SNI ISO/IEC 27001 dan CSIRT Kampus: Strategi Kolaboratif dalam Menjaga Ketahanan Siber

Kurniawan Teguh Martono., ST., MT
Departemen Teknik Komputer
Fakultas Teknik – Universitas Diponegoro
https://scholar.undip.ac.id/en/persons/kurniawan-teguh-martono

Outline Paparan

- Pendahuluan
- Tujuan
- ISO/IEC 27001
- CSIRT Kampus
- Strategi Kolaboratif
- Kesimpulan

Pedahuluan

- Keamanan Siber di Dunia Pendidikan Tinggi?
  - Transformasi Digital Kampus
    - Perguruan tinggi kini sangat bergantung pada teknologi informasi:
      - Sistem akademik (registrasi, nilai, e-learning).
      - Layanan keuangan (pembayaran, beasiswa).
      - Repository digital (skripsi, jurnal, data penelitian).
    - Semua sistem ini menjadi target serangan karena berisi data bernilai tinggi.
  - Ancaman Nyata yang Terjadi
    - Meningkatnya insiden peretasan situs kampus dan *defacement*.
    - Penyebaran *phishing* lewat email mahasiswa dan dosen.
    - Kebocoran data pribadi mahasiswa/alumni untuk kejahatan digital.
    - Potensi penyalahgunaan data penelitian atau inovasi teknologi.

Dampak Insiden Siber pada Perguruan Tinggi?

Hilangnya kepercayaan mahasiswa, dosen, dan mitra industri.

Gangguan pada layanan akademik (kuliah online, ujian, pendaftaran).

Kerugian finansial dan reputasi kampus.

Hambatan pada kolaborasi internasional jika standar keamanan tidak dipenuhi .

Urgensi Penguatan Keamanan Siber

Dunia pendidikan tinggi tidak hanya menjaga data administratif, tetapi juga menjaga aset intelektual bangsa.

Kampus sebagai pusat riset dan inovasi harus memastikan hasil penelitiannya aman dari pencurian maupun sabotase.

Keamanan siber yang kuat menjadi syarat untuk menjaga keberlangsungan layanan akademik dan reputasi global perguruan tinggi.

Jenis Ancaman yang Mengalami Peningkatan

Phishing & Social Engineering

- Email palsu yang mengaku dari pihak kampus untuk mencuri kredensial mahasiswa/dosen.

Ransomware

- Enkripsi data akademik atau penelitian, lalu menuntut tebusan.

