WhoisXML API Participates in Cybersec 2025

Posted on May 15, 2025

Ching Chiao, Head of APAC & Global Partnership at WhoisXML API, joined more than 20,000 security professionals from around the world in the recently concluded Cybersec 2025. He participated as a speaker at the three-day conference and expo that aims to take on digital threats as one cybersecurity community.

Held in Taiwan on 15–17 April 2025, Cybersec 2025 hosted more than 300 sessions and speakers and focused on 28 various themes, including artificial intelligence (AI), cloud, AI of Things (AIoT) and hardware, financial technology (fintech), and open-source security. Several of the topics resonated with us, and we'll dive into some of them in this post.

The Role of AI in Security

AI was among the major themes across numerous forums and sessions at Cybersec 2025, including the dedicated AI Security & Safety Forum and the Zero-Trust Forum. Specifically, the dual role of AI as an escalating threat and promising defense tool was heavily discussed, echoing the World Economic Forum (WEF)'s analysis that revealed 47% of organizations are concerned about the potential of generative AI to power more sophisticated cyber attacks.

In addition to that worry, AI-powered threats can enable threat actors to supersize their weapons. Ransomware, for instance, can move away from basic file encryption to advanced extortion techniques that compromise not only data but also business operations and reputations.

On the other hand, the cybersecurity community can also utilize AI capabilities, such as through predictive threat intelligence (PTI) and proactive threat defense and response—two tactics that were also tackled in several sessions.

Predictive Threat Intelligence

Ching Chiao's topic, "Empowering Cyber Defense with Predictive Threat Intelligence and External Attack Surface Management (EASM)," focused on how PTI can transform cybersecurity by allowing organizations to detect and neutralize threats early on.

He talked about the best practices for implementing PTI, including its integration into EASM to protect publicly accessible assets from modern cyber risks. He went deeper by providing practical guidance on aligning PTI and EASM, which involves using sophisticated data analysis and DNS information for immediate threat identification.

Proactive Threat Detection and Response

The theme of leveraging intelligence to anticipate and proactively defend against threats is woven into discussions around several conference agendas. Some Cybersec 2025 sessions, for instance, mentioned how AI and machine learning (ML) give defense tools the capability to analyze vast amounts of data in real time, which facilitates fast threat detection and automated response.

A demonstration by threat researchers from PSIRT and Threat Research Team TXOne Networks Inc., highlighted the role of AI in threat detection and response. The team showed how their AI system was able to detect 67% more hidden threats that most antivirus programs miss. The system was designed to mimic expert malware analysis and predict how different malicious code will behave without actually running it.

Cloud Security as a Priority

Various sessions at Cybersec 2025 tackled the widespread adoption of cloud services and the corresponding security challenges they introduce that traditional security models can no longer sufficiently address. Central to these discussions were the innovative strategies to address these challenges.

Among the security approaches cited to provide adequate and intelligent security protection in hybrid cloud environments were next-generation managed security service providers (MSSPs) that can monitor, detect, and respond to threats in the cloud and on-premises. These MSSPs integrate various security services, such as:

- Security operations centers (SOCs)

- Managed detection and response (MDR)
- Cloud-native application protection platforms (CNAPPs)

Experts also highlighted the need to tackle cloud security right from the start—during the security planning phase—through the Secure by Design and Security by Default cloud security management frameworks.

Another recurring concern was ensuring strong cloud governance and compliance, with several discussions around cyber and privacy regulations specifically pertaining to cloud environments. Participants were able to learn strategies for simplifying hybrid cloud governance and implementing cloud-native security governance.

Zero Trust as the Contemporary Cybersecurity Standard

The zero-trust security model has gained significant traction as a foundational approach to cybersecurity, and its prominence was evident throughout the Cybersec 2025 agenda. There was a dedicated Zero-Trust Forum, and the framework was also mentioned across various other sessions.

The core tenet of zero trust—often summarized as “trust none, verify all”—was highlighted as the contemporary cybersecurity standard because organizations simply cannot trust anything these days. “Cybercriminals exploit phishing websites and social engineering tactics to steal user credentials, disguising their attack devices as legitimate authentication endpoints. By doing so, they successfully bypass multifactor authentication (MFA) protections and gain unauthorized access to both cloud and on-premises systems,” said Huang Chien-Sheng, CEO of iTop Digital Technology Co. Ltd.

Sessions explored zero-trust principles, such as rigorous identity verification, granular microsegmentation, and the enforcement of least privilege access, alongside practical guidance on how organizations can effectively implement these principles across their infrastructure.

Securing the Supply Chain

Cybersec 2025 also had dedicated discussions about supply chain security, including sessions that talked about adopting transparency through Software Bill of Materials (SBOM), an essential component that improves visibility into software components and associated vulnerabilities.

Regulations surrounding supply chain security were also tackled as these have become increasingly stringent. The European Union (EU)'s Cyber Resilience Act (CRA), for instance, aims to enhance the cybersecurity of digital products with hardware and software elements placed on the EU market by establishing essential cybersecurity requirements and obligations for manufacturers and sellers. Ultimately, it seeks to improve the overall level of cybersecurity across the EU by making products more secure by design, and affected organizations must be able to adhere to its requirements.

About WhoisXML API

WhoisXML API is a seasoned OEM data provider, specializing in delivering well-parsed, normalized, and comprehensive WHOIS, IP, and DNS intelligence. With more than 15 years of industry experience, we have amassed a vast repository of data, encompassing more than 23.8 billion historical WHOIS records, 50+ billion hostnames, 116+ billion DNS records, 10.5+ million IP netblocks, and 99.5% coverage of active IPv4 and IPv6 addresses.

We offer a wide range of Internet intelligence solutions that serve as a robust foundation for leading cybersecurity products and services, empowering businesses to enhance their cybersecurity posture, gain deeper insights, and focus on core product development. For one, our predictive threat intelligence data feeds leverage AI predictive analytics capabilities, enabling organizations to detect potential malicious web properties early.

Trusted by more than 52,000 satisfied customers spanning cybersecurity, marketing, law enforcement, e-commerce, and financial services, WhoisXML API has consistently been recognized for its rapid growth and innovation, earning accolades as an Inc. 5000 honoree and a Financial Times Top Fastest-Growing Company.