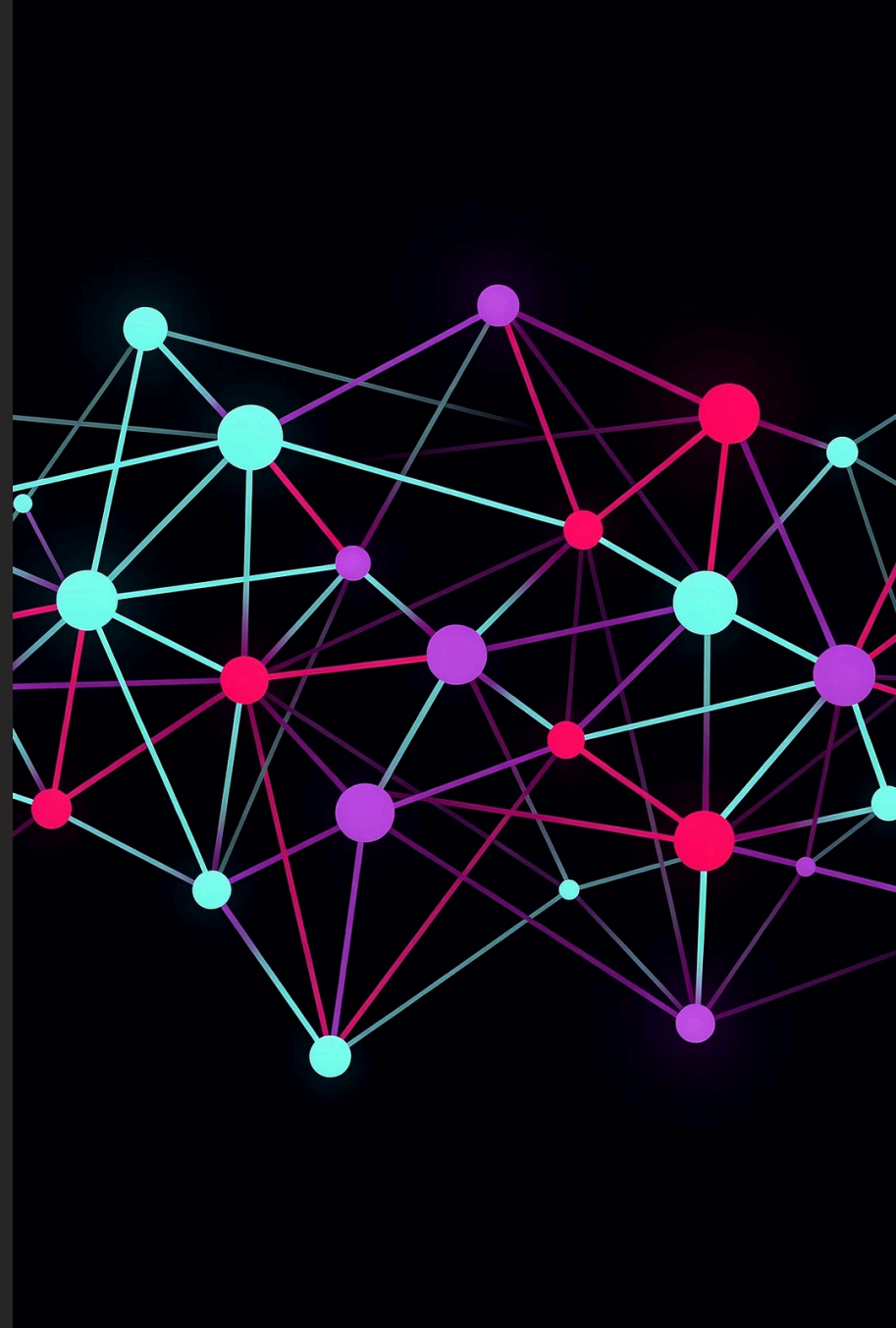
Modul 5 – OSINT & Dark Web Investigation

