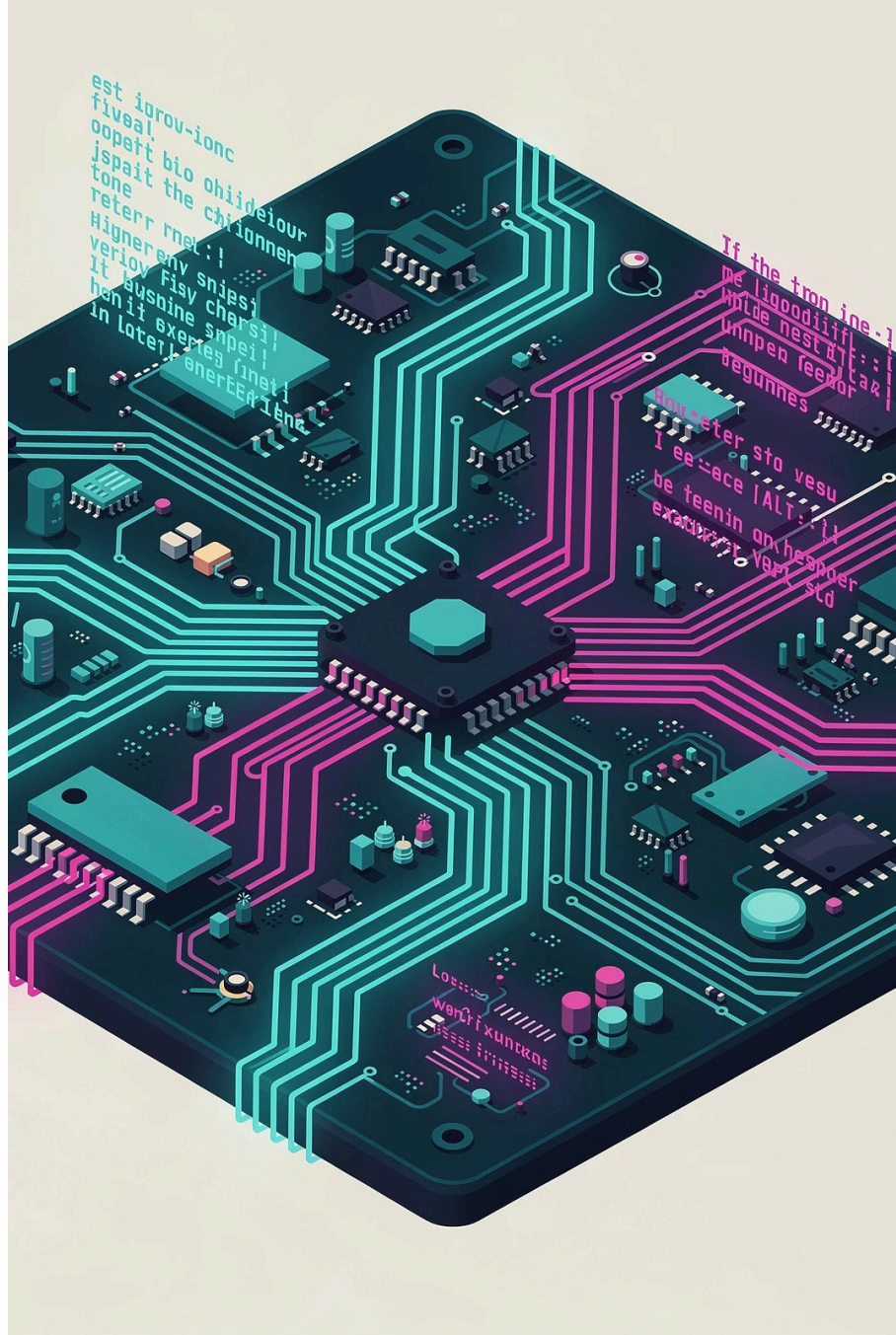
Modul 5 – Claude AI untuk Coding & Cyber Security

Memanfaatkan kecerdasan buatan Claude sebagai asisten teknis produktif untuk pengembangan kode, debugging, dokumentasi, dan analisis ancaman siber.

EDY SUSANTO - FOUNDER C-SIX SECURITY



Peta Materi

Apa yang Akan Kita Pelajari?

