CYSEC INDONESIA
21ST GLOBAL EDITION

20TH AUGUST, 2026
FOUR SEASONS HOTEL
JAKARTA, INDONESIA

ORGANIZED BY
CYSEC GLOBAL
REDEFINING CYBERSECURITY

EMPOWERING INDONESIA'S DIGITAL FUTURE: SECURE, RESILIENT, READY!

www.indonesia.cysecglobal.com

CYSEC INDONESIA
21ST GLOBAL EDITION

AGENDA

20TH AUGUST 2026, THURSDAY

8.00 - 9.00 — **REGISTRATIONS & NETWORKING**

9.00 - 9.10 — **Welcome Address and Introduction to the Conference**

9.15 - 9.30 — **Securing Indonesia's Digital Sovereignty: BSSN's Vision for a Resilient, Ready 2030**

GOVT ADDRESS

9.35 - 9.50 — **Securing AI Agents With Behavioral Analytics**

SPONSOR SPOTLIGHT

9.55 - 10.45 — **Strengthening National Cyber Resilience - Protecting Critical Infrastructure in the Digital Era**

PANEL DISCUSSION

This panel will bring together government leaders and cybersecurity experts to explore strategies for strengthening national cyber resilience.
Discussions will focus on safeguarding critical infrastructure, fostering public–private partnerships, developing effective national cyber defense strategies.

- Protecting National Critical Infrastructure from Cyber Threats: Critical infrastructure such as energy systems, transportation networks, healthcare services, financial institutions, and telecommunications forms the backbone of a nation's economy and public safety.
- Public–Private Collaboration: A large portion of critical infrastructure is owned or operated by the private sector, making collaboration between government and private organizations essential.
- National Cyber Defense Strategies: Developing a comprehensive national cyber defense strategy is vital for protecting a country's digital ecosystem.
- Cross-Border Cyber Threat Intelligence Sharing: Sharing threat intelligence, best practices, and incident response strategies with other nations and global organizations helps governments detect and mitigate threats more effectively.

10.50 - 11.20 — **COFFEE BREAK**

CYSEC INDONESIA
21ST GLOBAL EDITION

AGENDA

20TH AUGUST 2026, THURSDAY

11.25 - 11.50 **Cybersecurity Regulations, Data Protection & Ransomware: Strengthening Defences Against Financial Cybercrime**

FIRESIDE CHAT

This panel will explore how regulatory frameworks, industry collaboration, and advanced security strategies can help organizations protect sensitive data, prevent ransomware attacks, and combat the growing cybercrime economy while maintaining compliance and operational resilience.

- Financial Cybercrime - How evolving national and international cybersecurity regulations help organizations strengthen defences against ransomware, fraud, and financial cyber threats.
- Data Protection - The importance of protecting sensitive financial and personal data to prevent breaches that often lead to ransomware and cyber extortion attack.
- Ransomware & the Rise of Organized Cybercrime – Understanding how ransomware groups operate, including ransomware-as-a-service models, and the increasing targeting of financial institutions and enterprises.
- Compliance vs. Cyber Resilience – Why regulatory compliance alone is not enough and how organizations can build proactive, resilient cybersecurity strategies.

11.55 - 12.10 **Next-Gen Response: AI, XDR, and Managed Detection in Action**

SPONSOR SPOTLIGHT

12.15 - 12.30 **The PDP Law Is Live - Now What? A Conversation with Indonesia's Data Regulator**

KEYNOTE ADDRESS

Indonesia's Personal Data Protection Law crossed its transitional deadline in October 2024. The dedicated Lembaga PDP supervisory agency is still being established - as of mid-2026, enforcement sits with Komdigi's Directorate General. This conversation will unpack what enforcement looks like today, what the DPO appointment obligation means in practice, and how the incoming Cybersecurity Bill will change the landscape further.

- 72-hour breach notification: who has been complying and who hasn't?
- The Lembaga PDP: when will it be operational and what powers will it have?
- Cross-border data transfers and extraterritorial reach - what multinationals must know
- The pending Cybersecurity Bill and how it complements or conflicts with existing PDP obligations

12.35 - 13.25 **NETWORKING LUNCHEON**

CYSEC INDONESIA
21ST GLOBAL EDITION

AGENDA

20TH AUGUST 2026, THURSDAY

13.30 - 14.10 **CISOs on the Front Line: Managing Cyber Risk When You Can't Hire, Can't Pay, And Can't Fail**

FIRESIDE CHAT

Indonesia faces a critical shortfall of trained cybersecurity professionals the same talent crisis BSSN's 20-year workforce development plan is trying to address. Senior CISOs in an unscripted conversation about the unglamorous reality: underfunded teams, pressure to comply with BSSN Reg 1 & 2, OJK mandates, PDP obligations - and how they're making it work.

- Building a CIRT when you can't fill the headcount: automation, MSSP partnerships, and hard choices
- The SPBE e-government framework and what it means for SOEs managing public data
- How Indonesia's cyber talent gap compares to regional peers, and what academic partnerships are delivering
- What a CISO needs from the Cybersecurity Bill - and what they're afraid of.

