ISOCENTER INDONESIA
The Ultimate ISO and Management System Resources

AI-DRIVEN IT RISK STRATEGY & CONTINUOUS EXPOSURE MANAGEMENT:

Siapkan GRC Framework Anda untuk Ancaman Adaptif

20250806-01

Inti Pembahasan

Topik ini membahas bagaimana organisasi dapat **memanfaatkan kecerdasan buatan (AI)** untuk **membangun strategi manajemen risiko TI yang adaptif** melalui ***continuous exposure management***, sehingga **memberi penguatan terhadap kerangka kerja GRC yang diterapkan selama ini** agar **siap menghadapi ancaman yang semakin dinamis dan kompleks.**

Mengenal Lanskap Ancaman TI Modern (1)

No.	Ciri-Ciri	Penjelasan Singkat	Contoh Kasus
1	**Cepat Berubah & Adaptif**	Teknik serangan baru muncul terus, antivirus & firewall tradisional sering ketinggalan.	Dalam hitungan hari, sistem EDR perusahaan besar tidak mendeteksi malware karena signature-nya belum dikenal.
2	**Kompleks & Terdistribusi**	Serangan menyerang banyak sistem sekaligus—email, API, cloud, dll.	Hacker masuk lewat server IT vendor, tapi berhasil lompat ke sistem internal perusahaan karena koneksi API belum diamankan.
3	**Menargetkan Identitas & Data**	Pencurian kredensial dan pencurian data lebih sering daripada deface website.	Akun admin cloud disusupi lewat phishing, lalu digunakan untuk mengakses data pelanggan yang tersimpan di blob storage.
4	**Gunakan AI dan Deepfake**	AI bisa bikin email, suara, bahkan video yang tampak asli dan meyakinkan.	Tim keuangan menerima email berisi suara mirip CEO yang minta cepat transfer dana. Padahal itu suara palsu.
5	**Eksploitasi Zero-Day & Supply Chain**	Hacker menyerang lewat aplikasi pihak ketiga yang digunakan semua orang.	Software transfer file yang biasa dipakai HR ternyata punya celah zero-day, dan dimanfaatkan untuk mencuri data ribuan karyawan.

Mengenal Lanskap Ancaman TI Modern (2)

No.	Ciri-Ciri	Penjelasan Singkat	Contoh Kasus
6	**Motivasi Bukan Cuma Uang (Politik, Sabotase)**	Motif penyerang tidak hanya cari uang, tapi juga ingin rusak reputasi, pengaruhi opini, atau sabotase.	Sebuah media online tiba-tiba diserang DDoS saat memuat artikel sensitif—bukan minta uang, tapi agar berita tak bisa dibaca.
7	**Sasar Infrastruktur Kritis**	Rumah sakit, pelabuhan, dan perusahaan energi makin sering diserang.	Server rumah sakit disusupi ransomware hingga pasien tak bisa dilayani sistem digital. Pelayanan terhambat total.
8	**Cloud, SaaS & Mobile Endpoint Jadi Target**	Hacker lebih suka menyerang akun cloud & device karyawan karena lebih rentan.	Karyawan buka file dari email di HP pribadi—tanpa disadari, device-nya dipakai hacker buat masuk ke OneDrive kantor.
9	**Social Engineering Lebih Canggih & Personal**	Email dan pesan jebakan makin pintar, pakai data personal yang meyakinkan.	Anda dapat email HR tentang promosi gaji, padahal itu jebakan phishing pakai data profil LinkedIn Anda.
10	**Advanced Persistent Threat (APT)**	Serangan diam-diam, bisa bertahan berbulan-bulan tanpa ketahuan.	Server data center disusupi malware yang tidak aktif langsung, tapi mencuri data secara perlahan selama 9 bulan baru terdeteksi.

Contoh Kasus AI Enabled Hacker (1)

No.	Aktivitas Hacker	Bagaimana AI Membantu Hacker	Ilustrasi Kasus
1	**Belajar Eksploitasi CVE** (Common Vulnerabilities and Exposures) **Baru**	AI merangkum detail celah keamanan (CVE), menyederhanakan exploit, bahkan membuat *PoC* (Proof of Concept) otomatis.	Hacker pemula cukup copy-paste CVE baru ke chatbot → langsung keluar skrip serangan & penjelasan langkah demi langkah.
2	**Membuat Phishing Email yang Lolos Filter**	AI membuat email yang lolos filter spam karena menggunakan bahasa alami yang mirip manusia.	Email dengan gaya bahasa khas bos HR, disertai file 'rincian gaji' palsu – sangat meyakinkan, tidak terdeteksi spam filter.
3	**Deepfake Voice & Video Generation**	AI cloning suara atau wajah seseorang hanya dari rekaman pendek, membuat social engineering makin realistis.	Karyawan menerima voice note dari "CFO" yang ternyata suara palsu hasil AI, minta transfer dana mendesak.
4	**Serangan Otomatis & Adaptif**	AI mendeteksi serangan yang gagal, lalu modifikasi payload secara real-time tanpa campur tangan manual.	Payload awal ditolak firewall → AI langsung encode ulang jadi obfuscated → payload berhasil masuk tanpa alarm.