Teknik investigasi digital: dari permukaan hingga lapisan terdalam internet

EDY SUSANTO - FOUNDER C-SIX SECURITY



Ubah Data Gelap Jadi Intelijen yang Bisa Dipakai

Telusuri yang Tidak Terlihat

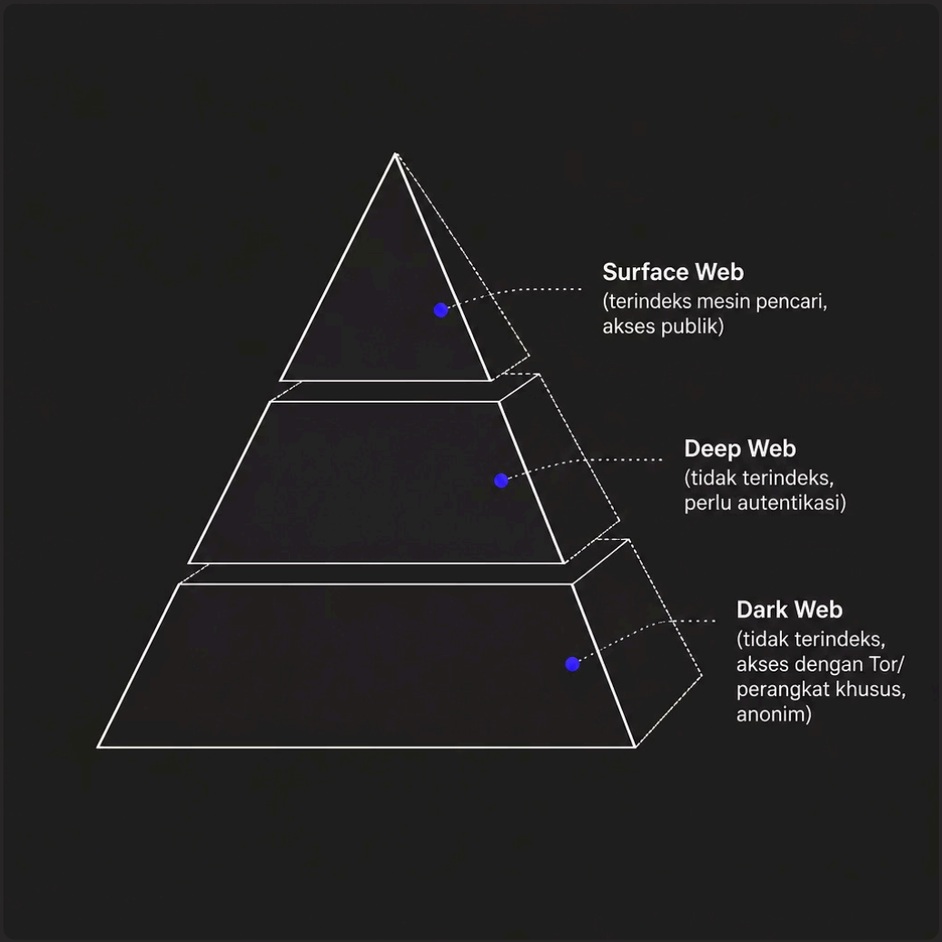
Peserta mampu menggabungkan teknik OSINT untuk menelusuri informasi yang tidak terindeks mesin pencari biasa — termasuk forum anonim dan marketplace tersembunyi.

Validasi Sebelum Kesimpulan

Peserta memahami proses validasi, korelasi, dan verifikasi data — memastikan setiap kesimpulan didasarkan pada bukti yang dapat dipertanggungjawabkan.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Peta Dunia Informasi: Surface, Deep, Dark



Fokus Dark Web OSINT

Dark Web adalah lapisan yang tidak terindeks mesin pencari umum dan hanya dapat diakses menggunakan perangkat khusus seperti Tor Browser.

