

**RECAP FREE ROADMAP DARI CYBER SECURITY BASIC (CAREERS  
IN CYBER, SECURITY PRINCIPLES, GOVERNANCE & REGULATION,  
CYBER KILL CHAIN)**

**Untuk memenuhi tugas dari  
Keamanan Sistem dan Jaringan Komputer**

**Oleh:**

**MUHAMMAD FARID MAULUDIN      NIM. 2231740009**



**PROGRAM STUDI DIII TEKNOLOGI INFORMASI  
JURUSAN TEKNOLOGI INFORMASI  
POLITEKNIK NEGERI MALANG  
KAMPUS LUMAJANG  
2025**

## **Daftar isi**

Careers in Cyber .....	3
Security Principles .....	5
Governance & Regulation.....	9
Cyber Kill Chain .....	15

## Careers in Cyber

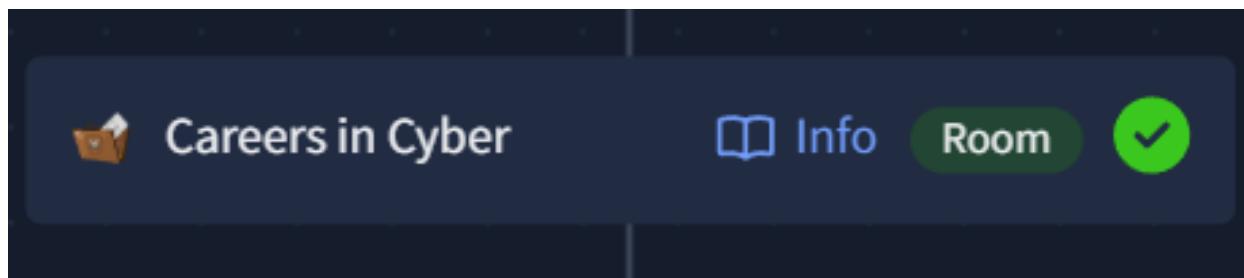
The screenshot shows a digital learning platform interface titled "Careers in Cyber". At the top, there's a banner with a briefcase icon and the text "Learn about the different careers in cyber security.", followed by "Info 30 min". Below the banner are buttons for "Share your achievement", "Help", "Save Room", and "Options". A progress bar at the bottom indicates "Room completed (100%)". The main content area lists nine tasks, each with a green checkmark and a small icon:

- Task 1 ✓ Introduction
- Task 2 ✓ Security Analyst
- Task 3 ✓ Security Engineer
- Task 4 ✓ Incident Responder
- Task 5 ✓ Digital Forensics Examiner
- Task 6 ✓ Malware Analyst
- Task 7 ✓ Penetration Tester
- Task 8 ✓ Red Teamer
- Task 9 ✓ Quiz

Pada pembelajaran ini terdapat penjelasan mengenai jenis dan tugas tentang pekerjaan di bidang cyber security. Berikut merupakan poin-poin yang sudah saya rangkum dalam 7 poin utama. yaitu;

1. **Security analyst**, mencari dan mengevaluasi jaringan perusahaan untuk menemukan data yang dapat ditindaklanjuti dan merekomendasikan untuk insinyur untuk membuat tindakan pencegahan. Jobdesk dari security analyst. yaitu;
  - a. Bekerja dengan variasi pemangku kepentingan untuk analisis kemananan siber seluruh perusahaan
  - b. Kompilasi yang sedang berlangsung melaporkan tentang jaringan yang aman. Dokumentasi isu kemananan dan tindakan untuk memberikan tanggapan.
  - c. Pembuatan rencana keamanan. Di dalam perusahaan mencari alat penyerangan baru dan tren, dan tindakan yang membutuhkan seluruh tim untuk menjaga keamanan data.
2. **Security engginer**, membuat dan mengimplementasikan solusi keamanan menggunakan ancaman dan kerentanan data. Jobdesk dari security engginer. yaitu;
  - a. Menguji dan menyaring tindakan keamanan lintas perangkat lunak
  - b. Memantau jaringan dan laporan untuk memperbarui sistem dan mengurangi kerentanan
  - c. Mengidentifikasi dan membutuhkan implementasi sistem untuk keamanan yang optimal
3. **Incident responder**, merespon produktifitas dan efisiensi dari pelanggaran keamanan. Jobdesk dari incident responder. Yaitu;

