Modul 5: Menjadi Threat Intelligence Analyst

Menjadi Penjaga di Garis Depan Pertahanan Digital

C-SIX SECURITY

EDY SUSANTO

Apa Itu CTI Analyst?

🕵️ Detektif Digital

Bukan sekadar teknisi — seorang CTI Analyst memetakan niat dan kapabilitas penyerang untuk mengantisipasi langkah mereka berikutnya.

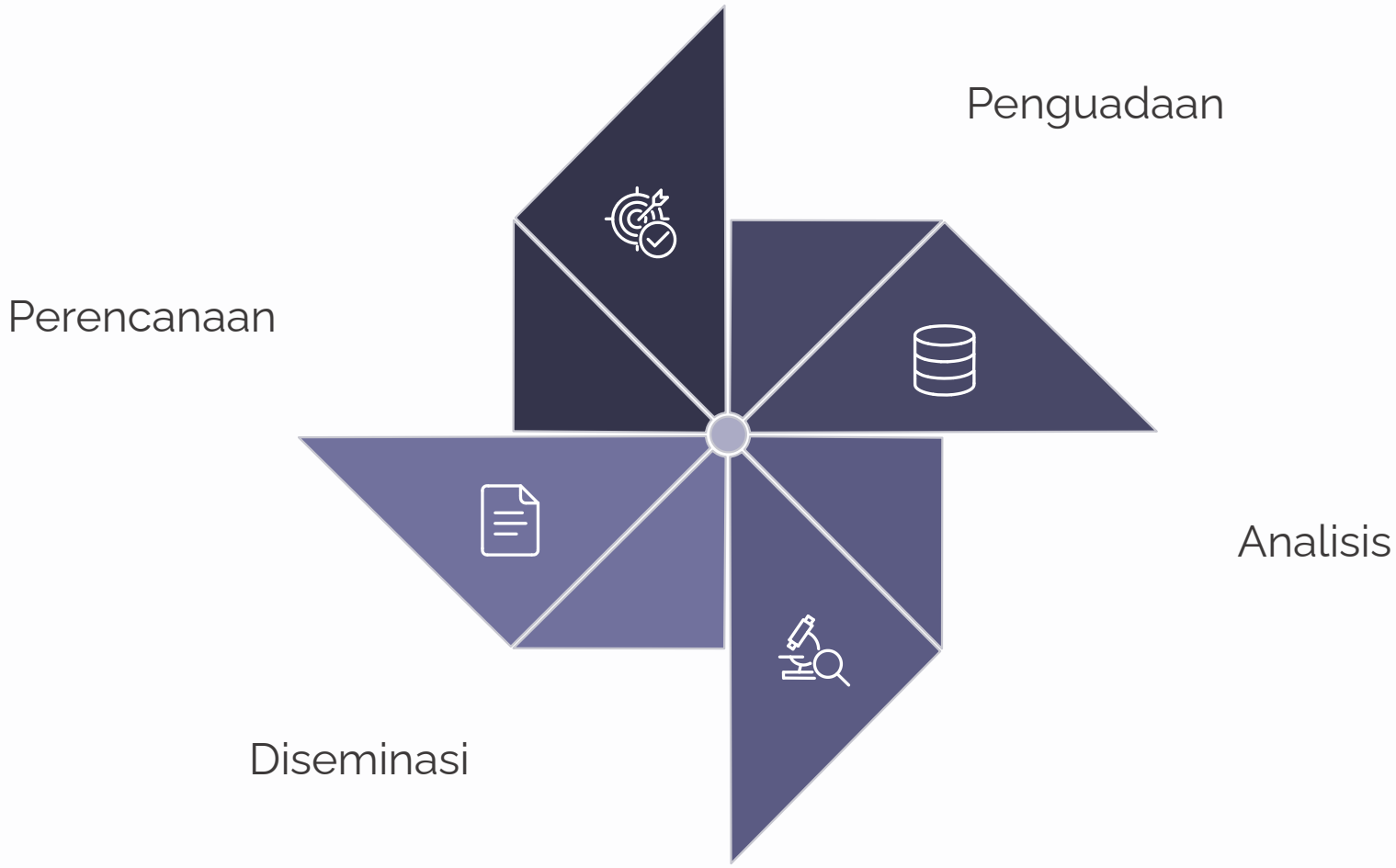
🔗 Penghubung Data

Menghubungkan titik-titik data yang tersebar untuk memprediksi serangan sebelum benar-benar terjadi.