Website Defacement

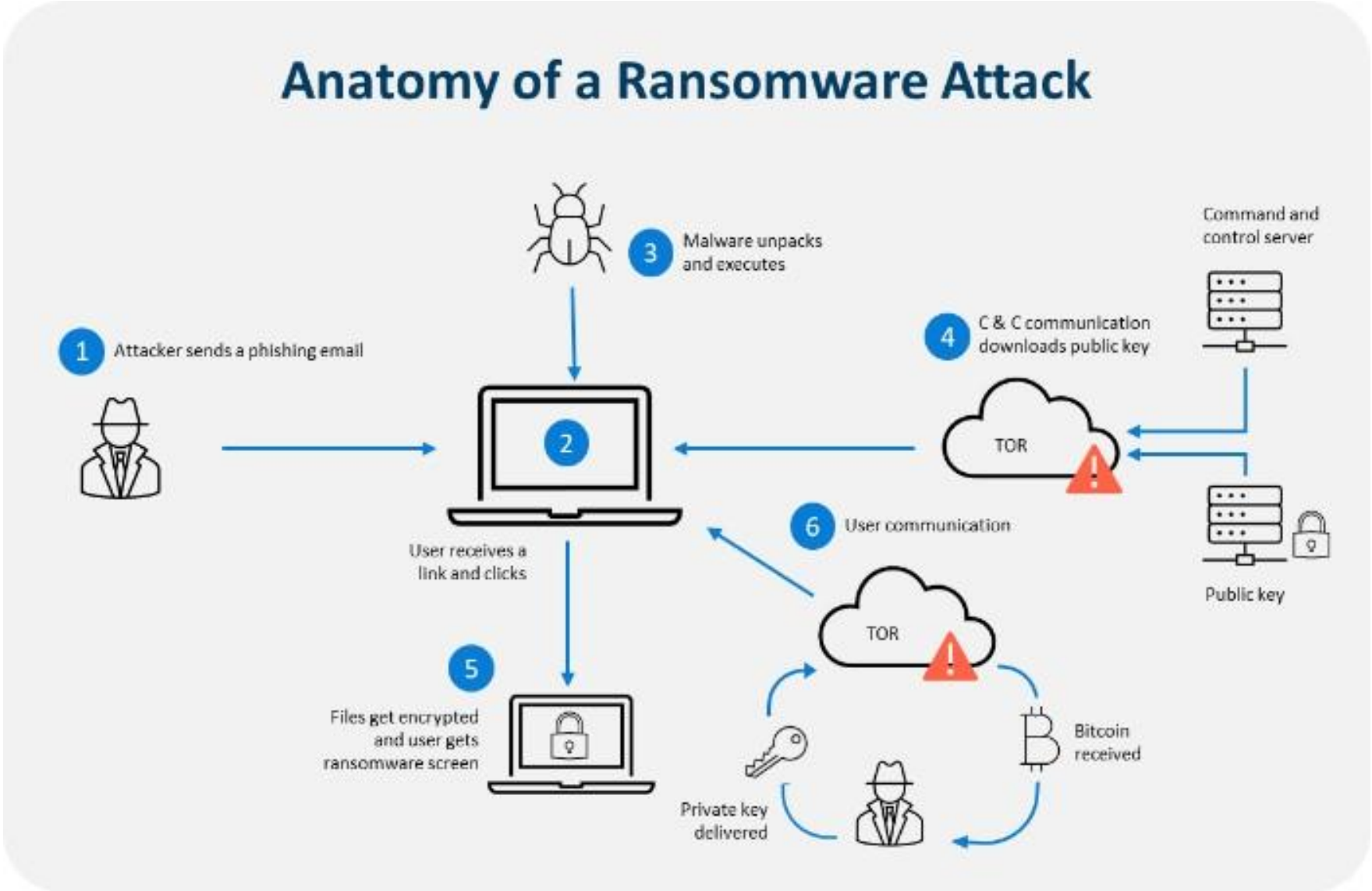
- Situs resmi kampus diretas dan diubah tampilannya → merusak reputasi.

