoft Exchange Server which allow hackers to gain pre-authentication remote code execution. From there, hackers install a shell that sends commands to the compromised server. Microsoft patched them last March. Another characteristic of BlackByte is "print bombing" which causes all printers connected to an infected network to print ransom notes at the top of each hour stating, "Your [sic] HACKED by BlackByte team. Connect us to restore your system."

The amount demanded and the team's willingness or unwillingness to pay have not been disclosed. The 49ers said it notified law enforcement and is working with third-party cybersecurity firms to perform their investigation.

AI Technique Leverages Reward-Seeking to Control Nuclear Fusion



DeepMind created an AI that leverages reward learning to control nuclear fusion.

Nuclear fusion is the process of squeezing two light atoms to create one large atom. The energy created by nuclear fusion powers all the stars in the universe. In space, the gravitational mass is strong enough to pull hydrogen atoms together to overcome their opposing charges. Alternatively, nuclear fission occurs when a neutron slams into a larger atom and causes it to split. Nuclear fission in used in nuclear power plants because the process is easy to control. Both processes generate huge amounts of energy. Nuclear fusion is praised as a limitless source of clean energy but has long been an engineering challenge because it requires sustained extreme pressure and temperature.

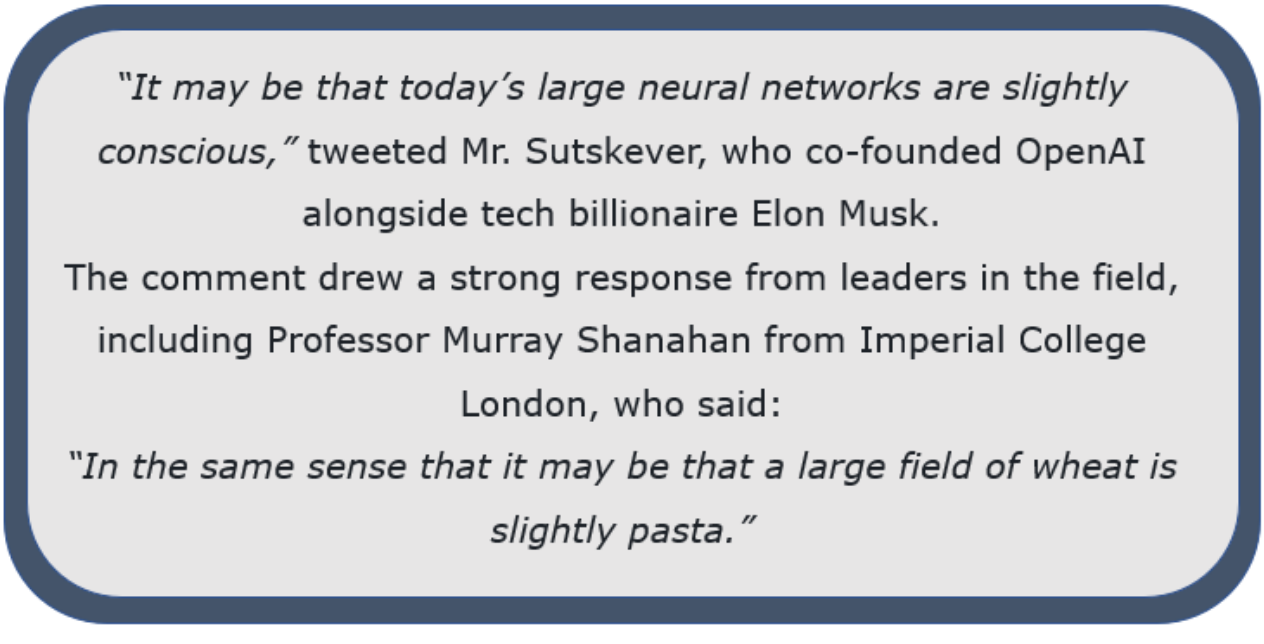
Scientists replicate nuclear fusion using donut-shaped vessels surrounded by electromagnetic coils called tokamaks to confine the reaction. The magnets contain volatile hydrogen plasma hotter than the sun's core. It is challenging to keep the plasma stable long enough to store the energy. Extensive engineering and design work is required to change the configuration of the plasma and try out different shapes that may yield more power or a cleaner plasma. Plasmas in these machines are inherently unstable. A control system must coordinate tokamak's magnetic coils and adjust voltage thousands of times per second to ensure plasma never touches walls of the vessel, to avoid heat loss and damage.

