Modul 3: Menjadi Pemburu Ancaman

Menguasai Seni Deteksi dan Analisis **Indikator Kompromi (IOC)** untuk melindungi aset digital dari ancaman tersembunyi.

EDY SUSANTO | FOUNDER C-SIX SECURITY

CHAPTER 1

Mengenal Musuh Kita

Sebelum bisa berburu, kita harus memahami apa yang kita cari.

Apa Itu Indicator of Compromise (IOC)?

IOC adalah **artefak digital** yang berfungsi sebagai bukti jejak serangan di jaringan atau endpoint — seperti sidik jari pelaku di tempat kejadian perkara.

IP Address

Alamat server mencurigakan

Domain

URL berbahaya atau palsu

File Hash

Sidik jari unik malware

Kenapa IOC Sangat Penting?

IOC mengubah cara tim keamanan merespons ancaman — dari reaktif menjadi terukur dan presisi.

Deteksi Dini

Memberikan data konkret untuk identifikasi ancaman sebelum kerusakan meluas.

Blokir Presisi

Memungkinkan tim keamanan memblokir akses penyerang secara tepat sasaran.

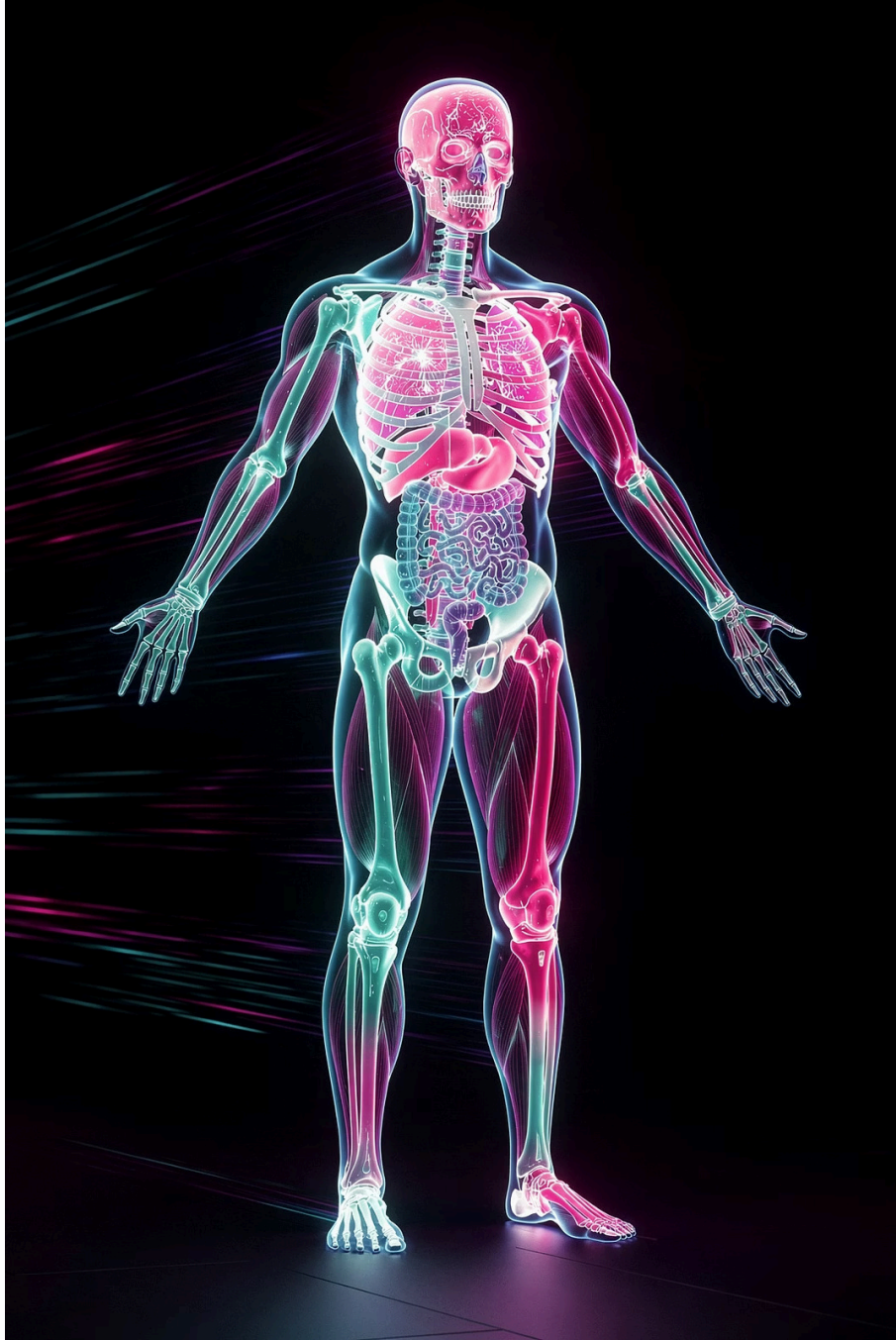
Pertahanan Terukur

Mengubah reaksi pasif menjadi strategi pertahanan yang berbasis data.

