CyAN

Cybersecurity
Advisors
Network

Cyber (In)Securities

Issue #133

NEWS:

1. Microsoft: New RAT malware used for crypto theft, reconnaissance

Original Source: BleepingComputer by Sergiu Gatlan

Microsoft has identified a new form of RAT (Remote Access Trojan) malware that is being used for cryptocurrency theft and detailed reconnaissance of infected systems.

This sophisticated malware targets digital wallets and can extract a wide array of sensitive information, paving the way for more invasive attacks.

This discovery underscores the evolving nature of cyber threats, particularly those aimed at financial gain.

Organisations are advised to enhance their cybersecurity protocols to defend against these stealthy, financially motivated attacks, stressing the importance of continuous monitoring and advanced threat detection systems to thwart these malicious actors effectively.

CyberSecurity Advisors Network

NEWS:

2. Exploit Code for Apache Tomcat RCE Vulnerability Published on Chinese Forum

Original Source: SecurityWeek by Ryan Naraine

Exploit code for a critical Remote Code Execution (RCE) vulnerability in Apache Tomcat has been published on a popular Chinese forum, raising concerns about potential widespread attacks.

This vulnerability allows attackers to execute arbitrary code remotely, compromising the security of any unpatched Tomcat servers.

Security experts urge administrators to apply the latest patches immediately to mitigate the risk.

The publication of this exploit code marks a significant escalation in the threat landscape, as it provides attackers with ready access to a powerful tool for infiltrating and taking control of affected systems.

CyberSecurity Advisors Network

NEWS:

3. DOGE staffer violated security policies at Treasury Department, court filing shows

Original Source: Cyberscoop by Tim Starks

A court filing has revealed that a staffer from the DOGE project violated several security policies at the Treasury Department.

This breach involved unauthorised access to sensitive financial data, potentially compromising critical economic information. The incident has sparked significant concern over internal security protocols and the enforcement of access controls within government agencies.

This case underscores the need for stringent security measures and continuous monitoring to protect sensitive governmental data from insider threats, emphasising the importance of compliance with established security policies to prevent similar incidents in the future.

CyberSecurity Advisors Network

NEWS:

4. RansomHub Taps FakeUpdates to Target US Government Sector

Original Source: Dark Reading by Elizabeth Montalbano

RansomHub, a notorious cybercrime group, has started leveraging FakeUpdates, a deceptive tactic involving fake software update alerts, to infiltrate US government networks.

This sophisticated strategy targets vulnerabilities in outdated software, tricking employees into installing malicious updates that deploy ransomware.

The attacks have heightened concerns about the resilience of government cybersecurity defenses and underscored the necessity for agencies to maintain software updates and educate staff on recognizing phishing attempts.

These developments highlight the evolving techniques of cybercriminals in bypassing traditional security measures to access highly sensitive government data.

CyberSecurity Advisors Network

NEWS:

5. Denmark Warns of Increased Cyber Espionage Against Telecom Sector

Original Source: Dark Reading by Alexander Culafi

Denmark's intelligence services have issued a warning about a significant increase in cyber espionage activities targeting the nation's telecommunications sector.

These espionage efforts are aimed at accessing sensitive communications and gaining strategic advantages.

The alert specifies that foreign state-sponsored actors are primarily responsible, seeking to compromise critical infrastructure to disrupt services or gather intelligence.

This escalation prompts a call for enhanced security measures within the telecom industry, highlighting the need for robust cybersecurity strategies to protect against sophisticated and persistent threats.

For more on this article see Article 31: ‘Fostering Australia's Autonomy: The Imperative for Sovereign Satellite Communication Systems’ by CyAN’s Kim Chandler McDonald

NEWS:

6. Cybercriminals Exploit CSS to Evade Spam Filters and Track Email Users' Actions

Original Source: The Hacker News by Ravie Lakshmanan

Cybercriminals are increasingly exploiting Cascading Style Sheets (CSS) to circumvent traditional spam filters and track user actions within emails.

This method involves embedding malicious CSS code into emails, which not only bypasses spam detection systems but also enables attackers to gather detailed information about how recipients interact with the email content.

The technique poses significant privacy and security risks, as it can be used to refine phishing campaigns and increase their effectiveness.

This emerging threat highlights the need for more advanced email security solutions that can detect and mitigate such sophisticated tactics.

