Modul 6 – Reporting & Security Recommendations

Mengubah hasil assessment teknis menjadi laporan keamanan profesional yang dapat dipahami oleh manajemen maupun tim teknis — dari temuan risiko hingga rekomendasi perbaikan yang actionable.

Edy Susanto - Founder C-SIX Security

Gambaran Modul

Tujuan Pembelajaran

Pada akhir modul ini, peserta akan mampu menyusun laporan keamanan yang komprehensif, terstruktur, dan komunikatif — menjembatani bahasa teknis dengan kebutuhan strategis organisasi.

01

Memahami Struktur Laporan

Menyusun Executive Summary, temuan teknis, dan klasifikasi risiko secara sistematis.

02

Mengklasifikasikan Risiko

Menggunakan standar industri untuk menilai dan memprioritaskan temuan keamanan.

03

Memberikan Rekomendasi

Menyusun langkah remediasi yang konkret, terukur, dan sesuai prioritas bisnis.

04

Mengkomunikasikan Hasil

Menyampaikan laporan kepada audiens yang berbeda — teknis maupun non-teknis.

Edy Susanto - Founder C-SIX Security

Materi Utama

Struktur Laporan Keamanan Profesional

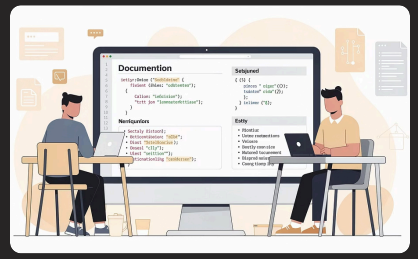
Sebuah laporan keamanan yang efektif memiliki arsitektur yang jelas dan konsisten. Setiap bagian melayani audiens yang berbeda namun saling mendukung satu sama lain.

Executive Summary

Ringkasan eksekutif yang menyampaikan temuan utama, dampak bisnis, dan rekomendasi prioritas dalam bahasa non-teknis untuk pengambil keputusan.

Risk Classification

Kategorisasi temuan berdasarkan tingkat keparahan — Critical, High, Medium, Low — menggunakan metodologi CVSS atau standar internal organisasi.



Technical Findings

Detail teknis setiap temuan: deskripsi kerentanan, bukti (evidence), sistem yang terdampak, dan potensi eksploitasi.

Edy Susanto - Founder C-SIX Security

Executive Summary: Seni Komunikasi Risiko

Executive Summary adalah bagian terpenting dari laporan — sering kali menjadi satu-satunya bagian yang dibaca oleh manajemen senior. Harus padat, jelas, dan strategis.

Konteks & Ruang Lingkup

Jelaskan apa yang diuji, kapan, dan metode apa yang digunakan. Berikan batasan dan asumsi yang relevan agar manajemen memahami cakupan pekerjaan.

Temuan Utama

Sampaikan jumlah temuan per kategori risiko. Sorot 2–3 temuan paling kritis yang memerlukan perhatian segera beserta potensi dampak bisnisnya.

Postur Keamanan Keseluruhan

Berikan penilaian menyeluruh terhadap tingkat kematangan keamanan organisasi — apakah *baik*, *perlu perbaikan*, atau *kritis* — disertai justifikasi singkat.