- a. Membuat dan mengadopsi rencara secara menyeluruh, respon insiden yang dapat ditindaklanjuti
  - b. Menjaga kekuatan keamanan dengan percobaan terbaik dan mendukung langkah penanggap kejadian
  - c. Pasca kejadian melaporkan dan mempersiapkan untuk serangan masa depan, mempertimbangkan pembelajaran dan adaptasi untuk keluar dari kejadian
4. **Digital formatic examiner**, mengumpulkan dan menganalisis untuk membantu memecahkan kejahatan; mengisi yang bersalah dan membebaskan yang tidak bersalah. Jobdesk dari Digital formatic. Yaitu;
    - a. Mengumpulkan bukti digital sesuai prosedur observasi legal
    - b. Menganalisis bukti digital untuk menemukan jawaban yang sesuai dengan kasus
    - c. Dokumentasi temuan anda dan laporkan kasus
  5. **Malware analyst**, melibatkan analisis program yang mencurigakan. Menemukan apa yang mereka lakukan dan menulis laporan tentang temuan mereka. Jobdesk dari digital formatic examiner. Yaitu;
    - a. Melakukan analisis statik dari program jahat, yang memerlukan insinyur balik
    - b. Melakukan analisis dinamis contoh perangkat lunak berbahaya dari observasi banyak aktifitas lingkungan yang terkendali
    - c. Dokumentasi dan melaporkan semua temuan
  6. **Penetration tester**, berperan untuk menguji kemaanan dari sistem dan perangkat lunak dalam sebuah perusahaan. Jobdesk dari penetration tester. Yaitu;
    - a. Melakukan pengujian pada sistem komputer, jaringan, dan aplikasi web
    - b. Menampilkan penilaian keamanan, audit, dan analisis kebijakan
    - c. Mengevaluasi dan melaporkan wawasan, recomendasi tindakan untuk mencegar serangan
  7. **Red teamer**, menguji kemampuan deteksi perusahaan dan respon perusahaan. Pekerjaan ini memerlukan tindakan peniruan penjahat siber. Jobdesk dari red teamer. Yaitu;
    - a. Emulate peran tindakan jahat untuk menemukan kerentanan yang dapat dieksplorasi. Menjaga akses dan menghindari deteksi
    - b. Menilai control keamanan organisasi, pengetahuan jahat, dan prosedur tanggap insiden
    - c. Mengevaluasi dan melaporkan temuan, dengan data yang dapat ditindaklanjuti untuk perusahaan menghindari contoh di kehidupan nyata



# Security Principles

Security Principles

Learn about the security triad and common security models and principles.

Easy 90 min

Share your achievement Help Save Room 2870 Options

Room completed (100%)

Task 1 ✓ Introduction

Task 2 ✓ CIA

Task 3 ✓ DAD

Task 4 ✓ Fundamental Concepts of Security Models

Task 5 ✓ Defence-in-Depth

Task 6 ✓ ISO/IEC 19249

Task 7 ✓ Zero Trust versus Trust but Verify

Task 8 ✓ Threat versus Risk

Task 9 ✓ Conclusion

## 1. CIA

- a. CIA (confidentiality, integrity, dan availability)
  - **Confidentiality** memastikan bahwa hanya orang atau penerima yang dimaksud yang dapat mengakses data.  
Contoh: Nomor kartu kredit saat belanja online harus dijaga dari pihak tak terpercaya.
  - **Integrity** bertujuan untuk memastikan bahwa data tidak dapat diubah; lebih jauh lagi, kami dapat mendeteksi perubahan apa pun jika terjadi  
Contoh: Alamat pengiriman yang diubah penyusup bisa membuat paket salah kirim
  - **Availability** bertujuan untuk memastikan bahwa sistem atau layanan tersedia saat dibutuhkan  
Contoh: Situs belanja tidak bisa diakses → pelanggan pindah ke toko lain.
- b. Diluar CIA kita dapat memikirkan;
  - **Authenticity**, Memastikan data/asal dokumen benar, bukan palsu.
  - **Nonrepudiation**, Pihak yang mengirim data tidak bisa menyangkal bahwa mereka melakukannya.
- c. Parkerian Hexad (2 tambahan dari triad security)

- **Utilitas**, berfokus pada kegunaan informasi. Misalnya pengguna mungkin telah kehilangan kunci deskripsi untuk mengakses laptop dengan penyimpanan terenkripsi.
- **NonRepudiation**, elemen keamanan ini mengharuskan kita untuk melindungi informasi dari pengambilan, penyalinan, atau pengendalian yang tidak sah

## 2. DAD (Disclosure, Alteration, Destruction)

- a. **Disclosure** (Pengungkapan), lawan dari kerahasiaan, ini terjadi ketika data rahasia diakses atau dibocorkan tanpa izin  
Contoh; rekam medis pasien dicuri dan disebarluaskan ke publik
- b. **Alteration** (Perubahan), lawan dari integritas, ini terjadi saat data diubah tanpa izin, disengaja atau tidak  
Contoh; penyerang mengubah rekam medis jika perawatan salah maka bisa mengancam nyawa
- c. **Destruction/Denial** (Penghancuran/Penolakan), lawan dari ketersediaan, ini terjadi saat sistem / data dibuat tidak tersedia atau dihancurkan  
Contoh; sistem database rumah sakit lumpuh sehingga Layanan tidak bisa berjalan

## 3. Fundamental konsep security model

- a. Model Bell-Lapadula(fokus: kerahasiaan), Mencegah pengungkapan informasi rahasia (confidentiality). Aturan utama:
  - **Simple Security Property ("No Read Up")**, Subjek tidak boleh membaca data dari tingkat keamanan yang lebih tinggi.
  - **Star (\*) Security Property ("No Write Down")**, Subjek tidak boleh menulis ke tingkat keamanan yang lebih rendah.
  - **Discretionary Security Properti**, Menggunakan matriks akses untuk mengatur hak baca/tulis secara spesifik.
- b. Model Biba (fokus : integritas), Mencegah perubahan data yang tidak sah (integrity). Aturan Utama:
  - **Simple Integrity Property ("No Read Down")**, Subjek tingkat integritas tinggi tidak boleh membaca dari data tingkat rendah.
  - **Star (\*) Integrity Property ("No Write Up")**, Subjek tingkat integritas rendah tidak boleh menulis ke data tingkat tinggi.
- c. Model Clark-Wilson (fokus: integritas melalui control bisnis), Menjaga integritas data dalam konteks sistem bisnis. Komponen Utama:
  - **Constrained Data Items (CDI)**: Data penting yang perlu dijaga integritasnya.
  - **Unconstrained Data Items (UDI)**: Data yang tidak dibatasi, seperti input pengguna.
  - **Transformation Procedures (TP)**: Prosedur resmi untuk memodifikasi data.
  - **Integrity Verification Procedures (IVP)**: Prosedur untuk memverifikasi keakuratan CDI.
4. **Defense in Depth (Pertahanan Bertingkat)**, strategi keamanan dengan menerapkan beberapa lapisan perlindungan untuk melindungi sistem atau data penting. Konsep ini mirip dengan mengunci dokumen penting di laci, kemudian mengunci ruangan, apartemen, gerbang gedung, hingga menambahkan kamera pengawas. Tujuan utamanya:
  - Menghambat atau memperlambat penyerang
  - Tidak bergantung pada satu titik pertahanan saja
  - Memberikan waktu untuk mendeteksi dan merespons ancaman