14.15 - 14.30 **AI as Both Shield and Threat: Indonesia's Research Agenda for Intelligent Cybersecurity**

SPOTLIGHT SESSION

AI is no longer a future consideration for cybersecurity it is the present battlefield. Adversaries are already deploying AI to automate attacks, craft undetectable phishing, bypass legacy defences, and probe critical infrastructure at machine speed. And yet, the same technology holds the greatest promise for building Indonesia's next gen of intelligent cyber defence. In this session, we will move beyond the global AI-security conversation and anchor it firmly in Indonesia's context: what threats are already here, what research is underway, and what Indonesia must do right now.

- How AI has fundamentally changed the attacker's economics - what used to take a nation-state now takes a laptop and an API key
- What BRIN's national research agenda looks like specifically for AI in cybersecurity
- How the Presidential mandate on digital economy (Regulation 78/2021) connects to national cyber readiness?
- Autonomous malware and polymorphic attacks - what happens when malware rewrites itself to evade detection in real time
- Where Indonesia's research is ahead, and where the gaps are dangerously wide
- What intelligent cybersecurity architecture actually looks like at a national level beyond buying tools

14.35 - 14.55 **COFFEE BREAK**

CYSEC INDONESIA
21ST GLOBAL EDITION

AGENDA

20TH AUGUST 2026, THURSDAY

15.00 - 15.30 — **The Boardroom Mandate: Why Cybersecurity Has Become a Business Growth Strategy**

FIRESIDE CHAT

As Indonesia accelerates toward its Golden Vision 2045 and digital economy ambitions, the country's largest enterprises and state-owned companies are discovering that security posture has become a direct input to business outcomes. This fireside conversation moves beyond the security-as-defence narrative and examines cybersecurity as a strategic growth lever — one that belongs in the conversation with the CFO, the board, and the CEO, not just the CISO.

- When did your board stop asking "what does security cost?" and start asking "what does a breach cost us?"
- Security as a sales tool - have you won or lost a deal because of your security credentials?
- The one thing Indonesian boards consistently underfund - and why it's not the firewall
- What does a genuinely security-mature Indonesian organisation look like in 2026, and who's closest to it?

15.30 - 16.15 — **Adopting Zero Trust: From Strategy to Implementation**

FIRESIDE CHAT

This panel will explore how organizations can successfully adopt the Zero Trust model to strengthen cyber resilience, protect critical data, and adapt to modern IT environments. Experts will discuss implementation strategies, the importance of identity-driven security, and the role of continuous monitoring in building a secure and resilient digital ecosystem.

- Implementing Zero Trust in Modern Digital Environments: As organizations increasingly adopt cloud services, remote work, and connected devices, traditional security models are becoming less effective.
- Protecting Critical Data and Applications: At the core of the Zero Trust model is the protection of sensitive data and critical applications.
- The Role of Identity and Access Management: Identity has become the new security perimeter in modern cybersecurity frameworks. Strong IAM solutions are essential for implementing Zero Trust, enabling organizations to authenticate users, manage privileges and enforce least-privilege access.

16.15 - 16.20 — **CLOSING REMARKS**

CYSEC GLOBAL CALENDAR 2026

CYSEC AFRICA	26TH FEBRUARY | 2026 | JOHANNESBURG, SA	
CYSEC THAILAND	22ND JULY | 2026 | BANGKOK, THAILAND	
CYSEC INDONESIA	20TH AUGUST | 2026 | JAKARTA, INDONESIA	
CYSEC QATAR	8TH – 9TH SEPTEMBER | 2026 | DOHA, QATAR	
CYSEC KUWAIT	30TH SEPTEMBER | 2026 | KUWAIT CITY, KUWAIT	
CYSEC KENYA	7TH OCTOBER | 2026 | NAIROBI, KENYA	
CYSEC MENA	14TH OCTOBER | 2026 | MANAMA , BAHRAIN	
CYSEC U.A.E	22ND OCTOBER | 2026 | ABU DHABI, UAE	
CYSEC EGYPT	5TH NOVEMBER | 2026 | CAIRO, EGYPT	
CYSEC OMAN	19TH NOVEMBER | 2026 | MUSCAT, OMAN	

CYSEC INDONESIA
21ST GLOBAL EDITION

ORGANIZED BY
CYSEC GLOBAL
REDEFINING CYBERSECURITY

20TH AUGUST 2026

FOUR SEASONS HOTEL JAKARTA, INDONESIA

save the **date**

BOOK YOUR SPOT NOW

FOR SPEAKING ENQUIRIES

pavani@cysecglobal.com
Phone: +91-8439819560

SPONSORSHIP OPPORTUNITIES

mausam.khan@cysecglobal.com
Phone: +971 50 376 1665

MEDIA PARTNERSHIPS

media@cysecglobal.com