CHAPTER 2

Anatomi Indikator Berbahaya

Mengenal tiga jenis IOC utama yang digunakan pelaku ancaman.



Mengungkap IP Address Berbahaya

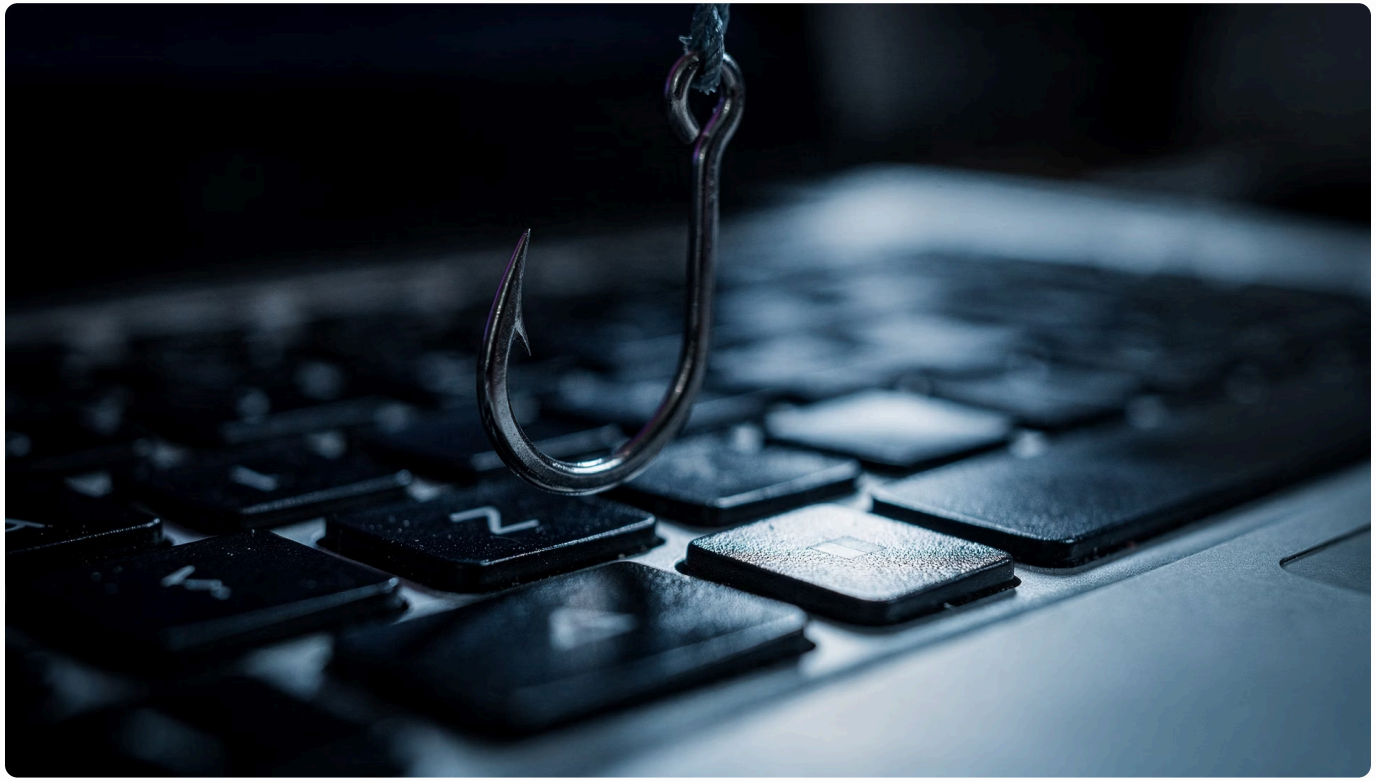
Apa yang Dicari?

IP address berbahaya sering berfungsi sebagai **Command & Control (C2)** — pusat kendali yang digunakan penyerang untuk mengelola malware dan botnet dari jarak jauh.

- Identifikasi server C2 aktif milik penyerang
- Lacak sumber serangan dan aktivitas botnet
- Reputasi IP menjadi filter keamanan pertama

Gunakan **AbuseIPDB** untuk mengecek reputasi IP secara real-time.

Menelusuri Domain Berbahaya



Kedok Digital Penyerang

Domain berbahaya digunakan sebagai kedok untuk **phishing** atau pengalihan trafik ke situs jahat. Penyerang sering mendaftarkan domain baru yang menyerupai situs resmi.

- Deteksi domain baru terdaftar yang mencurigakan
- Analisis pola nama domain yang meniru entitas resmi
- Gunakan **URLScan** untuk membedah situs berbahaya secara aman

File Hash: Sidik Jari Digital Malware

Setiap file memiliki nilai hash unik — bahkan perubahan satu byte pun menghasilkan hash yang berbeda.

MD5 Hash

32 karakter heksadesimal. Cepat dihitung namun rentan terhadap kolisi — masih umum digunakan untuk verifikasi awal.

