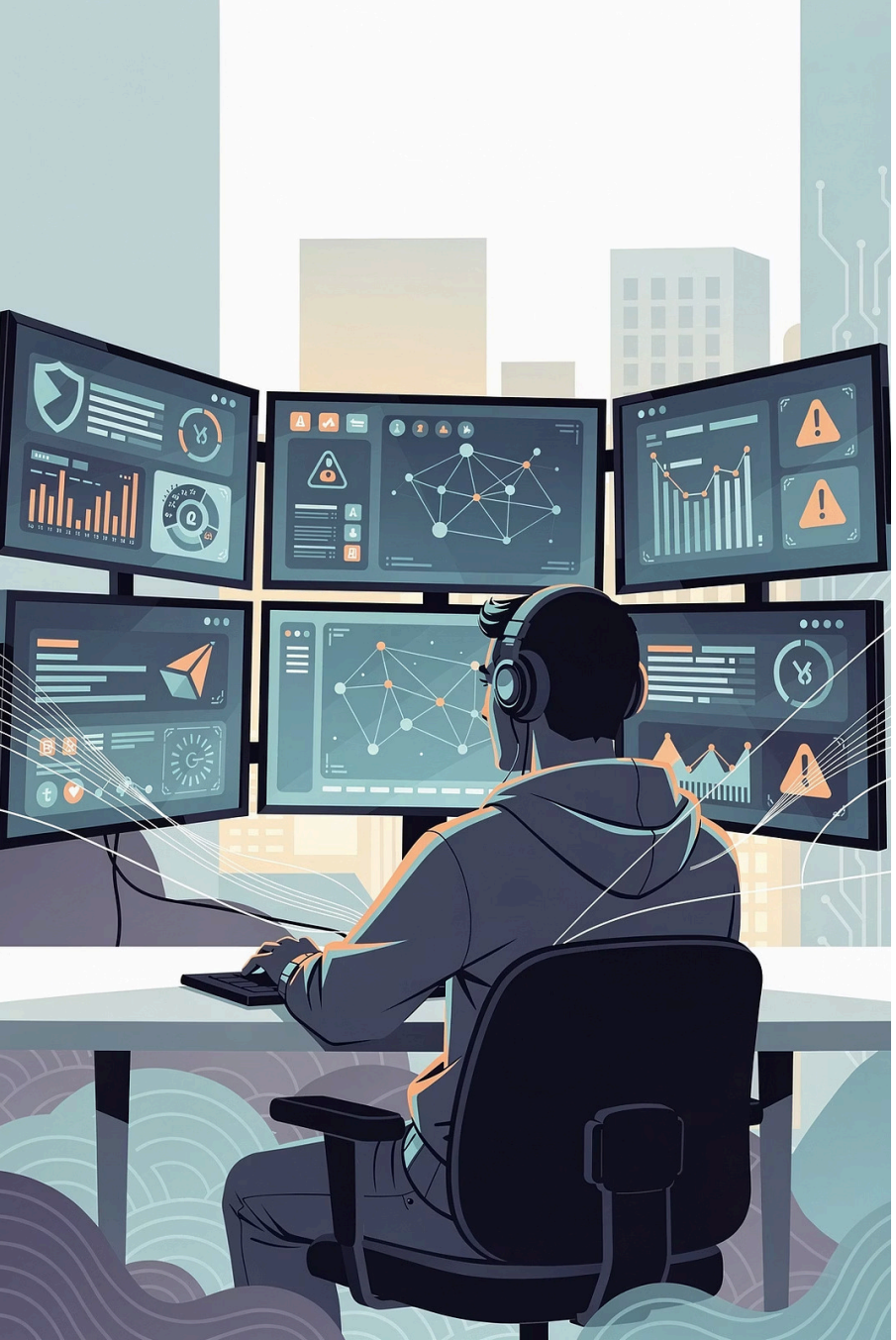


20 Role Prompt untuk Cyber Security dan IT

Modul 4 — Panduan Praktis AI Prompting

Pelajari cara memanfaatkan kecerdasan buatan dengan menggunakan **role prompt** yang tepat untuk berbagai peran dalam ekosistem keamanan siber. Dari Ethical Hacker hingga Auditor, setiap role menghasilkan respons AI yang lebih akurat, kontekstual, dan dapat langsung diterapkan.

Edy Susanto - Founder C-SIX Security

Apa Itu Role Prompt?

Definisi

Role prompt adalah teknik memberikan instruksi kepada AI dengan menetapkan **peran spesifik** sebelum mengajukan pertanyaan. Hasilnya: respons yang lebih terarah, teknis, dan profesional.

Mengapa Penting?