Modul ini dirancang untuk membekali Anda dengan kemampuan praktis menggunakan Claude AI dalam konteks teknis dan keamanan siber — dari membaca kode hingga threat intelligence.

01

Claude untuk Kode

Membaca, menganalisis, dan mendokumentasikan kode program secara efisien.

02

Debugging & Dokumentasi

Menemukan bug, memperbaiki error, dan membuat dokumentasi teknis yang berkualitas.

03

Analisis Script & Keamanan

Menganalisis skrip berbahaya dan menyusun checklist keamanan siber.

04

Threat Intelligence & OSINT

Memanfaatkan AI untuk mendukung riset ancaman dan pengumpulan intelijen sumber terbuka.

Claude untuk Membaca Kode Program

Claude mampu membaca dan memahami kode dalam berbagai bahasa pemrograman — Python, JavaScript, Bash, PHP, dan lainnya. Cukup tempelkan kode ke dalam percakapan dan minta Claude menjelaskan fungsi, logika, atau potensi masalah yang ada.

Yang Bisa Claude Lakukan

- Menjelaskan fungsi setiap blok kode
- Mengidentifikasi alur logika program
- Mendeteksi potensi kerentanan atau kelemahan
- Merangkum tujuan keseluruhan skrip

Contoh Prompt Efektif

- *"Jelaskan apa yang dilakukan kode ini baris per baris."*
- *"Apakah ada potensi security issue pada kode ini?"*
- *"Apa output dari fungsi ini jika input-nya adalah X?"*

EDY SUSANTO - FOUNDER C-SIX SECURITY

Debugging Dasar dengan Claude

Debugging adalah salah satu tugas paling memakan waktu bagi pengembang. Claude dapat mempercepat proses ini secara signifikan dengan menganalisis pesan error, menelusuri logika kode, dan menyarankan perbaikan yang tepat.

1

1. Identifikasi Error

Tempelkan kode dan pesan error ke Claude. Ia akan mengidentifikasi baris bermasalah dan jenis kesalahannya.

2

2. Analisis Akar Masalah

Claude menelusuri logika untuk menemukan penyebab utama — bukan sekadar gejala permukaan dari bug.

3

3. Saran Perbaikan

Claude memberikan kode yang sudah diperbaiki lengkap dengan penjelasan mengapa solusi tersebut bekerja.

ⓘ 💡 **Tips:** Sertakan selalu pesan error lengkap, versi bahasa/framework, dan konteks apa yang diharapkan kode lakukan agar Claude memberikan jawaban yang lebih akurat.

Dokumentasi Teknis Otomatis

Dokumentasi yang baik adalah fondasi proyek perangkat lunak yang sehat, namun sering kali diabaikan karena memakan waktu. Claude dapat membuat dokumentasi teknis berkualitas tinggi secara otomatis dari kode yang ada.

README File

Deskripsi proyek, cara instalasi, konfigurasi, dan panduan penggunaan yang lengkap dan terstruktur.

Komentar Kode

Docstring, inline comment, dan anotasi fungsi secara otomatis dalam format standar industri.

API Documentation

Daftar endpoint, parameter, contoh request/response, dan penjelasan kode status HTTP.

Runbook & SOP

Prosedur operasional standar untuk deployment, troubleshooting, dan pemeliharaan sistem.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Analisis Script Berbahaya

Dalam konteks keamanan siber, analis sering berhadapan dengan skrip mencurigakan — malware, dropper, reverse shell, atau payload yang diobfuskasi. Claude dapat membantu membedah skrip tersebut dengan aman tanpa perlu menjalankannya.

Jenis Script yang Dapat Dianalisis

- PowerShell dan Bash script berbahaya
- Python payload dan dropper
- Obfuscated JavaScript (malvertising)
- Macro VBA dalam dokumen Office
- PHP webshell dan backdoor

Output Analisis Claude

- Tujuan dan fungsi utama skrip
- Teknik obfuskasi yang digunakan
- Indikator of Compromise (IoC)
- Pemetaan ke framework MITRE ATT&CK
- Rekomendasi mitigasi dan deteksi

⚠ ⚠️ **Catatan Etika:** Gunakan kemampuan ini hanya untuk tujuan defensif yang sah. Jangan meminta Claude membuat malware baru atau skrip serangan aktif.