Data Breach / Kebocoran Data

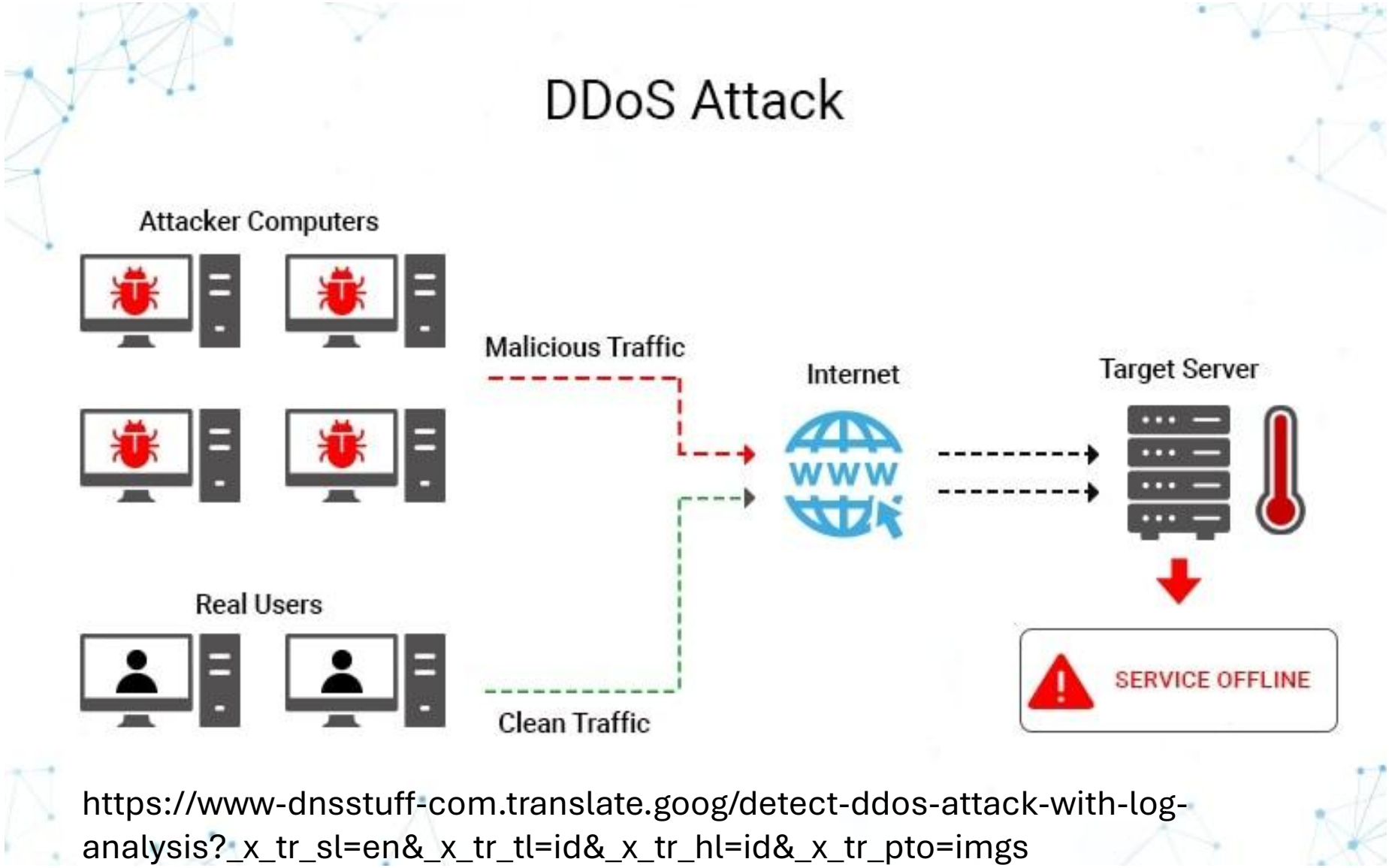
- Basis data mahasiswa dan alumni dijual di forum gelap (dark web).

Serangan DDoS

- Menjatuhkan sistem e-learning atau portal akademik saat periode kritis (misalnya registrasi kuliah/ujian online).



https://www-proserveit-com.translate.goog/blog/what-is-a-ransomware-and-how-to-protect-your-organization?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=imgs



https://www-dnsstuff-com.translate.goog/detect-ddos-attack-with-log-analysis?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=imgs

Faktor Penyebab Meningkatnya Ancaman

Tingginya digitalisasi → hampir semua layanan kampus berbasis sistem informasi.

Keragaman pengguna → mahasiswa, dosen, staf dengan tingkat kesadaran keamanan yang berbeda-beda.

Keterbatasan SDM keamanan → tidak semua kampus punya tim khusus keamanan siber.

Koneksi global → kampus banyak terlibat kolaborasi internasional, sehingga eksposur terhadap ancaman lebih luas.

ISO/IEC 27001

ISO/IEC 27001 adalah standar internasional yang mengatur tentang Sistem Manajemen Keamanan Informasi (Information Security Management System / ISMS).

Standar ini memberikan kerangka kerja (framework) untuk melindungi kerahasiaan (Confidentiality), integritas (Integrity), dan ketersediaan (Availability) informasi — dikenal sebagai prinsip CIA triad.

Digunakan secara global oleh organisasi pemerintahan, bisnis, maupun perguruan tinggi untuk memastikan pengelolaan keamanan informasi yang terstruktur.

Tujuan Utama ISO/IEC 27001

Melindungi informasi penting dari akses tidak sah, perubahan, atau kehilangan.

