Modul 3 – Dark Web Intelligence Collection

Teknik dan metodologi pengumpulan intelijen dari sumber-sumber Dark Web secara sistematis, legal, dan profesional untuk mendukung operasi keamanan siber.

C-SIX SECURITY

EDY SUSANTO – FOUNDER C-SIX SECURITY

Peta Materi

Tujuan Pembelajaran Modul Ini

Modul ini dirancang untuk membekali praktisi keamanan siber dengan kemampuan mengumpulkan informasi yang tersedia secara publik dari sumber Dark Web — mulai dari pengenalan alat, metodologi penelusuran, hingga alur kerja pengumpulan data yang terstruktur.

01

Pengenalan Dark Web

Memahami ekosistem Dark Web, search engines, dan infrastruktur .onion

02

Forum & Marketplace

Teknik monitoring forum, komunitas threat actor, dan marketplace intelijen

03

Leak & Threat Monitoring

Identifikasi kebocoran data dan observasi pelaku ancaman secara aman

04

Data Collection Workflow

Membangun alur kerja pengumpulan data yang sistematis dan dapat direplikasi

Edy Susanto – Founder C-SIX Security

Pengenalan Dark Web Search Engines

Dark Web bukanlah satu entitas tunggal — melainkan lapisan internet yang tidak terindeks oleh mesin pencari konvensional dan hanya dapat diakses melalui jaringan seperti Tor. Memahami cara kerja search engine khusus adalah fondasi dari Dark Web Intelligence Collection.

Apa Itu Dark Web?

Bagian dari internet yang memerlukan perangkat lunak khusus (Tor) untuk diakses. Menggunakan domain .onion yang tidak terdaftar di DNS publik dan menawarkan anonimitas tinggi bagi penggunanya.

Search Engine Utama

- **Ahmia.fi** – Indeks .onion yang bisa diakses dari clearnet maupun Tor
- **Torch** – Salah satu mesin pencari tertua di Dark Web
- **DuckDuckGo via Tor** – Alternatif privasi yang merespons query .onion
- **Haystak** – Indeks besar dengan filter konten ilegal

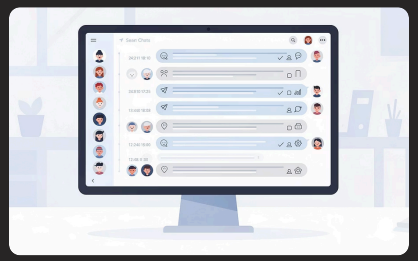
Edy Susanto – Founder C-SIX Security

Forum Monitoring

Forum di Dark Web merupakan salah satu sumber intelijen paling kaya. Di sinilah para pelaku ancaman berdiskusi, berbagi alat, menjual akses, dan merekrut kolaborator. Memantau forum secara sistematis memungkinkan analis mendeteksi ancaman sebelum terjadi insiden.

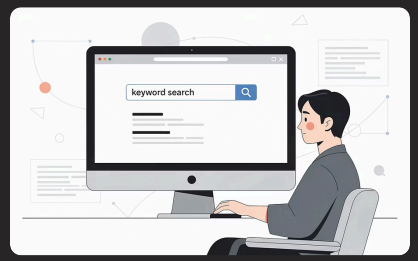
Forum Umum Cybercrime

Forum seperti XSS, Exploit.in, dan BreachForums membahas teknik serangan, jual beli akses, dan distribusi malware. Analis perlu memahami struktur dan terminologi yang digunakan.



Teknik Passive Monitoring

Membaca tanpa berinteraksi (lurking) adalah pendekatan paling aman. Gunakan akun alias yang tidak terhubung dengan identitas nyata. Hindari registrasi kecuali benar-benar diperlukan.



Keyword & Keyword Alerting

Tentukan kata kunci relevan seperti nama organisasi, domain, atau teknologi yang digunakan target. Dokumentasikan setiap temuan dengan timestamp dan URL arsip.

Edy Susanto – Founder C-SIX Security

Konsep Dasar

Marketplace Intelligence

Dark Web marketplace adalah platform transaksi tempat berbagai komoditas ilegal diperdagangkan — mulai dari kredensial curian, akses awal ke jaringan korporat, hingga exploit zero-day. Dari perspektif intelijen, marketplace memberikan sinyal awal tentang ancaman yang sedang berkembang.