Rekomendasi Prioritas

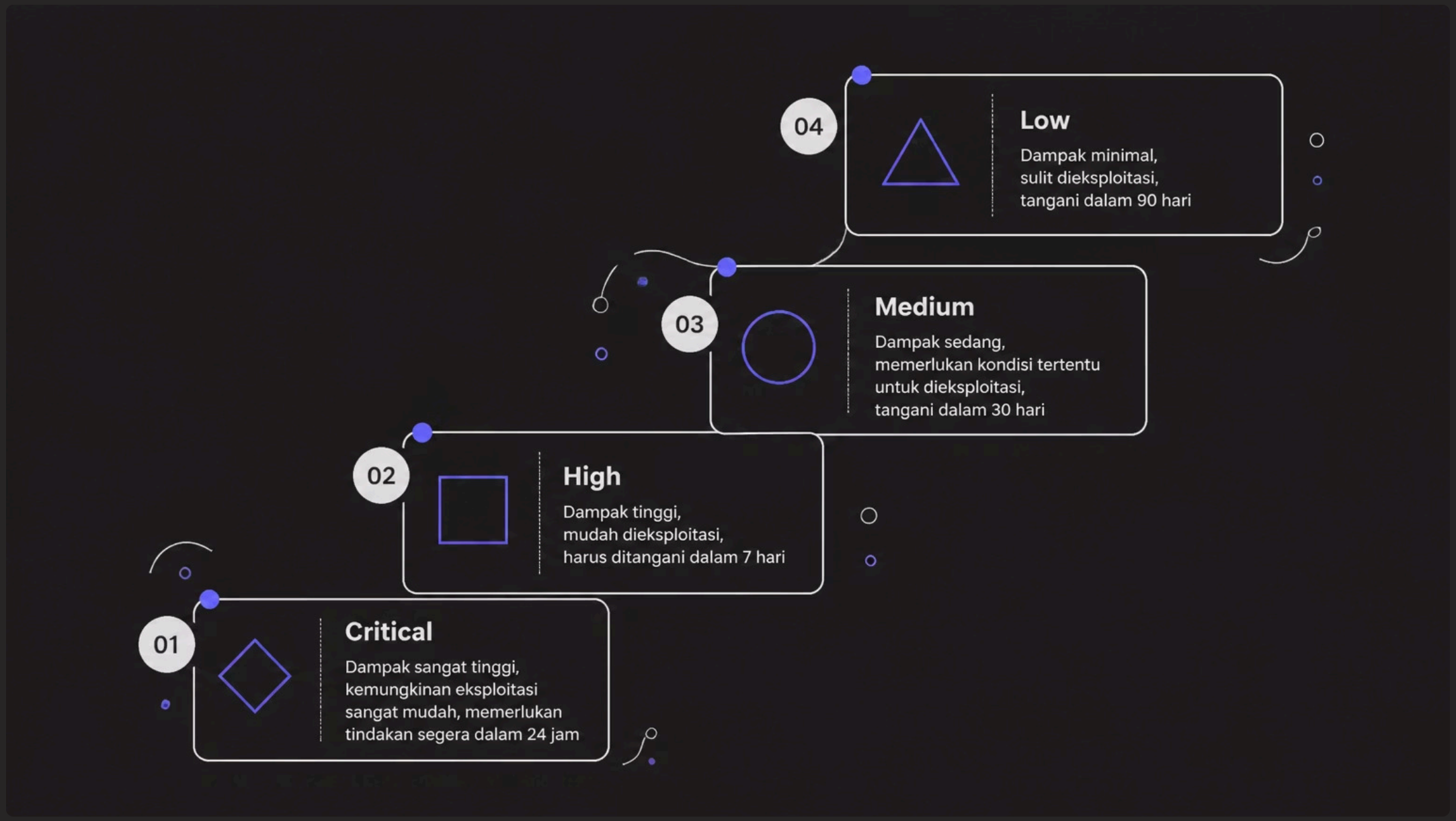
Daftar tindakan remediation paling penting dalam urutan prioritas. Gunakan bahasa bisnis, bukan jargon teknis, agar mudah ditindaklanjuti oleh manajemen.

Edy Susanto - Founder C-SIX Security

Materi Inti

Risk Classification: Memahami Tingkat Keparahan

Klasifikasi risiko yang tepat memungkinkan organisasi memprioritaskan sumber daya remediasi secara efektif. Gunakan standar yang konsisten dan dapat dipertahankan secara metodologis.



Setiap temuan harus dinilai berdasarkan dua dimensi: **kemungkinan eksploitasi** (likelihood) dan **dampak bisnis** (impact). Kombinasi keduanya menentukan level risiko akhir yang dicantumkan dalam laporan.

Edy Susanto - Founder C-SIX Security

Materi Inti

Technical Findings: Mendokumentasikan Bukti dengan Tepat

Komponen Wajib Setiap Temuan

- **ID & Judul** — Identifikasi unik temuan
- **Deskripsi** — Penjelasan kerentanan secara teknis
- **Risk Rating** — Critical / High / Medium / Low
- **Affected Systems** — IP, hostname, atau URL yang terdampak
- **Evidence** — Screenshot, output tool, atau log
- **Impact** — Konsekuensi jika dieksploitasi
- **Recommendation** — Langkah remediasi spesifik
- **References** — CVE, CWE, atau standar relevan

Prinsip Penulisan Temuan yang Baik

Setiap temuan harus dapat **direproduksi** dan **diverifikasi** oleh pihak ketiga. Hindari bahasa yang ambigu — gunakan fakta dan bukti konkret.

