

Pengantar Keamanan Siber dan CIA Triad

Minggu 1 - 13S4121 Keamanan Siber

Aset digital, ancaman, kerentanan, risiko, kontrol, etika, dan batas laboratorium

Albert Sagala, S.T., M.T.

Sarjana Teknik Elektro - Institut Teknologi Del

Posisi Materi dalam RPS

Sub-CPMK 1

Menjelaskan aset, CIA triad, ancaman, kerentanan, risiko, dan kontrol keamanan. [C2]

Kata kunci minggu ini

- ▶ Aset dan pemilik aset
- ▶ Confidentiality, integrity, availability
- ▶ Ancaman, kerentanan, risiko
- ▶ Kontrol, bukti, residual risk

Orientasi belajar

- ▶ Mulai dari tujuan organisasi
- ▶ Tetapkan batas sistem dan asumsi
- ▶ Susun skenario risiko yang dapat diuji
- ▶ Pilih kontrol yang proporsional

Dokumen ini adalah materi mahasiswa: tidak memuat kunci jawaban asesmen final.

Capaian Pembelajaran Mingguan

Pada akhir pertemuan, mahasiswa mampu:

- ▶ Membedakan **aset**, **ancaman**, **kerentanan**, **risiko**, **kejadian**, **insiden**, dan **kontrol**.
- ▶ Menjelaskan **confidentiality**, **integrity**, dan **availability** melalui kebutuhan organisasi.
- ▶ Menentukan batas sistem dan pemilik aset pada studi kasus sederhana.
- ▶ Menerapkan prinsip otorisasi, minimisasi dampak, dan dokumentasi pada laboratorium keamanan.

Indikator keberhasilan kelas

Mahasiswa dapat menulis risk statement yang menyebutkan penyebab, kejadian, dampak, kontrol, dan bukti verifikasi secara konsisten.

Rencana Perkuliahan 100 Menit

Waktu	Aktivitas pembelajaran
0-10 menit	Apersepsi: mengapa keamanan siber dimulai dari tujuan dan aset.
10-30 menit	Konsep dasar: CIA triad, aset, ancaman, kerentanan, risiko, kontrol.
30-50 menit	Studi kasus terpandu: portal akademik dan data nilai mahasiswa.
50-75 menit	Aktivitas kelompok: memetakan aset, aliran data, dan risk statement.
75-90 menit	Presentasi singkat kelompok dan klarifikasi istilah.
90-100 menit	Rangkuman, tugas mingguan, dan pertanyaan pemahaman.

Alokasi waktu dapat disesuaikan dengan dinamika diskusi kelas.

Mengapa Keamanan Siber Dipelajari?

Keamanan siber adalah **pengelolaan risiko** terhadap informasi, layanan, perangkat, manusia, dan proses.

Fokusnya bukan membuat serangan mustahil, melainkan:

- ▶ menurunkan kemungkinan dan dampak;
- ▶ mendeteksi penyimpangan;
- ▶ merespons secara tertib;
- ▶ memulihkan layanan pada tingkat yang dapat diterima.

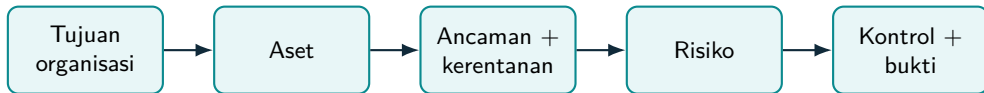
Pertanyaan pembuka

Sistem apa yang paling penting di kampus, dan apa akibatnya bila sistem itu tidak dapat dipercaya selama satu hari?

Pesan utama

Keamanan adalah kualitas sistem yang harus dirancang, dioperasikan, dibuktikan, dan dievaluasi.

Alur Berpikir Keamanan



Prinsip pengarah

RISIKO = fungsi(likelihood, impact, konteks, kontrol)

Rekomendasi keamanan harus dapat ditelusuri ke risiko dan pemilik keputusan.

Rute Belajar Analisis Risiko

1. Tetapkan **tujuan organisasi** dan kebutuhan layanan.
2. Identifikasi **aset** dan **pemilik aset**.
3. Nyatakan **batas sistem**, fakta, dan asumsi.
4. Bangun **skenario risiko** yang spesifik.
5. Pilih **kontrol** yang proporsional terhadap risiko.
6. Tentukan **bukti** dan **acceptance criterion**.

Kesalahan umum yang harus dihindari

Menulis rekomendasi alat atau teknologi tanpa menunjukkan aset, risiko, bukti, dan pemilik keputusan yang relevan.