SHA-256 Hash

64 karakter, jauh lebih aman dan menjadi standar industri modern untuk identifikasi malware yang akurat.

VirusTotal

Platform validasi utama — unggah file atau hash untuk dianalisis oleh puluhan mesin antivirus sekaligus.

CHAPTER 3

Dasar-Dasar Threat Hunting

Dari deteksi pasif menuju perburuan aktif terhadap ancaman.

Apa Itu Threat Hunting?

Threat Hunting adalah pendekatan **proaktif** untuk mencari ancaman yang bersembunyi di dalam jaringan — tidak menunggu alarm berbunyi, tetapi aktif mencari anomali sebelum kerusakan terjadi.

- Fokus pada **pola perilaku** yang tidak wajar, bukan sekadar mencocokkan tanda-tanda serangan yang sudah dikenal.

Metodologi Berburu Ancaman

Metodologi ini membentuk siklus investigasi yang sistematis — memastikan tidak ada jejak ancaman yang terlewat dalam proses perburuan.

Toolkit Wajib bagi Hunter

VirusTotal

Pusat analisis file, URL, domain, dan hash dengan 70+ mesin antivirus terintegrasi.

AbuseIPDB

Database reputasi IP berbasis pelaporan komunitas global secara real-time.

URLScan

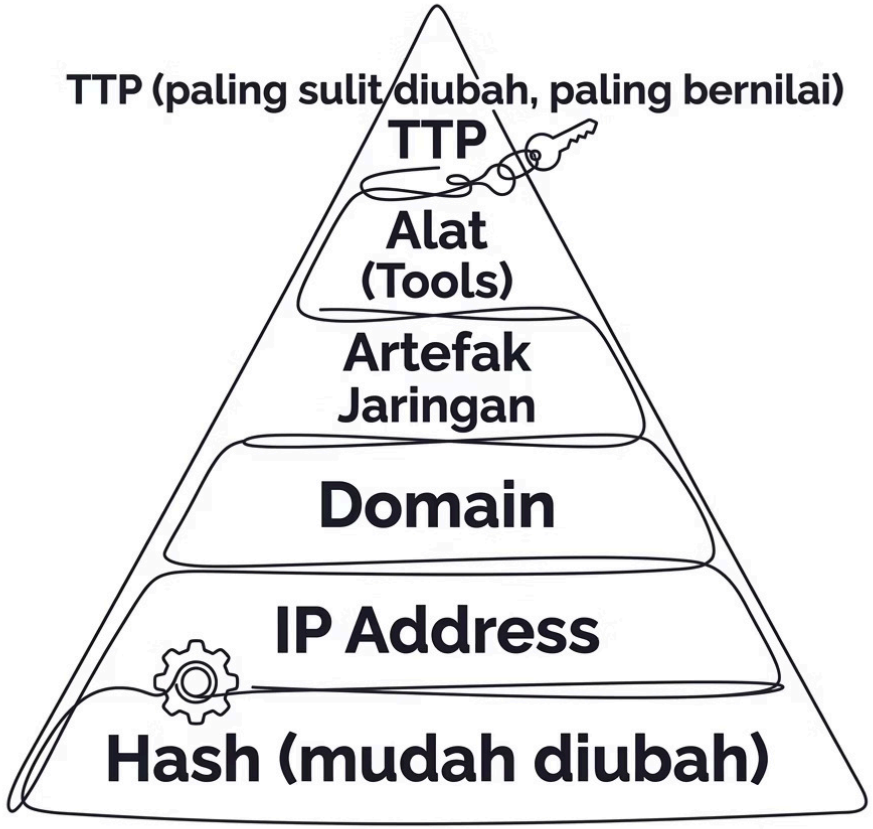
Visibilitas mendalam terhadap konten, skrip, dan perilaku situs web mencurigakan.

Menuju Deteksi yang Lebih Cerdas

Dari IOC ke TTP

IOC hanyalah titik awal. Hunter berpengalaman memahami **Tactics, Techniques & Procedures (TTP)** — pola perilaku penyerang yang lebih sulit disembunyikan dibanding sekadar mengubah file hash atau domain.

- Temuan IOC dikonversi menjadi aturan deteksi otomatis
- Intelijen ancaman yang akurat memperkuat lapisan pertahanan
- Kontribusi aktif ke komunitas threat intelligence global



Ringkasan Outcome Peserta

Setelah menyelesaikan Modul 3, peserta diharapkan mampu:

Kenali Jejak Serangan

Mengidentifikasi IOC secara sistematis dari log, jaringan, dan endpoint.

Kuasai Alat Industri

Terampil menggunakan VirusTotal, AbuseIPDB, dan URLScan untuk investigasi.

Jadilah Defender Proaktif

Siap bertransformasi dari pengguna pasif menjadi pembela jaringan yang aktif berburu ancaman.

Jadilah Pemburu yang Tak Terlihat

Ancaman tidak akan pernah berhenti berkembang — namun kemampuan deteksi Anda pun harus terus tumbuh. Praktikkan, eksplorasi, dan amankan aset digital Anda mulai hari ini.

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