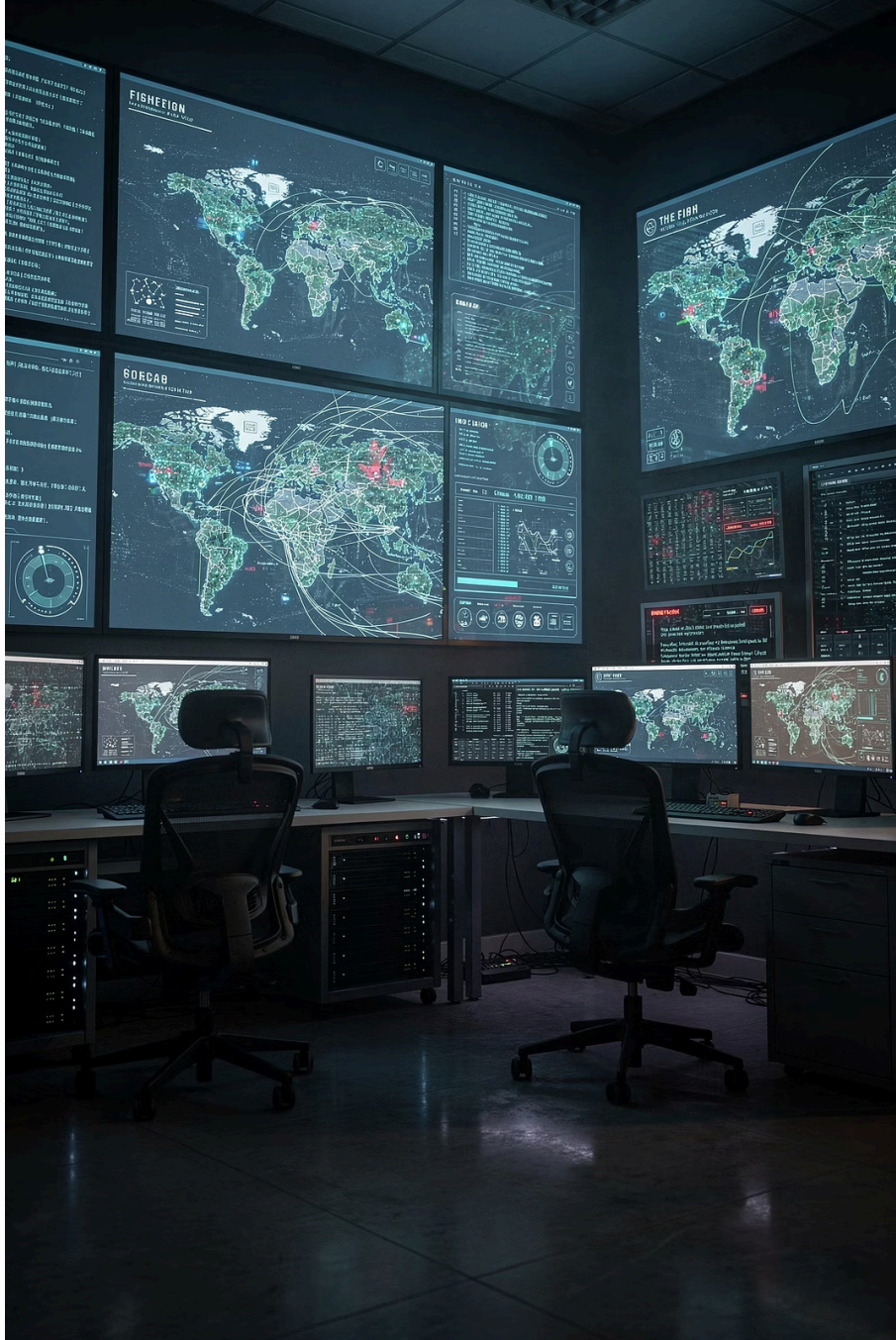
Modul 4: Analisis Ancaman dan Laporan Intelijen

Mengubah Data Menjadi Keputusan Strategis

C-SIX SECURITY

EDY SUSANTO



Mengapa Intelijen Ancaman Penting?