CyberSecurity Advisors Network

NEWS:

7. Critical RCE flaw in Apache Tomcat actively exploited in attacks

Original Source: BleepingComputer by Bill Toulas

A critical Remote Code Execution (RCE) flaw in Apache Tomcat is currently being exploited in the wild, posing serious risks to systems running unpatched versions of the server software.

This vulnerability allows attackers to remotely execute malicious code, potentially gaining full control over affected systems.

The urgency for administrators to apply security patches cannot be overstated as exploitation of this flaw could lead to significant data breaches and system takeovers.

This situation underscores the continuous threat landscape facing web servers and the importance of timely updates and vigilance in cybersecurity practices.

CyberSecurity Advisors Network

NEWS:

8. Telegram founder returns to Dubai as French inquiry continues

Original Source: The Guardian by Dan Milmo

The founder of Telegram, Pavel Durov, has returned to Dubai amid ongoing inquiries in France concerning the platform's compliance with data protection laws and its role in spreading misinformation.

This move comes as French authorities intensify their scrutiny of social media platforms, focusing on how they manage user data and content.

Durov's return to Dubai, where Telegram has significant operations, highlights the challenges tech companies face in balancing user privacy with governmental demands for greater transparency and control over digital content.

CyberSecurity Advisors Network

NEWS:

9. Nvidia Patches Vulnerabilities That Could Let Hackers Exploit AI Services

Original Source: SecurityWeek by Eduard Kovacs

Nvidia has issued patches for several vulnerabilities in its software that could allow hackers to exploit its AI services.

These vulnerabilities were identified in various components of Nvidia's platforms, which are widely used for AI processing and deep learning tasks. If exploited, these flaws could lead to unauthorised access to sensitive data, disruption of AI operations, or manipulation of AI functionalities.

The prompt release of these security patches underscores Nvidia’s commitment to safeguarding its technologies against emerging cyber threats and maintaining the integrity of its AI ecosystems.

CyberSecurity Advisors Network

CyAN Members Only

Are You In the #CyANQuiz?

Hey CyAN Champions,

Have you got what it takes to outsmart your fellow cybersecurity pros? It's time to put your skills to the test in our Quarterly #CyANQuiz Challenge, kicking off on March 31st!

- 🔹 30 Questions. Timed. No second chances.
- 🔹 Based on Recent Cybersecurity News & Events – Watch out for recent news and Cybersecurity events.

📅 **Check your email on March 31st for the quiz link**; just click, answer, and climb the leaderboard!

💡 Why Play? Compete, have fun, and win awesome prizes (while proving your cybersecurity dominance!

Join the fun—this isn't just a quiz, it's a year-long challenge to **shine in the CyAN community!**

Think you can take the cyber crown? Prove it!

NEWS:

10. Malicious Adobe, DocuSign OAuth apps target Microsoft 365 accounts

Original Source: BleepingComputer by Bill Toulas

Cybercriminals are targeting Microsoft 365 users by creating malicious OAuth applications disguised as legitimate Adobe and DocuSign services.

These deceptive apps trick users into granting them access to their Microsoft 365 accounts, enabling attackers to obtain sensitive data and potentially launch further malicious activities.

The sophistication of these scams highlights the importance of vigilance when authorising third-party applications, emphasising the need for users to verify app authenticity before granting any permissions.

This tactic reflects a growing trend in using OAuth apps for phishing and data breaches.

CyberSecurity Advisors Network

NEWS:

11. A Ransomeware Attack Hit the Micronesians State of Yap, Causing the Health System Network To Go Down

Original Source: Security Affairs by Pierluigi Paganini

The Micronesian state of Yap has been severely impacted by a ransomware attack that brought down its health system network.

This cyberattack has disrupted medical services and access to crucial patient data, highlighting the vulnerability of critical infrastructure to such threats.

The incident underscores the need for enhanced cybersecurity measures in healthcare systems, particularly in regions that may lack the resources to adequately defend against sophisticated cyber threats.

The focus is now on recovery and strengthening defenses to prevent future disruptions.

CyberSecurity Advisors Network

NEWS:

12. Back to cash: life without money in your pocket is not the utopia Sweden hoped

Original Source: The Observer by Miranda Bryant

In a surprising shift, Sweden, once at the forefront of the cashless movement, is reconsidering the role of cash in daily transactions.

This reflection arises as citizens encounter challenges and limitations with digital-only payments, such as technical failures, exclusion of non-digital natives, and privacy concerns.

