

Webinars/Events

4/18/2022 - 4/20/2022	The Art of Third Party Risk conference
5/5/2022 1:00 pm CST	ARMA & Zasiio - Poking Holes in Big Buckets – The Impacts of Data Privacy and Security on Simplified Retention Schedules

Latest Tech News

Washington state universities get funding to create cybersecurity programs as industry demand grows	At the federal level, the Biden administration’s FY 2023 budget includes an 11% increase for cybersecurity spending, Cybersecurity Dive reported.
Google Cloud’s BigQuery gains an Automatic Data Loss Prevention feature	Google Cloud said today it’s enabling Automatic Data Loss Prevention in Google BigQuery to help users find, classify and protect sensitive information that may have inadvertently been scattered around their cloud deployments.
Kyndryl rolls out Dell partnership for disaster recovery and security	Kyndryl provides an orchestration tool that offers users a way to respond programmatically and immediately to a cybersecurity event, an analytics tool that uses machine learning to do regular integrity checking on system configuration data (ensuring that it hasn't been compromised by bad actors), and the company's own in-house expertise in deployment and configuration of large-scale, enterprise systems.
Critical vulnerability in popular WordPress plugin exposes millions of sites to hacking	The vulnerability is caused by an absence of a critical access check in one of the plugin’s files, which is loaded on every request, even if users are not logged in. Because the check does not occur, access to the file and hence the plugin is open to all and sundry, including bad actors.
Bitdefender tackles cyber resilience challenges with a new XDR solution	GravityZone XDR aims to provide enterprises with a platform they can use to automatically detect known and unknown threats throughout their environment, while providing human analysts with the intelligence they need to respond to quickly control security incidents.
Microsoft: We've just disrupted this ransomware-spreading botnet	Microsoft has now received a court order from the US District Court for the Northern District of Georgia that allowed it to seize 65 domains the ZLoader gang had been using for command and control (C&C) for its botnet built from malware that infected businesses, hospitals, schools, and homes.
Obsidian Security lands \$90M to detect and fix major SaaS risks	Notably, the SaaS Security and Posture Management (SSPM) platform leverages Obsidian’s proprietary “knowledge graph” — which ties together data from different apps to “create a comprehensive and deeply contextual view of the SaaS world” that’s inhabited by customers.
Silverfort raises \$65 million to extend its identity threat protection solution	Essentially, the provider offers a solution that enterprises can use to implement multi-factor authentication, identity threat detection and response, and zero-trust policies for critical data assets in a single location, to ensure there’s end-to-end identity protection.
SaaS security startup DoControl raises \$30M to scale up innovations	The problem being tackled by DoControl is a real one. Accelerated SaaS adoption, the growing complexity of SaaS ecosystems and the lack of granular, automated access control can leave organizations exposed to unauthorized and undetected data exfiltration.


Analysis, Reports, Trends

eWeek - Machine Identities Are Dangerously Vulnerable	Identity security is in the spotlight these days, and it’s easy to see why. The most recent Verizon Data Breach Investigations Report found that 61% of all breaches involve credential data.
sdxCentral - Netskope: Unified SASE Is at Least a Decade From Practicality	The real value of SSE isn’t that it’s Cloud based or that because it’s cloud-native it’s more scalable — though these factors do help, he said. It’s that “you’ve created one brain” for security intelligence.
Network World - What is DRaaS and how it can save your business from disaster	The DRaaS market is a sprawling, complicated one, with hundreds of providers offering a wide range of different approaches that replicate everything from data and virtual machines (VMs) to on-premises servers and mainframes.
eWeek - Key Advice for Improving Your Company’s Cybersecurity	In cases where third-party hardware or software is not scrutinized, vulnerabilities can be harder to discover but also more broadly distributed, which can make them harder to remediate. For example, the Equifax breach in 2017 was reported to be the result of a vulnerability in open-source software. And more recently, the world reacted to another open-source vulnerability in Log4j.
sdxCentral - Palo Alto Networks' Unit 42 Claims Cloud Identities Too Permissive	In analyzing more than 680,000 identities across 18,000 cloud accounts from more than 200 different organizations as part of its latest Cloud Threat Report, researchers found that nearly 99% of IAM policies are overly permissive.
VentureBeat - 10 things CISOs need to know about zero trust	Over the last eighteen months, the exponential rise in cyberattacks shows that patching perimeter-based network security isn’t working. Cyberattackers can still access networks by exploiting unsecured endpoints, capturing and abusing privileged access credentials and capitalizing on systems that are months behind on security patches.

Blogs

Check out our curated blogs. We separate by category. Privacy and Security is one of our popular sections.

<https://docs.teckedin.info/docs/curated-blogs-privacy-and-security>



How to keep your online practice management software secure

Apr 16, 2022 techbullion.com/

In recent years, we’ve seen a significant increase in cybercrime in Australia, and healthcare practices are among those commonly targeted.



Banks must be vigilant against the new forms of cyber threat

Apr 16, 2022 tbsnews.net/

As new cybersecurity features are being developed, the hackers and cybercriminals are also coming up with newer forms of cyberattacks



The Risks and Costs of The Public Sector’s Device Sanitization and Destruction Practices

Apr 16, 2022 cyberdefensema...

New report highlights concern over financial costs and environmental impacts associated with device destruction as well as a lack of data sanitization best