- AI memahami konteks dan terminologi domain
- Respons lebih akurat dan actionable
- Menghemat waktu iterasi prompt
- Output siap pakai untuk kebutuhan profesional

Contoh dasar: *"Bertindaklah sebagai seorang Ethical Hacker berpengalaman. Jelaskan..."*

Edy Susanto - Founder C-SIX Security

ROLE 1–4

Peran Ofensif & Intelijen

1

Ethical Hacker

Simulasikan serangan siber untuk menemukan celah keamanan sebelum penyerang nyata menemukannya.

Contoh Prompt: *"Bertindaklah sebagai Ethical Hacker bersertifikat CEH. Buat rencana penetration testing untuk aplikasi web e-commerce berbasis OWASP Top 10."*

2

Threat Intelligence Analyst

Kumpulkan dan analisis data ancaman dari berbagai sumber untuk mengantisipasi serangan.

Contoh Prompt: *"Sebagai Threat Intelligence Analyst, identifikasi TTP (Tactics, Techniques, Procedures) dari kelompok APT yang menargetkan sektor perbankan Indonesia."*

3

OSINT Investigator

Manfaatkan sumber terbuka untuk mengumpulkan informasi intelijen tentang target atau ancaman.

Contoh Prompt: *"Sebagai OSINT Investigator, jelaskan metodologi pengumpulan informasi dari media sosial, domain records, dan dark web untuk profiling ancaman."*

4

SOC Analyst

Pantau, deteksi, dan respons terhadap insiden keamanan secara real-time dari Security Operations Center.

Contoh Prompt: *"Sebagai SOC Analyst Tier 2, bantu saya menganalisis log SIEM ini dan tentukan apakah ini merupakan true positive atau false positive: [paste log]."*

ROLE 5–8

Peran Konsultasi & Respons

Security Consultant

Berikan rekomendasi strategis kepada organisasi untuk meningkatkan postur keamanan secara menyeluruh.

Contoh Prompt: *"Sebagai Security Consultant berpengalaman 10 tahun, buatkan roadmap keamanan siber 12 bulan untuk perusahaan fintech dengan 500 karyawan."*

Security Awareness Trainer

Rancang program edukasi untuk meningkatkan kesadaran keamanan di seluruh lapisan organisasi.

Contoh Prompt: *"Sebagai Security Awareness Trainer, buat modul pelatihan phishing awareness 1 jam untuk karyawan non-teknis di perusahaan manufaktur."*

Incident Responder

Tangani dan pulihkan sistem dari serangan siber dengan cepat dan terstruktur mengikuti framework NIST.

Contoh Prompt: *"Sebagai Incident Responder, buat playbook penanganan insiden ransomware mulai dari deteksi, containment, eradication, hingga recovery."*

Risk Assessor

Identifikasi, evaluasi, dan prioritaskan risiko keamanan berdasarkan dampak dan kemungkinan terjadinya.

Contoh Prompt: *"Sebagai Risk Assessor bersertifikat CISM, lakukan penilaian risiko menggunakan matriks 5x5 untuk sistem ERP perusahaan logistik."*

Edy Susanto - Founder C-SIX Security

ROLE 9–10

Peran Teknis & Kepatuhan

🔧 Network Security Engineer

Rancang, implementasikan, dan kelola infrastruktur keamanan jaringan termasuk firewall, IDS/IPS, dan segmentasi jaringan.

> **Contoh Prompt:** *"Sebagai Network Security Engineer berpengalaman dengan Cisco dan Palo Alto, rancang arsitektur jaringan zero-trust untuk kantor pusat dengan 3 cabang regional di Indonesia."*

- Firewall policy review
- VPN architecture design
- Network segmentation planning
- IDS/IPS rule configuration

📋 Cyber Security Auditor

Lakukan pemeriksaan mendalam terhadap sistem, proses, dan kebijakan keamanan untuk memastikan kepatuhan terhadap standar dan regulasi yang berlaku.

> **Contoh Prompt:** *"Sebagai Cyber Security Auditor bersertifikat ISO 27001 Lead Auditor, buat checklist audit keamanan informasi untuk perusahaan yang ingin mendapatkan sertifikasi ISO 27001:2022."*

- ISO 27001 compliance audit
- POJK/OJK compliance review
- Audit report preparation
- Gap analysis documentation