The move back towards cash underscores a growing recognition of the need for a balanced approach to payment methods that ensures accessibility and security for all segments of society, highlighting the practical realities of a digital economy that may not fully cater to everyone's needs.

CyberSecurity Advisors Network

NEWS:

13. New Akira ransomware decryptor cracks encryptions keys using GPUs

Original Source: BleepingComputer by Bill Toulas

A breakthrough has been achieved with the development of a new decryptor for Akira ransomware, utilising GPUs to crack encryption keys rapidly.

This tool offers hope to victims by significantly speeding up the decryption process, potentially restoring access to encrypted files faster than ever before.

The introduction of this GPU-powered decryptor represents a critical advancement in the fight against ransomware, providing an effective countermeasure that can mitigate the impact of these devastating cyber attacks. It also underscores the ongoing arms race between cybercriminals and cybersecurity professionals striving to protect user data.

CyberSecurity Advisors Network

NEWS:

14. New MassJacker CLIPPER Targets Pirated Software Seekers

Original Source: Security Affairs by Pierluigi Paganini

The newly identified "MassJacker" clipper malware is targeting individuals seeking pirated software, exploiting their quest for free content to steal cryptocurrency.

This malicious software modifies clipboard data to redirect crypto transactions to attacker-controlled wallets, seamlessly replacing intended recipient addresses. This method underscores the risks associated with downloading unofficial software, as users inadvertently expose themselves to sophisticated cyber threats.

The emergence of MassJacker highlights the need for heightened awareness and preventive measures against the malware threats that lurk in pirated software.

CyberSecurity Advisors Network

NEWS:

15. Malicious PyPI Packages Stole Cloud Tokens—Over 14,100 Downloads Before Removal

Original Source: The Hacker News by Ravie Lakshmanan

Over 14,100 instances of malicious packages downloaded from Python's package index, PyPI, have led to widespread theft of cloud tokens.

These packages, cleverly disguised as legitimate software, siphoned off cloud credentials from unsuspecting developers, compromising numerous cloud environments.

This incident highlights the vulnerability of software supply chains and emphasises the critical need for developers to verify the integrity and source of third-party libraries. It also underscores the importance of robust security practices in managing and safeguarding cloud-based resources from such deceptive attacks.

CyberSecurity Advisors Network

NEWS:

16. Ransomware gang creates tool to automate VPN brute-force attacks

Original Source: BleepingComputer by Bill Toulas

A notorious ransomware gang has developed a new tool that automates brute-force attacks on VPNs, increasing the efficiency of their attacks on corporate networks.

This tool targets VPN accounts with weak or default passwords, enabling rapid unauthorised access and subsequent deployment of ransomware.

This development poses a significant threat to businesses, stressing the urgent need for robust password policies and enhanced VPN security measures.

Companies are advised to enforce strong authentication practices and monitor network traffic to mitigate the risks of such sophisticated attacks.

CyberSecurity Advisors Network

NEWS:

17. California’s legal push on geolocation data collection must take aim at the right targets, privacy experts say

Original Source: Cyberscoop by Derek B. Johnson

California is advancing legislation aimed at tightening controls on geolocation data collection, prompting discussions among privacy experts about the precision and effectiveness of these legal measures.

The experts advocate for legislation that accurately targets harmful practices without stifling innovation or overburdening businesses with compliance challenges.

This legal push reflects growing concerns over privacy rights and the potential misuse of sensitive location data, underscoring the need for laws that balance protection with practicality in the rapidly evolving digital landscape.

CyberSecurity Advisors Network

NEWS:

18. Lockbit Ransomware Developer Rostislav Panev was Extradited From Israel to the U.S.

Original Source: Dark Reading by Kristina Beek

A key developer of the Lockbit ransomware group has been extradited and has admitted involvement with the notorious ransomware operations.

This significant legal development marks a pivotal moment in the global fight against cybercrime, as the individual in question was responsible for creating and refining the ransomware used in numerous high-profile attacks worldwide.

The extradition and confession are part of a broader international effort to dismantle cybercriminal networks that have caused extensive financial and data losses across various sectors.

This case highlights the increasing effectiveness of international cooperation in cybersecurity enforcement and the growing legal repercussions for cybercriminals.

CyberSecurity Advisors Network

Has Trust in Democracy Survived the 2024 Election Year?

The Trust and Safety Forum is hosting a must-attend discussion on elections, disinformation, and democracy's resilience in the digital age as part of InCyber Forum Europe 2025.

