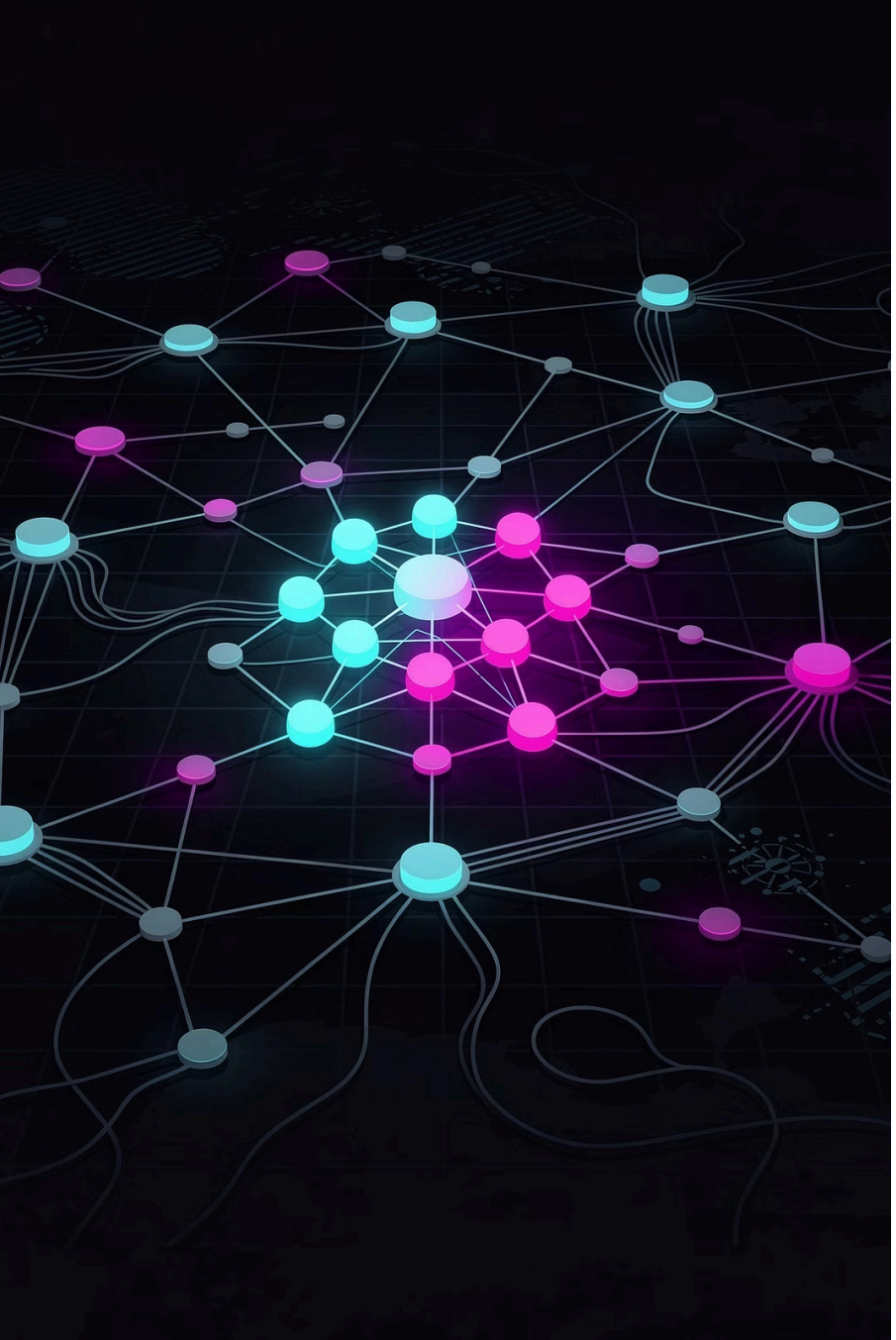


Modul 4 – Threat Intelligence & Leak Monitoring

Menggunakan informasi Dark Web untuk memahami, menganalisis, dan merespons ancaman siber secara proaktif. Modul ini dirancang untuk profesional keamanan yang ingin meningkatkan kemampuan dalam threat intelligence dan pemantauan kebocoran data.