Contoh Kasus AI Enabled Hacker (2)

No.	Aktivitas Hacker	Bagaimana AI Membantu Hacker	Ilustrasi Kasus
5	**Bypass MFA dan CAPTCHA**	AI pecahkan CAPTCHA dengan computer vision, lalu bantu intersep OTP dari MFA (via SIM swap).	Meski MFA aktif, akun tetap berhasil diretas karena OTP diambil dari nomor korban yang sudah di-*swap* ke SIM hacker.
6	**Profilisasi Target**	AI menganalisis data publik (LinkedIn, GitHub, media sosial) untuk personalisasi social engineering.	Korban dapat email 'proyek open source' dari rekan developer palsu, lengkap dengan nama proyek yang sedang ia kerjakan.
7	**Malware Polimorfik** (malware yg dapat berubah bentuk)	AI bantu buat varian malware yang selalu berbeda tiap kali dijalankan agar tak dikenali antivirus.	File .exe diunduh lima kali → tiap kali bentuknya beda → semua lolos deteksi EDR (*Endpoint Detection & Response*).
8	**Penyesuaian Taktik Otomatis via MITRE ATT&CK** (framework taktik dan teknik yang digunakan oleh penyerang siber)	AI bantu pilih taktik baru dari MITRE jika pendekatan lama gagal, misalnya ganti teknik privilege escalation.	Awalnya coba spear phishing, gagal. AI rekomendasi LLMNR spoofing → jalankan & berhasil menembus sistem internal.

Mengapa Manajemen Risiko Tradisional Tidak Lagi Memadai?

- Masih bergantung pada pendekatan manual dan bersifat periodik.
- Perubahan ancaman terjadi sangat cepat, melampaui kecepatan proses penilaian risiko.
- Tidak mampu mendeteksi jenis serangan baru yang semakin canggih (misalnya: berbasis AI, deepfake, dan social engineering).
- Fokus utama pada pelaporan dan dokumentasi, bukan pada respons terhadap ancaman aktual.
- Sistem deteksi dan respons belum terotomatisasi, sehingga menimbulkan keterlambatan penanganan.
- Semua risiko diperlakukan secara setara tanpa mempertimbangkan tingkat paparan (exposure) yang berbeda-beda.
- Tidak adanya proses pembelajaran dari insiden sebelumnya.

Strategi Manajemen Risiko Zaman Now: Adaptive Risk Management

- Mampu merespons ancaman secara real-time dengan pendekatan otomatis dan terukur.
- Mengadopsi teknologi berbasis AI.
- Terintegrasi dengan sumber threat intelligence global & pemantauan sistem internal 24/7.
- Penerapan Continuous Exposure Management (CEM) untuk deteksi celah secara real-time, kuantifikasi tingkat eksposur risiko aktual, dan penyusunan prioritas mitigasi berbasis data.
- Adaptasi cepat kebijakan dan kontrol berdasarkan pembelajaran dari insiden yang terjadi.

Apakah Register Risiko Masih Diperlukan?

- Jawaban singkat: Ya, tetapi sebaiknya ditingkatkan menjadi **"Dynamic Risk Register"**.
- Risk Register masih diperlukan karena:
  - Memberikan kerangka dasar untuk mencatat risiko secara sistematis (sumber risiko, penyebab, dampak, likelihood, mitigation plan, PIC).
  - Wajib dalam banyak kerangka kerja GRC, standar ISO (seperti ISO 31000, ISO/IEC 27001), dan regulasi formal (seperti POJK, GDPR).
  - Memudahkan diskusi manajemen dan audit atas posisi risiko saat ini.
- Konsep **Dynamic Risk Register** adalah:
  - Integrasikan Register Risiko dengan data-data yang berasal dari sistem keamanan (SIEM, XDR, SOAR) dan penerapan sistem Continuous Exposure Management (CEM) agar eksposur nyata langsung tercermin sebagai prioritas risiko.
  - Risiko di dalam Register Risiko bisa di-skor ulang otomatis berdasarkan porsture internal (data-data dari sistem keamanan dan CEM) dan perubahan threat landscape global.

Contoh Dynamic Risk Register

ID Risiko	Risiko TI	Sumber Ancaman	Likelihood (AI)	Impact (AI)	Level Risiko	Eksposur CEM (AI)	Status Respon	Update Otomatis Terakhir
R-001	Ransomware pada endpoint staff	Email phishing, USB tidak aman	Sedang	Tinggi	**Tinggi**	Endpoint: 90% exposed	Direspon oleh SOAR	06/08/2025 14:22
R-002	Credential stuffing ke akun cloud	IP anonim dari luar negeri	Tinggi	Sedang	**Tinggi**	Cloud: 70% exposed	Blok otomatis oleh XDR	06/08/2025 14:30
R-003	Eksploitasi zero-day web apps	Threat Intel: CVE-2025-XXXX	Rendah	Tinggi	**Sedang**	Web App: 55% exposed	Sedang diinvestigasi	06/08/2025 14:18
R-004	Kegagalan update SIEM	Sistem tidak sinkron log	Tinggi	Rendah	**Sedang**	SIEM: 40% eksposur	Eskalasi ke admin log	06/08/2025 14:10
R-005	Serangan brute force ke login VPN	Log XDR mencatat 1000+ attempt	Tinggi	Sedang	**Tinggi**	Jaringan: 65% exposed	Auto-block + alert via SOAR	06/08/2025 14:35