Ringkasan 10 Role Prompt Cyber Security

No	Role	Fokus Utama
1	Ethical Hacker	Penetration testing, vulnerability assessment
2	SOC Analyst	Monitoring, deteksi, respons insiden real-time
3	Threat Intelligence Analyst	Analisis ancaman, TTP, threat landscape
4	OSINT Investigator	Pengumpulan intelijen dari sumber terbuka
5	Security Consultant	Strategi keamanan, roadmap, rekomendasi
6	Security Awareness Trainer	Edukasi, pelatihan, konten kesadaran keamanan
7	Incident Responder	Penanganan insiden, forensik, pemulihan
8	Risk Assessor	Penilaian risiko, matriks risiko, mitigasi
9	Network Security Engineer	Infrastruktur jaringan, firewall, zero-trust
10	Cyber Security Auditor	Audit kepatuhan, ISO 27001, gap analysis

Edy Susanto - Founder C-SIX Security

PRAKTIK

Membuat Checklist Keamanan dengan AI

Cara Menggunakan Role Prompt

Gunakan kombinasi role + konteks spesifik untuk menghasilkan checklist yang komprehensif dan relevan dengan industri Anda.

Tentukan Scope

Sebutkan sistem, platform, atau aset yang ingin diaudit

Pilih Role yang Tepat

Auditor untuk compliance, Engineer untuk teknis

Tentukan Standar

ISO 27001, NIST CSF, CIS Controls, atau POJK

Contoh Prompt Checklist:
"Bertindaklah sebagai Cyber Security Auditor bersertifikat ISO 27001. Buat checklist keamanan komprehensif untuk audit infrastruktur cloud AWS yang digunakan perusahaan e-commerce, mencakup: akses kontrol, enkripsi data, logging, dan backup. Format dalam tabel dengan kolom: Item, Standar Referensi, Status, Catatan."

Checklist yang dihasilkan AI dapat langsung diadaptasi, disesuaikan dengan regulasi lokal, dan digunakan sebagai dasar audit formal.

PRAKTIK

Analisis Risiko & Threat Assessment

🎯 Analisis Risiko

Role: Risk Assessor

Contoh Prompt:
"Sebagai Risk Assessor bersertifikat CISM, lakukan analisis risiko kuantitatif untuk sistem pembayaran digital menggunakan metodologi FAIR (Factor Analysis of Information Risk). Identifikasi 5 risiko teratas beserta nilai ALE-nya."

🔍 Threat Assessment

Role: Threat Intelligence Analyst

Contoh Prompt:
"Sebagai Threat Intelligence Analyst, lakukan threat assessment untuk sektor perbankan Indonesia. Gunakan framework MITRE ATT&CK untuk memetakan ancaman aktif, identifikasi threat actor yang relevan, dan berikan rekomendasi mitigasi prioritas tinggi."

📊 Output yang Diharapkan

Dari kedua prompt di atas, AI dapat menghasilkan:

- Matriks risiko 5x5 (Likelihood vs Impact)
- Register risiko terstruktur
- Peta ancaman berdasarkan MITRE ATT&CK
- Rekomendasi kontrol prioritas

PRAKTIK

Membuat Security Awareness Content

Strategi Konten Kesadaran Keamanan

Gunakan role **Security Awareness Trainer** untuk menghasilkan konten edukasi yang menarik, mudah dipahami, dan efektif mengubah perilaku karyawan.

- Email phishing simulation scenario
- Video script awareness bulanan
- Quiz keamanan interaktif
- Poster dan infografis digital
- Newsletter keamanan internal

Contoh Prompt Lengkap:

"Bertindaklah sebagai Security Awareness Trainer berpengalaman. Buat kampanye awareness keamanan siber bertema 'Waspada Phishing' untuk karyawan non-teknis. Sertakan: (1) Email pengantar kampanye, (2) 5 tips mengenali phishing dalam bahasa Indonesia yang mudah dipahami, (3) Skenario simulasi phishing yang realistis, dan (4) Quiz 10 pertanyaan untuk mengukur pemahaman."

Edy Susanto - Founder C-SIX Security

Tips Memaksimalkan Role Prompt

Tambahkan Kredensial

Sebutkan sertifikasi seperti CEH, CISSP, CISM, atau ISO 27001 Lead Auditor agar AI memberikan respons setara ahli bersertifikat.

Spesifikasikan Industri & Konteks

Sebutkan sektor (perbankan, kesehatan, pemerintah) dan ukuran organisasi untuk mendapatkan rekomendasi yang lebih relevan dan applicable.