Ancaman Terus Berkembang

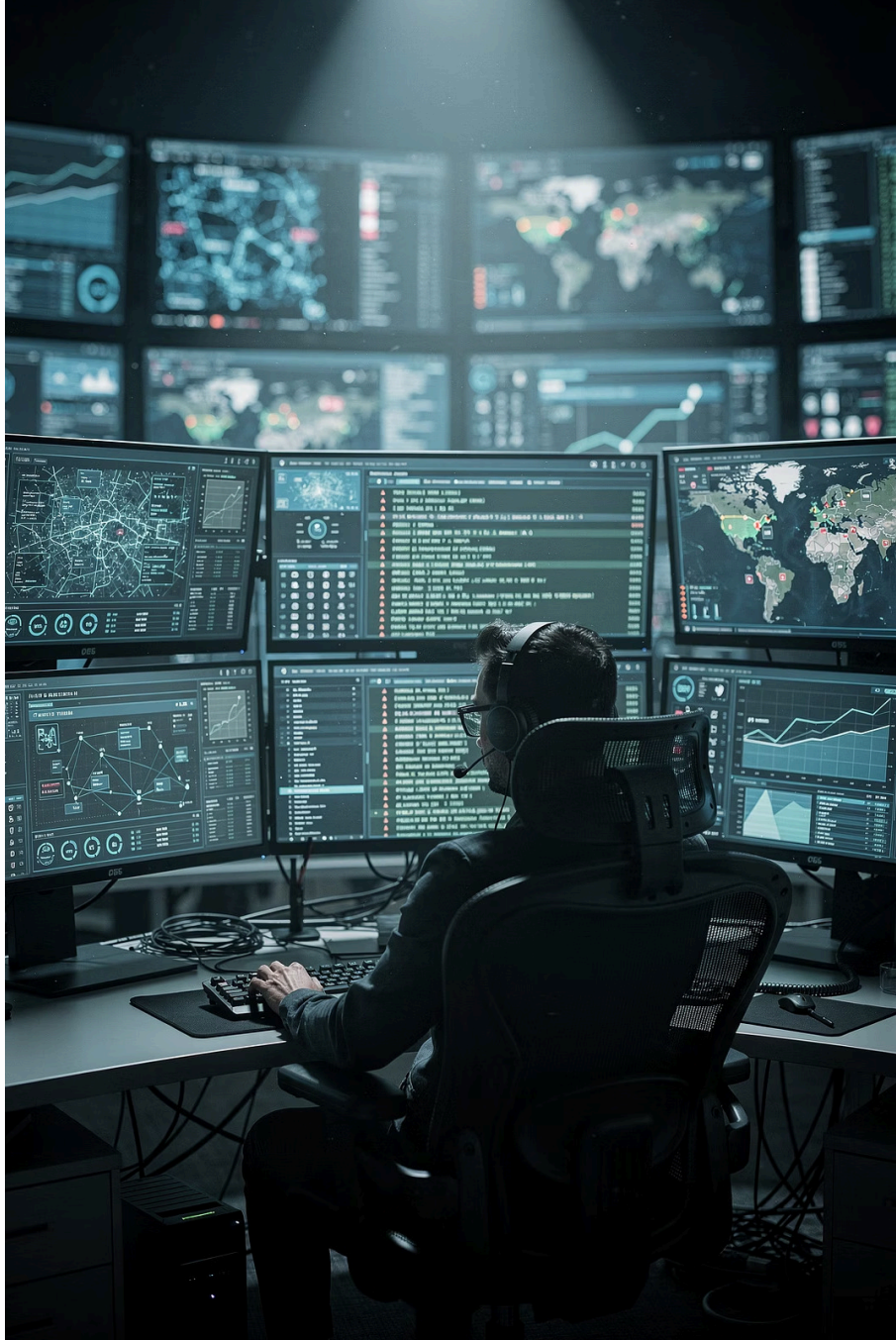
Tidak ada organisasi yang kebal. Ancaman siber berevolusi lebih cepat dari pertahanan konvensional.

