

# Syllabus

## Cyber Security for IT Leaders and Professional

- 3 hari fullday (8.30-4.00 sore)
- Jumlah peserta: 5 orang (minimum)
- Biaya: *sesuai dengan kesepakatan dan tempat pelaksanaan.*

Di era transformasi digital, **ancaman siber** menjadi risiko strategis yang dapat berdampak langsung pada operasional, reputasi, dan keberlanjutan organisasi. Cyber Security tidak lagi hanya menjadi tanggung jawab tim IT, tetapi merupakan tanggung jawab bersama, termasuk para officers sebagai pengambil keputusan, pengawas proses, dan penjaga kepatuhan. Program Cyber Security for IT Leaders dan Profesional ini dirancang untuk membekali peserta dan leader IT di suatu perusahaan dengan pemahaman fundamental mengenai lanskap ancaman siber, prinsip-prinsip keamanan informasi, serta peran dan tanggung jawab officers dalam mencegah, mendeteksi, dan merespons insiden keamanan siber serta beberapa prinsip dan teknik *ethical hacking* dasar. Melalui silabus ini, peserta akan memahami bagaimana kebijakan, tata kelola, dan perilaku kerja yang aman berkontribusi terhadap perlindungan aset informasi organisasi.

Pelatihan ini menekankan pendekatan praktis dan kontekstual, sehingga officers mampu menerapkan prinsip cyber security dalam pengambilan keputusan sehari-hari, memastikan kepatuhan terhadap regulasi, serta mendukung budaya keamanan informasi yang kuat di lingkungan kerja.

### Sesi 1 – Pengantar Cyber Security

- Definition of Cyber Security and Ethical Hacking.
- Examples of *threats* in internet and networking.
- The role of IT leaders and officers in Cyber Security.

### Sesi 2 – Cyber Threat Landscape

- IP Address and Networking essential
- Types of threats: malware, ransomware, phishing, insider threats
- Advanced Persistent Threats (APT)
- Current cyber-attack trends.

### Sesi 3 – Konsep Information Security

- CIA Triad: Confidentiality, Integrity, Availability
- Assets, threats, vulnerabilities, and risks

- Organizational impact of cyber incidents
- Case study

#### **Sesi 4 – Cyber Risk Management for IT Leaders**

- Cyber risk identification and assessment
- Risk appetite and risk tolerance
- Integrating cyber risk into enterprise risk management
- Case study

#### **Sesi 5 – Cyber Security Governance**

- Information security governance principles
- Roles and responsibilities (RACI model)
- Relationship between IT, management, and officers
- Case study

#### **Sesi 6 – Ethical Hacking**

- Introduction to Ethical Hacking
- Penetration Testing Execution Standard (PTES)
- OWASP Top 10
- NIST & ISO 27001
- Case study
- Project Presentation

**Target Pelatihan:** Setelah mengikuti pelatihan ini, peserta diharapkan mampu:

1. Memahami konsep dasar Cyber security dan berbagai jenis ancaman (*threats*).
2. Menyediakan pemahaman komprehensif dari konsep Cyber Security dan ethical hacking, metodologi dan Teknik mengidentifikasi kelemahan system.

Fasilitator:

- Dr (Cand). Yohan Muliono, S.Kom., M.TI.

Kontak:

[wbudiharto@binus.edu](mailto:wbudiharto@binus.edu)

Bpk. Prof. Widodo (WA: 08569887384)

Ibu Dr. Emny (WA: 081387413863)