# Modul 5 – OSINT untuk Security Assessment

Menggunakan teknik Open Source Intelligence (OSINT) untuk mengidentifikasi informasi yang terekspos secara publik dan memahami bagaimana data tersebut dapat meningkatkan risiko keamanan organisasi.

*Edy Susanto – Founder C-SIX Security*

Modul 5 – OSINT untuk Security Assessment

# Tujuan Pembelajaran

## Apa yang Akan Dipelajari

Peserta akan memahami bagaimana informasi publik yang tampak tidak berbahaya dapat dimanfaatkan oleh penyerang untuk meningkatkan efektivitas serangan terhadap organisasi.

## Kompetensi yang Dibangun

- Mengidentifikasi data yang terekspos secara publik
- Menganalisis eksposur email dan akun digital
- Memahami risiko metadata dokumen
- Menerapkan alur kerja OSINT secara defensif
- Mengevaluasi jejak digital organisasi

*Edy Susanto – Founder C-SIX Security*

Modul 5 – OSINT untuk Security Assessment

# Tools OSINT yang Digunakan

### Google Advanced Search

Memanfaatkan operator pencarian lanjutan untuk menemukan informasi spesifik yang terindeks secara publik di internet.

### Google Dorking

Teknik pencarian terstruktur untuk tujuan defensif — memverifikasi sejauh mana data sensitif organisasi terekspos di mesin pencari.

### Have I Been Pwned

Layanan pengecekan apakah alamat email atau akun pengguna telah termasuk dalam kebocoran data yang diketahui secara publik.

### URLScan.io

Platform analisis URL yang memindai dan merekam informasi teknis tentang situs web, termasuk aset, skrip, dan metadata jaringan.

*Edy Susanto – Founder C-SIX Security*

Modul 5 – OSINT untuk Security Assessment

# Public Data Exposure

Informasi publik yang terekspos mencakup berbagai jenis data yang secara tidak sengaja dapat diakses oleh siapa saja melalui internet. Bagi penyerang, data ini menjadi titik awal reconnaissance sebelum melancarkan serangan.

⚠ Data yang tampak tidak sensitif seperti nama karyawan, alamat email, atau struktur organisasi — jika dikombinasikan — dapat membentuk profil serangan yang sangat berbahaya.

## Contoh Data yang Terekspos

- Nama dan jabatan karyawan di LinkedIn
- Subdomain dan infrastruktur teknis
- Dokumen internal yang terindeks mesin pencari
- Konfigurasi server yang tidak terproteksi
- Alamat email format standar organisasi
- Informasi registrasi domain (WHOIS)

*Edy Susanto – Founder C-SIX Security*

Modul 5 – OSINT untuk Security Assessment

# Email Exposure Analysis

## Identifikasi Format Email

Pola alamat email organisasi (misal: nama.belakang@perusahaan.com) sering dapat diprediksi dari sampel yang tersedia publik, memungkinkan penyerang membuat daftar target untuk phishing.