## 5. ISO/IEC 19249:2017

a. Lima prinsip dasar

- **Pemisahan Domain**, Memisahkan komponen (aplikasi, data, sumber daya) ke dalam domain berbeda dengan atribut keamanan tertentu. Contoh: perbedaan hak istimewa antara kernel dan aplikasi pengguna.
- **Pelapisan**, Mengorganisasi sistem ke dalam beberapa lapisan, seperti model OSI. Tiap lapisan memiliki peran dan kebijakan keamanan masing-masing.
- **Enkapsulasi**, Menyembunyikan detail internal dan hanya menyediakan akses melalui antarmuka khusus. Contoh: penggunaan metode dalam OOP atau API untuk akses data.
- **Redundansi**, Menyediakan cadangan atau sistem ganda untuk menjamin ketersediaan dan **integritas**. Contoh: RAID, catu daya ganda.
- **Virtualisasi**, Membagi satu perangkat keras ke beberapa sistem virtual untuk **isolasi**, **sandboxing**, dan pengamatan yang aman terhadap aktivitas mencurigakan.

b. Lima prinsip desain;

- **Hak Istimewa Terkecil**, Memberikan hanya akses minimum yang dibutuhkan pengguna. Contoh: hanya hak baca jika tidak perlu menulis.
- **Minimalisasi Permukaan Serangan**, Mengurangi potensi kerentanan dengan menonaktifkan layanan yang tidak digunakan atau memperkecil jumlah titik masuk sistem.
- **Validasi Parameter Terpusat**, Melindungi sistem dari input berbahaya dengan memusatkan pemeriksaan/validasi data di satu lokasi atau pustaka.
- **Layanan Keamanan Terpusat**, Mengelola fitur keamanan dari satu sistem atau server, misalnya autentikasi pusat. Harus dirancang agar tidak menjadi titik kegagalan tunggal.
- **Penanganan Kesalahan dan Pengecualian**, Sistem harus aman ketika gagal (fail-safe). Contoh: firewall yang rusak tetap memblokir lalu lintas. Jangan membocorkan informasi sensitif dalam pesan kesalahan.

## 6. Zero Trust vs Trust but Verify

a. Trust but Verify (Percaya Tapi Verifikasi)

- **Prinsip:** Tetap memverifikasi meskipun sudah mempercayai entitas (pengguna/sistem).
- **Implementasi:** Gunakan pencatatan/log yang tepat. Lakukan pemeriksaan terhadap aktivitas (log review, sistem deteksi/pencegahan intrusi, proksi, dll).
- **Keterbatasan:** Tidak mungkin memverifikasi semua aktivitas secara manual; perlu otomasi

b. Zero Trust (Nol Kepercayaan)

- **Prinsip:** "*Jangan pernah percaya, selalu verifikasi.*"
- **Konsep:** Kepercayaan dianggap sebagai **kerentanan**. Semua entitas dianggap **bermusuhan** hingga terbukti sebaliknya. Tidak mempercayai perangkat hanya karena berada di jaringan internal.

- **Implementasi:** Autentikasi & otorisasi ketat sebelum mengakses sumber daya. **Mikrosegmentasi** jaringan (setiap segmen bisa sekecil satu host). Setiap komunikasi antar segmen memerlukan pengecekan keamanan tambahan.

## 7. Threat vs risk

- **Kerentanan (Vulnerability)** → Kelemahan dalam sistem yang bisa dieksplorasi.
- **Ancaman (Threat)** → Potensi bahaya yang bisa memanfaatkan kerentanan.
- **Risiko (Risk)** → Kemungkinanancaman terjadi dan dampaknya terhadap bisnis.

Contoh:

- a. Ruang pamer dengan pintu kaca
  - **Kerentanan** → Kaca mudah pecah.
  - **Ancaman** → Seseorang bisa memecahkan kaca dan masuk.
  - **Risiko** → Tingkat kemungkinan kaca pecah dan dampaknya terhadap bisnis.
- b. Sistem database rumah sakit
  - **Kerentanan** → Ada bug dalam sistem database.
  - **Ancaman** → Peretas bisa mengeksplorasi bug untuk mencuri data.
  - **Risiko** → Data pasien bocor, menyebabkan masalah hukum dan reputasi.