Membangun Kapabilitas Real-Time Response

Aspek	Penjelasan
Pengertian	Kemampuan sistem keamanan untuk mendeteksi, menganalisis, dan merespons ancaman TI secara langsung begitu terjadi, tanpa intervensi manual, menggunakan automasi dan metrik terukur.
Tujuan	Meminimalkan waktu respons dan mengurangi dampak insiden keamanan dengan automasi berbasis data.
Komponen Utama	**- Sensor & detektor otomatis**, seperti: Intrusion Detection System (IDS), Intrusion Prevention System (IPS), EDR (Endpoint Detection & Response) **- Threat intelligence feed** yang berisi data real-time yang berisi informasi terkini tentang ancaman keamanan siber, seperti: IP address berbahaya, Hash file malware, dsb) **- Decision engine (AI/ML)**: Sistem otomatis yang mengambil keputusan atas insiden atau anomali keamanan dengan bantuan kecerdasan buatan (AI) dan machine learning (ML). **- Otomasi mitigasi** (mis: menggunakan SOAR) **- Dashboard metrik real-time**
Manfaat Utama	☑ Waktu deteksi lebih cepat (seconds, bukan days) ☑ Mengurangi beban tim SOC ☑ Mengurangi risiko kelengahan manusia ☑ Bisa ditrigger di luar jam kerja

Mengenal Teknologi AI

AI (Kecerdasan Buatan) adalah kemampuan sistem komputer untuk melakukan **tugas-tugas yang biasanya membutuhkan kecerdasan manusia**, seperti memahami bahasa (NLP), mengenali pola visual (vision), membuat keputusan, dan bahkan menyelesaikan tugas. Contoh:

- Chatbot yang bisa menjawab pertanyaan pelanggan.
- Sistem keamanan yang bisa mendeteksi file berbahaya tanpa campur tangan manusia.
- Sistem yang bisa belajar dari ribuan email yang diklasifikasikan sebagai spam, lalu mengenali pola spam baru.

Cabang-Cabang AI

Cabang AI	Penjelasan Singkat	Contoh Penerapan
1. Machine Learning (ML)	Sistem belajar dari data dan meningkatkan kinerja seiring waktu tanpa diprogram ulang.	Rekomendasi film di Netflix, deteksi penipuan kartu kredit, Google Photos mengenali wajah
2. Natural Language Processing (NLP)	Memungkinkan mesin memahami, menganalisis, dan menghasilkan bahasa manusia.	ChatGPT, Siri, Google Translate, voice-to-text di WhatsApp
3. Computer Vision (CV)	Memungkinkan komputer "melihat" dan menginterpretasi gambar atau video.	Face unlock di HP, Google Lens, deteksi plat nomor otomatis (ANPR), analisis citra medis
4. Expert Systems	Sistem berbasis aturan IF-THEN yang meniru keputusan pakar manusia.	Sistem diagnosa medis seperti MYCIN, sistem troubleshooting printer HP
5. Robotics	AI yang digunakan untuk mengontrol perangkat fisik dan interaksi dengan lingkungan.	Robot vacuum (Roomba), robot warehouse Amazon, lengan robotik di pabrik mobil
6. Planning & Reasoning	AI yang mampu merencanakan langkah dan mengambil keputusan berdasarkan tujuan akhir.	Google Maps (merencanakan rute tercepat), chatbot yang menyesuaikan respons strategis
7. Fuzzy Logic	Sistem pengambilan keputusan berbasis “tingkat kepastian” bukan hitam-putih.	Mesin cuci otomatis (atur kekuatan putar berdasarkan beban cucian), kontrol AC pintar
8. Speech Recognition	Mengubah ucapan manusia menjadi teks atau perintah digital.	Voice command di Google Assistant, Apple Dictation, transcription Zoom
9. Reinforcement Learning	Sistem belajar dari trial-error melalui umpan balik dari lingkungan.	AlphaGo (AI main Go), robot main bola, AI optimisasi jadwal produksi

Cabang-Cabang AI yang Paling Sering Digunakan untuk Adaptive Risk Management

Cabang AI	Peran Utama dalam Adaptive Risk Management	Contoh Penerapan Nyata (Case: Mitigasi Risiko TI)
Machine Learning (ML)	Menganalisis pola historis dan mendeteksi anomali secara otomatis.	- Deteksi *zero-day threat* dan malware baru di endpoint (CrowdStrike, SentinelOne) - Scoring risiko user login abnormal (UEBA: User & Entity Behavior Analytics)
Natural Language Processing (NLP)	Memahami dan mengekstrak insight dari teks atau log tidak terstruktur.	- Analisis email phishing canggih berbasis konteks - Pemantauan dark web untuk kata kunci tertentu (brand leak, access sale)
Computer Vision (CV)	(Lebih jarang) Digunakan untuk pengawasan fisik dan keamanan visual.	- Face recognition untuk akses data center - Visual threat detection via CCTV AI (contoh: mendeteksi penyusupan fisik ke ruang server)
Expert Systems	Memberikan keputusan berbasis aturan untuk respons awal atau mitigasi risiko.	- Jika patch belum diterapkan dan skor CVE tinggi → kirim alert otomatis - Decision tree untuk eskalasi insiden ke tim SOC
Planning & Reasoning	Menyusun skenario respons otomatis saat risiko meningkat.	- Menentukan urutan mitigasi saat ransomware aktif (shutdown isolasi, backup recovery) - Simulasi skenario risiko eskalatif secara otomatis
Reinforcement Learning	Menyesuaikan strategi mitigasi seiring waktu berdasarkan hasil sebelumnya	- Adaptive firewall rules (belajar dari insiden sebelumnya) - Autotuning sistem SIEM untuk menekan false positive
Fuzzy Logic	Menghadapi ketidakpastian risiko dengan pendekatan probabilistik.	- Penilaian risiko berbasis kombinasi sinyal lemah (low-confidence logs) - Keputusan saat ancaman tidak jelas (misalnya: moderate anomaly + unknown IP)

Dampak Penerapan AI dalam Adaptive Risk Mgt

- AI secara nyata meningkatkan resiliensi TI, mulai dari deteksi lebih cepat, mitigasi lebih efisien, hingga pengurangan biaya.
- Organisasi yang mengintegrasikan AI sejak awal lebih tangguh terhadap serangan modern.
- Statistik menunjukkan manfaat signifikan: lebih hemat biaya, lebih cepat merespon, dan lebih sehat dari sisi visibilitas serta kesiapan TI.

