Modul 6 – Intelligence Reporting & Case Study

Mengubah informasi mentah menjadi laporan intelijen yang terstruktur, akurat, dan siap digunakan oleh pengambil keputusan strategis.

Edy Susanto – Founder C-SIX Security

Tujuan Pembelajaran

Pada akhir modul ini, peserta diharapkan mampu mengolah data intelijen dari berbagai sumber menjadi laporan yang profesional, terstruktur, dan dapat ditindaklanjuti oleh tim keamanan maupun pimpinan organisasi.

🎯 Analisis

Memahami dan menginterpretasikan data ancaman dari berbagai sumber intelijen.

📝 Pelaporan

Menyusun laporan intelijen yang terstruktur sesuai standar profesional.

🛡️ Rekomendasi

Menghasilkan rekomendasi mitigasi risiko yang konkret dan dapat dieksekusi.

Edy Susanto – Founder C-SIX Security

Threat Intelligence Report

Threat Intelligence Report adalah dokumen inti yang merangkum temuan ancaman siber secara menyeluruh. Laporan ini mencakup identifikasi aktor ancaman, taktik, teknik, dan prosedur (TTP) yang digunakan, serta konteks geopolitik atau motivasi di balik serangan.

Komponen Utama

- Identifikasi Threat Actor
- Analisis TTP (Taktik, Teknik, Prosedur)
- Indikator Kompromi (IOC)
- Konteks & Motivasi Ancaman

Standar Referensi

- MITRE ATT&CK Framework
- STIX/TAXII Format
- Traffic Light Protocol (TLP)
- NIST SP 800-150

Edy Susanto – Founder C-SIX Security

Executive Summary

Executive Summary adalah bagian terpenting dari sebuah laporan intelijen. Dirancang untuk pembaca tingkat pimpinan yang tidak memiliki waktu membaca laporan teknis secara menyeluruh, ringkasan ini harus mampu menyampaikan inti ancaman, dampak bisnis, dan rekomendasi dalam satu halaman.

📌 Pernyataan Ancaman

Jelaskan ancaman utama secara singkat dan jelas — siapa, apa, dan kapan.

💼 Dampak Bisnis

Terjemahkan risiko teknis ke dalam bahasa bisnis: kerugian finansial, reputasi, operasional.

✅ Rekomendasi Utama

Sajikan 3–5 langkah prioritas yang dapat segera dieksekusi oleh manajemen.