Lebih dari Sekadar Data

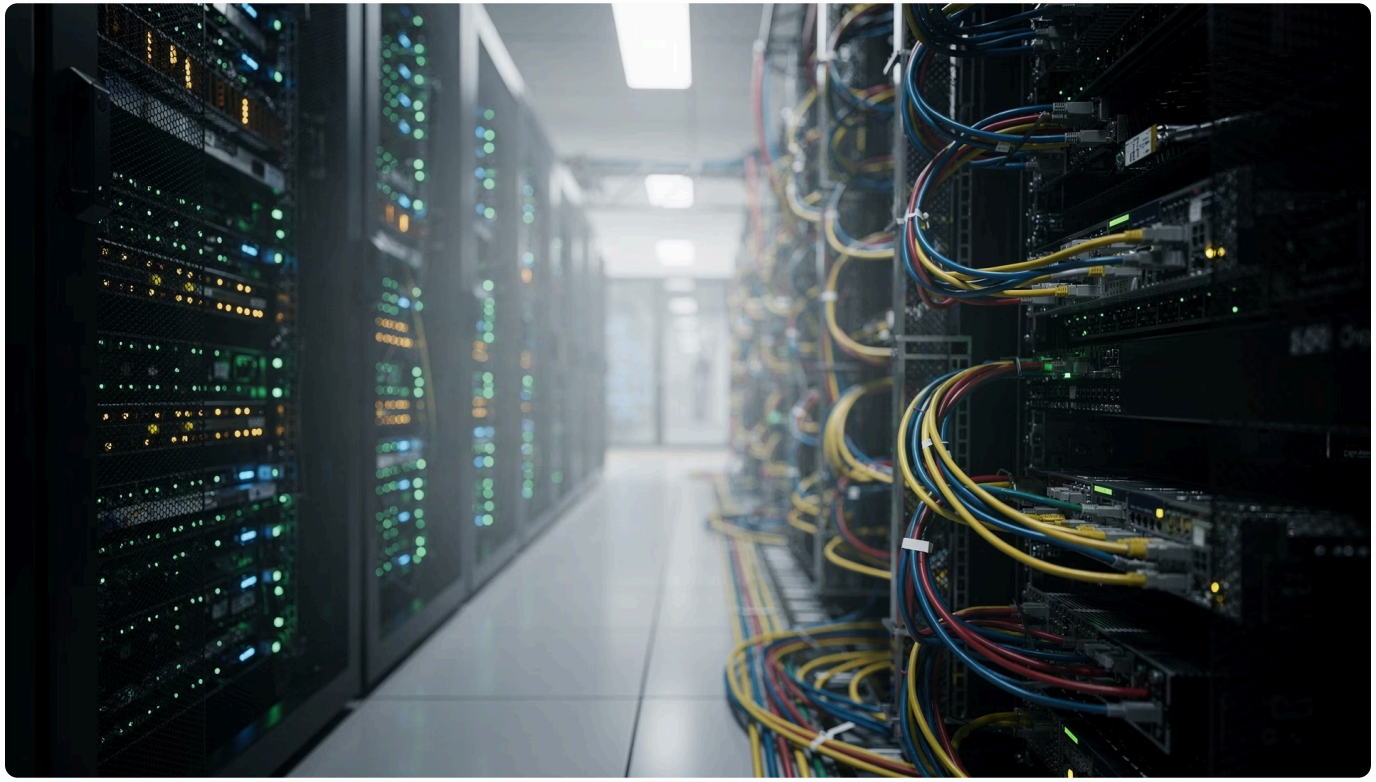
Intelijen adalah informasi teranalisis yang dapat langsung ditindaklanjuti — bukan sekadar kumpulan log mentah.

Tujuan Utama

Deteksi proaktif, mitigasi risiko nyata, dan pencegahan serangan sebelum terjadi.



Mengumpulkan Data Ancaman



Langkah Pengumpulan

→ Identifikasi Kebutuhan

Tentukan pertanyaan prioritas: apa yang paling perlu diketahui pengambil keputusan saat ini?