# Governance & Regulation

The screenshot shows a digital learning platform interface. At the top, there's a header with the title 'Governance & Regulation' and a subtitle 'Explore policies and frameworks vital for regulating cyber security in an organisation.' Below the header, there are buttons for 'Share your achievement', 'Help', 'Save Room', '1748', and 'Options'. A progress bar at the bottom indicates 'Room completed (100%)'. The main content area is a list of tasks:

- Task 1 ✓ Introduction
- Task 2 ✓ Why is it important?
- Task 3 ✓ Information Security Frameworks
- Task 4 ✓ Governance Risk and Compliance (GRC)
- Task 5 ✓ Privacy and Data Protection
- Task 6 ✓ NIST Special Publications
- Task 7 ✓ Information Security Management and Compliance
- Task 8 ✓ Conclusion

1. Why is important?
  - a. Istilah penting
    - **Tata Kelola:** Mengarahkan organisasi untuk mencapai tujuan dan memastikan kepatuhan.
    - **Peraturan:** Aturan/hukum dari badan pengatur untuk melindungi dari bahaya.
    - **Kepatuhan:** Mematuhi hukum, peraturan, dan standar yang berlaku.
  - b. Tata Kelola keamanan informasi  
Struktur dan kebijakan untuk emmastikan kerahasiaan, integritasm dan ketersediaan infromasi
    - **Strategi:** Sejalan dengan tujuan bisnis.
    - **Kebijakan dan Prosedur:** Atur perlindungan aset informasi.
    - **Manajemen Risiko:** Identifikasi & mitigasi ancaman.
    - **Pengukuran Kinerja:** KPI untuk mengevaluasi efektivitas.
    - **Kepatuhan:** Pastikan organisasi taat regulasi.
  - c. Peraturan keamanan informasi, Kerangka hukum untuk mengatur **penggunaan & perlindungan**  
Wajib diikuti, diawasi oleh pemerintah atau lembaga pengatur.
  - d. Manfaat tata Kelola dan regulasi
    - **Keamanan lebih kuat:** Cegah pelanggaran & lindungi data.
    - **Kepercayaan pemangku kepentingan:** Tunjukkan keseriusan keamanan.
    - **Kepatuhan regulasi:** Hindari sanksi hukum & reputasi buruk.
    - **Selaras dengan bisnis:** Keamanan mendukung tujuan bisnis.
    - **Pengambilan keputusan yang lebih baik:** Berdasarkan data dan risiko nyata.

- **Keunggulan kompetitif:** Komitmen keamanan = nilai tambah.

e. Contoh regulasi dan hukum terkait

Regulasi/Hukum	Domain	Deskripsi
<b>GDPR</b>	Privasi	Perlindungan data pribadi warga EU.
<b>HIPAA</b>	Kesehatan	Jaga kerahasiaan informasi kesehatan di AS.
<b>PCI-DSS</b>	Keuangan	Atur keamanan data pemegang kartu.
<b>GLBA</b>	Keuangan	Lindungi informasi pribadi pelanggan lembaga keuangan.

## 2. Information security framework

Kerangka kerja keamanan informasi adalah Kumpulan dokumen formal yang mengatur bagaimana keamanan informasi diterapkan, dikelola, dan ditegakkan dalam organisasi;

### a. Komponen utama framework

- **Kebijakan:** Pernyataan formal tujuan dan prinsip.
- **Standar:** Persyaratan teknis spesifik.
- **Pedoman:** Rekomendasi dan praktik terbaik (tidak wajib).
- **Prosedur:** Langkah-langkah teknis untuk tugas tertentu.
- **Dasar Keamanan (Baseline):** Standar minimum keamanan yang harus dipenuhi.

### b. Langkah-langkah mengembangkan dokumen tata Kelola

- **Identifikasi cakupan dan tujuan:** Misal, kebijakan kata sandi atau baseline sistem.
- **Penelitian dan tinjauan:** Tinjau regulasi dan dokumen yang relevan.
- **Susun dokumen:** Spesifik, jelas, dan selaras dengan nilai organisasi.
- **Tinjauan dan persetujuan:** Libatkan pemangku kepentingan dan manajemen.
- **Implementasi dan komunikasi:** Sosialisasikan dokumen, berikan pelatihan.
- **Tinjau dan perbarui:** Secara berkala untuk menyesuaikan perubahan risiko dan regulasi.

### c. Contoh scenario dunia nyata

- **Kebijakan kata sandi**
  - 1) Panjang, kompleksitas, dan masa berlaku kata sandi.
  - 2) Larangan berbagi atau menggunakan default password.
  - 3) Enkripsi untuk penyimpanan dan transmisi.
  - 4) Edukasi dan pemantauan kepatuhan.
- **Prosedur respon insiden**
  - 1) Identifikasi jenis insiden.
  - 2) Tentukan peran dan tanggung jawab.
  - 3) Langkah respons: isolasi, investigasi, mitigasi, pemulihan.
  - 4) Dokumentasi dan pelaporan.
  - 5) Edukasi serta review berkala.

### 3. Governance risk and compliance

GRG (**Governance, Risk, and Compliance**) adalah pendekatan terpadu yang membantu organisasi:

- Menetapkan arah dan kebijakan keamanan informasi,
- Mengelola risiko secara efektif,
- Memastikan kepatuhan terhadap hukum dan standar industri.

GRG selaras dengan tujuan organisasi dan memperkuat postur keamanan serta ketahanan bisnis.

#### a. Tiga komponen GRC

- 1) **Tata Kelola (Governance):** Menetapkan arah organisasi (strategi keamanan, kebijakan, kerangka kerja). Menentukan metode pemantauan dan evaluasi kinerja keamanan.
- 2) **Manajemen Risiko (Risk Management):** Mengidentifikasi, menilai, dan memprioritaskan risiko. Menerapkan kontrol dan strategi mitigasi. Evaluasi dan pelaporan risiko secara berkelanjutan.
- 3) **Kepatuhan (Compliance):** Memastikan organisasi memenuhi hukum, regulasi, dan standar industri. Audit, pelaporan, dan penanganan isu ketidakpatuhan.