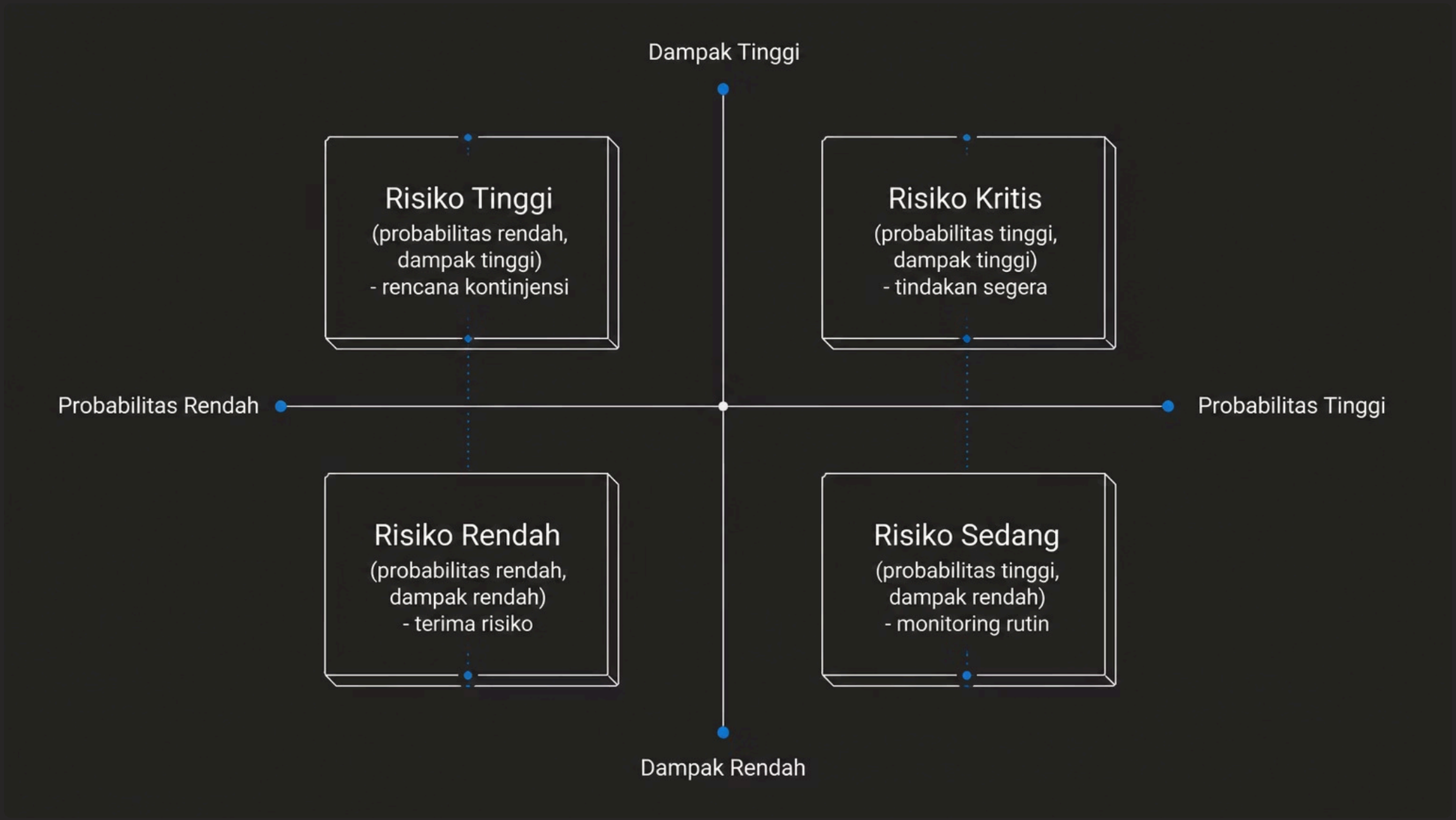
📊 Tingkat Kepercayaan

Nyatakan tingkat keyakinan analitik (High/Medium/Low) berdasarkan kualitas sumber.

Edy Susanto – Founder C-SIX Security

Risk Assessment

Risk Assessment mengukur potensi dampak dan probabilitas terjadinya ancaman terhadap aset organisasi. Proses ini menghasilkan matriks risiko yang menjadi dasar pengambilan keputusan mitigasi.



Setiap ancaman yang teridentifikasi ditempatkan dalam matriks berdasarkan dua dimensi utama: **kemungkinan terjadinya** dan **besarnya dampak** terhadap keberlangsungan operasi organisasi.

Edy Susanto – Founder C-SIX Security

Findings & Recommendations

Bagian Findings & Recommendations adalah jembatan antara analisis teknis dan tindakan nyata. Temuan harus disajikan secara objektif berdasarkan bukti, sementara rekomendasi harus spesifik, terukur, dan realistis untuk diimplementasikan.