Metrik	Dampak AI
Waktu deteksi & respons	MTTI turun dari 168 → 148 hari, MTTR dari 64 → 42 hari
Risiko serangan canggih	Risiko serangan canggih berkurang 69% pada organisasi AI-enabled
Visibilitas sistem	Meningkat 1,3× untuk organisasi yang AI-driven
Biaya pelanggaran data	Hemat sekitar £600 ribu per insiden dengan AI

Mengenal Teknologi SOAR

SOAR = Security Orchestration, Automation, and Response, merupakan platform yang menggabungkan tiga kemampuan utama (sesuai singkatannya) yang bertujuan untuk mengurangi waktu respon, menstandarkan tindakan keamanan, dan mengurangi beban kerja tim SOC (Security Operations Center).

- **Orchestration:** Mengintegrasikan berbagai alat keamanan (SIEM, firewall, threat intel feed, ticketing, dll) yang sebelumnya silo untuk berbagi data ancaman secara real-time.
- **Automation:** Mengotomatisasi alur kerja respons insiden, seperti (contoh): isolasi endpoint → buat tiket → kirim notifikasi → blokir IP, yang dapat berupa playbook otomatis atau semi-otomatis dengan persetujuan manusia.
- **Incident Response:** Menyediakan dokumentasi, pelacakan, dan dashboard tindakan terhadap insiden siber, sehingga dapat mendukung proses investigasi forensik dan audit trail.

Case Study Penerapan SOAR

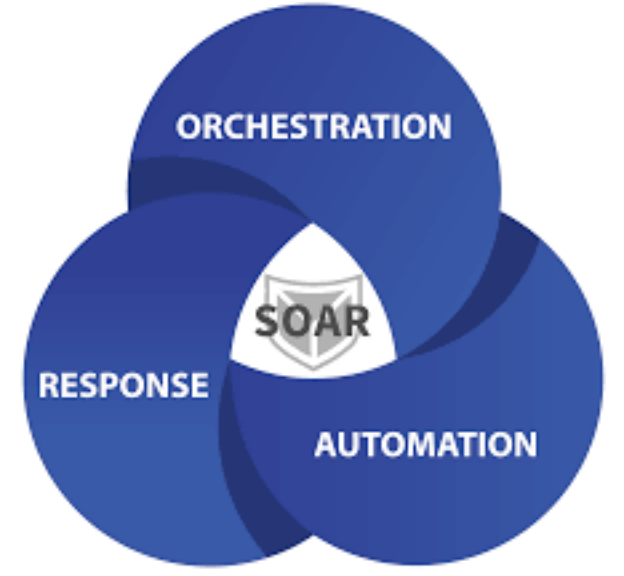
Deteksi Phishing:

- SIEM mendeteksi email mencurigakan.
- SOAR secara otomatis:
  - ✓ Mengekstrak IP & domain dari email.
  - ✓ Mengecek reputasi IP/domain ke threat intelligence feed.
  - ✓ Jika malicious → memblokir domain, isolasi endpoint, kirim tiket ke tim IT
  - ✓ Semua tindakan tercatat & dapat diaudit.
- Catatan Penting:
  - ✓ SOAR tidak menggantikan SIEM, tapi melengkapi SIEM dengan tindakan otomatis.
  - ✓ Implementasi SOAR yang efektif memerlukan playbook yang disesuaikan, kolaborasi antar tim, dan integrasi alat keamanan lainnya.

Penggunaan AI/ML dalam SOAR

Komponen SOAR	Peran AI dalam Penerapan	Contoh Penerapan Nyata
Threat Detection & Triage	AI/ML mengklasifikasikan alert berdasarkan prioritas. Mengurangi false positive.	Model AI mengenali bahwa alert scanning adalah benign, sedangkan exfiltration adalah
Playbook Recommendation	AI merekomendasikan langkah respons berdasarkan pola historis dan jenis insiden.	Untuk malware jenis A, AI menyarankan blokir IP + isolasi endpoint dalam 3 detik.
Automated Decision Engine	AI memutuskan apakah eskalasi perlu dilakukan ke manusia atau tidak.	Sistem auto-close 70% phishing alert karena confidence score AI tinggi.
Threat Intelligence Correlation	AI mencocokkan indikator dari berbagai feed intelijen global. NLP memproses unstructured data.	AI menyimpulkan bahwa IP baru mirip pola serangan APT China berdasarkan pola sebelumnya.
Response Orchestration	AI mengatur urutan eksekusi playbook berdasarkan efisiensi & waktu.	AI menyusun ulang: isolasi endpoint dulu sebelum email delete → menghindari propagasi.
Adaptive Learning	ML belajar dari tiap insiden untuk terus menyempurnakan playbook otomatis.	Setelah 10x insiden serupa, AI tahu kapan perlu eskalasi cepat ke tim keamanan.
Root Cause Analysis	AI menelusuri asal muasal insiden melalui log dan timeline otomatis.	AI menemukan bahwa breach berasal dari token expired yang tidak dicabut.
User Behavior Analysis	AI menganalisis perilaku user untuk mendeteksi insider threat.	User biasa akses jam 9–5, tiba-tiba akses besar jam 3 pagi → trigger alert otomatis.

