



Modul 6: Building a Sustainable Bug Bounty Career

Strategi jangka panjang untuk menjadi Bug Hunter profesional – dari metodologi hunting hingga membangun reputasi di dunia nyata.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Gambaran Umum

Apa yang Akan Kamu Pelajari di Modul Ini?

Modul 6 dirancang untuk membekali kamu dengan fondasi karir bug bounty yang kuat dan berkelanjutan. Bukan hanya teknik, tapi juga mindset, sistem kerja, dan strategi profesional.

01

Strategi Program

Memilih program yang tepat sesuai skill dan goals kamu

03

Otomatisasi & Recon

Memanfaatkan tools untuk mempercepat proses reconnaissance

02

Metodologi Personal

Membangun workflow dan checklist hunting yang efisien

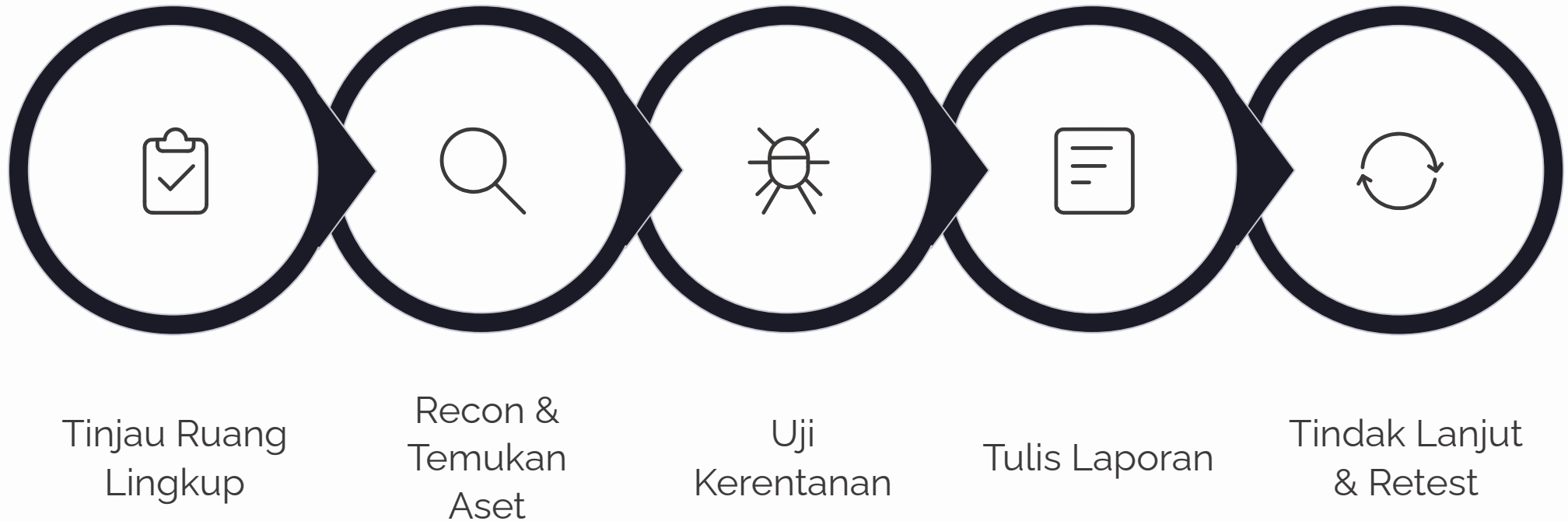
04

Karir & Reputasi

Membangun portfolio, Hall of Fame, dan menghindari burnout

Hunting Workflow yang Efektif

Bug Hunter sukses bekerja dengan sistem, bukan dengan coba-coba. Workflow yang terstruktur membantu kamu konsisten dan produktif setiap sesi hunting.




Dengan mengikuti alur ini secara konsisten, kamu mengurangi waktu yang terbuang dan meningkatkan kualitas setiap laporan yang dikirimkan kepada program.

Produktivitas

Time Management untuk Bug Hunter

Salah satu tantangan terbesar bug bounty adalah mengelola waktu secara mandiri. Tanpa struktur, mudah terjebak dalam rabbit hole yang tidak produktif.

