Modul 1: Introduction to Cyber Threat Intelligence

Memahami intelijen ancaman siber sebagai fondasi pertahanan organisasi modern.

C-SIX SECURITY ACADEMY

DEFINISI

Apa Itu Cyber Threat Intelligence?

CTI adalah proses pengumpulan, analisis, dan interpretasi data untuk memahami ancaman siber secara mendalam — bukan sekadar data mentah, melainkan **insight yang dapat ditindaklanjuti**.

Ibarat sistem peringatan dini: mengetahui siapa musuh, bagaimana cara mereka menyerang, dan kapan ancaman itu datang — sebelum serangan benar-benar terjadi.

Mengapa CTI Begitu Penting?

🎯 Deteksi Dini

Selangkah lebih maju dari taktik penyerang sebelum serangan terjadi.

⚡ Respons Cepat

Mengurangi waktu investigasi dan mempercepat penanganan insiden.

💰 Efisiensi Biaya

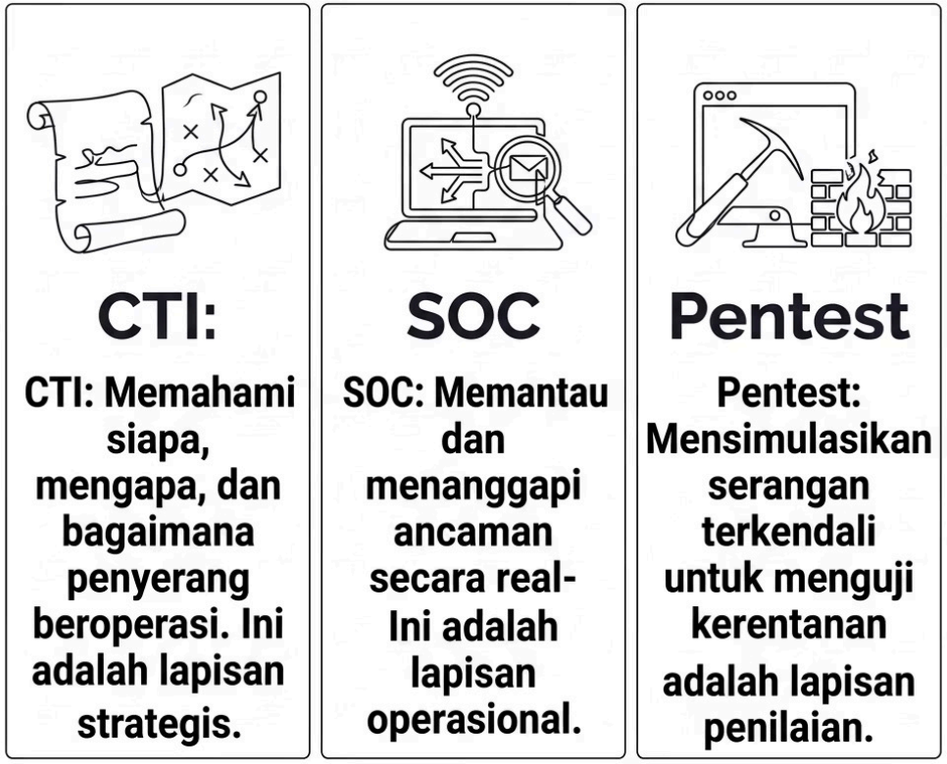
Mencegah kerugian finansial dan reputasi yang berpotensi fatal.

📊 Berbasis Data

Menggantikan asumsi dengan bukti nyata dan analisis terverifikasi.

CTI vs SOC vs Pentest

Ketiganya saling melengkapi, namun memiliki peran yang berbeda dalam ekosistem keamanan siber.



CTI

Memahami **siapa, mengapa, dan bagaimana** musuh menyerang melalui intelijen strategis.