Beberapa Produk SOAR di Pasaran



- Cortex XSOAR – Palo Alto Networks
- Splunk SOAR (dulu Phantom)
- IBM Security QRadar SOAR
- Swimlane, Siemplify (sekarang bagian Google Chronicle)

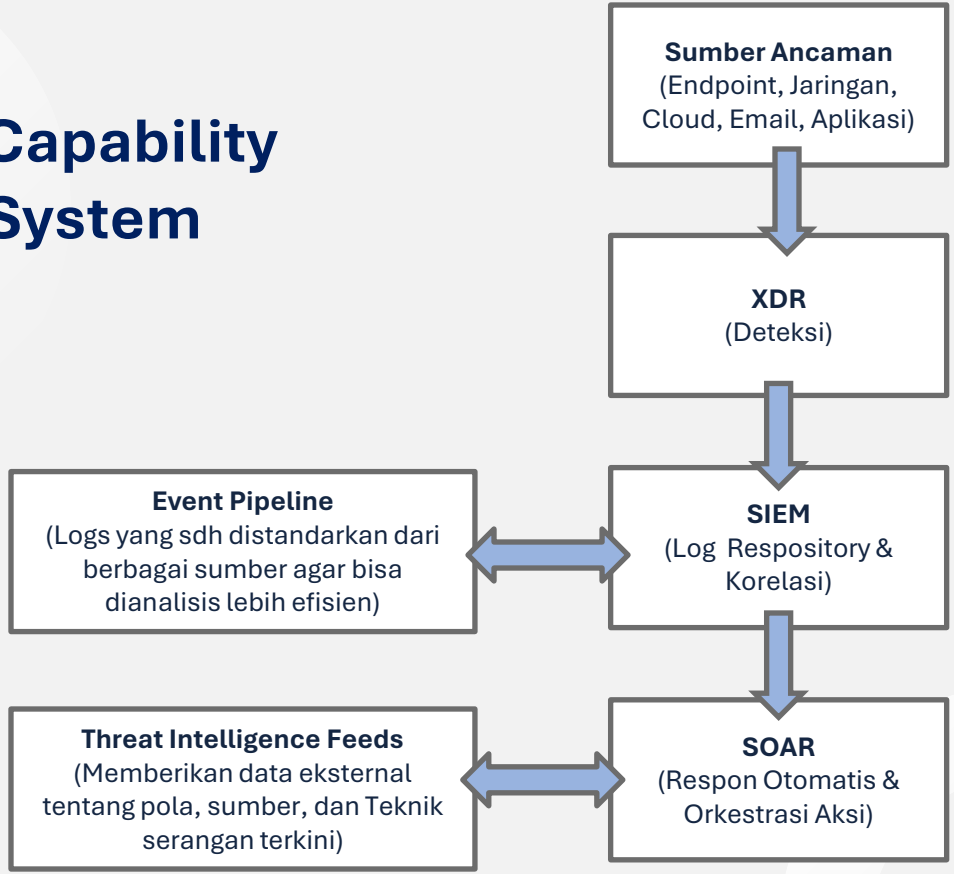
Mengenal Teknologi XDR

- **XDR = Extended Detection and Response**, merupakan evolusi dari EDR (Endpoint Detection and Response) dengan cakupan yang lebih luas dan terintegrasi dengan tujuan mendeteksi ancaman yang lebih dalam, analitik yang lebih cerdas, dan respons yang lebih cepat dan otomatis
- Komponen utama XDR:
  - ✓ **Data Collection Multisource:** endpoint, jaringan, email, identitas, aplikasi SaaS.
  - ✓ **Threat Correlation Engine:** menghubungkan indikasi ancaman dari berbagai sumber menjadi satu konteks.
  - ✓ **Automated Response:** mengambil tindakan otomatis (isolasi host, blokir IP, hapus email).
  - ✓ **Threat Intelligence Integration:** memanfaatkan feed intelijen global (CVE, MITRE ATT&CK).

XDR vs SIEM vs SOAR

Aspek	XDR *(Extended Detection and Response)*	SIEM *(Security Information and Event Management)*	SOAR *(Security Orchestration, Automation, and Response)*
Peran Utama	Mendeteksi dan merespons ancaman lintas berbagai vektor secara terintegrasi dan otomatis	Mengumpulkan, menyimpan, dan menganalisis log untuk keperluan pemantauan keamanan dan kepatuhan	Mengotomatisasi dan mengorkestrasi respons terhadap insiden keamanan menggunakan playbook dan integrasi sistem
Kekuatan Utama	- Deteksi berbasis AI/ML - Korelasi lintas endpoint, jaringan, cloud - Mengurangi alarm palsu (false positive)	- Visibilitas log menyeluruh - Mendukung audit dan kepatuhan - Korelasi insiden berdasarkan aturan manual	- Otomatisasi tindakan respons - Eksekusi playbook - Meningkatkan efisiensi tim keamanan (SOC)
Kelemahan Utama	- Biasanya bergantung pada ekosistem vendor tertentu - Tidak berfokus pada kepatuhan - Keterbatasan dokumentasi	- Tidak memiliki deteksi cerdas otomatis - Tidak mendukung respons otomatis - Perlu konfigurasi manual	- Tidak memiliki deteksi mandiri - Butuh integrasi input dari SIEM atau XDR - Implementasi awal cukup kompleks
Cocok Untuk	- Organisasi menengah-besar dengan banyak endpoint dan sistem cloud - Ancaman kompleks - Butuh respons adaptif	- Organisasi tahap awal pengamanan TI - Kebutuhan pelaporan audit & kepatuhan - Pemantauan log terpusat	- Organisasi dengan SOC aktif - Ingin respons insiden cepat dan otomatis - Fokus pada efisiensi operasional
Contoh Aktivitas	- Deteksi aktivitas mencurigakan dari email atau endpoint - Pemblokiran otomatis akses mencurigakan - Korelasi antar sumber	- Analisis log firewall, server, aplikasi - Investigasi insiden berbasis pola log - Pelaporan insiden reguler	- Otomatisasi pembuatan tiket insiden - Isolasi host secara otomatis - Eksekusi SOP respons secara otomatis