📅 **April 1, 2025** | 🕒 **13:45 – 14:30 CET**
📍 **Lille, France** | **INCYBER FORUM EUROPE 2025**

The Panel:
🎙 **Lorena Martinez** – Head of Editorial Operations, Europe & UK, Logically Facts
🎙 **Laetitia Avia** – Digital Policy Expert, Lawyer & Former French MP
🎙 **Stéphanie Ladel** – OSINT, IMINT & GEOINT Researcher & Trainer
🗣 **Moderated by John Sullivan**, CyAN Board Member & Communications Chief

Discussion Topics:
✅ **Debunking disinformation** – What's working, and what needs to change?
✅ **The role of fact-checkers** – Minimising misinformation in real time
✅ **Building a balanced political environment** – The resources needed for election integrity

🎟 **Scan the QR code above to get your free visitor's badge!**

NEWS:

19. GSMA Confirms End-to-End Encryption for RCS, Enabling Secure Cross-Platform Messaging

Original Source: The Hacker News by Ravie Lakshmanan

The GSMA (Global System for Mobile Communications Association) has officially confirmed the implementation of end-to-end encryption for Rich Communication Services (RCS), marking a significant advancement in secure messaging across platforms.

This move aims to enhance privacy and security for users by protecting messages from interception and unauthorised access.

The adoption of encryption for RCS addresses longstanding security concerns and positions it as a more secure alternative to traditional SMS and other messaging services. This development is expected to bolster user confidence in RCS, encouraging wider adoption and integration across communication networks.

CyberSecurity Advisors Network

NEWS:

20. Remote Access Infra Remains Riskiest Corp. Attack Surface

Original Source: Dark Reading by Robert Lemos

Remote access infrastructure continues to be the riskiest attack surface for corporations, as highlighted in recent cybersecurity reports.

The surge in remote work has expanded the attack vectors available to cybercriminals, who exploit vulnerabilities in remote systems to gain unauthorised access to corporate networks.

This vulnerability emphasises the need for companies to strengthen their remote access protocols, implement multi-factor authentication, and conduct regular security audits.

By prioritising the security of remote access points, businesses can significantly mitigate the risk of data breaches and cyberattacks.

CyberSecurity Advisors Network

NEWS:

21. ClickFix Widely Adopted by Cybercriminals, APT Groups

Original Source: SecurityWeek by Ionut Arghire

Consumer advocacy groups are intensifying their push for legislation that addresses security concerns with Internet of Things (IoT) devices, particularly around the end-of-life phase.

The proposed IoT security bill aims to ensure that manufacturers are legally required to maintain software updates and security patches for a defined period after a product is discontinued.

This legislation is seen as crucial for preventing outdated devices from becoming security liabilities within consumer networks. The bill also seeks to enhance transparency, requiring companies to clearly inform consumers about the lifespan of product support from the point of purchase, thus promoting better consumer awareness and decision-making regarding IoT devices.

CyberSecurity Advisors Network

NEWS:

22. Apple's alleged UK encryption battle sparks political and privacy backlash

Original Source: The Register by Connor Jones

Apple is at the centre of a contentious debate in the UK over its encryption practices, which have ignited significant political and privacy backlash.

Allegations suggest that Apple's stringent encryption methods hinder law enforcement's ability to access critical data during investigations, sparking a heated dispute about balancing privacy rights with national security needs.

This controversy highlights the ongoing global tension between technology companies committed to protecting user data and government agencies advocating for backdoor access to facilitate criminal investigations. The outcome of this battle could have far-reaching implications for privacy laws and tech company operations worldwide.

For more on this article see Article 32: 'Opinion: Yet Another Encryption Kerfuffle' by CyAN's John Salomon

NEWS:

23. Consumer Groups Push IoT Security Bill to Address End-of-Life Concern

Original Source: Dark Reading by Arielle Waldman

Consumer advocacy groups are intensifying their push for legislation that addresses security concerns with Internet of Things (IoT) devices, particularly around the end-of-life phase.

The proposed IoT security bill aims to ensure that manufacturers are legally required to maintain software updates and security patches for a defined period after a product is discontinued.

This legislation is seen as crucial for preventing outdated devices from becoming security liabilities within consumer networks. The bill also seeks to enhance transparency, requiring companies to clearly inform consumers about the lifespan of product support from the point of purchase, thus promoting better consumer awareness and decision-making regarding IoT devices.

