ITSEC
SECURITY DELIVERED

Edisi 4

Desember 2024

ITSECBUZZ

MAJALAH KEAMANAN SIBER

Ratusan Hotel di Indonesia Jadi Korban Peretasan

Mengamankan Sistem Operation Technology

Chatbot Sebagai Pendamping Keamanan

Editor-in-chief:
M. Rasyid Sahputra

Penulis
Muhamad Fatah
Hutri Cika A.B.
Meyta Zenis
M.Adami Rayeuk
M. Alif R.
Irra Fachriyanthi
Z. Ananda

Design & Layout
Agung Prasetya
Z. Ananda

Illustrasi Komik
Cristyna

Properti Gambar:
AI Generated
Cristyna
ITSEC Asia
Freepik.com
Unsplash.com

Security is not a product, but a process.

Daftar Isi

Informasi

Mengamankan Sistem Operations Technology

Ditulis oleh Z. Ananda

Operations Technology (OT) menjadi kekhawatiran baru karena rentan terhadap serangan siber. Yang bikin berbahaya, kerugian yang ditimbulkan bisa berupa kerusakan fisik ataupun jiwa

Kita semua pasti sudah mengenal istilah Information Technology (IT), yang erat kaitannya dengan komputer, pemrosesan, dan penyimpanan data. Namun, di dunia industri, ada juga istilah Operations Technology (OT) yang lebih fokus pada perangkat keras dan aplikasi untuk mengendalikan komponen dalam menjalankan proses operasional. Selama bertahun-tahun, OT banyak dilakukan secara manual hingga akhirnya perlahan-lahan terintegrasi dengan IT.

Contoh Sistem OT

Ada banyak sistem OT yang mungkin Anda familiar, diantaranya:

1. Supervisory Control and Data Acquisition Systems (SCADA)
Sistem SCADA mengambil data dari sensor dan sistem input/output yang tersebar pada area operasional. Dari informasi yang didapat, perintah dikirimkan ke endpoint untuk mengeksekusi suatu proses. Sistem ini cukup sering ditemukan pada jaringan KRL, jaringan listrik dan aliran pipa.

2. Distributed Control Systems (DCS)
DCS dipakai untuk pengendalian dan pemantauan proses secara tersentral. Kalau SCADA cakupannya sangat luas, mengatur perpindahan dari satu titik ke titik lain. Sedangkan DCS lebih ke pengendalian proses yang berulang-ulang. Cukup sering dipakai pada proses manufaktur dan penyulingan, dimana kestabilan proses sangat dibutuhkan.

3. Sistem Medis
Mungkin belum banyak yang tahu, banyak peralatan medis di rumah sakit saling terkoneksi agar dapat mengatur atau memonitor secara tersentral. Contohnya alat MRI, pompa infus, EKG/ECG dan lain-lain.

4. Manajemen Gedung
Didalam gedung, banyak komponen yang dikendalikan secara tersentral. Sebagai contoh, sistem ventilasi dan pengaturan suhu (HVAC), akses pintu, sistem lift atau kamera CCTV.

Perbedaan Keamanan IT dan OT

Kedua istilah ini bisa dibilang berasal dari dua dunia yang berbeda. OT lebih terfokus pada industri, dengan teknologi yang mendukung proses operasional dan produksi. Mungkin Anda bisa membayangkan kapan satu mesin harus berjalan, kapan kran pipa harus dibuka atau kapan harus memindahkan satu barang dari mesin A ke mesin B. Semua itu diatur secara terpusat agar berjalan efektif dan efisien. Jika ada kegagalan dalam satu proses, bisa berdampak pada tujuan akhir. Dalam beberapa kasus, kegagalan ini bisa menimbulkan insiden fatal, seperti korban jiwa atau kerugian fisik. Meskipun jarang terjadi, dampaknya sangat besar. Itulah mengapa OT sangat mengutamakan keamanan, dan semua orang yang terlibat didoktrin sejak awal untuk selalu berhati-hati dan mengutamakan keselamatan diri sendiri, orang lain, dan seluruh fasilitas.

Di sisi lain, keamanan IT lebih fokus pada perlindungan data dan pergerakannya, memastikan data atau informasi rahasia tidak dicuri, diubah, atau diakses tanpa izin. Gangguan pada akses atau transmisi data dari titik A ke titik B bisa menyebabkan gangguan proses atau kerugian finansial. Karena IT selalu diperbarui secara rutin, titik kerentanannya pun terus berubah. Teknik penyerangan juga bervariasi, sehingga pengamanan IT harus dilakukan secara konstan. Sayangnya, ba- nyak pengguna IT tidak teredukasi dengan baik, menjadi kan mereka titik lemah dalam serangan.

Perbedaan	OT	IT
Produk	PLC, RTU, HMI	Router, Server, Cloud
Protokol	MODBUS, VNET, S7COMM	HTTP, HTTPS
Prioritas	Keselamatan dan *Complience*	Keamanan
Serangan	Jarang	Sering
Pembaruan	Terjadwal Tiap Tahun	Terjadwal Harian
Kerugian	Jiwa, Kerusakan, Finansial	Reputasi, Data Rahasia, Finansial