Integrated Real Time Capability Response System



Tantangan Kapabilitas Real-Time Response (1)

Tantangan Umum	Penjelasan	Contoh Nyata / Ilustrasi
1. False Positive Tinggi	Sistem otomatis kadang menganggap aktivitas sah sebagai ancaman karena sensitivitas model deteksi terlalu tinggi.	Di tahun 2023, sebuah perusahaan e-commerce global melaporkan kerugian akibat pemblokiran otomatis terhadap traffic pengguna sah dari Asia karena sistem AI mendeteksinya sebagai DDoS bot. Penjualan turun 8% dalam 2 hari.
2. False Negative (Ancaman Tidak Terdeteksi)	Model AI tidak mendeteksi pola baru yang belum dikenali, karena belum cukup data pelatihan.	Serangan 0-day pada MOVEit Transfer (2023) tidak terdeteksi oleh beberapa XDR besar karena menggunakan teknik baru yang belum pernah dikenali sebelumnya.
3. Over-Automation (Respons Otomatis Tanpa Validasi)	Tindakan otomatis seperti pemblokiran, isolasi, atau shutdown dapat mengganggu operasi bisnis jika tidak dikaji lebih lanjut.	Sistem SOAR salah mengisolasi server produksi akibat mendeteksi login dari alamat IP asing yang ternyata milik developer jarak jauh. Proyek terhenti selama 4 jam.

Tantangan Kapabilitas Real-Time Response (2)

Tantangan Umum	Penjelasan	Contoh Nyata / Ilustrasi
4. Noise & Alert Fatigue	Sistem SIEM/XDR menghasilkan terlalu banyak alert, membuat tim kewalahan dan kehilangan fokus pada ancaman sebenarnya.	Studi IBM X-Force (2023): rata-rata SOC menerima 11.000 alert per hari, 77% tidak ditindaklanjuti karena overload.
5. Integrasi yang Rumit	Otomasi real-time harus terhubung dengan sistem lain (email, endpoint, firewall, CMDB), yang kadang tidak kompatibel.	Bank regional di Asia Tenggara gagal mengimplementasikan isolasi otomatis karena sistem core banking mereka tidak kompatibel dengan solusi XDR.

Mengenal Continuous Exposure Management (CEM)

CEM merupakan **pendekatan berkelanjutan berbasis AI untuk mengidentifikasi, memprioritaskan, dan mengurangi risiko keamanan TI** berdasarkan *exposure analysis* yang dapat dieksploitasi oleh penyerang.

Karakteristik Utama CEM:

- **Berbasis Siklus Berkelanjutan** (pemantauan, penilaian risiko risiko secara terus-menerus/real-time, bukan hanya secara periodik).
- Tidak hanya melihat kerentanan, tapi juga **menilai & memprioritisasi potensi eksposur nyatanya**, yaitu dengan menilai apakah kerentanan tersebut benar-benar dapat dieksploitasi dalam sistem yang ada.
- **Terintegrasi dengan realtime response systems** seperti SIEM & Threat Intelligence untuk menilai urgensi setiap eksposur dan SOAR untuk tindakan otomatis atas eksposur prioritas tinggi.

Peran AI dalam CEM (1)

Fungsi dalam CEM	Jenis AI	Peran AI	Contoh Penerapan
1. Deteksi Eksposur & Anomali	Machine Learning (ML)	Menganalisis pola lalu lintas jaringan dan aktivitas pengguna untuk mendeteksi eksposur yang tidak biasa	Deteksi aktivitas mencurigakan di port yang tiba-tiba terbuka di server produksi
2. Korelasi Data Keamanan & Risiko	Knowledge Reasoning + ML	Menghubungkan data dari berbagai sumber untuk menilai risiko secara kontekstual	Menghubungkan data asset inventory, CVE, dan akses jaringan untuk memprioritaskan eksposur
3. Prioritisasi Risiko secara Otomatis	ML + Decision Engine (Rule-Based AI)	Menentukan urutan mitigasi berdasarkan potensi dampak, exposure, dan cost	Sistem otomatis menyarankan patch untuk kerentanan CVE-2023-XXXX lebih dahulu karena dampak bisnis tinggi
4. Simulasi Jalur Serangan (Attack Path)	Graph AI / ML	Memetakan dan mengevaluasi jalur serangan realistis yang dapat ditempuh oleh hacker dari satu aset ke aset lain	XM Cyber memvisualisasikan kemungkinan jalur dari server user ke Active Directory core