#### b. Langkah mengembangkan program GRC

- 1) **Tentukan cakupan dan tujuan:** Contoh: Mengurangi risiko siber 50% dalam 12 bulan pada sistem data pelanggan.
- 2) **Lakukan penilaian risiko:** Identifikasi kerentanan (misal: kontrol akses lemah), dan prioritaskan risiko.
- 3) **Kembangkan kebijakan & prosedur:** Misal: Kebijakan kata sandi yang kuat, prosedur pemantauan akses sistem.
- 4) **Tetapkan proses tata kelola:** Bentuk komite pengarah, tetapkan peran & tanggung jawab.
- 5) **Terapkan kontrol:** Misal: Firewall, IDS/IPS, SIEM, pelatihan keamanan untuk karyawan.
- 6) **Pantau dan ukur kinerja:** Gunakan metrik untuk evaluasi efektivitas kebijakan dan kontrol.
- 7) **Perbaikan berkelanjutan:** Tinjau rutin, analisis insiden, dan sesuaikan program berdasarkan feedback dan ancaman baru.

#### c. Contoh implementasi GRC di sektor keuangan

- **Tata Kelola:** Penunjukan pejabat pengarah keamanan, kebijakan AML, audit keuangan, manajemen krisis.
- **Manajemen Risiko:** Mengantisipasi penipuan finansial, phishing, ATM palsu, serangan siber.
- **Kepatuhan:** Mematuhi PCI-DSS, GLBA; menerapkan SSL/TLS, patching otomatis, dan kampanye kesadaran pengguna.

### 4. Privacy and data protection

#### a. Pentingnya peraturan privasi dan perlindungan data

- Diterapkan di berbagai sektor seperti keuangan, kesehatan, pemerintahan, dan industri.
- Tujuan utamanya: melindungi **Informasi Identitas Pribadi (PII)** warga negara.

- Manfaat: Menjamin penanganan data yang etis dan bertanggung jawab. Membangun kepercayaan pengguna. Memastikan kepatuhan terhadap regulasi yang berlaku.
  - b. Peraturan perlindungan data umum (GDPR) – uni eropa
    - **Tujuan:** Melindungi data pribadi warga negara UE.
    - **Cakupan:** Berlaku untuk semua organisasi yang mengelola data penduduk UE, baik di dalam maupun luar UE.
    - **Poin-poin penting:**
      - 1) Harus ada **persetujuan eksplisit** sebelum mengumpulkan data pribadi.
      - 2) Hanya **mengumpulkan data yang diperlukan** (prinsip minimisasi data).
      - 3) Harus ada **langkah-langkah perlindungan data** yang memadai.
    - **Sanksi atas ketidakpatuhan:**
      - 1) **Tingkat 1:** Pelanggaran berat (misal: pengumpulan tanpa izin, berbagi data ke pihak ketiga).
        - ◆ Denda: hingga **4%** dari pendapatan tahunan atau **€20 juta** (mana yang lebih tinggi).
      - 2) **Tingkat 2:** Pelanggaran ringan (misal: pelaporan pelanggaran lambat).
        - ◆ Denda: hingga **2%** dari pendapatan tahunan atau **€10 juta**.
  - c. Standart keamanan data pci dss
    - **Tujuan:** Menjaga keamanan transaksi berbasis kartu dan mencegah penipuan data.
    - **Diterapkan oleh:** Perusahaan besar seperti **Visa, MasterCard, American Express**
    - **Fokus utama:** Proteksi terhadap data pemegang kartu. Kontrol akses yang ketat. Pemantauan akses tidak sah. Penggunaan **firewall aplikasi web** dan **enkripsi** data
5. NIST special publication
- a. NIST 800-53 (control keamanan dan privasi untuk sistem informasi dan organisasi)
    - Dikembangkan oleh:** NIST (National Institute of Standards and Technology), AS.
    - Tujuan:** Menyediakan katalog kontrol keamanan dan privasi untuk melindungi sistem informasi berdasarkan prinsip **CIA Triad** (Confidentiality, Integrity, Availability).
    - Poin poin utama
      - 1) Digunakan untuk melindungi operasi, aset, personel, dan organisasi dari berbagai ancaman:
      - 2) Serangan siber, kesalahan manusia, bencana alam, kegagalan infrastruktur, spionase, dan masalah privasi.
      - 3) **Revisi ke-5** mencakup **20 kelompok kontrol**, masing-masing fokus pada kategori keamanan tertentu.
      - 4) Digunakan untuk kepatuhan terhadap berbagai regulasi dan kebijakan.
    - Implementasi program keamanan Berbasis NIST 800-53
      - Fokus penting:** *Manajemen Program* → menetapkan dan memantau keamanan informasi secara menyeluruh di organisasi
      - Subkontrol yang harus diterapkan**
        - 1) **Penemuan aset:** Identifikasi data, sistem informasi, dan potensi ancaman.
        - 2) **Pemetaan kontrol:** Sesuaikan kontrol dengan aset dan risiko yang ada.
        - 3) **Struktur tata kelola:** Tentukan tugas, prosedur, dan tanggung jawab implementasi kontrol.

