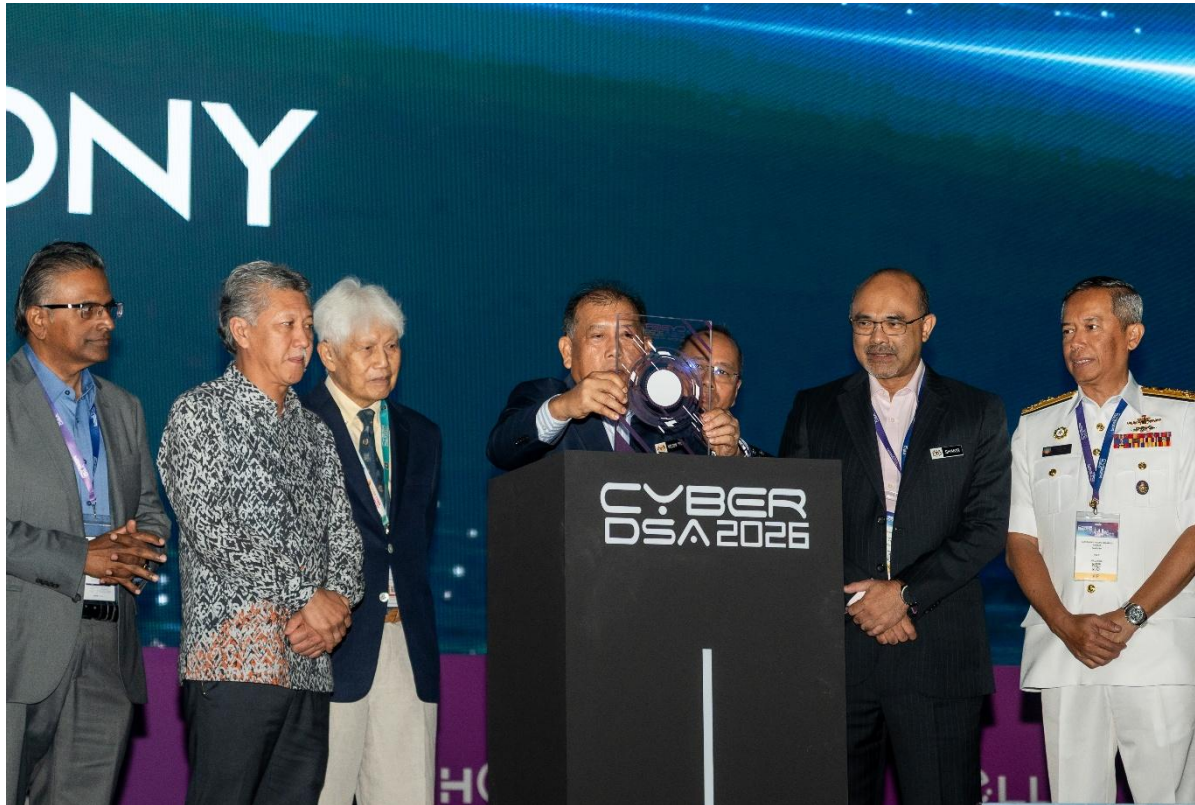




YB Datuk Wilson Ugak Anak Kumbong, Deputy Minister of Digital Malaysia (middle), officially opens CyberDSA 2026 at the Malaysia International Trade and Exhibition Centre (MITEC), Kuala Lumpur, on 5 October 2026. The Deputy Minister is accompanied by Encik Ma. Sivanesan, Deputy Secretary General (Digital Development), Ministry of Digital, Dato' Shahrudin bin Abu Sohot, Secretary General, Ministry of Tourism, Arts and Culture Malaysia, Tan Sri Asmat Kamaludin, Chairman of Aerosea Exhibitions Sdn Bhd, Dato' Sri Noor Hisam bin Nordin, Director of Crime Prevention and Community Safety Department of the Royal Malaysia Police, Encik Shakib Ahmad Shakir Jamaludin, Deputy Secretary General (Strategic & Management), Ministry of Digital, and Rear Admiral Dato' Fadhl bin Abdul Rahman, Commander, Defence Cyber and Electromagnetic Command, Malaysian Armed Forces.

CyberDSA 2026 Opens in Kuala Lumpur as Malaysia's AI Ambition Puts Cybersecurity, Trust and Sovereign Capability in Sharper Focus

As CyberDSA opens its fourth edition at MITEC, attention turns from what AI can deliver to what Malaysia must be able to secure, govern and control as AI becomes embedded across the economy.

Kuala Lumpur, 5th October 2026 – Cyber Digital Services, Defence & Security Asia (CyberDSA) 2026 officially opened today at the Malaysia International Trade and Exhibition Centre (MITEC), Kuala Lumpur, bringing together government, defence and security agencies, regulators, industry leaders, technology providers and researchers as Malaysia advances its ambition to become an AI Nation by 2030.

The three-day event, now in its fourth edition, was officially opened by YB Datuk Wilson Ugak Anak Kumbong, Deputy Minister of Digital Malaysia.

FOR IMMEDIATE RELEASE

The opening comes as the race to adopt artificial intelligence creates another, less visible challenge: securing the data, infrastructure, networks and digital systems on which AI, businesses and essential services increasingly depend.