Terminologi Dasar

Istilah	Makna operasional
Aset	Sesuatu yang bernilai bagi organisasi dan perlu dilindungi.
Ancaman	Penyebab potensial kejadian yang merugikan.
Kerentanan	Kelemahan yang dapat dimanfaatkan oleh ancaman.
Kejadian	Peristiwa yang terjadi pada sistem, belum tentu merugikan.
Insiden	Kejadian yang mengganggu keamanan atau operasi.
Kontrol	Tindakan yang mengubah likelihood, impact, atau kemampuan deteksi.

CIA Triad sebagai Kebutuhan Sistem

C - Confidentiality

Membatasi pengungkapan informasi hanya kepada pihak yang berwenang.

I - Integrity

Menjaga ketepatan, kelengkapan, keaslian, dan ketertelusuran perubahan.

A - Availability

Memastikan informasi atau layanan tersedia ketika diperlukan.

Catatan penting

CIA tidak cukup menjadi label. Setiap unsur harus diterjemahkan menjadi kebutuhan terukur dan dapat diverifikasi.

Confidentiality: Siapa Boleh Melihat?

- ▶ Tujuan: mencegah pengungkapan informasi kepada pihak tidak berwenang.
- ▶ Pertanyaan kendali: siapa boleh melihat data, kapan, dari mana, dan melalui mekanisme apa?
- ▶ Contoh kontrol: autentikasi, otorisasi, least privilege, enkripsi, klasifikasi data, masking.

Contoh bukti

- ▶ Matriks hak akses
- ▶ Log akses
- ▶ Hasil review akun
- ▶ Bukti konfigurasi enkripsi

Integrity: Bagaimana Perubahan Divalidasi?

- ▶ Tujuan: memastikan data tetap tepat, lengkap, autentik, dan dapat ditelusuri.
- ▶ Pertanyaan kendali: siapa mengubah apa, kapan, mengapa, dan bagaimana perubahan diverifikasi?
- ▶ Contoh kontrol: validasi input, persetujuan perubahan, hash, audit trail, rekonsiliasi, backup teruji.

Contoh bukti

- ▶ Checksum atau hash
- ▶ Riwayat perubahan
- ▶ Log approval
- ▶ Hasil rekonsiliasi data

Perbaikan istilah: validasi berarti proses memastikan data atau perubahan memenuhi aturan yang ditentukan.

Availability: Berapa Lama Gangguan Dapat Diterima?

- ▶ Tujuan: menjaga layanan tetap tersedia pada tingkat yang disepakati.
- ▶ Pertanyaan kendali: berapa lama layanan boleh terganggu dan seberapa besar kehilangan data yang dapat diterima?
- ▶ Contoh kontrol: redundansi, kapasitas, monitoring, backup, disaster recovery, incident response.

Contoh bukti

- ▶ SLA atau SLO
- ▶ Hasil uji pemulihan
- ▶ Laporan downtime
- ▶ Monitoring kapasitas

Trade-off dalam CIA Triad

Tidak semua sistem memprioritaskan CIA dengan bobot yang sama.

- ▶ Portal nilai: integrity sangat dominan.
- ▶ Sistem presensi real-time: availability penting pada jam operasi.
- ▶ Repositori dokumen rahasia: confidentiality menjadi dominan.

Diskusi kelas

Pada sistem rumah sakit, kondisi apa yang membuat availability lebih penting daripada confidentiality?

Prinsip keputusan

Prioritas CIA ditentukan oleh tujuan, konteks, dampak, dan toleransi risiko organisasi.

Aset dan Pemilik Aset

Jenis aset digital

- ▶ Data: nilai, identitas, log, dokumen.
- ▶ Layanan: portal akademik, email, LMS.
- ▶ Perangkat: server, laptop, router, sensor.
- ▶ Akun: admin, dosen, mahasiswa, API key.
- ▶ Proses: validasi nilai, registrasi, backup.

Mengapa pemilik aset penting?

- ▶ Menentukan kebutuhan CIA.
- ▶ Menyetujui akses dan perubahan.
- ▶ Menerima atau menolak residual risk.
- ▶ Menentukan prioritas mitigasi.

Batas Sistem dan Asumsi

Analisis keamanan harus menyatakan batas yang jelas.

Elemen batas	Contoh yang perlu dinyatakan
Pemilik	Unit akademik, unit TI, pengelola layanan.
Lokasi	Server lokal, cloud, perangkat pengguna, jaringan kampus.
Aliran data	Input, pemrosesan, penyimpanan, output, integrasi API.
Ketergantungan	Database, jaringan, SSO, layanan pihak ketiga.
Kondisi gagal	Layanan tidak tersedia, data tidak sinkron, akun diambil alih.

Tanpa batas sistem, daftar ancaman menjadi tidak terarah dan klaim keamanan sulit diverifikasi.

Ancaman, Kerentanan, Kejadian, dan Insiden

Hubungan konsep

- ▶ Ancaman memanfaatkan kerentanan.
- ▶ Pemanfaatan tersebut menghasilkan kejadian.
- ▶ Kejadian menjadi insiden bila berdampak pada keamanan atau operasi.

