Terms of Reference

Talk Show IDNOG 08: Cyber Security

Overview

Indonesia Network Operator Group (IDNOG) is a community of network operators, engineers, and professionals in Indonesia who come together to discuss and collaborate on various topics related to networking and internet infrastructure. IDNOG serves as a platform for knowledge sharing, technical discussions, and the advancement of networking technologies in Indonesia.

The main objectives of IDNOG include Knowledge Exchange, Collaboration, Industry Advocacy, Capacity Building. By bringing together network operators and professionals from various organizations, IDNOG plays a crucial role in fostering collaboration, sharing knowledge, and promoting the advancement of networking technologies in Indonesia.

IDNOG (Indonesia Network Operator Group) organizes workshops and conferences to facilitate knowledge sharing, networking, and collaboration among network operators and professionals in Indonesia. These events provide a platform for participants to learn about the latest developments in networking technologies, exchange ideas, and discuss industry trends.

In this 2023 Workshop and Conference event, IDNOG plan to host a session of Talk show / Panel Discussions with title "Cyber Security" by bringing together experts from different organizations and sectors to discuss relevant topics, share diverse viewpoints, and engage in meaningful conversations.

Indonesia, like many other countries, faces various internet security issues. Some common challenges and concerns related to internet security in Indonesia are Cybercrime, Phishing and Social Engineering Attacks, Malware and Ransomware, Weak Cybersecurity Infrastructure, Data Breaches and Privacy Concerns, Lack of Awareness and Education and Regulatory and Legal Challenges.

But efforts are continuously made by the Indonesian government, industry stakeholders, and cybersecurity organizations to tackle these challenges. These include raising awareness through campaigns, improving cybersecurity infrastructure, promoting cybersecurity education, and collaborating with international partners to combat cyber threats effectively.

Objective

Encourage collaboration and engagement by panellist's discussion and inviting viewers to participate, ask questions, and share their experiences or concerns related to internet security. It can foster a sense of community and create a platform for discussions and knowledge sharing among viewers.

Topics

- Latest trends and emerging threats in the Indonesian cybersecurity landscape.

- Network Monitoring and Incident Response: Techniques and tools for monitoring network traffic, detecting security incidents, and responding effectively to mitigate risks. This may involve discussions on intrusion detection and prevention systems (IDS/IPS), Security Information and Event Management (SIEM), and incident response frameworks
- Data Protection and Encryption: Techniques and protocols for protecting sensitive data in transit and at rest, including encryption technologies, secure data transfer protocols, and data loss prevention (DLP) strategies.

Questions

1. What are the most prevalent cyber threats targeting individuals and businesses in Indonesia?
2. What are the latest trends and emerging threats in the Indonesian cybersecurity landscape?
3. What are the key metrics and indicators that organizations should monitor to detect and respond to network security incidents effectively?
4. How can organizations establish a baseline of normal network behaviour to facilitate anomaly detection and early threat identification?
5. What are the essential tools and technologies for network monitoring, and how can they be leveraged for effective incident response?
6. What are the best practices for securing personal data and privacy in the Indonesian online landscape?
7. How can organizations protect against insider threats and ensure that data remains encrypted even within their own environments?
8. What are the key principles and best practices for ensuring the protection of sensitive data in transit and at rest?
9. What are the challenges and considerations organizations face when implementing encryption in highly regulated industries, such as healthcare or financial services?
10. What are the emerging trends and advancements in data protection and encryption, such as homomorphic encryption or post-quantum cryptography?
11. What role do you wish government agencies play in promoting and ensuring cybersecurity in Indonesia?

Flow of the Talk Show:

a. Introduction of each panellist by moderator
b. Discussion by question (by moderator) and answer/response either speaker/panellist. (*One panellist may challenge/ask question to the other panellist related to the discussed matter*)
c. Questions from the floor/audience moderated mode.
d. Closing remarks by each panellist @ 2 minutes.

Note:
The Talk Show will delivered in balance between fun and professionalism, ensuring that the questions provoke interesting and engaging discussions while still addressing important cybersecurity topics.

Talk Show duration: 60 minutes, 27 July 2023, 11:15 AM to 12:15 PM.

Panellist *(in alphabetical order)*:

1. Farah Fitria Rahmayanti
   Head of Digital Business at Peruri
2. Gildas Arvin Deograt
   Ketua FORMASI (Forum Keamanan Siber dan Informasi)
   dan Senior Konsultan Keamanan Siber dan Informasi
3. Prof. Martianus Frederic Ezerman.
   Adjunct Professor, Nanyang Technological University, Singapore.
   Teaching Graduate Classes in Cryptography
4. Muhammad Salahuddien Manggalanny
   Deputy of Operation CSIRT.ID
5. Semuel A. Pangerapan
   Dirjen Aptika Kementerian Kominfo

Moderator	:	Parlindungan Marius – Komite IDNOG
Date and Location	:	27th July 2023 Raffles Hotel Jakarta Ciputra World Jl. Prof. DR. Satrio Kav. 3 Karet Kuningan - Setiabudi Jakarta Selatan 12940
Audience	:	The audience of the Indonesia Network Operators Group (IDNOG) primarily consists of network operators, engineers, and professionals in Indonesia who are involved in the planning, deployment, operation, and maintenance of networks. These individuals work in various sectors, including telecommunications, internet service providers (ISPs), data centers, government agencies, educational institutions, and other organizations that rely on network infrastructure.