- 4) **Pemantauan berkala:** Audit dan evaluasi keamanan untuk menjaga kepatuhan.
  - 5) **Sistem deteksi dini:** Identifikasi dan tangani insiden secara proaktif.
- b. NIST 800-63B (pedoman autentikasi dan verifikasi identitas digital)
  - Fokus utama:** Autentikasi dan verifikasi identitas digital untuk akses sistem, layanan, dan jaringan.
  - Poin penting
    - 1) Memberikan panduan untuk berbagai **tingkat jaminan identitas:** **Low**, **Moderate**, dan **High Assurance** tergantung sensitivitas akses.
    - 2) Menjelaskan penggunaan berbagai **faktor autentikasi:** **Kata sandi**, **biometrik**, dan **token**.
    - 3) Memberikan arahan tentang **pengelolaan dan penyimpanan kredensial pengguna** secara aman.
    - 4) Digunakan sebagai referensi standar dalam sistem autentikasi modern.

## 6. Information security management and compliance

- a. Manajemen Keamanan informasi (IS) vs Kepatuhan
  - **Manajemen IS:** Melindungi aset informasi dari akses, penggunaan, perubahan, dan penghancuran yang tidak sah melalui:
    - 1) Identifikasi risiko
    - 2) Pengembangan kontrol
    - 3) Respons insiden
    - 4) Pelatihan kesadaran keamanan
  - **Kepatuhan:** Pemenuhan standar hukum, peraturan industri, dan kontrak terkait keamanan informasi.
- b. ISO /IEC 27001
 

**Dikembangkan oleh:** ISO dan IEC

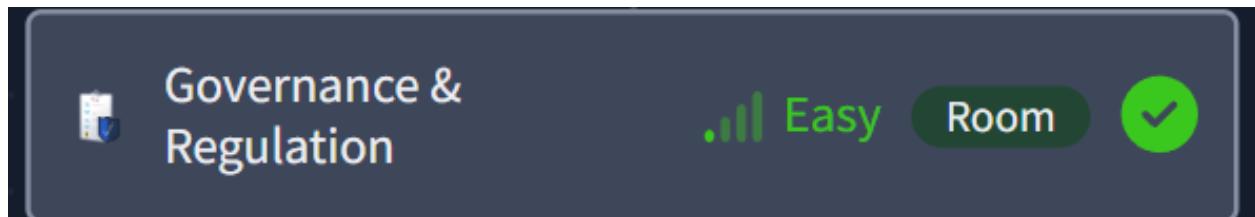
**Fungsi:** Menyediakan kerangka kerja untuk merancang, menerapkan, dan memelihara ISMS secara sistematis

  - Komponen utama
    - 1) **Ruang lingkup:** Menetapkan batasan ISMS dan aset yang dilindungi.
    - 2) **Kebijakan keamanan informasi:** Panduan utama pendekatan organisasi terhadap keamanan.
    - 3) **Penilaian & Penanganan Risiko:** Identifikasi risiko dan penerapan kontrol untuk mengelolanya.
    - 4) **Pernyataan Penerapan (SoA):** Menentukan kontrol yang relevan dan alasan penggunaannya.
    - 5) **Audit internal & Tinjauan manajemen:** Evaluasi rutin efektivitas ISMS.
  - Sukses implementasi ISMS
    - 1) Dukungan manajemen
    - 2) Evaluasi prosedur dan celah keamanan
    - 3) Penyesuaian kontrol (akses, insiden, dll.)
    - 4) Pemantauan dan peningkatan berkelanjutan
- c. SOC 2
 

**Dikembangkan oleh:** AICPA

**Fungsi:** Kerangka audit untuk menilai kontrol organisasi layanan dalam menangani data sensitif, berdasarkan **CIA Triad**.

- Fokus SOC 2
  - 1) **Digunakan oleh:** Penyedia layanan yang memproses data pelanggan (misalnya: cloud service).
  - 2) **Kontrol yang diaudit:** Kerahasiaan, ketersediaan, integritas, privasi, dan keamanan.
- Langkah audit Soc 2
  - 1) **Tentukan cakupan audit** (sistem/proses/lokasi)
  - 2) **Pilih auditor yang sesuai**
  - 3) **Rencanakan audit** (jadwal & kriteria)
  - 4) **Persiapan audit** (tinjau kontrol dan kebijakan)
  - 5) **Laksanakan audit** (review, wawancara, pengujian)
  - 6) **Terima laporan audit** (hasil & rekomendasi)
- Perlindungan SOC 2
  - 1) Menjamin pihak ketiga menyimpan dan memproses data sensitif secara **aman**.
  - 2) Digunakan sebagai bukti bagi klien dan regulator bahwa organisasi memiliki **pengendalian yang efektif**



## Cyber Kill Chain

The screenshot shows a digital learning platform interface for a course titled "Cyber Kill Chain". At the top, there is a circular icon with a gear and a shield, followed by the title "Cyber Kill Chain". Below the title, a descriptive text states: "The Cyber Kill Chain framework is designed for identification and prevention of the network intrusions. You will learn what the adversaries need to do in order to achieve their goals." A difficulty level indicator shows "Easy" and a duration of "45 min". Below this, there are buttons for "Share your achievement", "Help", "Save Room", and "Options". A progress bar at the bottom indicates "Room completed (100%)". The main content area lists ten tasks, each with a green checkmark and a sub-label:

- Task 1 ✓ Introduction
- Task 2 ✓ Reconnaissance
- Task 3 ✓ Weaponization
- Task 4 ✓ Delivery
- Task 5 ✓ Exploitation
- Task 6 ✓ Installation
- Task 7 ✓ Command & Control
- Task 8 ✓ Actions on Objectives (Exfiltration)
- Task 9 ✓ Practice Analysis
- Task 10 ✓ Conclusion

1. Reconnaissance, Pengintaian adalah **fase awal dalam siklus serangan siber**, di mana penyerang mengumpulkan informasi sebanyak mungkin tentang target (individu atau organisasi) untuk merencanakan serangan lebih lanjut.
  - a. OSINT (open source intelligence)
    - Informasi yang dikumpulkan dari sumber public (web, media social, forum, dll)
    - OSINT digunakan untuk
      - 1) Mengetahui struktur organisasi
      - 2) Menemukan alamat email, nomor telepon, dan data karyawan
      - 3) Mengidentifikasi potensi titik lemah
  - b. Study kasus “megatron”
    - Seorang penyerang fiktif yang memulai serangan dari fase **pengintaian**
    - Megatron menggunakan teknik OSINT untuk menemukan target dan merancang serangan
  - c. Pengumpulan email  
Tujuannya: Menggunakan alamat email untuk **serangan phishing**  
Sumber email bisa diperoleh dari:
    - Layanan publik atau komersial
    - Media sosial
    - Website resmi perusahaan
  - d. Alat pengintaian popular

Alat	Fungsi Utama
<b>theHarvester</b>	Mengumpulkan email, nama, subdomain, IP, dan URL dari sumber publik
<b>Hunter.io</b>	Mencari kontak email berdasarkan domain
<b>OSINT Framework</b>	Direktori alat OSINT berdasarkan kategori penggunaan

- e. Media social sebagai sumber OSINT
- LinkedIn: Jabatan, struktur tim, alamat email kerja
  - Facebook, Twitter, Instagram: Informasi pribadi, kebiasaan, lokasi
  - Informasi ini membantu penyerang membuat **email phishing yang meyakinkan**
2. Weaponization
- Definisi:**
- Fase di mana penyerang menggabungkan **malware** dan **exploit** menjadi satu **payload** yang bisa dikirim ke korban tanpa interaksi langsung.
- Terminologi penting
    - **Malware:** Perangkat lunak jahat untuk merusak atau mengakses sistem secara ilegal.
    - **Exploit:** Kode yang memanfaatkan kelemahan atau celah sistem.
    - **Payload:** Kode berbahaya yang dijalankan di sistem korban.
    - **Command and Control (C2):** Saluran komunikasi yang digunakan penyerang untuk mengontrol perangkat korban.
    - **Implan / Backdoor:** Akses tersembunyi ke sistem korban, melewati keamanan.
  - Strategi Megatron
    - Tidak menulis malware sendiri.
    - Membeli **payload jadi** dari DarkWeb untuk menghemat waktu dan menghindari deteksi.
  - Contoh taktik Weaponization
    - 1) Dokumen office berbahaya
      - Mengandung **makro** atau skrip **VBA**
      - Digunakan untuk menjalankan payload ketika dibuka oleh korban
    - 2) Drive USB berbahaya
      - Berisi worm/malware
      - Ditinggalkan di area publik untuk menarik korban (strategi “drop attack”)
    - 3) Pemilihan teknik
      - Untuk mengirim perintah ke sistem korban
      - Untuk mengunduh muatan tambahan
    - 4) Penamanaan backdoor
      - Memungkinkan penyerang masuk kembali ke sistem secara diam-diam

3. Delivery

**Definisi:**

Tahap di mana penyerang mengirimkan **payload/malware** ke korban menggunakan berbagai metode pengiriman.

- a. Tujuan megatron, Mengirim muatan berbahaya ke target secara efektif dan seringkali **tanpa terdeteksi**, berdasarkan hasil pengintaian.
- b. Metode pengiriman umum
  - 1) Email phising / spearphising
    - Email disesuaikan secara personal (contohnya meniru email dari seseorang yang dikenal korban)
    - Menggunakan domain palsu yang mirip perusahaan asli
    - Menyisipkan **lampiran berbahaya** (misal: "Faktur" palsu)  
*Contoh: Megatron menyamar sebagai "Scott" dan mengirimkan file ke Nancy dari perusahaan A.*
  - 2) Distribusi USB berbahaya
    - Menyebar **USB berisi malware** di tempat umum
    - Strategi USB Drop canggih bisa melibatkan logo perusahaan untuk meningkatkan kredibilitas
    - Kadang dikirim lewat pos dengan alasan sebagai "hadih" dari "klien"
  - 3) Serangan Watering Hole
    - Menargetkan situs web yang sering dikunjungi target
    - Situs disusupi dan diarahkan ke **situs berbahaya**
    - Metode serangan: **drive-by download**  
(korban otomatis mengunduh malware tanpa sadar saat mengunjungi situs)
- 4. Exploitation

**Definisi:**

Tahapan di mana penyerang **menjalankan kode berbahaya** untuk mengeksplorasi kerentanan dan mendapatkan akses ke sistem target