Edy Susanto – Founder C-SIX Security

Tujuan Pembelajaran

Pada akhir modul ini, peserta akan mampu menghubungkan informasi yang beredar di Dark Web dengan risiko nyata yang dihadapi organisasi, serta mengambil langkah mitigasi yang tepat dan terukur.

🔍 Identifikasi

Mengenali threat actor, pola serangan, dan indikator ancaman yang relevan

📊 Analisis

Mengolah data kebocoran dan IOC menjadi intelijen yang dapat ditindaklanjuti

🛡️ Mitigasi

Menghubungkan temuan Dark Web dengan strategi perlindungan organisasi

Edy Susanto – Founder C-SIX Security

Threat Actor Profiling

Threat Actor Profiling adalah proses sistematis untuk mengidentifikasi, mendokumentasikan, dan memahami pelaku ancaman siber — mulai dari motivasi, kapabilitas teknis, hingga target yang mereka incar. Pemahaman mendalam tentang siapa musuh Anda adalah fondasi dari strategi pertahanan yang efektif.

Motivasi & Tujuan

Finansial, espionase, hacktivisme, atau sabotase — setiap motivasi menentukan pola serangan yang berbeda

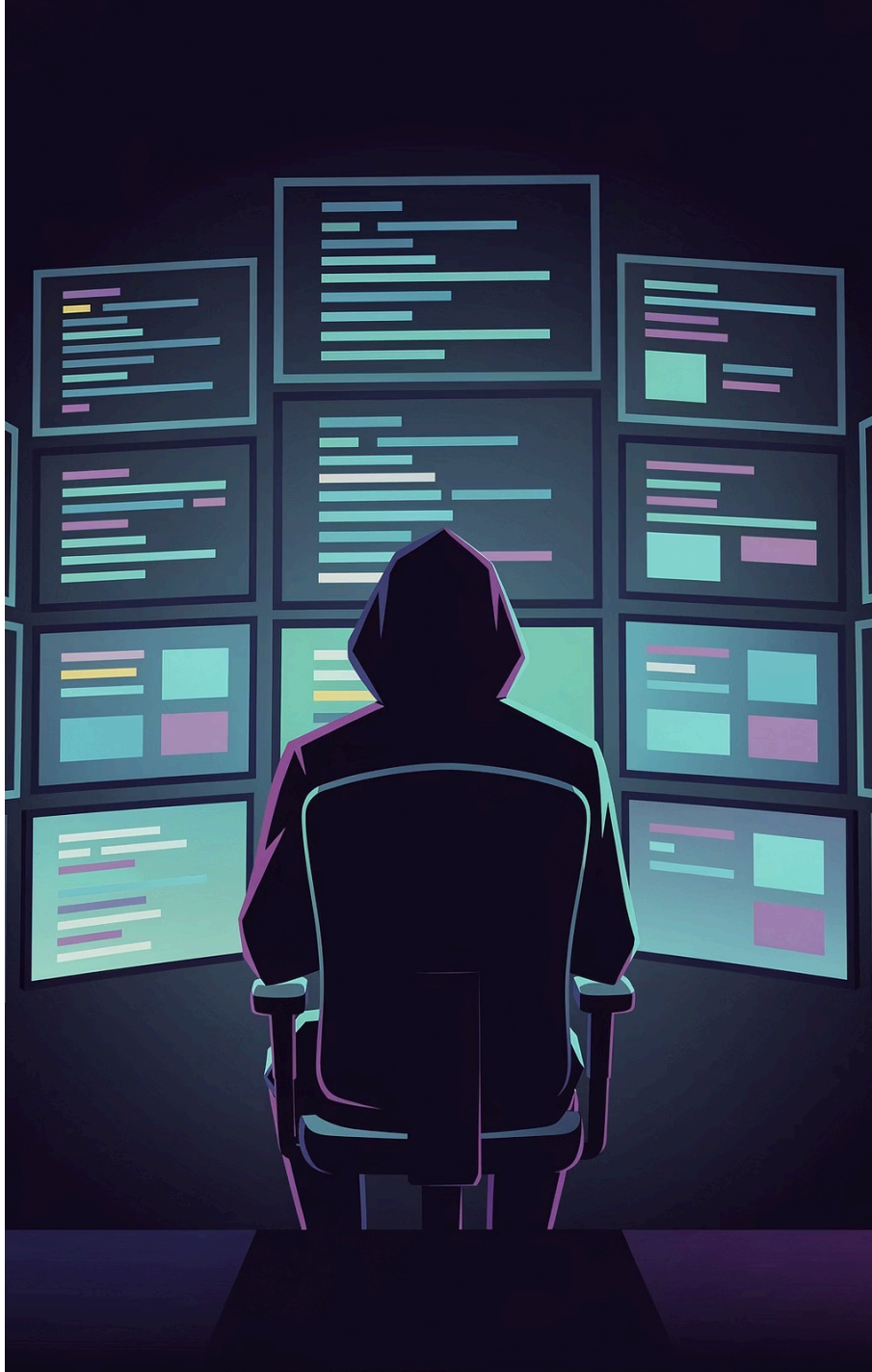
Kapabilitas Teknis

Tingkat kecanggihan alat, infrastruktur C2, dan TTP (Tactics, Techniques & Procedures) yang digunakan

Target & Industri

Sektor keuangan, kesehatan, pemerintahan, dan infrastruktur kritis menjadi target paling sering

Edy Susanto – Founder C-SIX Security



Data Leak Awareness & Credential Exposure Monitoring

🔓 Data Leak Awareness

Kebocoran data terjadi ketika informasi sensitif organisasi—seperti data pelanggan, dokumen internal, atau kode sumber—dipublikasikan atau diperjualbelikan di forum Dark Web. Kesadaran terhadap kebocoran ini memungkinkan respons sebelum kerugian meluas.

- Pemantauan forum dan marketplace Dark Web
- Deteksi dini data sensitif yang bocor
- Klasifikasi tingkat kekritisan kebocoran