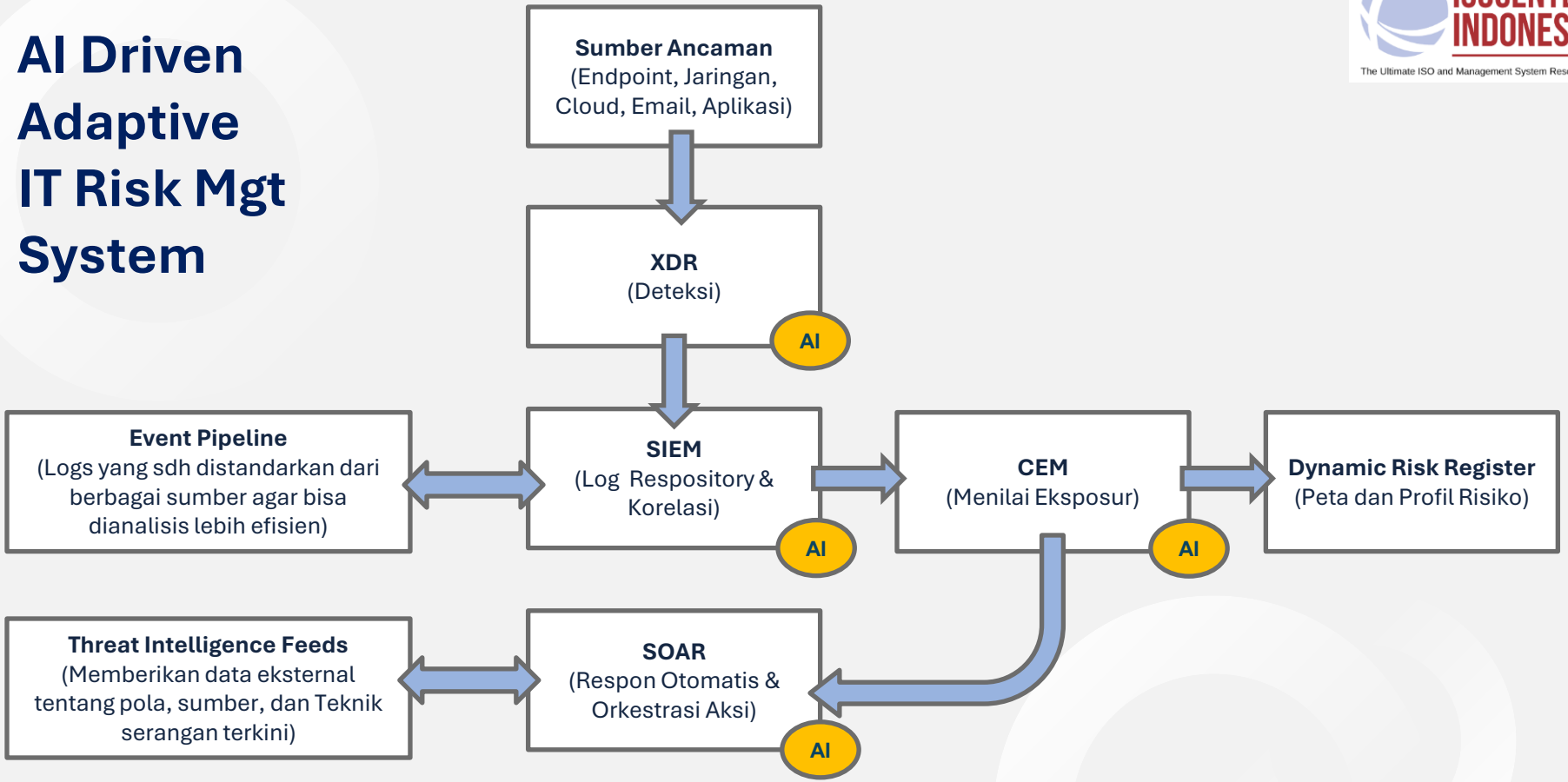
Peran AI dalam CEM (2)

Fungsi dalam CEM	Jenis AI	Peran AI	Contoh Penerapan
5. Analisis Bahasa dari Threat Intelligence	Natural Language Processing (NLP)	Mengekstrak insight dari laporan threat intelligence dalam bahasa alami (PDF, web, forum darkweb)	Sistem membaca laporan CISA & FBI lalu mengaitkannya dengan aset yang terdampak di lingkungan internal
6. Respons Otomatis terhadap Paparan Risiko	AI Automation + ML	Mengaktifkan respon seperti blokir IP, tutup port, isolasi endpoint, sesuai tingkat urgensi	SOAR platform menutup port terbuka di perimeter firewall setelah AI memberi label “eksposur
7. Pembelajaran Berkelanjutan dari Insiden	ML (Supervised & Unsupervised)	Belajar dari insiden masa lalu untuk meningkatkan deteksi dan rekomendasi ke depan	Setelah insiden ransomware, sistem mempelajari pola akses awal & memperbarui rule deteksi

Case Study CEM

No.	Situasi	Analisis Paparan (Exposure Analysis)	Tindakan (Response)
1	**Port RDP terbuka di server produksi**	Port RDP dapat diakses publik, meskipun tidak ada kerentanan CVE. Namun, RDP sering menjadi target brute-force & ransomware (berdasarkan threat intelligence global).	Prioritas tinggi. Port ditutup dan akses dialihkan melalui VPN internal yang aman.
2	**Kerentanan CVE di perangkat router (mis. CVE-2023-XXXX)**	Router mengandung CVE kritikal dan terhubung langsung ke internet. Kerentanan tersebut aktif dieksploitasi menurut threat feed terkini.	Patch segera diterapkan. Mitigasi sementara (akses dibatasi) dilakukan hingga patch selesai.
3	**Library jQuery usang di aplikasi web internal**	Versi library rawan hanya digunakan di aplikasi internal tanpa akses eksternal, dan berada di jaringan tertutup. Risiko eksploitasinya sangat rendah saat ini.	Diprioritaskan rendah. Ditandai sebagai backlog perbaikan jangka menengah tanpa urgensi perbaikan cepat.