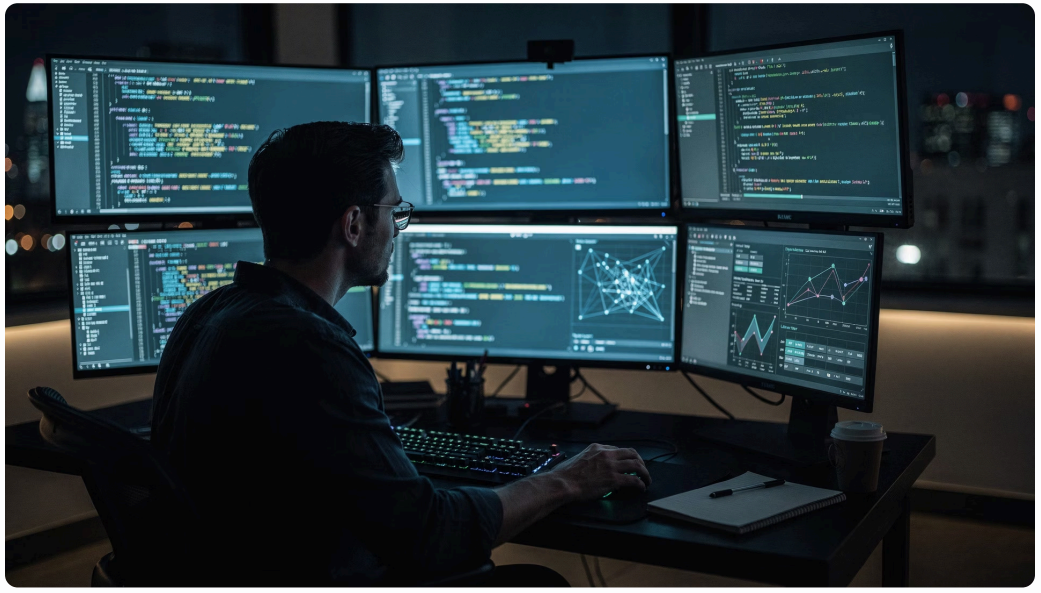
🛡️ Senjata Rahasia

Membawa organisasi beralih dari pendekatan **reaktif** menjadi **proaktif** dalam menghadapi ancaman siber.

Workflow: Siklus Intelijen



Setiap tahap siklus saling bergantung — kualitas intelijen akhir ditentukan oleh kedisiplinan di setiap langkahnya.



SKILL MATRIX

Skill yang Dibutuhkan

🖥️ Teknis

Jaringan, Sistem Operasi, analisis malware, serta pemahaman **SIEM** dan **IDS**.

🧠 Analitis

Berpikir kritis dan menghubungkan pola dari data yang tampak acak dan tidak terstruktur.

📝 Komunikasi

Mengubah bahasa teknis yang rumit menjadi laporan strategis yang mudah dipahami manajemen.

Sertifikasi & Jalur Karier

Fondasi

CompTIA Security+ — Titik awal yang diakui secara global untuk membangun pemahaman keamanan siber dasar.

Spesialisasi CTI

EC-Council CTIA atau **GIAC GCTI** — Sertifikasi khusus yang membuktikan kompetensi Anda sebagai Threat Intelligence Analyst.

Tingkat Profesional

CISSP — Untuk pemahaman keamanan tingkat manajerial dan pengakuan di level senior industri.

Sumber Belajar Gratis

Coursera / IBM

Jalur **IBM Cybersecurity Analyst** adalah pintu masuk terbaik bagi pemula yang ingin terstruktur.

Komunitas & Blog

Pelajari laporan threat intelligence dari **Mandiant** dan **SOCRadar** untuk wawasan dunia nyata.

Latihan OSINT

Eksplorasi sumber OSINT publik seperti Shodan dan VirusTotal untuk riset ancaman terkini secara langsung.

2026

Tren Ancaman Siber 2026

Lanskap ancaman terus berevolusi. CTI Analyst harus selalu berada selangkah lebih maju dari para penyerang yang semakin canggih dan terorganisir.

⚠ Ancaman tidak lagi hanya menyasar perusahaan besar — UMKM dan klinik kini menjadi target utama.

🤖 AI-Powered Attacks

Serangan siber semakin terautomasi dengan kecerdasan buatan, membuat deteksi tradisional tidak lagi efektif.

🏥 Target Skala Kecil

UMKM dan fasilitas kesehatan menjadi sasaran empuk karena keterbatasan sumber daya keamanan mereka.

💰 Lonjakan Ransomware

Serangan ransomware meningkat drastis, menuntut kemampuan pemulihan cepat dan strategi pencegahan yang matang.

Final Project: Mini Threat Intelligence Report

01

Pilih Ancaman Nyata

Pilih satu ancaman siber aktual — misalnya kampanye ransomware spesifik yang sedang aktif atau kelompok APT yang relevan.

02

Lakukan Analisis Mendalam

Identifikasi siapa aktornya, apa motivasinya, dan bagaimana taktik TTP mereka dijalankan di lapangan.

03

Buat Rekomendasi Mitigasi

Susun rekomendasi yang dapat langsung diimplementasikan oleh organisasi Anda untuk mengurangi risiko serangan.

Langkah Awal Karier Anda

Bangun Portofolio

Mulailah dengan menulis laporan intelijen sederhana. Setiap tulisan adalah bukti nyata kemampuan Anda.

Utamakan Konteks

Intelijen bukan tentang volume data — melainkan tentang **konteks** yang mengubah data menjadi wawasan yang dapat ditindaklanjuti.

Tanya "Mengapa"

Jadilah analis yang tidak hanya tahu *apa* yang terjadi, tetapi memahami **mengapa** itu terjadi dan apa implikasinya.

Terima Kasih

Menjadi Threat Intelligence Analyst adalah komitmen seumur hidup untuk terus belajar, beradaptasi, dan menjaga mereka yang tidak bisa menjaga diri sendiri.

> Intelijen terbaik lahir dari rasa ingin tahu yang tidak pernah padam.

👤 Instruktur

Edy Susanto
Founder, C-SIX Security

📞 Kontak

26137180
Hubungi untuk konsultasi & kolaborasi

🔰 Modul

Modul 5 / Final
Menjadi Threat Intelligence Analyst