SOC

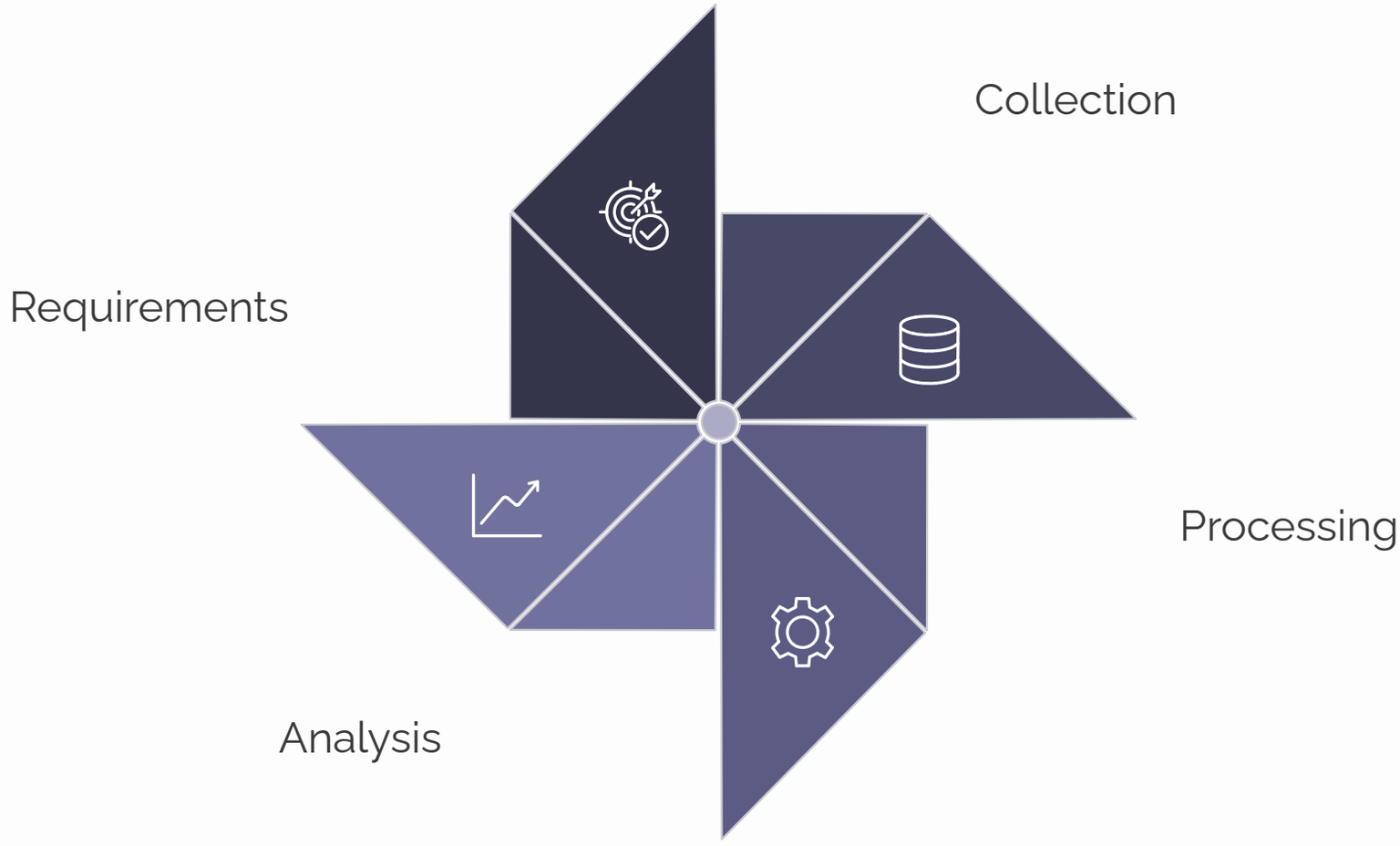
Tim operasional yang **memantau dan merespons** ancaman secara real-time.

Pentest

Simulasi serangan terkontrol untuk **menguji kerentanan** sistem yang ada.

Intelligence Cycle: Dari Data Menjadi Aksi

Enam tahap sistematis yang mengubah data mentah menjadi intelijen yang dapat digunakan pengambil keputusan.



Siklus ini bersifat iteratif — setiap putaran menghasilkan intelijen yang semakin akurat dan relevan bagi organisasi.

Jenis-Jenis Intelligence (1/2)

Strategic Intelligence

Informasi tingkat tinggi untuk arah kebijakan keamanan jangka panjang. Ditujukan untuk level eksekutif dan CISO dalam pengambilan keputusan strategis.

Tactical Intelligence

Berfokus pada taktik, teknik, dan prosedur (TTP) penyerang untuk mendukung konfigurasi dan penguatan pertahanan sistem secara operasional.

Jenis-Jenis Intelligence (2/2)

Operational Intelligence

Detail teknis serangan yang sedang berlangsung. Digunakan langsung oleh tim respons insiden untuk menghentikan dan menangani ancaman aktif.

Technical Intelligence

Indikator kompromi teknis seperti alamat IP berbahaya, domain mencurigakan, dan hash file malware (IoC) untuk sistem deteksi otomatis.

Setiap jenis intelijen melayani audiens yang berbeda — dari CISO hingga analis SOC di garis terdepan.

Mengantisipasi Ancaman Modern

Teknologi pasif tidak lagi cukup menghadapi ancaman siber yang terus berevolusi. Organisasi harus bertransisi dari postur **reaktif** menuju pendekatan **proaktif** berbasis intelijen.

> CTI menggeser paradigma keamanan: dari *"kita sudah diserang"* menjadi *"kita tahu sebelum diserang"*.

Kesimpulan Modul 1

01

CTI adalah Senjata Strategis

Bukan hanya alat teknis — CTI adalah keunggulan kompetitif dalam pertahanan siber modern.

02

Pahami Siklus & Jenisnya

Intelligence Cycle dan empat jenis intelijen meningkatkan kesiapan serta kematangan keamanan organisasi.

03

Proaktif Menentukan Keunggulan

Keunggulan organisasi ditentukan oleh seberapa cepat dan tepat kita merespons ancaman yang akan datang.

Terima Kasih

Modul 1 telah membawa kita pada fondasi pemahaman Cyber Threat Intelligence. Mari terus tingkatkan ketahanan siber organisasi Anda.

Edy Susanto — Founder, C-SIX Security

C-SIX SECURITY ACADEMY