Investigasi Kebocoran Data

Menelusuri data sensitif yang dijual di forum/marketplace anonim

Identifikasi Pelaku Ancaman

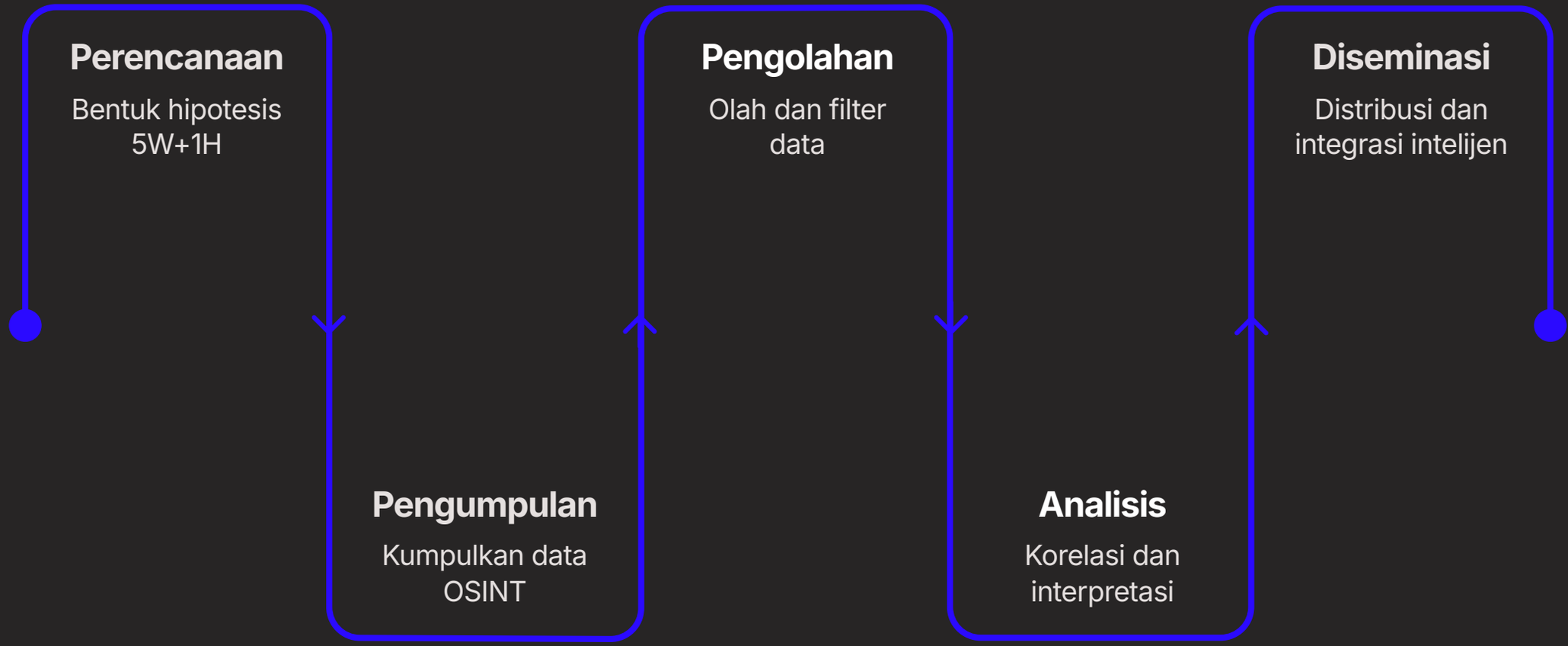
Mengungkap identitas di balik aktivitas ilegal lintas platform

Pemantauan Aktivitas Ilegal

Monitoring forum dan kanal tersembunyi secara terstruktur

EDY SUSANTO - FOUNDER C-SIX SECURITY

Intelligence Cycle: Mesin Utama Investigasi



Setiap tahap dirancang untuk mengurangi bias — dari hipotesis awal menuju bukti yang terverifikasi dan dapat dipertanggungjawabkan secara hukum maupun profesional.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Correlation Analysis: Cari "Jejak yang Berulang"

Entity Tracking

Hubungkan indikator seperti user ID, alamat email, dan dompet crypto yang muncul berulang lintas platform untuk melacak satu entitas.

Network Mapping

Petakan jaringan antar pelaku untuk mengungkap pola hubungan — siapa yang terhubung dengan siapa, kapan, dan lewat kanal mana.

Social Media Correlation

Ikat aktivitas dark web ke identitas yang tampak di permukaan — menggabungkan data publik dan tersembunyi menjadi satu profil.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Timeline Analysis: Bukti yang "Berjalan" Itu Lebih Jujur

Mengapa Timeline Penting?

Urutan waktu adalah lapisan validasi tersendiri — klaim yang tidak konsisten dengan timestamp akan terungkap saat disusun secara kronologis.

- **Susun kronologi** dari postingan, log transaksi, dan referensi antar entitas
- **Deteksi inkonsistensi** dengan mencocokkan waktu klaim vs waktu kemunculan artefak
- **Visualkan modus operandi** pelaku: kapan mulai, kapan eskalasi, kapan berpindah kanal

EDY SUSANTO - FOUNDER C-SIX SECURITY

Source Validation: Nilai Sumber Sebelum Nilai Informasi

Periksa Konteks Sumber

Siapa yang mem-posting? Apa motifnya? Bagaimana konsistensinya dari waktu ke waktu? Sumber anonim tidak otomatis tidak valid — tapi harus diuji lebih ketat.