 Gunakan teknik **time-boxing**: tetapkan durasi maksimal per target atau per teknik sebelum memutuskan untuk lanjut atau berhenti.



Jadwal Tetap

Alokasikan sesi hunting di waktu yang sama setiap hari untuk membangun kebiasaan



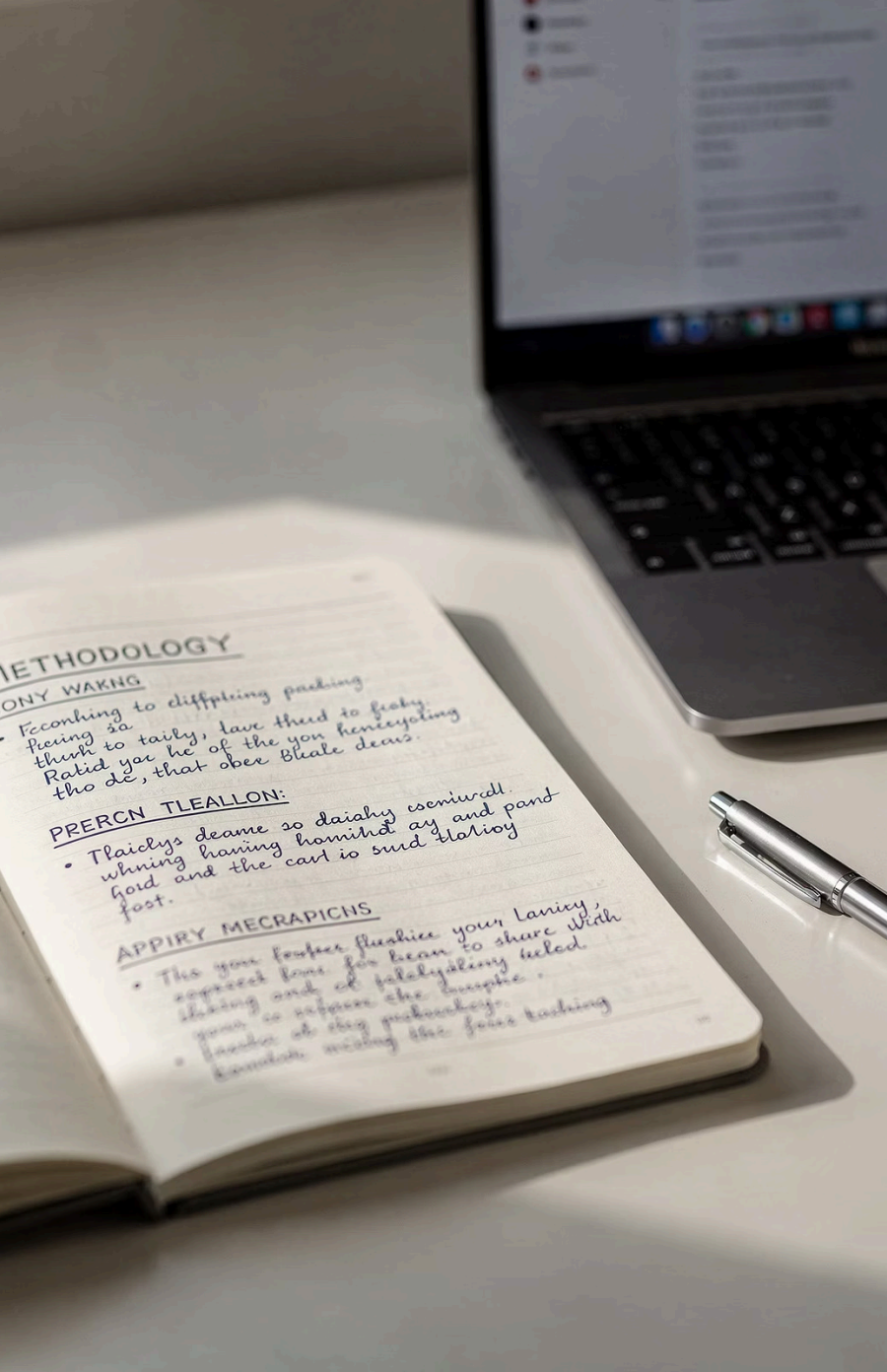
Fokus Satu Target

Hindari berpindah program terlalu cepat; kedalaman lebih baik dari lebar



Log Aktivitas

Catat setiap sesi: apa yang dites, hasil, dan next steps



Membangun Metodologi Personal

Metodologi personal adalah keunggulan kompetitif kamu. Bug hunter terbaik di dunia tidak hanya mengikuti checklist umum – mereka memiliki pendekatan unik yang terasah dari pengalaman.