Menjamin sistem informasi tetap aman dan dapat diandalkan.

Memberikan pendekatan berbasis manajemen risiko dalam keamanan siber.

Menciptakan budaya keamanan informasi di seluruh organisasi (tidak hanya bagian IT).

Komponen Utama ISO 27001

Konteks Organisasi

- Memahami kondisi internal dan eksternal yang memengaruhi keamanan informasi, serta menentukan lingkup penerapan ISMS (Information Security Management System).

Kepemimpinan dan Kebijakan

- Memastikan manajemen puncak terlibat dan berkomitmen terhadap keamanan informasi.

Penilaian Risiko & Mitigasi

- Mengidentifikasi, menilai, dan mengendalikan risiko terhadap aset informasi.

Kontrol Keamanan

- Menentukan dan menerapkan kontrol keamanan sesuai kebutuhan organisasi.

Komponen Utama ISO 27001 (2)

- Peningkatan Berkelanjutan
  - Menjaga agar ISMS selalu relevan, efektif, dan adaptif terhadap perubahan ancaman.
  - Model PDCA (Plan–Do–Check–Act):
    - Plan: Rencanakan kebijakan dan kontrol berdasarkan risiko.
    - Do: Terapkan kontrol dan jalankan ISMS.
    - Check: Audit internal, evaluasi efektivitas, review oleh manajemen.
    - Act: Perbaiki kelemahan dan tingkatkan kinerja ISMS.

Manfaat ISO 27001 untuk Kampus

- Meningkatkan Keamanan Data dan Informasi Akademik
- Membangun Budaya Keamanan Siber di Lingkungan Kampus
- Mendukung Kepatuhan terhadap Regulasi
- Meningkatkan Kepercayaan Mitra, Stakeholder, dan Publik

CSIRT Kampus: Peran & Implementasi

- Computer Security Incident Response Team:
  - tim khusus yang menangani insiden siber.
- Mencegah, mendeteksi, merespons, dan memulihkan sistem dari serangan atau insiden siber.
- Menjadi pusat koordinasi ketika terjadi gangguan keamanan, seperti peretasan, kebocoran data, atau serangan malware.
- Menjaga agar aktivitas operasional organisasi tetap berjalan dengan aman dan berkelanjutan.

Mengapa Kampus Butuh CSIRT

- Banyak data sensitif (mahasiswa, penelitian, dosen).
- Aktivitas TI terdistribusi (laboratorium, fakultas, cloud).
- Kecepatan respons menjadi faktor kritikal.

Fungsi Utama CSIRT

Fungsi	Penjelasan Singkat
Deteksi (Detection)	Memonitor jaringan dan sistem untuk mendeteksi aktivitas mencurigakan.
Analisis (Analysis)	Menilai tingkat keparahan insiden, sumber serangan, dan dampaknya.
Respons (Response)	Mengambil tindakan segera untuk menghentikan serangan dan meminimalkan kerusakan.
Pemulihan (Recovery)	Mengembalikan sistem ke kondisi normal, misalnya dengan restore data dari backup.
Pencegahan (Prevention)	Memberikan rekomendasi untuk mencegah insiden serupa di masa depan.

Struktur dan Peran dalam CSIRT

Peran	Tanggung Jawab
Incident Handler	Personel utama yang menerima laporan dan mengelola penanganan insiden.
Security Analyst / Forensic Expert	Melakukan analisis teknis dan forensik digital terhadap insiden.
Communications Officer	Mengelola komunikasi internal dan eksternal saat terjadi insiden, termasuk dengan BSSN atau publik.
Policy & Awareness Officer	Mengembangkan kebijakan keamanan dan melakukan edukasi ke pengguna.
CSIRT Manager / Coordinator	Mengarahkan strategi, prioritas, dan memastikan proses penanganan insiden berjalan sesuai SOP.

Jenis-jenis CSIRT

National CSIRT

- Tim tingkat nasional, misalnya ID-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center) di bawah BSSN.

Sectoral CSIRT

- Dibentuk untuk sektor tertentu, seperti keuangan, pendidikan, atau pemerintahan.