For Malaysia, where AI adoption is moving from policy ambition to implementation, the two agendas cannot be separated.

The question is no longer simply what AI can do for Malaysia, but what Malaysia must be able to secure, govern and control as AI becomes more deeply embedded across the economy.

Cybersecurity is therefore no longer a protective function at the edge of digital transformation; it is a condition on which digital transformation depends.

In his opening address, YB Datuk Wilson Ugak Anak Kumbong emphasised that Malaysia's ambition to become an AI Nation must be underpinned by security, trust and national capability. *"An AI nation must also be a secure nation. AI depends on data. Data depends on infrastructure. Infrastructure depends on security. And ultimately, the willingness of people and businesses to participate in the digital economy depends on trust. Remove trust from that equation, and the entire proposition becomes considerably weaker,"* he said.

Malaysia's current direction reflects this shift. The Malaysia Digital Action Plan 2030 (MD2030) sets out the country's pathway towards becoming an AI Nation by 2030, while the National AI Action Plan 2026–2030 translates that ambition into implementation across government, business and society. The establishment of AI Malaysia Berhad, the country's national lead AI agency under the Ministry of Digital, places governance, trust, assurance and national capability alongside adoption and innovation in that agenda.

The greater the role of AI, data and connected systems in the economy, the greater the consequence when those systems are compromised.

Held under the theme *"Advancing Secure AI, Strengthening Digital Trust, and Safeguarding Data Sovereignty,"* CyberDSA 2026 brings the security implications of rapid digitalisation into the same room as the technologies driving it.

The opening ceremony brought together government, defence and security agencies, regulators, cybersecurity practitioners, technology companies, researchers and industry leaders from Malaysia and abroad.

This breadth reflects how far the cybersecurity conversation has moved. Financial systems, telecommunications, energy, water, transportation, public services and increasingly connected cities are generating and relying on growing volumes of data,

FOR IMMEDIATE RELEASE

while automation and AI are becoming more deeply integrated into decision-making and service delivery.

Cybersecurity is therefore about more than preventing intrusion. It is about preserving confidence in the integrity of information, maintaining continuity when systems are attacked, protecting sensitive and strategic data, and ensuring critical digital capabilities remain resilient under pressure.

Data sovereignty adds another dimension to the challenge. As organisations increasingly rely on cloud infrastructure, AI models and technology ecosystems that cross jurisdictions, questions over where data resides, who can access it and under whose rules it is governed are becoming strategic considerations for governments and businesses.

That breadth is also visible on the exhibition floor, where 167 participating companies and organisations from 21 countries are presenting technologies and capabilities spanning system integration, Security Information and Event Management (SIEM), Security Operations Centre (SOC) capabilities and managed security services, data protection and encryption, cryptography, cyber ranges, threat monitoring and intelligence, network, cloud and endpoint security, telecommunications and satellite capabilities, as well as cyber defence, cyber warfare, electronic warfare and AI infrastructure.

The range reflects an increasingly interconnected security environment, where protecting an organisation, critical infrastructure or national system requires securing data, networks, endpoints, cloud environments, communication infrastructure and the intelligence used to detect and respond to threats.

Across its exhibition, conference, flash talks, MoU signings and specialised programmes, CyberDSA 2026 brings together policymakers, regulators, defence and law enforcement agencies, critical infrastructure operators, CISOs, researchers and technology providers—stakeholders that may approach cybersecurity from different perspectives but increasingly share the same dependencies.

For Aerosea Exhibitions Sdn Bhd, organiser of CyberDSA, the event's continued development is shaped not simply by its growth, but by its relevance to the governments, industries and technology communities it was created to serve.

Tan Sri Asmat Kamaludin, Chairman of Aerosea Exhibitions, said the value of a platform such as CyberDSA lies in its ability to keep pace with the priorities and challenges taking shape beyond the exhibition hall.

“A platform such as this must reflect what governments are prioritising, what industries are confronting, what capabilities the market is developing, and where greater understanding between these communities is needed,” he said.

FOR IMMEDIATE RELEASE

Aerosea has positioned CyberDSA not as a marketplace for cybersecurity technologies, but as a point of convergence between national priorities and the capabilities being developed by industry.

With two days still to come, CyberDSA 2026 continues on 6 and 7 October 2026.

For those responsible for building, operating, protecting or governing the systems on which an increasingly digital world depends, the conversation is far from over.

-END-

For further information, kindly contact:

Aerosea Exhibitions Sdn Bhd

Tengku Dayana

PR & Communications

Email: dayana@aeroseaexhibitions.com

Tel: +603 2702 7702

Website: www.cyberdsa.com

Social Media:

1. Facebook: @CyberDSA <https://www.facebook.com/CyberDSA>
2. Instagram: @CyberDSA <https://www.instagram.com/cyberdsa/>
3. LinkedIn: @CyberDSA <https://www.linkedin.com/company/cyber-dsa>
4. YouTube: @CyberDSA <https://www.youtube.com/@cyberdsa8206>
5. TikTok: @CyberDSA <https://www.tiktok.com/@cyberdsa>
6. X: @CyberDSA <https://x.com/CyberDsa>