Contoh

Akun admin menggunakan kata sandi lemah. Pihak tidak berwenang berhasil login dan mengubah data nilai. Perubahan itu menjadi insiden karena integritas catatan akademik terganggu.

Risk Statement yang Dapat Dianalisis

Pola penulisan

Sebab/ancaman → kejadian → dampak

Kurang baik

Server diretas.

Lebih baik

Pihak tidak berwenang mengambil alih akun pengelola dan mengubah nilai mahasiswa, sehingga integritas catatan akademik serta kepercayaan terhadap proses akademik terganggu.

Kontrol Keamanan

Jenis kontrol	Fungsi
Preventif	Mengurangi kemungkinan kejadian, misalnya MFA dan least privilege.
Detektif	Menemukan penyimpangan, misalnya logging dan alert.
Korektif	Mengurangi dampak setelah kejadian, misalnya patch dan revocation.
Pemulihan	Mengembalikan layanan, misalnya backup restore dan DR plan.
Kompensasi	Mengurangi risiko ketika kontrol utama belum dapat diterapkan.

Prinsip proporsionalitas

Kontrol dipilih berdasarkan likelihood, impact, konteks operasi, biaya, dan residual risk.

Bukti dan Acceptance Criterion

Bukti minimum

- ▶ Scope dan otorisasi.
- ▶ Topologi atau setup.
- ▶ Versi konfigurasi.
- ▶ Raw log dengan identifier dan timestamp.
- ▶ Hasil uji positif dan negatif.
- ▶ Anomali, keterbatasan, rollback, residual risk.

Acceptance criterion

Pernyataan terukur yang menentukan kapan kontrol dianggap memenuhi tujuan keamanan.

Contoh

Semua akses admin tercatat dengan user ID, waktu, alamat asal, dan aksi.
Perubahan nilai tanpa approval otomatis menghasilkan alert.

Studi Kasus Terpandu: Portal Akademik

Situasi

Portal akademik menyimpan nilai mahasiswa. Aset utamanya adalah data nilai dan layanan akses portal.

Analisis aset

- ▶ Data nilai mahasiswa
- ▶ Akun dosen dan admin akademik
- ▶ Database dan aplikasi portal
- ▶ Log perubahan nilai

Kebutuhan CIA

- ▶ Confidentiality: nilai hanya dilihat pihak berwenang.
- ▶ Integrity: perubahan nilai sah dan tertelusur.
- ▶ Availability: portal tersedia pada periode akademik kritis.

Tabel Analisis dan Keputusan

Konsep	Pertanyaan kendali	Contoh bukti
Aset	Apa yang bernilai dan siapa pemiliknya?	Inventaris dan klasifikasi.
Confidentiality	Siapa boleh melihat data?	Matriks akses dan log.
Integrity	Bagaimana perubahan divalidasi?	Hash, persetujuan, riwayat.
Availability	Berapa lama gangguan dapat diterima?	SLA, backup, hasil uji pemulihan.
Risiko	Skenario apa yang dapat mengganggu tujuan?	Risk statement dan keputusan treatment.

Contoh Kontrol pada Portal Akademik

Risiko	Kontrol yang relevan	Bukti verifikasi
Akun admin diambil alih	MFA, least privilege, review akun berkala	Screenshot konfigurasi, daftar role, log login.
Nilai diubah tanpa otorisasi	Approval workflow, audit trail, rekonsiliasi perubahan	Riwayat approval, log perubahan, hasil rekonsiliasi.
Portal tidak tersedia saat KRS	Monitoring, kapasitas, backup, prosedur pemulihan	Uji pemulihan, laporan uptime, hasil load test.

Inti pembelajaran

Satu risiko biasanya membutuhkan kombinasi kontrol preventif, detektif, korektif, dan pemulihan.

Etika, Otorisasi, dan Batas Laboratorium

Aturan dasar

Kegiatan keamanan hanya dilakukan pada aset yang berada dalam ruang lingkup izin eksplisit dan terdokumentasi.

- ▶ Gunakan sistem, akun, dan data laboratorium yang disediakan.
- ▶ Jangan melakukan pemindaian atau akses ke sistem nyata di luar scope.
- ▶ Gunakan metode non-destruktif dan minimalkan data.
- ▶ Catat perubahan, parameter, waktu, dan hasil observasi.
- ▶ Hentikan kegiatan dan laporkan bila muncul dampak tidak terduga.

Aktivitas Kelompok: Pemetaan Risiko

Skenario

Portal akademik fiktif menyimpan nilai, jadwal, data mahasiswa, dan riwayat aktivitas pengguna.

Tugas kelompok

- ▶ Petakan minimal 8 aset.
- ▶ Tentukan pemilik aset.
- ▶ Tandai kebutuhan CIA utama.
- ▶ Gambarkan aliran data dan batas kepercayaan.