Dokumentasikan Semua

Catat setiap teknik yang berhasil dan gagal. Pola akan muncul seiring waktu.

Spesialisasi Awal

Pilih 2-3 kelas vulnerability untuk dikuasai secara mendalam sebelum memperluas.

Review & Iterasi

Evaluasi metodologimu setiap bulan. Sesuaikan berdasarkan hasil nyata di lapangan.

Pelajari Write-ups

Analisis laporan publik dari hunter lain untuk memperkaya sudut pandang.

Automation untuk Recon

Recon manual memakan waktu. Otomatisasi memungkinkan kamu menemukan lebih banyak attack surface dalam waktu yang lebih singkat, sehingga energi kamu fokus pada analisis dan eksploitasi.



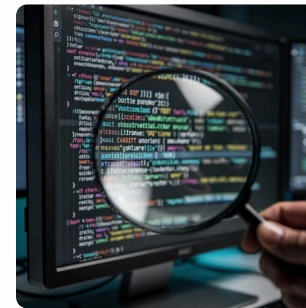
Subdomain Enumeration

Tools: **Amass, Subfinder, Assetfinder**. Temukan semua subdomain aktif secara otomatis dan monitor perubahan baru.



Port & Service Scanning

Tools: **Naabu, Masscan, Nmap**. Identifikasi port terbuka dan layanan yang berjalan pada skala besar.



Content Discovery

Tools: **ffuf, Feroxbuster, Gospider**. Temukan endpoint tersembunyi, direktori, dan parameter yang tidak terdokumentasi.

Karir & Reputasi

Portfolio dan Reputation Building

Di dunia bug bounty, reputasi adalah modal utama. Portfolio yang kuat membuka pintu program private, undangan eksklusif, dan peluang karir yang lebih besar.

Apa yang Harus Ada di Portfolio?

- Write-up vulnerability yang telah dipublikasikan
- Screenshot bukti temuan (dengan izin program)
- Daftar CVE atau Hall of Fame yang diraih
- Blog teknikal atau thread Twitter/X
- Profil aktif di HackerOne / Bugcrowd

Platform untuk Membangun Visibilitas

- **Medium / Blog Pribadi** – publikasikan write-up teknikal
- **GitHub** – bagikan tools dan script recon buatanmu
- **LinkedIn** – bangun jaringan profesional keamanan siber

Hall of Fame Strategy

Hall of Fame (HoF) bukan sekadar penghargaan – ini adalah bukti kredibilitas yang dapat dilihat oleh seluruh komunitas dan perusahaan yang merekrut. Strategi yang tepat memaksimalkan peluangmu masuk HoF.



Targetkan Program VDP

Vulnerability Disclosure Programs sering mencantumkan nama hunter di HoF meski tidak membayar bounty uang tunai.



Kualitas Laporan Tinggi

Laporan yang jelas, lengkap, dan disertai proof-of-concept meningkatkan kemungkinan diterima dan diakui.



Bangun Relasi dengan Triage

Komunikasi profesional dan responsif membuat program lebih cenderung mencantumkan namamu di HoF.



Menghindari Burnout dalam Bug Bounty

Burnout adalah ancaman nyata bagi bug hunter, terutama ketika laporan berulang kali ditolak atau tidak mendapat respons. Menjaga kesehatan mental dan energi adalah bagian dari karir yang berkelanjutan.

Tetapkan Ekspektasi Realistis

Tidak setiap sesi hunting akan menghasilkan temuan. Proses belajar itu sendiri adalah progress yang bernilai.