🔑 Credential Exposure Monitoring

Kredensial yang bocor — username, password, token — adalah tiket masuk bagi penyerang. Pemantauan aktif terhadap exposure ini memungkinkan tim keamanan untuk menonaktifkan atau mereset akun sebelum dieksploitasi.

- Pemantauan kombinasi email & password yang bocor
- Integrasi dengan sistem IAM organisasi
- Notifikasi real-time untuk credential at risk

Edy Susanto – Founder C-SIX Security

Ransomware Group Monitoring

Kelompok ransomware modern beroperasi layaknya perusahaan dengan model Ransomware-as-a-Service (RaaS). Mereka memiliki situs "leak site" sendiri di Dark Web untuk mempublikasikan data korban dan menekan pembayaran tebusan. Pemantauan aktif terhadap kelompok ini memberikan peringatan dini kritis bagi organisasi.

Identifikasi Kelompok Aktif

Pantau aktivitas LockBit, BlackCat/ALPHV, Cl0p, Play, dan kelompok baru yang muncul

Analisis Target & Pola

Pelajari industri dan geografi yang menjadi target utama setiap kelompok ransomware

Early Warning System

Dapatkan notifikasi jika nama organisasi muncul di leak site sebelum publikasi penuh

Edy Susanto – Founder C-SIX Security

IOC Collection & Threat Trend Analysis

🧩 IOC Collection

Indicators of Compromise (IOC) adalah artefak forensik digital yang mengindikasikan potensi intrusi atau aktivitas jahat. Pengumpulan IOC yang sistematis memungkinkan deteksi dan respons yang lebih cepat.

- **IP Address & Domain** – infrastruktur penyerang
- **Hash File** – sidik jari malware
- **URL & Email Header** – vektor phishing
- **Registry Keys** – persistensi malware

📈 Threat Trend Analysis

Analisis tren ancaman membantu tim keamanan memahami lanskap ancaman yang terus berkembang dan mengalokasikan sumber daya secara strategis.