⚠ Penting: Tujuan pemantauan marketplace adalah intelijen, bukan partisipasi. Analis tidak boleh melakukan pembelian atau transaksi apapun yang dapat melanggar hukum.

Edy Susanto – Founder C-SIX Security

Threat Actor Observation

Memahami siapa pelaku ancaman, bagaimana mereka beroperasi, dan apa motivasi mereka adalah inti dari intelijen strategis. Observasi threat actor di Dark Web memungkinkan analis membangun profil yang akurat untuk mendukung keputusan defensif.

Identifikasi Alias & Handle

Lacak alias yang konsisten digunakan di berbagai forum. Satu threat actor sering memiliki beberapa handle namun menunjukkan pola perilaku, gaya bahasa, atau teknik yang serupa.

Analisis Pola Aktivitas

Perhatikan waktu posting, bahasa yang digunakan, dan topik yang diminati. Pola ini dapat mengungkap zona waktu, latar belakang linguistik, dan spesialisasi teknis pelaku.

Pemetaan Afiliasi & Kelompok

Banyak threat actor berafiliasi dengan kelompok ransomware, APT, atau komunitas crimeware. Identifikasi koneksi ini untuk memahami kapabilitas dan potensi ancaman yang lebih luas.

Edy Susanto – Founder C-SIX Security

Konsep Dasar

Leak Monitoring

Kebocoran data adalah salah satu ancaman terbesar bagi organisasi. Dark Web sering menjadi tempat pertama data yang dicuri dipublikasikan — jauh sebelum organisasi korban menyadari terjadinya pelanggaran. Leak monitoring yang proaktif dapat memperpendek waktu deteksi secara signifikan.

Apa yang Dimonitor?

- Domain dan email korporat organisasi
- Nama karyawan kunci dan eksekutif
- Nomor rekening, NPWP, atau identifikasi unik
- Nama produk atau proyek rahasia
- Rentang IP dan ASN organisasi