Batas aktivitas

- ▶ Tidak ada pemindaian sistem nyata.
- ▶ Tidak menggunakan data pribadi nyata.
- ▶ Semua asumsi harus ditulis eksplisit.
- ▶ Semua klaim harus memiliki bukti atau alasan.

Template Hasil Diskusi Kelompok

Aset	Pemilik	CIA utama	Risk statement	Kontrol dan bukti
Data nilai	Akademik	Integrity	Akun dosen diambil alih dan nilai diubah tanpa approval.	MFA, approval, audit trail, log perubahan.
Portal KRS	TI kampus	Availability	Lonjakan akses membuat portal tidak tersedia pada masa KRS.	Monitoring, kapasitas, backup, uji pemulihan.
Akun admin	TI kampus	Confidentiality	Hak akses berlebih membuka data yang tidak relevan.	Least privilege, review role, log akses.

Tambahkan baris lain sesuai hasil identifikasi kelompok.

Tugas Mingguan

Tugas 1

Buat inventaris minimal **delapan aset** dan **tiga risk statement** yang mengikuti pola sebab-kejadian-dampak.

Untuk tiap risiko, tuliskan:

- ▶ satu kontrol preventif;
- ▶ satu kontrol detektif;
- ▶ bukti verifikasi untuk masing-masing kontrol;
- ▶ residual risk secara singkat.

Larangan

Jangan menggunakan data pribadi nyata, kredensial nyata, atau hasil pemindaian sistem di luar laboratorium.

Checklist Mutu Pengumpulan

- ▶ Istilah dan identifier digunakan secara konsisten.
- ▶ Batas sistem, tanggal, scope, dan otorisasi terlihat.
- ▶ Bukti mendukung klaim dan dapat ditelusuri.
- ▶ Rahasia dan data pribadi tidak dimasukkan tanpa kebutuhan yang sah.
- ▶ Keterbatasan, confidence, dan residual risk dinyatakan.
- ▶ Rekomendasi memiliki owner, prioritas, dan acceptance test.

Standar kualitas jawaban

Jawaban yang baik tidak hanya menyebut kontrol, tetapi menjelaskan bagaimana kontrol tersebut mengubah risiko dan bagaimana efektivitasnya dibuktikan.

Pertanyaan Pemeriksaan Diri

1. Mengapa aset harus dikaitkan dengan tujuan organisasi?
2. Apa perbedaan ancaman dan kerentanan?
3. Kapan availability lebih dominan daripada confidentiality?
4. Apa yang membuat kontrol dapat diverifikasi?
5. Mengapa izin eksplisit harus terdokumentasi?

Instruksi diskusi

Pilih dua pertanyaan. Jawab dengan contoh sistem nyata atau fiktif, tetapi jangan menggunakan data sensitif atau kredensial nyata.

Dua Pertanyaan Penutup

Pertanyaan 1

Dalam sebuah sistem akademik, mengapa pernyataan risiko “*server diretas*” belum cukup untuk menentukan kontrol keamanan yang tepat?

Pertanyaan 2

Bagaimana cara membuktikan bahwa suatu kontrol benar-benar menurunkan risiko, bukan hanya terlihat sebagai rekomendasi teknis?

Pertanyaan ini digunakan untuk menguji pemahaman konseptual, bukan untuk menghafal definisi.

Rangkuman Minggu 1

- ▶ Keamanan siber adalah pengelolaan risiko terhadap aset dan tujuan organisasi.
- ▶ CIA triad harus diterjemahkan menjadi kebutuhan yang terukur.
- ▶ Ancaman, kerentanan, risiko, dan kontrol adalah konsep yang berbeda tetapi saling berhubungan.
- ▶ Analisis yang baik selalu menyebutkan scope, pemilik aset, asumsi, kontrol, bukti, dan residual risk.
- ▶ Aktivitas keamanan wajib memiliki otorisasi eksplisit dan batas laboratorium yang jelas.

Referensi dan Bacaan Lanjutan

1. Stallings, W. *Cryptography and Network Security: Principles and Practice*. Pearson.
2. Easttom, C. *Computer Security Fundamentals*. Pearson.
3. NIST. *Cybersecurity Framework (CSF) 2.0*. <https://www.nist.gov/cyberframework>
4. ISO. *ISO/IEC 27001:2022 overview*. <https://www.iso.org/standard/27001>

Catatan penggunaan referensi

Standar, threat intelligence, katalog kerentanan, dan dokumentasi alat dapat diperbarui. Catat judul, versi, tanggal akses, parameter, serta lingkungan yang digunakan.

Terima kasih

Diskusi dan klarifikasi

Minggu 1 - Pengantar Keamanan Siber dan CIA Triad