Uji Kredibilitas Lintas Sumber

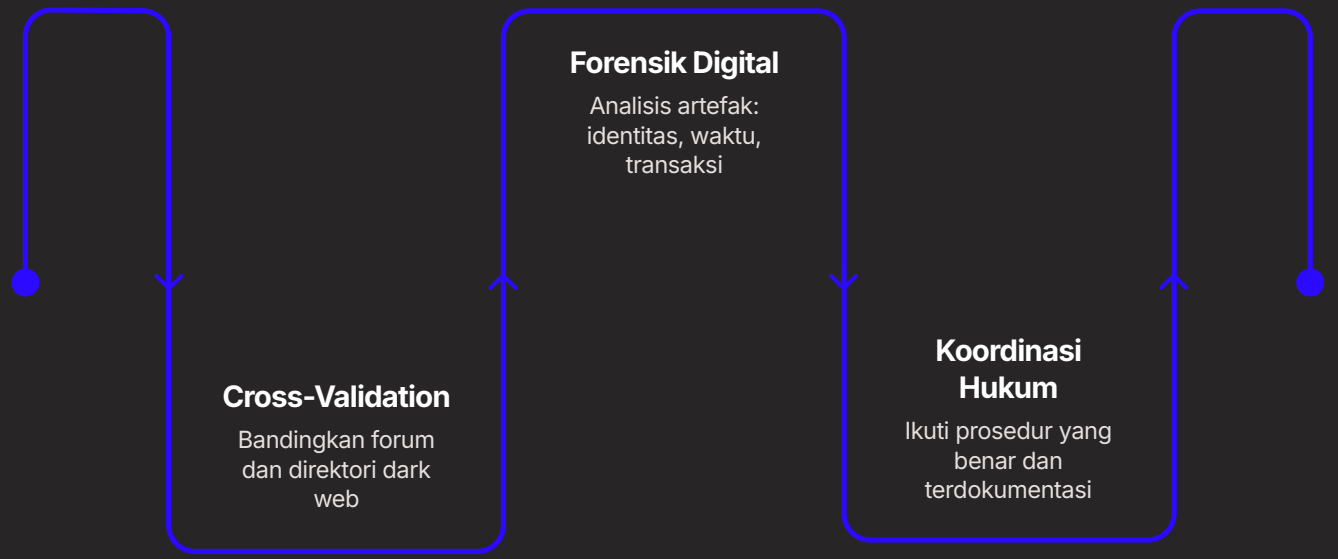
Jangan hanya mengandalkan satu thread atau satu marketplace. Bandingkan klaim dari minimal tiga sumber berbeda sebelum menarik kesimpulan.

Tangkap Sinyal Disinformasi

Waspadai pola akun palsu, narasi yang dikoordinasikan, dan operasi manipulasi yang sengaja menyebarkan informasi menyesatkan.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Verification Techniques: Dari Klaim ke Konfirmasi



> Verifikasi bukan langkah opsional — ini adalah fondasi yang membuat intelijen bisa digunakan di luar ruang investigasi.

Gunakan pendekatan **artefak-sentris**: setiap klaim harus dikunci oleh referensi yang mengunci identitas, waktu, dan transaksi secara bersamaan.

Koordinasi hukum diperlukan bila intelijen akan digunakan untuk pelaporan formal atau tindakan hukum.

Alat Praktis — Tapi Tetap "Proses" yang Menentukan

Dark Web Search

Ahmia, Kilos, Candle — mesin pencari dan direktori untuk menjelajahi konten .onion secara terstruktur

Tor Browser

Akses aman ke konten .onion dengan anonimitas jaringan — pintu masuk utama ke dark web

Analisis Visual

Maltego, IBM i2, dan DarkOwl untuk memetakan hubungan antar entitas dan menganalisis data secara visual

EDY SUSANTO - FOUNDER C-SIX SECURITY

Studi Kasus Mini + Output Intelijen

⚠ **Skenario:** Database klien perusahaan ditemukan dijual di dark web marketplace. Tim OSINT ditugaskan untuk menelusuri asal kebocoran sebelum dilaporkan ke manajemen dan pihak berwajib.

Dark Web OSINT digunakan untuk menelusuri wallet Bitcoin penjual, mengkorelasikan akun lintas forum, dan mengidentifikasi sumber kebocoran internal.