CyberSecurity Advisors Network

ANALYSIS:

24. How Economic Headwinds Influence the Ransomware Ecosystem

Original Source: Dark Reading by Alexander Culafi

Economic fluctuations are significantly impacting the ransomware ecosystem, shifting the dynamics of how and why attacks are conducted.

Recent economic headwinds have led cybercriminals to adapt their strategies, increasingly targeting sectors perceived as more vulnerable to disruption.

This analysis explores how economic downturns lead to a rise in ransomware incidents, as attackers capitalise on the heightened desperation of businesses to recover data and maintain operations.

It also discusses the evolving ransomware economy, where demand for quick financial returns drives the innovation of ransomware techniques, making it imperative for organisations to adapt their cybersecurity strategies to this changing landscape.

ANALYSIS:

25. Kids can bypass anything if they’re clever enough!’ How tech experts keep their children safe online

Original Source: The Guardian by Amy Fleming

This article explores the challenges that tech-savvy parents face in keeping their children safe online, emphasising the cunning and ingenuity that kids often exhibit in circumventing digital safeguards.

Tech experts share personal strategies and insights on fostering a safe online environment, including open communication about internet risks, the use of advanced parental controls, and educating children about digital footprints and privacy.

The piece highlights the balance between protecting children and empowering them with the skills to navigate the online world responsibly, stressing the importance of adapting safety measures as technology and online behaviours evolve.

CyberSecurity Advisors Network

EPIC's 2025 International Privacy Champion Award

Nominations Now Open!

The search is on for the next EPIC International Privacy Champion—an award recognizing exceptional contributions to privacy, data protection, and human rights beyond the U.S.

Who deserves the spotlight? Think legal pioneers, fearless journalists, dedicated advocates, groundbreaking researchers, and those leading impactful campaigns.

Nominate an individual or group making a difference in the fight for privacy! 🏆🔍

epic.org / ELECTRONIC PRIVACY INFORMATION CENTER

ANALYSIS:

26. U.S. Cybersecurity and Data Privacy Review and Outlook – 2025

Original Source: Gibson Dunn

The U.S. Cybersecurity and Data Privacy Review and Outlook for 2025 provides a comprehensive analysis of the current state and future projections in cybersecurity and data privacy landscapes.

This report highlights the increasing complexity of cyber threats and the evolving regulatory frameworks aimed at enhancing data protection.

Key insights include the escalation of state-sponsored attacks, the rising importance of cybersecurity in corporate governance, and the challenges and opportunities posed by new technologies such as AI and IoT.

The outlook underscores the necessity for businesses to integrate robust cybersecurity measures and for lawmakers to craft policies that balance security with privacy rights.

CyberSecurity Advisors Network

ANALYSIS:

27. Apple vs. UK Government

Original Source: PrivID (Substack)

The ongoing legal battle between Apple and the UK government centres on the contentious issue of encryption and access to digital communications.

This clash is part of a broader debate over privacy and security, with the UK seeking ways to circumvent encryption to combat crime and terrorism.

Apple, steadfast in its commitment to user privacy, argues that creating backdoors for government access undermines security for all users globally.

This analysis delves into the implications of such legal confrontations for tech companies and consumers, emphasising the potential global fallout of weakening encryption standards.

CyberSecurity Advisors Network

ANALYSIS:

28. Biggest Cyber Threats to the Healthcare Industry Today

Original Source: Dark Reading by Bhavya Jain

The healthcare industry faces unprecedented cyber threats that jeopardise patient data and critical healthcare operations.

This article outlines the most significant threats, including ransomware attacks that lock access to vital records, phishing schemes targeting healthcare professionals, and breaches of sensitive patient information through insecure networks.

The need for robust cybersecurity measures has never been more urgent, as these threats not only risk patient confidentiality but also can disrupt entire healthcare systems. Enhanced security protocols, staff training, and investment in advanced cybersecurity technologies are crucial for safeguarding against these evolving threats.

CyberSecurity Advisors Network

ANALYSIS:

29. A Guide to Security Investments: The Anatomy of a Cyberattack

Original Source: SecurityWeek by Torsten George

This guide offers a comprehensive breakdown of the anatomy of a cyberattack, providing insights into the sequential stages that attackers often follow: reconnaissance, weaponisation, delivery, exploitation, installation, command and control, and actions on objectives. It emphasises the importance of understanding these phases to better invest in cybersecurity measures effectively.