Membuat Checklist Keamanan

Checklist keamanan yang komprehensif adalah alat vital bagi tim security. Claude dapat membuat checklist yang disesuaikan dengan konteks spesifik — apakah itu audit server, review kode, atau hardening jaringan.

1. **Hardening Server**
   Checklist konfigurasi OS, manajemen patch, disable layanan tidak perlu, dan pengaturan firewall.

2. **Secure Code Review**
   Poin pemeriksaan untuk input validation, autentikasi, enkripsi data, dan manajemen sesi.

3. **Incident Response**
   Langkah-langkah terstruktur dari deteksi, containment, eradikasi, recovery, hingga lessons learned.

4. **Compliance Audit**
   Checklist berbasis standar ISO 27001, NIST, PCI-DSS, atau peraturan lokal yang relevan.

EDY SUSANTO - FOUNDER C-SIX SECURITY

AI untuk Threat Intelligence & OSINT

Threat Intelligence dan OSINT (Open Source Intelligence) adalah pilar penting dalam operasi keamanan siber proaktif. Claude dapat menjadi akselerator yang kuat dalam proses pengumpulan, analisis, dan pelaporan intelijen ancaman.

Riset Ancaman Aktif

Merangkum profil kelompok APT, TTP (Tactics, Techniques, Procedures), dan kampanye serangan terkini berdasarkan laporan publik.

Analisis IoC

Membantu menginterpretasikan hash file, IP address mencurigakan, domain berbahaya, dan signature malware dari feed intelijen.

Pembuatan Laporan Intel

Mengubah data mentah dan temuan teknis menjadi laporan intelijen ancaman yang terstruktur dan dapat dipahami manajemen.

Pemetaan MITRE ATT&CK

Memetakan perilaku ancaman ke taktik dan teknik dalam framework MITRE ATT&CK untuk konteks yang lebih kaya.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Praktik Langsung

Sesi Praktik: Analisis Script & Dokumentasi

Pada sesi praktik ini, peserta akan menggunakan Claude secara langsung untuk dua tugas utama yang mencerminkan skenario dunia nyata. Ikuti langkah-langkah berikut untuk memaksimalkan hasil belajar Anda.

🔍 Praktik 1: Analisis Script

1. Pilih salah satu skrip sampel yang disediakan (Python/Bash/PowerShell)
2. Paste ke Claude dengan prompt: *"Analisis skrip ini dari perspektif keamanan siber."*
3. Minta Claude mengidentifikasi fungsi, risiko, dan IoC
4. Dokumentasikan temuan dalam format laporan singkat

📝 Praktik 2: Dokumentasi Teknis

1. Pilih kode program buatan sendiri atau sampel yang diberikan
2. Minta Claude membuat README lengkap dengan deskripsi, instalasi, dan penggunaan
3. Minta tambahan komentar inline untuk setiap fungsi
4. Review dan bandingkan hasil Claude dengan dokumentasi manual

✅ **Target Output:** Setiap peserta menghasilkan satu laporan analisis script dan satu set dokumentasi teknis yang siap digunakan dalam 30 menit.

Outcome & Kesimpulan Modul 5

Setelah menyelesaikan Modul 5, peserta diharapkan memiliki pemahaman praktis dan kepercayaan diri untuk mengintegrasikan Claude sebagai asisten teknis sehari-hari dalam pekerjaan mereka.

Membaca & Debug Kode

Mampu menggunakan Claude untuk memahami dan memperbaiki kode program secara efisien.

Dokumentasi Profesional

Menghasilkan dokumentasi teknis berkualitas tinggi dengan bantuan AI dalam waktu singkat.

Analisis Keamanan

Menganalisis skrip mencurigakan dan membangun checklist keamanan yang komprehensif.

Threat Intelligence

Memanfaatkan Claude untuk mendukung riset ancaman, OSINT, dan pembuatan laporan intelijen.

> Claude bukan pengganti keahlian Anda — ia adalah **multiplier** yang memperkuat dan mempercepat setiap tugas teknis yang Anda kerjakan.

EDY SUSANTO - FOUNDER C-SIX SECURITY