- a. Tujuan megatron
  - Menjalankan muatan (payload) berbahaya agar bisa:
    - Masuk ke sistem korban
    - Memperluas akses
    - Melangkah ke tahap berikutnya seperti kontrol sistem dan eksfiltrasi data
- b. Teknik eksplorasi yang digunakan
  - 1) Email phising dengan tautan berbahaya
    - Mengarahkan korban ke **halaman login palsu** (contoh: Office 365 phishing)
    - Mengambil kredensial saat korban login di halaman palsu
  - 2) Lampiran makro berbahaya
    - Dokumen dengan **makro VBA** yang menjalankan **ransomware**
    - Korban membuka file → ransomware aktif
  - 3) Zero day exploit
    - Eksplorasi kerentanan yang belum diketahui publik
    - **Tidak dapat dideteksi lebih awal**, sangat berbahaya
    - Menyerang tanpa peringatan atau tanda awal
  - 4) Eksplorasi human error
    - Memanfaatkan kesalahan pengguna, seperti: Mengklik link tanpa verifikasi
    - Membuka file dari sumber tidak dikenal
  - 5) Eksplorasi server/web
    - Menargetkan kerentanan dalam perangkat lunak server/web

- Contoh: SQL Injection, RCE, XSS, dsb.
  - Berguna untuk **pergerakan lateral** (menyusup ke bagian jaringan lain)
- c. Pergerakan lateral
- Setelah eksploitasi berhasil:
- Penyerang menjelajah sistem lain di dalam jaringan
  - Meningkatkan hak akses (privilege escalation)
  - Mencari data bernilai atau sistem kunci

## 5. Installation

### Tujuan:

Penyerang memasang **backdoor persisten** agar bisa kembali mengakses sistem meskipun koneksi awal hilang, sistem dipatch, atau malware terdeteksi dan dihapus.

a. Jenis persistensi yang digunakan penyerang

- 1) Web shell di serever web
  - Skrip berbahaya (ASP, PHP, JSP, dll.) yang ditanam di server web
  - Memberikan akses jarak jauh secara diam-diam
  - Sulit terdeteksi karena sering terlihat seperti file web biasa
  - Backdoor via meterpreter
- 2) Backdoor via meterpreter
  - a. Meterpreter dari Metasploit Framework digunakan untuk:
    - Akses shell interaktif
    - Eksekusi perintah
    - Transfer file
  - b. Dapat dipasang sebagai backdoor yang bertahan lama
- 3) Layanan windows (MITRE ATT & CK T1543.003)
  - Penyerang membuat/modifikasi layanan sistem
  - Alat: sc.exe, reg
  - Teknik penyamaran: menggunakan nama layanan resmi agar terlihat sah
- 4) Run keys & startup folder
  - Menambahkan entri ke registri atau folder startup Windows
  - Payload otomatis dijalankan saat pengguna login
  - Dapat diterapkan secara spesifik ke pengguna atau seluruh sistem

b. Teknik anti deteksi

TimeStomping

- Mengubah metadata file (waktu akses, pembuatan, modifikasi)
- Membuat file tampak lama/sah
- Menyulitkan analisis forensik

## 6. Command and control

### Tujuan:

Memberikan **kendali jarak jauh** kepada penyerang atas mesin korban melalui saluran komunikasi berbahaya antara malware dan server C2 (Command & Control).

a. Bagaimana c2 bekerja

- **Host yang terinfeksi** akan terus berkomunikasi dengan **server C2** milik penyerang → disebut **C2 Beaconing**

- Setelah koneksi terbentuk, penyerang memiliki **kontrol penuh** atas sistem korban
- b.** Jenis saluran c2 yang umum digunakan
- 1) HTTP (port 80) & HTTPS (port 443)
    - Menyamar sebagai lalu lintas web biasa
    - Sulit dibedakan oleh firewall dan IDS/IPS
  - 2) DNS Tunneling
    - Menggunakan **permintaan DNS** untuk menyampaikan perintah atau mencuri data
    - Menyamar sebagai lalu lintas DNS sah, meski digunakan untuk komunikasi berbahaya
  - 3) IRC (internet relay chat)
    - Dulu populer sebagai saluran C2
    - Kini mudah terdeteksi oleh sistem keamanan modern
- c.** Kepemilikan infrastuktur C2  
Server C2 dapat dimiliki langsung oleh penyerang atau oleh host lain yang telah sidudupi sebelumnya
7. Actions on objectives

**Tujuan:**

Menjalankan **tindakan akhir** yang sesuai dengan tujuan serangan awal penyerang setelah memperoleh akses penuh ke sistem korban.

- a.** Akses yang dimiliki penyerang  
Dengan akses penuh dan control langsung, penyerang dapat melakukan berbagai tindakan merusak atau mencuri data
- b.** Aktivitas yang dilakukan penyerang
- 1) **Mengumpulkan kredensial pengguna**  
Untuk memperluas akses ke akun dan sistem lain.
  - 2) **Peningkatan hak istimewa**  
Mendapatkan akses level tinggi seperti **administrator domain**.
  - 3) **Pengintaian internal**  
Menjelajahi sistem dan perangkat lunak internal untuk mencari kerentanan tambahan.
  - 4) **Pergerakan lateral**  
Berpindah ke sistem lain dalam jaringan untuk memperluas cakupan serangan.
  - 5) **Mengumpulkan & mengekstrak data sensitif**  
Seperti informasi rahasia, database, atau dokumen penting.
  - 6) **Menghapus cadangan & Shadow Copy**  
Mencegah pemulihan data oleh korban.
  - 7) **Menimpa atau merusak data**  
Untuk menyebabkan gangguan permanen atau menyamarkan jejak.



## Cyber Security Basics

Acquire the basic cyber security skills required to get started in cyber security.

👉 Careers in Cyber

Info

Room



🌐 Security Principles

Easy

Room



📘 Governance & Regulation

Easy

Room



🌐 Cyber Kill Chain

Easy

Room