DeepMind's AI controls the nuclear fusion plasma autonomously using deep reinforcement learning. Reinforcement learning is an AI training technique that involves programming an AI to take certain actions in order to maximize its chance of earning a reward in a particular situation. The algorithm "learns" to complete a task by seeking out these preprogrammed rewards. DeepMind's AI, developed on a virtual simulator, has been used around 100 times on a tokamak at the Swiss Plasma Center known as the Variable Configuration Tokamak. It controlled the magnets in the tokamak for two seconds, the maximum amount of time the reactor can run before it overheats.

Fusion offers a unique challenge because the state of a plasma constantly changes and it can't be continuously measured. AI researchers call this an "under–observed system." A core challenge is to shape and maintain a high-temperature plasma within the tokamak vessel. This requires high-dimensional, high-frequency, closed-loop control using magnetic actuator coils, further complicated by the diverse requirements across a wide range of plasma configurations. They successfully produced and controlled a diverse set of plasma configurations on the To kamak including elongated, conventional shapes, as well as advanced configurations, such as negative triangularity and 'snowflake' configurations, achieving accurate tracking of the location, current and shape for these configurations. They demonstrated sustained 'droplets' on TCV, in which two separate plasmas are maintained simultaneously within the vessel. This represents a notable advance for tokamak feedback control, showing the potential of reinforcement learning to accelerate research in the fusion domain, and is one of the most challenging real-world systems to which reinforcement learning has been applied.

Demis Hassabis, Founder and CEO, Deepmind:

> *Research into nuclear fusion is currently limited by researchers' ability to run experiments. While there are dozens of active tokamaks around the world, they're expensive machines and in high demand. For example, TCV can only sustain the plasma in a single experiment for up to three seconds, after which it needs 15 minutes to cool down and reset before the next attempt. Not only that, multiple research groups often share use of the tokamak, further limiting the time available for experiments.*
>
> *Given the obstacles to access a tokamak, researchers have turned to simulators to help advance research. Our partners at EPFL built powerful simulation tools to model the dynamics of tokamaks. We were able to use these to allow our RL system to learn to control TCV in simulation and then validate our results on the real TCV, showing we could successfully sculpt the plasma into the desired shapes. Whilst this is a cheaper and more convenient way to train our controllers; we still had to overcome many barriers. Plasma simulators are slow and require many hours of computer time to simulate one second of real time. The condition of TCV can change from day to day, requiring us to develop algorithmic improvements, both physical and simulated, and to adapt to the realities of the hardware.*
>
> *Existing plasma-control systems are complex, requiring separate controllers for each of TCV's 19 magnetic coils. Each controller uses algorithms to estimate properties of the plasma in real time and adjust voltage of the magnets accordingly. In contrast, our architecture uses a single neural network to control all of the coils at once, automatically learning which voltages are the best to achieve a plasma configuration directly from sensors.*



Russian Arsenol Includes Cyber Warfare

Top cybersecurity officials from the Department of Homeland Security and FBI warned of attacks on U.S. cyber infrastructure in concert with a physical invasion of Ukraine. The Cybersecurity and Infrastructure Security Agency (CISA) warned, "The Russian government has used cyber as a key component of their force projection over the last decade, including previously in Ukraine in the 2015 timeframe. The Russian government understands that disabling or destroying critical infrastructure—including power and communications—can augment pressure on a country's government, military and population and accelerate their acceding to Russian objectives."

In remarks at the Munich Cybersecurity Conference, deputy attorney general Lisa Monaco stated, "Given the very high tensions that we are experiencing, companies of any size and of all sizes would be foolish not to be preparing right now as we speak -- to increase their defenses, to do things like patching, to heighten their alert systems, to be monitoring in real-time their cybersecurity. They need to be as we say, 'shields up' and to be really on the most heightened level of alert that they can be and taking all necessary precautions." Monaco said the threat was in no way "hypothetical."

