

Webinars/Events

1/13/2021 11:00 am EST	OneTrust - The Automated Data Map: Your Foundation for Privacy, Security, and Governance
1/18/2021 11:00 am EST	Veriato - Insider Threat in the Healthcare Sector
1/20/2021 - 1:00 pm CST	ARMA & Onna - Maintaining Data Privacy During the Great Resignation
1/26/2022 - 1/27/2022	The Rise of Privacy Tech's Data Privacy Week 2022
4/18/2021 - 4/20/2021	The Art of Third Party Risk conference

Latest Tech News

APT 'Aquatic Panda' Targets Universities with Log4Shell Exploit Tools	Wiley said researchers uncovered the suspicious activity tied to the target's infrastructure. "This led OverWatch to hunt for unusual child processes associated with the VMware Horizon Tomcat web server service during routine operations," he wrote.
Chinese APT Hackers Used Log4Shell Exploit to Target Academic Institution	A never-before-seen China-based targeted intrusion adversary dubbed Aquatic Panda has been observed leveraging critical flaws in the Apache Log4j logging library as an access vector to perform various post-exploitation operations, including reconnaissance and credential harvesting on targeted systems.
Storage Devices of Major Vendors Impacted by Encryption Software Flaws	Earlier this month, SecurityWeek reported that Western Digital had updated its SanDisk SecureAccess product to address vulnerabilities that can be exploited to gain access to user data through brute force and dictionary attacks.
Microsoft investigating Defender issue with Log4j scanner	Additionally, Microsoft said it has launched a new schema in advanced hunting for Microsoft 365 Defender, "which surfaces file-level findings from the disk and provides the ability to correlate them with additional context in advanced hunting."
Microsoft launches new Defender capabilities for fixing Log4j	Defender for Containers debuted December 9, merging the capabilities of the existing Microsoft Defender for Kubernetes and Microsoft Defender for container registries and adding new features such as Kubernetes-native deployment, advanced threat detection, and vulnerability assessment.
LastPass users report attempted logins using their master passwords	That they were blocked is a positive, since LastPass managed to stop the attempts. But the obvious question is: How were the LastPass master passwords seemingly compromised?
Shutterfly reports ransomware incident	We do not store credit card, financial account information, or the Social Security numbers of our Shutterfly.com, Snapfish, Lifetouch, TinyPrints, BorrowLenses, or Spoonflower customers, and so none of that information was impacted in this incident," Shutterfly explained.
Nubeva Announces Third-Party Validation Of Its Upcoming Ransomware Reversal Solution	The findings validate previous claims that Nubeva can intercept encryption keys and decrypt (reverse) ransomware 96.84% of the time. Over four weeks, tests were conducted against thousands of random ransomware samples never seen by Nubeva

Analysis, Reports, Trends

threatpost - 5 Cybersecurity Trends to Watch in 2022	"Building on earlier analysis of companies across the United States that could present a strategic risk to the country if disrupted (known as the "Section 9" list), Congress will deliberate about how the federal government can help manage systemic cybersecurity risks to the U.S. economy and society, to include mission-critical functions in key sectors like healthcare, elections and energy."
GovTech - The Top 22 Security Predictions for 2022	We again see forecasts of more government compliance rules, 5G challenges, APTs, deepfakes getting really dangerous, privacy concerns, and another year of healthy growth in technology and cyber companies.
VentureBeat - Why IoT is the cornerstone of AWS's zero-trust strategy	For the first time in its annual trend analysis, Gartner prioritizes machine identity management for CISOs and their security teams. AWS' decision to release IoT ExpressLink now and fast-track enhancements to AWS IoT Greengrass shows its approach to zero-trust security being hardened at the endpoint first.
threatpost - Global Cyberattacks from Nation-State Actors Posing Greater Threats	We have seen increased interest in consumer internet of things (IoT) and home-router zero-day exploits, with attacks following close behind. In the past, the home as an attack vector was rarely interesting to sophisticated nation-state attackers or cybercriminal gangs, but we should expect to see more activity in this area over the coming year.
VentureBeat - Kubernetes security will have a breakout year in 2022	The fact that "shift left" has caught on suggests that big strides can now be made in terms of Kubernetes security, he told VentureBeat. Getting companies to grasp that securing containerized apps will involve bringing security earlier into the app development lifecycle is a crucial step.

Blogs

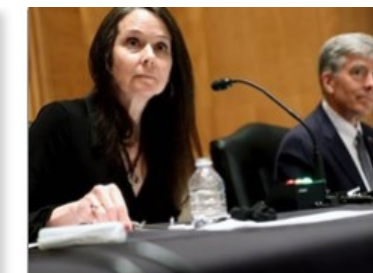
Check out our curated blogs. We separate by category. Privacy and Security is one of our popular sections.

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



Experts' Predictions for the Future of Tech in 2022

Jan 1, 2022 tech.co/
Here are the top ten tech predictions for the new year and beyond, from experts across a vast range of industries.



US Still Lacks Federal Cyber Strategy After Decades of Attempts

Dec 30, 2021 Nextgov.com
The United Kingdom, meanwhile, recently updated its approach, crediting strong regulatory measures with significant cyber-risk reduction over recent years.



Malicious apps found in popular Android app store - What to avoid

Dec 31, 2021 Komando, Kim
Separate from the Google Play Store, the apps discovered on the Samsung Galaxy Store could infect Android devices with malware.