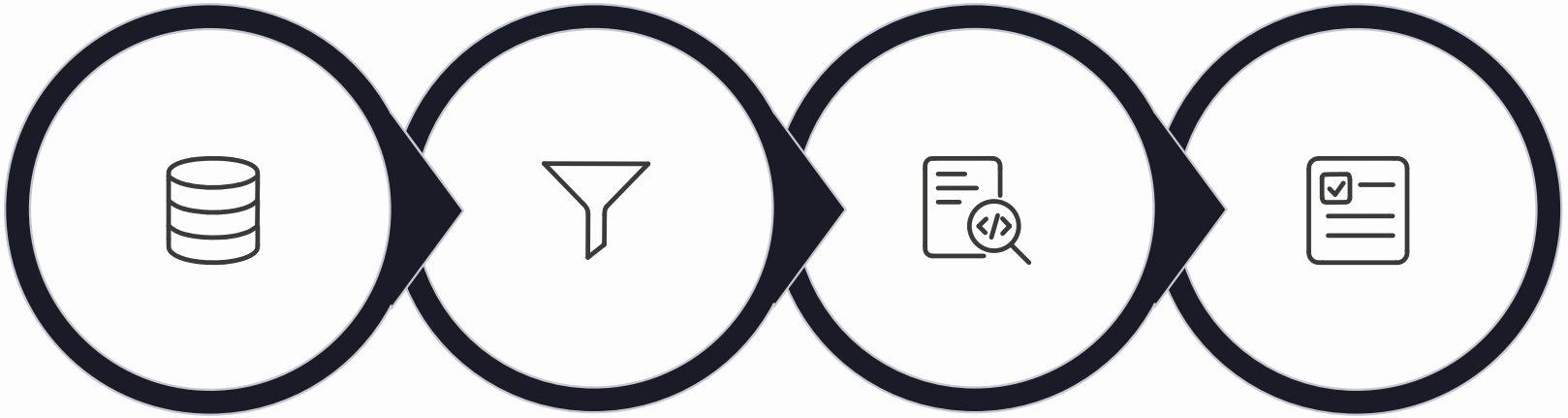
→ Sumber Internal

Log sistem, data endpoint, SIEM, dan rekaman aktivitas operasional jaringan internal.

→ Sumber Eksternal

Forum komunitas keamanan, threat feed publik, OSINT, dan masukan dari pakar industri.

Menganalisis Informasi



Normalisasi Deduplikasi Analisis TTP Poin Tindakan

Proses analisis mengubah data mentah yang berisik menjadi temuan terstruktur. Fokus pada Taktik, Teknik, dan Prosedur (TTP) membantu analis memahami *cara kerja* penyerang — bukan hanya apa yang mereka lakukan.

Membuat Threat Profile

Profiling Aktor Ancaman

Identifikasi siapa di balik serangan: kelompok APT, peretas bermotif finansial, atau insider threat.

Pola Perilaku & Motivasi

Analisis taktik berulang, waktu serangan, dan target pilihan untuk mengungkap motivasi penyerang.

Penilaian Kerentanan

Evaluasi seberapa rentan aset dan sistem organisasi terhadap ancaman yang telah dipetakan.

Menyusun Executive Summary

Kenali Audiens Anda

Eksekutif tidak butuh jargon teknis — mereka butuh konteks bisnis yang jelas dan ringkas.

Fokus pada Dampak & Risiko

Sajikan konsekuensi nyata bagi bisnis: potensi kerugian, reputasi, dan kepatuhan regulasi.

Rekomendasikan Tindakan

Akhiri dengan rekomendasi strategis konkret yang langsung mendukung keputusan manajemen.

Dasar Penulisan Laporan Intelijen

Prinsip Laporan yang Efektif

Laporan intelijen yang baik bukan laporan yang paling panjang — melainkan yang paling tepat sasaran.

> Gunakan format **brief singkat** atau **slide eksekutif** agar informasi cepat diserap oleh pembuat keputusan.