From 2020 to at least February 2022, Russian state sponsored cyber actors have targeted U.S. cleared defense contractors including intelligence, weapons and missile development and software development. "Russia maintains a range of offensive cyber tools that it could employ against US networks—from low-level denials-of-service to destructive attacks targeting critical infrastructure," stated the Department of Homeland Security. The Treasury Department held a classified briefing that covered the issue for big US banks and the Energy Department briefed America's largest electric utilities.

Cyber operations have been a recurring aspect of the military conflict in Ukraine starting when Russia annexed Crimea in 2014. The US Justice Department says Russia's GRU military intelligence agency cut off power in parts of Ukraine in 2015 and 2016 and infected computer systems with NotPetya malware in 2017 causing $10B in damage.

A pair of cyberattacks targeted several Ukrainian government agencies. Hackers replaced content on government websites with threatening messages claiming Ukrainians' data had been stolen. In other

cases, malicious software deleted data from roughly 20 computer servers and workstations at at least two Ukrainian government agencies.

"One possibility ... is that this attack is just a front for a much stronger attack that we may face in the future," stated Serhiy Demedyuk, deputy secretary of Ukraine's National Security and Defense Council. As Ukraine readies its military to defend against a potential Russian invasion, Ukrainian officials have held urgent cybersecurity meetings and drawn on US support to fortify their networks.

A series of cyberattacks on Tuesday knocked the websites of the Ukrainian army, the defense ministry and major banks offline, Ukrainian authorities said, as tensions persisted over the threat of a possible Russian invasion. At least 10 Ukrainian websites were unreachable, including the defense, foreign and culture ministries and Ukraine's two largest state banks.

In January a cyberattack damaged servers at Ukraine's State Emergency Service and at the Motor Transport Insurance Bureau with a malicious "wiper" cloaked as ransomware. The damage was minimal but experts believe that was intentional. A message posted simultaneously on dozens of defaced Ukrainian government websites said: "Be afraid and expect the worst."

"I am concerned that Russia has been using Ukraine as a sort of testing ground for its cyber capabilities," explained Senator Mark Warner, chairs of the Senate Intelligence Committee,. "For years, I've been making the case that we need rules of the road in cyberspace, just like we have defined norms around armed conflict," Warner said. "We need to ensure that the Kremlin knows that if they were to use destructive cyberattacks against the United States, there would be serious consequences." President Biden said the US could respond with cyberoperations of its own should Russia conduct additional cyberattacks in Ukraine. War has long not been fought on the ground.

Polls Results for Scale-Out Flash Storage:

Breaking Old-School Storage Rules

with Sponsors WEKA, Lightbits, Excelero

Does SOFS look like a solution that makes sense for your organization? (check one):

Definitely; we have several potential SOFS use cases:	21%
Probably; we have one/a few SOFS use cases:	11%
Maybe; would likely evaluate SOFS as a solution:	32%
Probably not; we would likely continue to acquire array-based storage solutions:	7%
Don't know/haven't studied SOFS as a solution:	29%

How do you see SOFS fitting into the overall storage solutions environment? (select one):

It is a game-changer – we see it as the leading way to deploy storage in the near-future:	17%
It is very important – we see it eventually replacing classical storage arrays over time:	13%
It is a useful "tool in the toolbelt" that gives our organization new storage options:	54%
It is interesting, but is likely a "niche" technology:	13%
We don't see it as a relevant technology:	4%