Rayakan Kemenangan Kecil

Setiap temuan valid, sekecil apapun, adalah bukti kompetensi. Catat dan apresiasi setiap pencapaian.

Ambil Jeda Terencana

Jadwalkan hari istirahat secara reguler. Otak yang segar jauh lebih produktif daripada yang kelelahan.

Bergabung dengan Komunitas

Komunitas bug hunter lokal dan global adalah sumber dukungan, motivasi, dan kolaborasi yang sangat berharga.

Analisis Laporan Bug Bounty Nyata

Mempelajari laporan bug bounty yang telah dipublikasikan adalah cara tercepat memahami pola berpikir hunter sukses. Berikut elemen kunci yang selalu ada dalam laporan berkualitas tinggi.

Anatomi Laporan Ideal

- **Judul yang jelas** – spesifik tentang jenis vulnerability dan lokasi
- **CVSS Score** – estimasi severity yang terukur dan beralasan
- **Steps to Reproduce** – langkah demi langkah yang dapat direplikasi
- **Proof of Concept** – screenshot, video, atau payload yang membuktikan dampak
- **Impact Statement** – penjelasan konkret risiko bisnis bagi perusahaan
- **Remediation Suggestion** – rekomendasi perbaikan yang actionable

Sumber Write-up Publik Terbaik

HackerOne Hacktivity

Ribuan laporan publik dari ratusan program, bisa difilter berdasarkan severity dan tipe bug.

Pentester Land

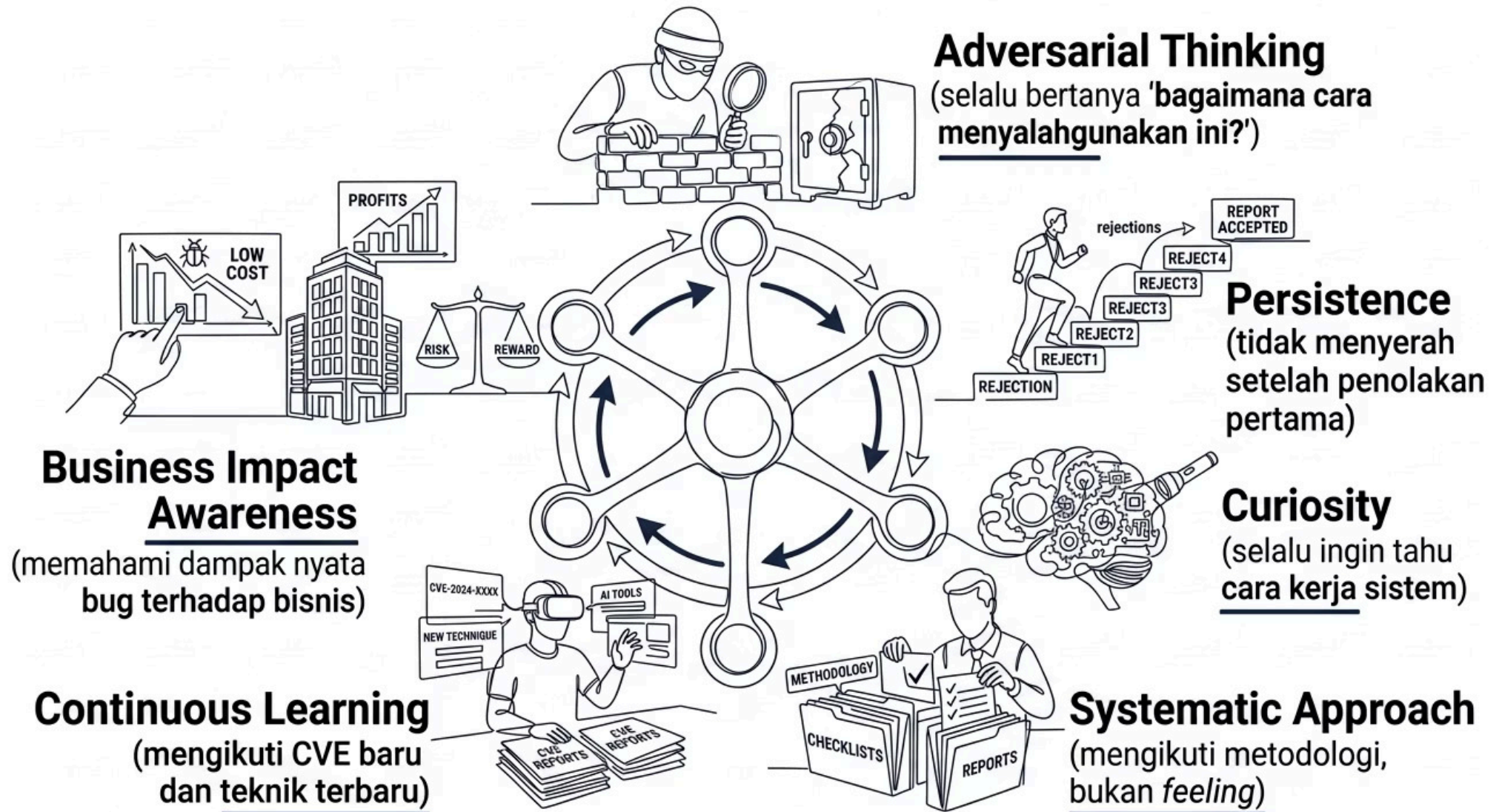
Kumpulan write-up bug bounty terkurasi dengan kategori yang mudah dinavigasi.