⚠ Jangan hanya mencantumkan nama kerentanan. Jelaskan MENGAPA temuan tersebut berbahaya dalam konteks spesifik organisasi yang diaudit.

✓ Sertakan langkah-langkah reproduksi (steps to reproduce) sehingga tim teknis dapat memvalidasi dan memperbaiki temuan dengan tepat.

Edy Susanto - Founder C-SIX Security

Materi Inti

Remediation Recommendations: Dari Temuan ke Tindakan

Rekomendasi yang baik bukan sekadar "perbarui software" — melainkan panduan yang spesifik, terukur, dan realistis berdasarkan konteks teknis dan kapasitas organisasi.

1

Identifikasi Akar Masalah

Pahami penyebab mendasar temuan — bukan hanya gejalanya. Remediasi yang tepat menyasar root cause, bukan sekadar symptom.

2

Prioritaskan Berdasarkan Risiko

Urutkan rekomendasi dari risiko tertinggi ke terendah. Pertimbangkan juga quick wins yang dapat segera meningkatkan postur keamanan.

3

Sertakan Detail Teknis

Berikan instruksi spesifik: versi patch yang diperlukan, konfigurasi yang direkomendasikan, atau referensi ke panduan hardening resmi.

4

Tetapkan Timeline Realistis

Sesuaikan tenggat waktu remediasi dengan tingkat risiko dan kapasitas tim. Critical: 24–48 jam, High: 7 hari, Medium: 30 hari.

Edy Susanto - Founder C-SIX Security

Reporting Best Practices

Laporan terbaik adalah yang **dibaca dan ditindaklanjuti**. Berikut prinsip-prinsip yang membedakan laporan profesional dari laporan biasa.

Kenali Audiens

Pisahkan bagian untuk manajemen (ringkas, berbasis risiko bisnis) dan tim teknis (detail, berbasis implementasi).

Konsistensi Format

Gunakan template standar dan terminologi yang konsisten di seluruh laporan. Ini meningkatkan kredibilitas dan memudahkan perbandingan antar assessment.

Validasi Sebelum Kirim

Periksa ulang setiap temuan — pastikan bukti akurat, severity benar, dan rekomendasi dapat diimplementasikan sebelum laporan diserahkan.

Keamanan Laporan

Laporan security assessment adalah dokumen sensitif. Kirimkan melalui kanal terenkripsi, batasi distribusi, dan tetapkan masa retensi yang jelas.

Edy Susanto - Founder C-SIX Security

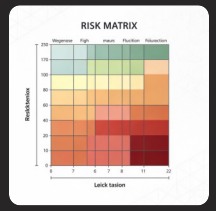
Final Project

Tugas Akhir Modul 6

Peserta akan mendemonstrasikan penguasaan materi dengan menghasilkan tiga deliverable utama yang mencerminkan praktik nyata di industri keamanan siber.

Security Assessment Report

Laporan lengkap yang mencakup Executive Summary, daftar temuan yang diklasifikasikan berdasarkan risiko, bukti teknis, dan rekomendasi remediasi. Format profesional siap diserahkan kepada klien.



Risk Matrix

Visualisasi semua temuan dalam matriks risiko dua dimensi (likelihood vs. impact). Membantu manajemen memahami distribusi risiko secara sekilas dan memprioritaskan tindakan perbaikan.

Security Improvement Plan

Rencana perbaikan keamanan jangka pendek (0–30 hari), jangka menengah (30–90 hari), dan jangka panjang (90+ hari) yang terstruktur dan dapat diimplementasikan secara bertahap.

Edy Susanto - Founder C-SIX Security

Rangkuman & Outcome

Kompetensi yang Diperoleh

Setelah menyelesaikan Modul 6, peserta telah membangun kemampuan end-to-end dalam pelaporan keamanan — dari pengumpulan temuan hingga komunikasi strategis kepada pemangku kepentingan.

5

Komponen Laporan

Executive Summary, Risk Classification, Technical Findings, Remediation, Best Practices

3

Deliverable Final Project

Assessment Report, Risk Matrix, dan Security Improvement Plan

2

Audiens Terlayani

Laporan dirancang untuk manajemen senior dan tim teknis sekaligus

Outcome Utama: Peserta mampu menyusun laporan keamanan profesional yang tidak hanya akurat secara teknis, tetapi juga komunikatif, strategis, dan dapat langsung ditindaklanjuti oleh seluruh lapisan organisasi.

Edy Susanto - Founder C-SIX Security