Setiap laporan harus menjawab satu pertanyaan kunci: *Apa yang perlu dilakukan organisasi sekarang?*

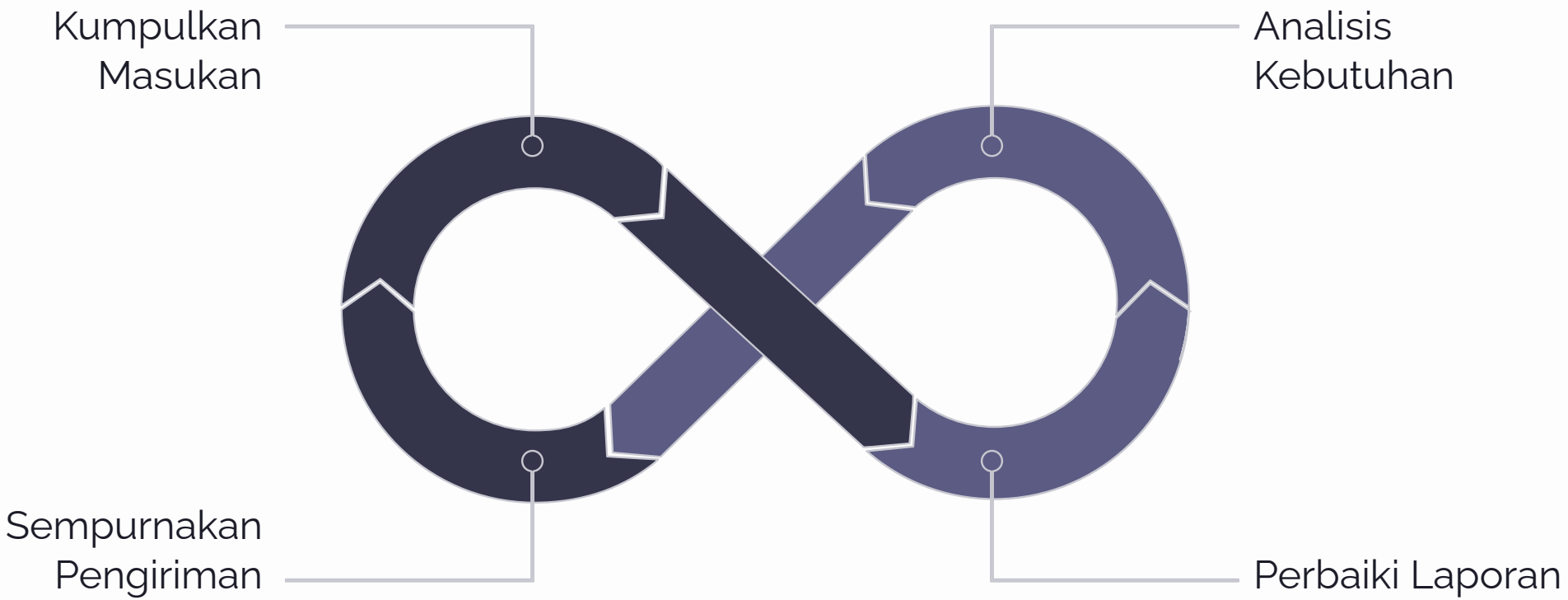
Praktik: Analisis Kasus Nyata

Simulasi Siklus Intelijen

Peserta menerapkan siklus intelijen penuh pada skenario serangan siber nyata — dari pengumpulan data hingga pelaporan.

- Identifikasi Indikator Penyusupan (IoC) dari bukti digital
- Petakan TTP ke dalam framework MITRE ATT&CK
- Susun laporan singkat yang siap disampaikan ke manajemen

Feedback dan Iterasi



Intelijen yang baik lahir dari proses iteratif. Setiap siklus pelaporan menghasilkan pemahaman yang lebih dalam tentang kebutuhan audiens — menjadikan laporan berikutnya lebih presisi dan berdampak nyata.

Kesimpulan: Intelijen sebagai Senjata Strategis

Proses Berkelanjutan

Intelijen bukan proyek sekali jalan — ia harus terus diperbarui seiring lanskap ancaman yang berubah.

Kecepatan & Ketepatan

Keamanan ditentukan oleh seberapa cepat organisasi beradaptasi dengan informasi yang tepat dan akurat.

Edy Susanto — Founder, C-SIX Security | **26137180**