GitHub Awesome Bug Bounty

Repository komunitas berisi link write-up, tools, dan resources terbaik.

Cara Berpikir Bug Hunter Sukses

Perbedaan antara hunter biasa dan hunter sukses bukan hanya pada teknik – melainkan pada pola pikir. Berikut mental model yang membedakan mereka.



Mindset ini bukan bakat bawaan – melainkan kebiasaan yang dapat dilatih dan diperkuat setiap hari melalui praktik yang konsisten.

Final Project

Proyek Akhir: Dari Latihan ke Dunia Nyata

Final project Modul 6 adalah simulasi penugasan bug bounty sesungguhnya. Kamu akan menghasilkan empat deliverable profesional yang siap masuk portfolio.

1

Recon Report

Laporan reconnaissance lengkap mencakup asset discovery, subdomain enumeration, dan pemetaan attack surface target.

2

Vulnerability Analysis

Analisis mendalam terhadap vulnerability yang ditemukan, termasuk root cause, severity, dan potensi dampaknya.

3

Professional Bug Report

Laporan bug berformat standar industri yang siap dikirimkan ke program bug bounty sungguhan.

4

Hunting Checklist Pribadi

Checklist metodologi personal yang dikustomisasi sesuai skill dan preferensi hunting kamu sendiri.

Kriteria Penilaian Final Project

Setiap deliverable dinilai berdasarkan standar yang digunakan oleh program bug bounty profesional, bukan sekadar kelengkapan akademis.

| Deliverable | Kriteria Utama | Bobot Nilai |
|-------------------------|--|-------------|
| Recon Report | Kelengkapan asset, akurasi data, metodologi recon | 25% |
| Vulnerability Analysis | Kedalaman analisis, ketepatan severity, root cause | 30% |
| Professional Bug Report | Kejelasan reproduksi, impact statement, PoC | 30% |
| Hunting Checklist | Relevansi, kelengkapan, dapat digunakan kembali | 15% |

✔ Peserta yang menyelesaikan semua deliverable dengan nilai minimal 75 akan mendapatkan **sertifikat kompetensi** dari C-SIX Security.



Outcome: Siap Berburu di Dunia Nyata

Setelah menyelesaikan Modul 6, kamu tidak hanya memiliki pengetahuan – kamu memiliki **sistem yang bekerja**.

✓ Metodologi Siap Pakai

Workflow dan checklist personal yang dapat langsung diterapkan pada program bug bounty nyata

✓ Portfolio Awal

Deliverable final project yang siap dipajang sebagai bukti kompetensi kepada rekruter dan program

✓ Karir Berkelanjutan

Strategi jangka panjang untuk terus berkembang, menghindari burnout, dan membangun reputasi di industri

Edy Susanto - Founder C-SIX Security