📋 Struktur Findings

- Deskripsi temuan yang objektif
- Bukti pendukung (log, screenshot, IOC)
- Klasifikasi tingkat keparahan
- Mapping ke framework (MITRE ATT&CK)

🔧 Struktur Recommendations

- Tindakan jangka pendek (0–30 hari)
- Tindakan jangka menengah (30–90 hari)
- Perbaikan sistemik jangka panjang
- KPI & indikator keberhasilan

Edy Susanto – Founder C-SIX Security

Intelligence Presentation

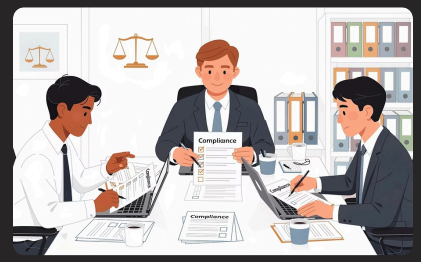
Menyampaikan laporan intelijen kepada audiens yang berbeda memerlukan pendekatan komunikasi yang berbeda pula. Analis harus mampu menyesuaikan kedalaman teknis, bahasa, dan format visualisasi dengan kebutuhan audiens.

Untuk Eksekutif

Fokus pada dampak bisnis, risiko finansial, dan rekomendasi strategis. Gunakan visualisasi sederhana dan hindari jargon teknis.

Untuk Tim Teknis

Sertakan IOC, TTP, payload, dan detail forensik. Gunakan format STIX/TAXII yang dapat langsung diintegrasikan ke tools keamanan.



Untuk Tim Legal/Compliance

Fokus pada implikasi regulasi, tanggung jawab hukum, dan dokumentasi insiden untuk keperluan pelaporan kepada otoritas.

Edy Susanto – Founder C-SIX Security

Final Project – Dark Web Intelligence Report

☆ FINAL PROJECT

Sebagai bagian dari proyek akhir, peserta akan melakukan investigasi terhadap aktivitas di dark web dan mendokumentasikannya dalam laporan intelijen yang komprehensif. Proyek ini menggabungkan seluruh keterampilan yang dipelajari sepanjang pelatihan.

01

Pengumpulan Data OSINT

Identifikasi forum, marketplace, dan kanal dark web yang relevan menggunakan teknik investigasi yang aman dan legal.

02

Analisis & Kontekstualisasi

Korelasikan temuan dengan threat actor yang diketahui, kampanye aktif, dan aset organisasi yang berpotensi terdampak.

03

Penyusunan Laporan

Dokumentasikan seluruh temuan dalam format laporan intelijen profesional dengan klasifikasi TLP yang sesuai.

Edy Susanto – Founder C-SIX Security

Final Project – Deliverables

Peserta wajib mengumpulkan tiga dokumen sebagai hasil akhir pelatihan. Setiap dokumen dirancang untuk melatih kemampuan berbeda dalam rantai pelaporan intelijen yang sesungguhnya digunakan oleh tim keamanan profesional.

Dark Web Intelligence Report

Laporan investigasi menyeluruh yang mendokumentasikan temuan dari dark web, termasuk IOC, TTP, dan profil aktor ancaman.

Threat Assessment Summary

Ringkasan penilaian ancaman yang ditujukan untuk pimpinan, mencakup tingkat risiko dan prioritas respons yang diperlukan.

Risk Recommendation Report

Dokumen rekomendasi mitigasi risiko yang terstruktur dengan timeline implementasi, penanggung jawab, dan indikator keberhasilan.

Outcome & Kompetensi Akhir

Setelah menyelesaikan Modul 6, peserta telah memiliki kompetensi lengkap sebagai Intelligence Analyst yang mampu bekerja secara profesional dalam ekosistem keamanan siber modern.

3

Dokumen Profisional

Laporan siap digunakan oleh tim SOC dan manajemen organisasi.

6

Modul Selesai

Rangkaian pelatihan intelijen siber yang komprehensif dari awal hingga akhir.

100%

Siap Lapangan

Peserta siap menghasilkan laporan investigasi profesional secara mandiri.

Peserta yang berhasil menyelesaikan seluruh modul dan final project akan mampu menghasilkan **laporan investigasi intelijen siber yang profesional** — siap digunakan dalam lingkungan kerja nyata maupun untuk keperluan sertifikasi internasional.

Edy Susanto – Founder C-SIX Security