AI Driven Adaptive IT Risk Mgt System



Roadmap Adaptive IT Risk Mgt System (1)

Tahap	Periode	Fokus Pembangunan	Solusi dari yang Termurah	Tujuan Kunci
1. Pondasi Dasar	0–3 bulan	- Inventarisasi aset TI - Identifikasi risiko utama secara manual - Buat risk register sederhana	- Gunakan spreadsheet/manual - Panduan kerangka kerja terbuka	Menyusun pemahaman awal tentang risiko dan aset yang dilindungi
2. Monitoring Dasar	3–6 bulan	- Kumpulkan log dasar dari sistem penting - Buat notifikasi manual jika terjadi anomali	- Konfigurasi log dasar dan email alert sederhana - Panduan insiden manual	Menyediakan deteksi awal secara sederhana untuk insiden TI
3. Analisis & Korelasi	6–9 bulan	- Korelasikan log secara manual atau semi-otomatis - Review risiko berdasarkan kejadian aktual	- Analisis korelasi dasar - Update risk register berdasarkan data log	Memberikan pemahaman yang lebih dalam terhadap pola serangan
4. Integrasi Intelijen Ancaman	9–12 bulan	- Tambahkan referensi eksternal mengenai pola serangan - Gunakan informasi untuk prioritisasi risiko	- Integrasikan sumber referensi terbuka - Update risk register secara	Memperkaya deteksi dan penilaian risiko dari sisi eksternal
5. Penilaian Eksposur	12–18 bulan	- Mulai menilai eksposur secara kuantitatif - Skor eksposur berdasarkan aset & insiden sebelumnya	- Buat metode skor eksposur - Visualisasi tingkat risiko dan prioritas	Fokus pada area yang paling rawan untuk mitigasi yang lebih cepat

Roadmap Adaptive IT Risk Mgt System (2)

Tahap	Periode	Fokus Pembangunan	Solusi dari yang Termurah	Tujuan Kunci
6. Otomatisasi Tanggapan Awal	18–24 bulan	- Otomatiskan tanggapan dasar terhadap insiden umum - Hubungkan deteksi ke sistem bantuan/tiket	- Gunakan skrip otomatis sederhana - Integrasikan alur kerja tanggapan awal	Mempercepat respon terhadap ancaman yang berulang
7. Risk Register Dinamis	24–30 bulan	- Hubungkan sistem log/deteksi ke risk register - Update otomatis profil risiko secara periodik	- Buat koneksi sistematis antara deteksi dan risk register - Gunakan logika berbasis aturan	Risk register berubah mengikuti dinamika ancaman dan eksposur yang terjadi
8. Adaptasi Cerdas (AI/ML)	30–36 bulan	- Tambahkan analitik cerdas untuk deteksi anomali dan pola - Terapkan pembelajaran dari data	- Kembangkan model deteksi sederhana - Gunakan logika adaptif untuk skor risiko	Sistem mulai mampu belajar dan menyesuaikan diri terhadap ancaman yang berubah

Kesimpulan

- Adaptive Risk Management (ARM) memungkinkan respons risiko secara real-time dan dinamis.
- ARM menggantikan pendekatan periodik dengan pemantauan dan pembaruan risiko terus-menerus.
- AI (termasuk ML dan NLP) memperkuat deteksi, klasifikasi, dan keputusan otomatis berbasis data.
- CEM membantu menilai dan memprioritaskan eksposur risiko secara kontekstual dan berkelanjutan.
- Dynamic Risk Register menyajikan pembaruan risiko otomatis dari sistem dan intelijen ancaman.
- SIEM, XDR, SOAR, dan threat intelligence mendukung ARM sebagai fondasi data real-time.
- Dengan ARM, organisasi menjadi proaktif, responsif, dan strategis dalam mengelola risiko TI.

ISOCENTER INDONESIA
The Ultimate ISO and Management System Resources

About Us

ISO CENTER INDONESIA adalah penyedia layanan terkait ISO dan Sistem Manajemen yang komprehensif. Kami adalah The Ultimate ISO and Management System Resources yang siap meningkatkan kinerja organisasi Anda melalui penyediaan informasi, pelatihan, implementasi, dan asesmen standar internasional berbasis ISO dan sistem manajemen yang efektif, efisien, out of the box, dan menggunakan metode terkini yang di-enable oleh teknologi dan AI.Jangan lupa untuk selalu kunjungi situs kami dan mengakses tautan Articles yang memuat kajian-kajian terkini kami dan Download yang berisi video-video pembalajaran, e-book hasil riset kami, dan alat-alat bantu yang berupa kertas-kertas kerja dan template yang selau kami kinikan.

Semua itu kami persembahkan untuk Anda!

ISOCENTER INDONESIA
The Ultimate ISO and Management System Resources

Thank You!

ISO Center Indonesia (Jakarta)

Permata Kuningan Building
17th Floor, HR Rasuna Said.
Kuningan Mulia, Menteng Atas,
Setia Budi, South Jakarta City,
Jakarta 12920

East Office (Surabaya)

AMG Tower Lantai 17,
Jl. Raya Dukuh Menanggal
No 1A, East Java, Gayungan
Surabaya, Indonesia 60234

Contact Us :

Website : https://isoindonesiacenter.com/
Email : admin@isoindonesiacenter.com
Telepon : +62 813-184-5942 (Sinthia - WhatsApp/Call)
+62 58-9002-6598 (Louqman – WhatsApp/Call)
+62 89-6551-88175 (Ardi - WhatsApp/Call)