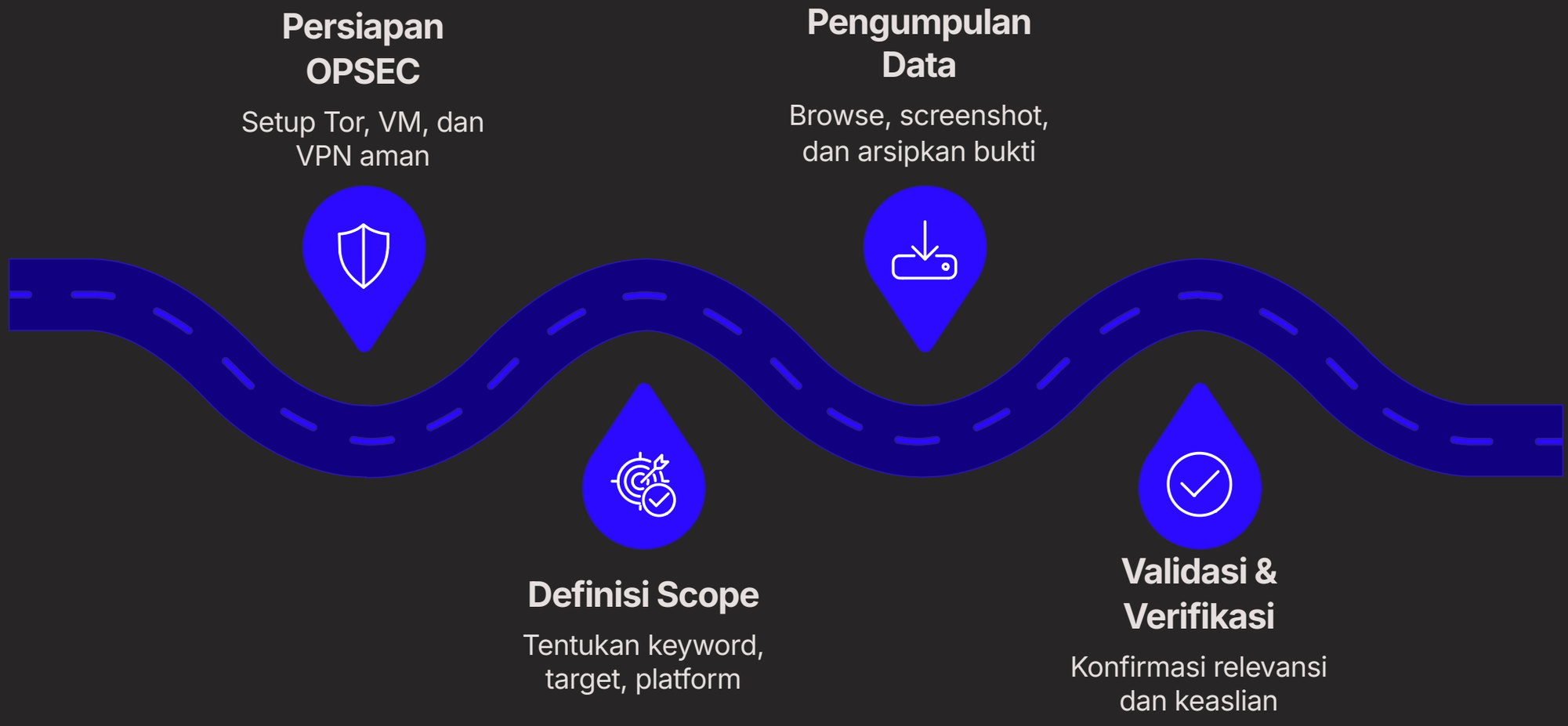
Platform & Sumber Leak

- **Dedicated leak sites** – halaman khusus grup ransomware
- **Paste sites** – Pastebin dark web equivalents
- **Telegram channels** – kanal publik berbagi data curian
- **Forum dump threads** – thread berbagi database di forum cybercrime

Edy Susanto – Founder C-SIX Security

Data Collection Workflow

Pengumpulan data yang efektif membutuhkan alur kerja yang terstruktur dan dapat direplikasi. Tanpa metodologi yang jelas, analis berisiko mengumpulkan data yang tidak dapat diverifikasi, tidak terdokumentasi, atau bahkan melanggar batas etika dan hukum.



Setiap langkah dalam workflow ini dirancang untuk menjaga integritas data, keamanan analis, dan nilai intelijen yang dapat ditindaklanjuti. OPSEC (Operational Security) adalah prioritas utama di setiap tahap pengumpulan.

Edy Susanto – Founder C-SIX Security

Tools yang Digunakan

Pemilihan alat yang tepat adalah faktor kritis dalam Dark Web Intelligence Collection. Alat-alat berikut merupakan standar industri yang digunakan oleh praktisi intelijen siber secara global — tersedia secara gratis dan legal untuk tujuan riset dan intelijen defensif.

Tor Browser

Browser berbasis Firefox yang merutekan traffic melalui jaringan Tor. Memberikan anonimitas berlapis dan akses ke domain .onion. Selalu gunakan dalam lingkungan virtual machine (VM) yang terisolasi.

Ahmia Search

Mesin pencari yang mengindeks situs .onion dan dapat diakses dari clearnet maupun melalui Tor. Memfilter konten ilegal dan merupakan titik awal yang aman untuk reconnaissance Dark Web.

Dark Web Intelligence Resources

Kumpulan sumber daya terseleksi termasuk forum monitoring lists, direktori .onion terpercaya, dan repositori OSINT khusus Dark Web untuk mendukung pengumpulan intelijen yang terarah.

Selalu gunakan VM yang terisolasi dari jaringan produksi, VPN, dan jangan pernah mengakses Dark Web dari perangkat atau jaringan kerja utama.

Edy Susanto – Founder C-SIX Security

Sesi Praktik & Outcome

Sesi praktik dirancang untuk membangun kemampuan hands-on dalam menelusuri sumber-sumber Dark Web secara aman, mengidentifikasi kategori ancaman, dan mendokumentasikan temuan dengan standar intelijen profesional.

Yang Akan Dilakukan

- Mengakses dan menggunakan Tor Browser dengan OPSEC yang benar
- Menelusuri sumber informasi publik menggunakan Ahmia
- Mengidentifikasi dan mengklasifikasikan kategori ancaman dari temuan
- Mendokumentasikan hasil temuan dalam format laporan standar

Outcome yang Dicapai

Setelah menyelesaikan modul ini, peserta mampu:

- Mengumpulkan informasi secara **sistematis dan aman** dari Dark Web
- Membedakan jenis-jenis ancaman berdasarkan konteks dan sumber
- Menerapkan workflow OSINT yang dapat direplikasi dalam operasi nyata
- Menjaga OPSEC selama seluruh proses pengumpulan data

Edy Susanto – Founder C-SIX Security