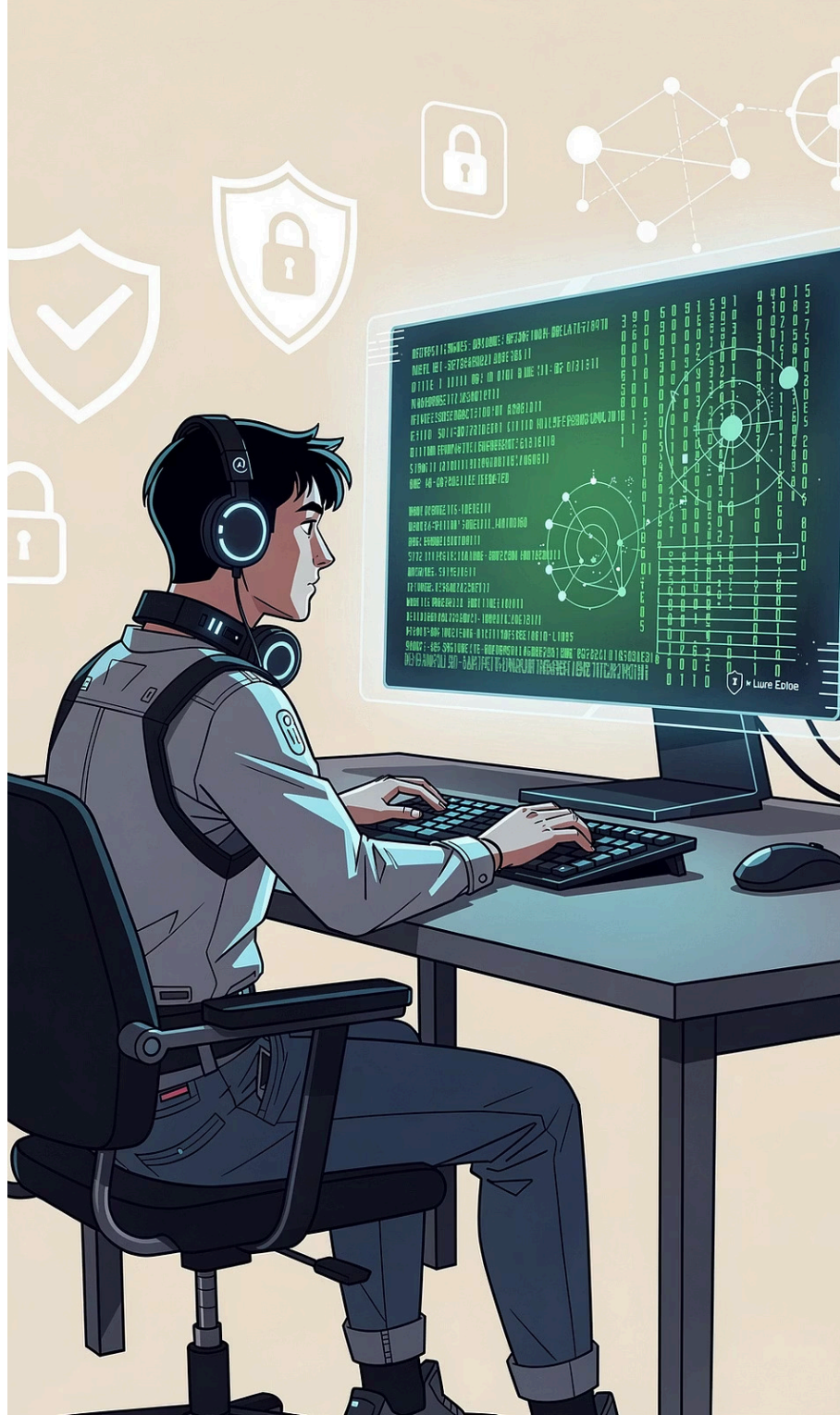
Tentukan Format Output

Minta output dalam format spesifik: tabel, checklist, playbook, laporan, atau template dokumen agar langsung dapat digunakan.

Referensikan Standar & Regulasi

Cantumkan standar yang relevan: NIST CSF, ISO 27001, MITRE ATT&CK, POJK, atau CIS Controls untuk output yang compliance-ready.

Edy Susanto - Founder C-SIX Security



PENUTUP

Key Takeaways Modul 4

Role = Konteks

Menetapkan role yang tepat adalah kunci menghasilkan respons AI yang akurat dan profesional di bidang keamanan siber.

10 Role Utama

Dari Ethical Hacker hingga Auditor — setiap role memiliki kegunaan spesifik yang saling melengkapi dalam ekosistem keamanan.

Langsung Praktik

Checklist, analisis risiko, threat assessment, dan awareness content dapat dihasilkan dengan prompt yang terstruktur dan tepat.

Hemat Waktu 10x

Dengan role prompt yang benar, pekerjaan yang biasa membutuhkan jam kerja dapat diselesaikan dalam hitungan menit.

Modul berikutnya: Praktik lanjutan menggunakan AI untuk Security Documentation dan Report Writing profesional.

Edy Susanto - Founder C-SIX Security