KIOXIA Webinar Series

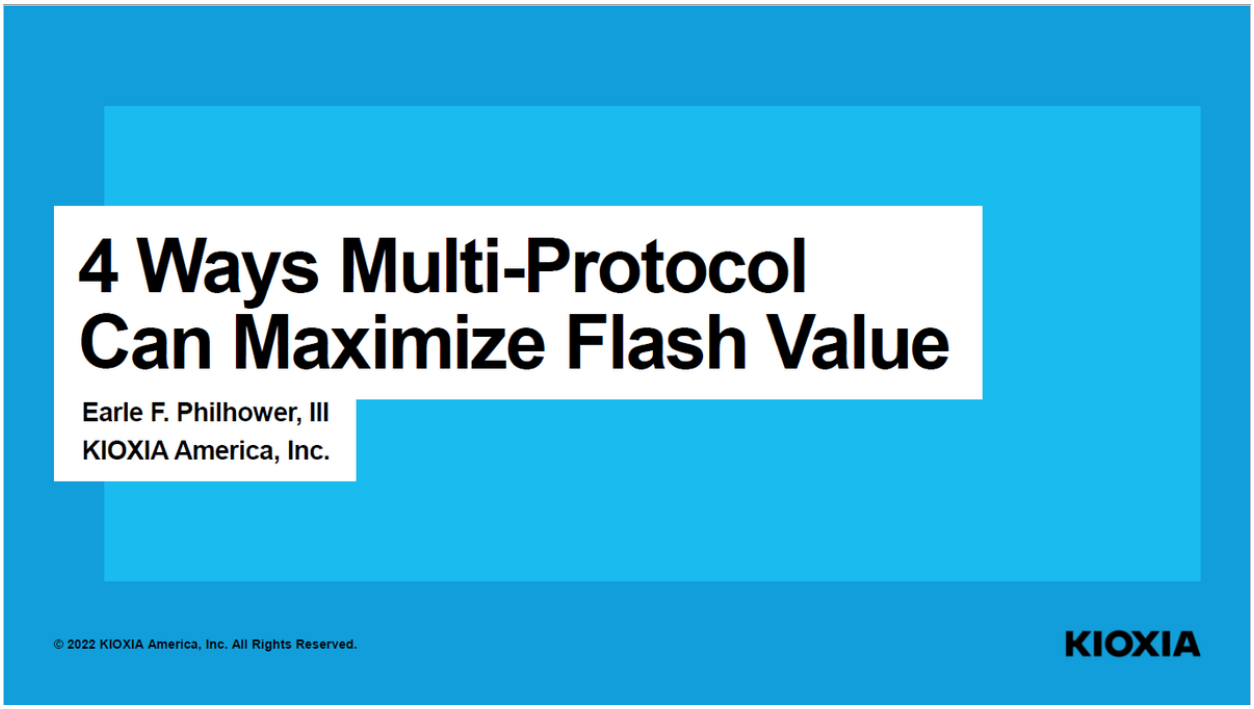
Tuesday, February 8, KIOXIA provided an analysis of “4 Ways Multi-Protocol Can Maximize Flash Value.” The webinar video is available to view here and the slidedeck is available here.

KIOXIA industry expert, Earle Philhower explains how flash memory revolutionized the data center by being backwards compatible with legacy hard drive protocols. However, in certain applications that backwards compatibility limits how valuable flash memory can be. In order to improve TCO and maximize performance and storage utilization, multiple unique and incompatible flash storage protocols have been developed. Unfortunately, managing all these different drive types at cloud scale can be a challenge.

This was the third in a four part webinar series to dive deeper into learning how an open-source, software-defined approach to flash protocols can deliver better economics, increased deployment flexibility and simpler supply management.

Each webinar stands alone and collectively provides an overview of the innovation, direction, and leadership KIOXIA provides in this enterprise storage space.

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.” 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.



Upcoming Conferences

February 28- March 3	MWC Barcelona
March 2-3	Big Data & AI World, London
March 2-3	Cloud Expo Europe, London
March 2-3	Cloud & Cyber Security Expo, 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
April 26-28	Smart NICs Summit, San Jose
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 11-12	Cyber Security & Cloud Congress, Santa Clara
May 18-19	Gartner Digital Workplace Summit, London
June 6-9	RSA Conference, San Francisco & Virtual
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 15	Cloud Security Summit, Virtual
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
July 19-20	Cyber Solutions Summit & Expo, Virtual
August 2-4	Flash Memory Summit, Santa Clara
August 6-11	Black Hat USA, Vegas
August 11-14	DEF CON 30, Vegas
September 13-14	CISO Forum, Virtual
September 19-20	Industry of Things World, Berlin
September 28-29	IoT World, Santa Clara
October 5-6	Evolve, Vegas
October 24-27	ICS Cybersecurity Conference, Hybrid/Virtual
November 16	San Diego Cybersecurity Conference, Hybrid
November 16	Threat Hunting Summit, Virtual
November 18-19	Data Strategy & Insights (Forrester Research), Virtual
December 1-2	AI & Big Data Expo Global, London
December 6	Security Operations Summit, Virtual