The article advocates for strategic security investments that can detect and respond to threats at each stage, reducing the potential impact on an organisation. This proactive approach is crucial for businesses to enhance their resilience against increasingly sophisticated cyber threats.

CyberSecurity Advisors Network

ANALYSIS:

30. Taming Agentic AI risks with FAIR-CAM

By CI-ISAC Australia Ambassador for Cyber Threat-Led/Informed Risk Measurement and Co-Chair of the Sydney Chapter of the FAIR Institute, Denny Wan

The article discusses the innovative FAIR-CAM framework, designed to mitigate risks associated with agentic Artificial Intelligence (AI).

FAIR-CAM, which stands for Fairness, Accountability, Integrity, and Resilience - Context, Agency, and Means, provides a structured approach to ensure AI systems are developed and deployed responsibly.

Denny Wan emphasises the importance of addressing the ethical implications of AI, particularly as systems gain more autonomy and decision-making capabilities.

The framework aims to guide organisations in creating AI that is not only technologically advanced but also ethically aligned, promoting transparency and trust in AI applications.

CyberSecurity Advisors Network

CyAN Members Quick Reminder! #CyANQuiz?

Hey CyAN Cyber Champs,

Are you ready to put your cybersecurity skills to the test? The Quarterly #CyANQuiz Challenge is back on March 31st—and this time, the stakes are even higher!

🔹 30 questions. Timed. No second chances.
🔹 All based on recent cybersecurity news & events—so keep your knowledge sharp!

📅 **Check your inbox** on March 31st for the quiz link—**just click, answer, and climb the leaderboard!**
🏆 Why play? **Challenge yourself, have fun, and compete for awesome prizes** (while proving your cyber dominance).

This isn’t just a quiz—it’s a **year-long battle for bragging rights in the CyAN community!**

Think you’ve got what it takes? Step up and prove it!

CyAN Cybersecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

31. Fostering Australia's Autonomy: The Imperative for Sovereign Satellite Communication Systems

By CyAN Board Member and Global VP, Kim Chandler McDonald

In a detailed exploration, CyAN Board Member and Global VP, Kim Chandler McDonald, addresses the urgent need for Australia to establish sovereign satellite communication systems.

This analysis highight the critical importance of self-reliance in satellite technology, essential for bolstering national security and driving economic prosperity.

As we face increasing global dependencies on foreign technologies amidst escalating geopolitical tensions, the push for robust, sovereign infrastructure becomes more than a precaution—it's a strategic imperative.

Kim emphasises that this move towards technological autonomy is crucial not only for maintaining Australia’s digital independence but also for ensuring its position in a competitive global arena.

This analysis serves as a call to action for nations worldwide, urging them to consider similar strategies to protect and empower their futures.

CyAN CyAN Members
Op Eds, Articles, etc

32. Opinion: Yet Another Encryption Kerfuffle

By CyAN Board Member and Communications Director John Salomon

In his latest opinion piece, CyAN Board Member and Communications Director John Salomon addresses the recurring debates surrounding encryption policies.

John argues against weakening encryption standards, citing that such measures would compromise global digital security without significantly aiding law enforcement efforts.

Additionally, he emphasises the critical importance of maintaining strong encryption to protect personal and national security interests.

John calls for a balanced approach that respects privacy rights while addressing legitimate security concerns, urging policymakers to consider the broader implications of encryption backdoors.

UPCOMING CyAN and CyAN Partner EVENTS:

- **Trust & Safety Forum at Forum INCYBER Europe (FIC), Lille, France: April 1-2**
- **GITEX AFRICA, Marrakesh, Morocco: 14-16 April**
- **GITEX ASIA: Singapore (Marina Bay Sands) 23-25 April**
- **GISEC: Dubai Word Trade Center, Dubai, UAE: 6- 8 May**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), May 8, London, UK**
- **World AI Technology Expo UAE, Dubai, UAE: 14-15 May 2025 https://worldaiexpo.i**
- **MaTeCC, Rabat, Morocco: 7-9 June, 2025**

CyAN Cybersecurity Advisors Network

Catch up on Past Issues:

Missed an issue of (In)Securities? No worries! Scan the QR code to explore our archive of past editions—packed with insights, trends, and actionable tips to keep you ahead in the ever-evolving world of cybersecurity. Dive in and catch up today!

CyberSecurity Advisors Network

If you found this interesting, please like and share it with your friends and colleagues!

#ReallyInterestingCyberStuff!
#SharingIsCaring