Organizational CSIRT

- Tim internal dalam organisasi atau kampus — disebut CSIRT Kampus.

Membangun Ekosistem CSIRT Antar Kampus

- Mewujudkan lingkungan kampus yang **tanggap, kolaboratif, dan resilien** terhadap insiden keamanan siber.
- Menuju kolaborasi keamanan siber yang tangguh, terintegrasi, dan berkelanjutan di dunia pendidikan tinggi.
- CSIRT Kampus (Computer Security Incident Response Team) bukan sekadar tim teknis, tapi merupakan ekosistem multi-pihak yang melibatkan seluruh elemen kampus
  - pimpinan,
  - unit TI,
  - dosen,
  - mahasiswa, dan
  - mitra eksternal (seperti BSSN, ID-SIRTII, atau industri keamanan).

Konsep Ekosistem CSIRT Antar Kampus

Ekosistem CSIRT antar kampus adalah jaringan kolaboratif antar CSIRT perguruan tinggi untuk:

- Berbagi informasi ancaman (Threat Intelligence Sharing)
- Berkoordinasi dalam respons insiden
- Meningkatkan kapasitas SDM keamanan siber
- Membangun standar tata kelola bersama

Tujuannya: menciptakan komunitas keamanan siber pendidikan tinggi yang saling mendukung dan belajar bersama.

Contoh Kasus

Insiden yang Terjadi

- Pada bulan Maret 2024, tim TI mendeteksi:
- **Lonjakan lalu lintas jaringan** dari IP asing pada dini hari.
- Website kampus tiba-tiba **tidak bisa diakses** selama 6 jam.
- Sebagian data pada sistem akademik **terindikasi berubah atau hilang.**

Setelah ditelusuri, ternyata kampus mengalami **serangan ransomware** melalui akun yang dikompromi akibat *phishing email*.

lanjutan

- Tantangan yang Dihadapi
  - Tidak ada tim CSIRT resmi yang menangani insiden.
  - SOP keamanan belum baku; setiap unit bertindak sendiri.
  - Log server tidak lengkap, sehingga sulit menelusuri pelaku.
  - Komunikasi publik tidak terkoordinasi, menimbulkan kepanikan di kalangan mahasiswa.

Lanjutan

- Penanganan
  - Membentuk Tim CSIRT yang dapat bekerja sama dengan BSSN dan ID-SIRTII untuk pelatihan insiden.
  - Menerapkan Kerangka ISO/IEC 27001 (ISMS)
    - Menetapkan kebijakan keamanan informasi melalui SK Rektor.
    - Melakukan risk assessment terhadap semua sistem kampus.
    - Menyusun SOP penanganan insiden siber
    - Melakukan backup terjadwal dan enkripsi data sensitif.
  - Edukasi & Awareness
    - Mengadakan kampanye “Think Before You Click!” untuk civitas akademika.
    - Simulasi serangan phishing dan pelatihan keamanan digital.
  - Peningkatan Infrastruktur
    - Menerapkan multi-factor authentication (MFA).
    - Mengembangkan portal CSIRT Kampus untuk pelaporan insiden.

Pelajaran dari Kasus Ini?

Insiden siber pasti terjadi, tapi dampaknya bisa dikendalikan jika kampus punya sistem yang kuat.

ISO 27001 memberi struktur dan kebijakan, CSIRT menjalankan respons di lapangan.

Budaya keamanan adalah benteng utama, bukan hanya firewall, tapi juga kesadaran manusia.

ISO 27001	CSIRT
Menyusun kebijakan keamanan	Menjalankan operasional keamanan
Mengelola risiko & kontrol	Menangani insiden nyata
Audit & peningkatan berkelanjutan	Memberi feedback dari insiden

- ISO 27001 sering dianggap “administratif”, CSIRT dianggap “teknis”.
- Padahal keduanya komplementer.

Sinergi ISO 27001 & CSIRT

Terima Kasih

- “Keamanan siber bukan sekadar teknologi, tapi kolaborasi dan budaya bersama.”