- Identifikasi teknik serangan yang sedang naik daun
- Pemetaan ancaman berdasarkan sektor industri
- Prediksi vektor serangan berikutnya
- Benchmark postur keamanan vs. industri

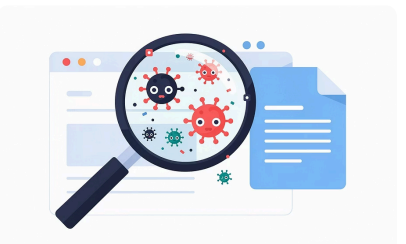
Edy Susanto – Founder C-SIX Security

Tools Esensial untuk Threat Intelligence

Tiga platform ini menjadi tulang punggung investigasi threat intelligence yang efektif — dari verifikasi kebocoran kredensial hingga analisis malware dan pengumpulan OSINT secara terstruktur.

Have I Been Pwned

Platform gratis untuk memeriksa apakah alamat email atau kredensial telah bocor dalam data breach yang terdokumentasi. Mendukung notifikasi otomatis dan API untuk integrasi enterprise.



VirusTotal

Agregator analisis ancaman yang memindai file, URL, IP, dan domain menggunakan lebih dari 70 antivirus engine dan threat intelligence feed. Standar industri untuk validasi IOC.

OSINT Framework

Direktori komprehensif alat dan sumber daya OSINT yang dikategorikan berdasarkan jenis informasi — mulai dari username, email, domain, hingga dark web monitoring.

Edy Susanto – Founder C-SIX Security

Sesi Praktik: Analisis Kasus Kebocoran Data Publik

Peserta akan menganalisis kasus kebocoran data nyata yang telah dipublikasikan secara publik, menggunakan metodologi threat intelligence untuk menarik kesimpulan yang dapat ditindaklanjuti.

📋 Skenario yang Digunakan

- Kebocoran database pelanggan e-commerce
- Credential dump dari forum Dark Web
- Leak dokumen internal organisasi publik

🎯 Target Kompetensi

- Menilai scope dan dampak kebocoran
- Mengidentifikasi data apa saja yang terekspos
- Menyusun rekomendasi mitigasi terstruktur

Edy Susanto – Founder C-SIX Security

Praktik: Identifikasi Indikator Ancaman

Latihan hands-on menggunakan VirusTotal dan OSINT Framework untuk mengumpulkan, memvalidasi, dan mengklasifikasikan IOC dari skenario serangan yang diberikan instruktur.

1

Ekstraksi IOC

Identifikasi IP mencurigakan, domain berbahaya, dan hash malware dari log dan laporan insiden

2

Validasi & Enrichment

Verifikasi IOC menggunakan VirusTotal, AbuseIPDB, dan threat feed publik untuk memperkaya konteks

3

Klasifikasi Risiko

Kategorikan IOC berdasarkan tingkat kepercayaan (confidence) dan dampak potensial terhadap organisasi

4

Distribusi Intel

Format hasil temuan dalam standar STIX/TAXII untuk dibagikan ke tim SOC dan platform SIEM

Edy Susanto – Founder C-SIX Security

Outcome Modul & Langkah Selanjutnya

Setelah menyelesaikan Modul 4, peserta memiliki kemampuan komprehensif untuk menjadikan Dark Web sebagai sumber intelijen strategis — bukan sekadar ancaman yang ditakuti, melainkan aset informasi yang dimanfaatkan.

Dark Web Intelligence

Mampu memantau dan menginterpretasikan informasi dari Dark Web secara legal dan etis

Koneksi Risiko

Mampu menghubungkan temuan intelijen dengan risiko spesifik yang dihadapi organisasi

Respons Proaktif

Mampu merekomendasikan langkah mitigasi berbasis bukti sebelum serangan terjadi

Modul Berikutnya: Incident Response & Digital Forensics — Dari deteksi ancaman hingga investigasi forensik dan pemulihan pasca-insiden secara terstruktur.

Edy Susanto – Founder C-SIX Security