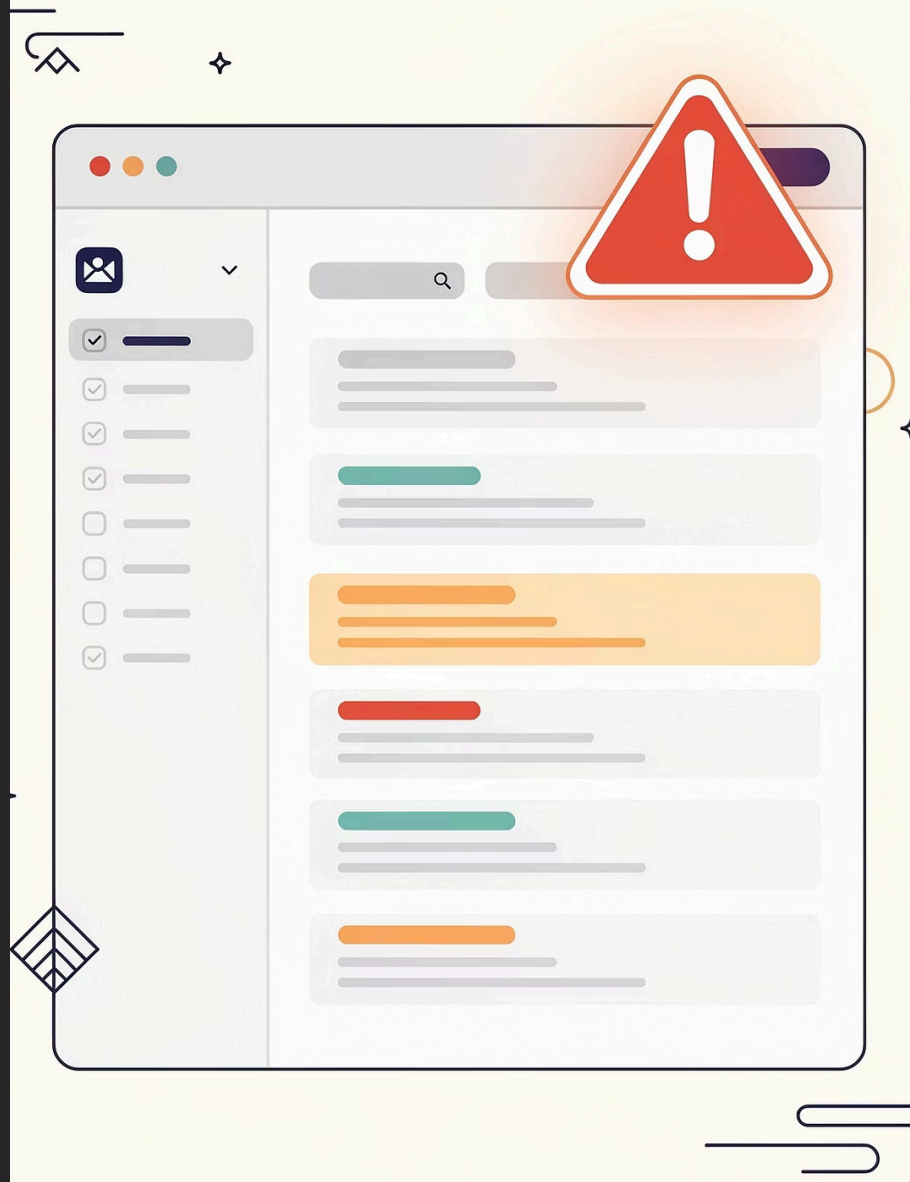
## Verifikasi dengan Have I Been Pwned

Periksa apakah email karyawan kunci telah tercatat dalam kebocoran data. Akun yang bocor berisiko digunakan untuk credential stuffing atau spear phishing yang lebih terarah.

## Dampak Eksposur Email

Email yang terekspos meningkatkan risiko serangan social engineering, Business Email Compromise (BEC), dan akses tidak sah ke sistem internal organisasi.

*Edy Susanto – Founder C-SIX Security*



Modul 5 – OSINT untuk Security Assessment

# Data Breach Awareness

## Mengapa Kesadaran Kebocoran Data Penting?

Kebocoran data dari layanan pihak ketiga sering kali menyertakan kata sandi, token, atau informasi sensitif lain yang masih digunakan kembali oleh karyawan di sistem perusahaan.

### Credential Reuse

Password lama yang bocor sering masih dipakai

### Dark Web Exposure

Data bocor kerap dijual di forum underground

### Third-Party Risk

Kebocoran dari vendor turut berdampak pada organisasi

*Edy Susanto – Founder C-SIX Security*

Modul 5 – OSINT untuk Security Assessment

# Document Metadata Awareness

Dokumen yang dipublikasikan secara online — seperti laporan tahunan, proposal, atau presentasi — sering menyimpan metadata tersembunyi yang mengungkapkan informasi sensitif tentang organisasi.

## Identitas Pembuat

Nama pengguna, nama asli penulis dokumen, dan nama komputer yang digunakan saat membuat file dapat terungkap dari metadata.

## Struktur Internal

Path penyimpanan file mengungkap struktur direktori jaringan internal, nama server, atau drive bersama yang digunakan organisasi.

## Versi Perangkat Lunak

Informasi tentang aplikasi yang digunakan (mis. versi Office) membantu penyerang mencari kerentanan yang belum ditambal (unpatched vulnerabilities).

## Timestamp & Revisi

Tanggal pembuatan, modifikasi, dan riwayat revisi dokumen dapat mengungkap pola kerja dan siklus proses bisnis internal.

*Edy Susanto – Founder C-SIX Security*

Modul 5 – OSINT untuk Security Assessment

# Open Source Intelligence Workflow


Alur kerja OSINT yang terstruktur memastikan proses pengumpulan informasi dilakukan secara sistematis, legal, dan berorientasi pada hasil yang dapat ditindaklanjuti oleh tim keamanan.

*Edy Susanto – Founder C-SIX Security*

Modul 5 – OSINT untuk Security Assessment

# Praktik: Meninjau Jejak Digital Organisasi

## Skenario Praktik

Peserta melakukan simulasi OSINT terhadap organisasi contoh untuk memetakan jejak digital yang terekspos secara publik tanpa melakukan akses tidak sah.

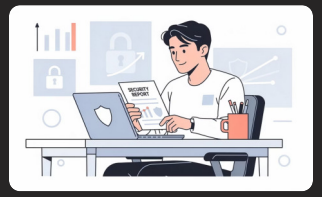
## Langkah-Langkah Praktik

1. Gunakan Google Dorking untuk menemukan dokumen dan subdomain yang terindeks
2. Periksa kebocoran email dengan Have I Been Pwned
3. Analisis situs web target menggunakan URLScan.io
4. Ekstrak dan periksa metadata dari dokumen publik yang ditemukan
5. Kompilasi temuan dalam laporan eksposur singkat

*Edy Susanto – Founder C-SIX Security*

Modul 5 – OSINT untuk Security Assessment

# Outcome & Takeaway Utama



## Kesadaran Risiko Publik

Peserta memahami bahwa informasi yang tersedia secara publik — jika tidak dikelola — dapat secara signifikan meningkatkan permukaan serangan (attack surface) organisasi.

## Pendekatan Defensif

OSINT bukan hanya alat penyerang. Tim keamanan dapat dan harus menggunakannya secara proaktif untuk mengidentifikasi dan memitigasi eksposur sebelum dimanfaatkan pihak jahat.

## Tindak Lanjut Nyata

Setiap temuan OSINT harus diikuti dengan rekomendasi konkret: penghapusan data, penguatan kebijakan, atau peningkatan kontrol akses berdasarkan tingkat risiko yang teridentifikasi.

Setelah menyelesaikan modul ini, peserta siap mengintegrasikan teknik OSINT ke dalam proses security assessment dan audit keamanan organisasi mereka.

*Edy Susanto – Founder C-SIX Security*