Output Intelijen Akhir

01

Timeline Kejadian

Kronologi lengkap dari tanggal posting pertama hingga transaksi terakhir

02

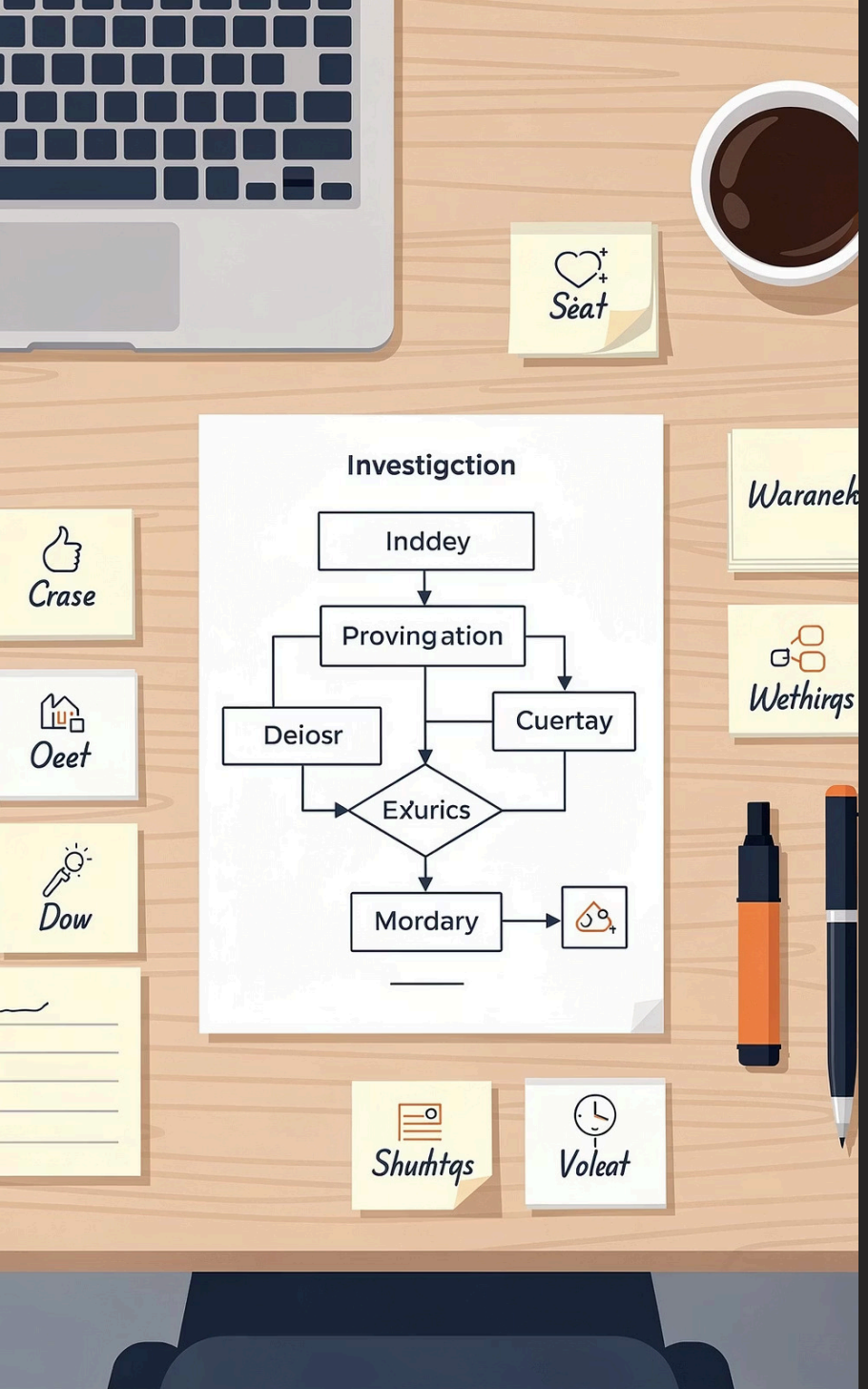
Peta Korelasi Entitas

Jaringan hubungan antar akun, wallet, dan platform yang terlibat

03

Daftar Sumber Tervalidasi

Semua sumber yang telah diuji kredibilitasnya dan siap untuk pelaporan



Investigasi Bukan Soal Berani — Tapi Terstruktur

> "Confidence lewat validasi, bukan dugaan tanpa bukti."

Dapat Ditelusuri

Setiap temuan memiliki jejak sumber yang jelas dan dapat diverifikasi ulang kapan saja

Dapat Direkonsiliasi

Data dari berbagai sumber saling mendukung dan tidak saling bertentangan tanpa penjelasan

Dapat Dipertanggungjawabkan

Intelijen yang dihasilkan siap digunakan untuk keputusan profesional dan pelaporan formal

EDY SUSANTO - FOUNDER C-SIX SECURITY