Perbedaan OT dan IT

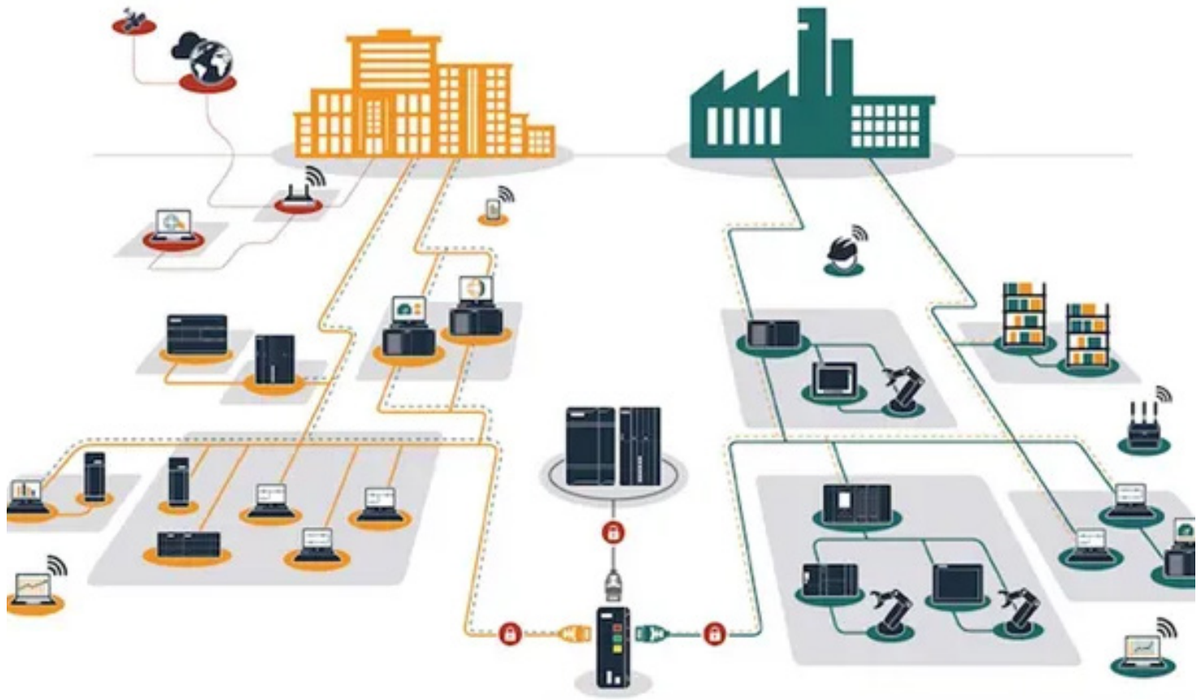
Resiko Keamanan OT

Jauh sebelum era internet, OT memiliki resiko serangan dari luar yang sangat kecil. Serangan lebih ke arah serangan fisik, menjadikan keamanan OT hanya berupa sterilisasi area. Tapi begitu era "komputer" tiba, sistem OT mulai terhubung dalam satu jaringan untuk mempermudah pengendalian dan pemantauan. Agar tetap aman, jaringan dibuat terisolasi dari jaringan lain dan internet. Resiko masih terbilang kecil, berupa serangan dari dalam.

Seiring berjalannya waktu, transformasi digital mulai menggantikan proses tradisional untuk membuat sistem OT lebih produktif, efisien dan hemat biaya. Untuk mencapai tujuan ini, analisis big data dan integrasi sistem enterprise diadopsi agar pengaturan dari hulu ke hilir bisa dilakukan dengan lebih baik. Ini berarti, sistem IT semakin banyak terintegrasi ke dalam OT, yang sayangnya juga meningkatkan risiko kerentanan terhadap akses yang tidak diinginkan. Dari sistem yang dulunya sepenuhnya terisolasi, kini menjadi sistem yang hampir mustahil untuk diisolasi sepenuhnya.

Yang menjadi permasalahan, lifespan peralatan pada sistem OT sangat panjang dan jarang ada pembaharuan, terutama dari sisi perangkat lunak. Akibatnya banyak yang masih menggunakan sistem operasi dan aplikasi yang sudah tidak ditunjang oleh si pembuat aplikasi. Begitu sistem ini terekspos ke "dunia luar", maka akan menjadi rentan terhadap serangan.

Tantangan lainnya adalah tidak banyak orang yang ahli di kedua bidang, IT dan OT. Orang IT yang memiliki pengetahuan dibidang pemrosesan dan pengamanan data belum tentu



Sinergi OT dan IT

Jenis Ancaman OT

Seperti yang dijelaskan diatas, awalnya ancaman OT hanyalah ancaman dari dalam, baik itu orang luar yang masuk ke dalam area OT atau pegawai internal yang melakukan serangan. Tapi begitu sudah terintegrasi dengan IT maka ancaman eksternal menjadi resiko baru. Sistem keamanan diperlukan agar tidak terjadi serangan IT dari luar dan berefek pada proses OT. Berikut adalah contoh serangan yang dapat terjadi pada sistem OT:

1. Malware/Ransomware

Baik itu menggunakan phishing, social engineering atau kerentanan pada OS dan jaringan untuk dapat mengakses OT sistem, serangan malware sangat berbahaya. Begitu malware berhasil masuk ke dalam jaringan OT maka banyak hal yang dapat dilakukan untuk mengganggu proses OT, mencuri atau memodifikasi data. Jenis serangan ini yang paling sering terjadi. Mungkin Anda masih ingat dengan Stuxnet yang menyerang SCADA pada reaktor nuklir milik Iran. Dianggap sebagai senjata digital yang pertama kali dipakai di dunia. Malware ini menyebar melalui USB drive yang dipakai oleh vendor luar. Ketika mereka terkoneksi ke jaringan SCADA, Stuxnet lansung melancarkan serangan dengan memanipulasi sistem pemantauan *centrifuge* dan menyerang sistem valve, menyebabkan tekanan berlebihan dan merusakan fisik dari *centrifuge*.

> **Centrifuge**
> Adalah tube silinder yang berputar pada kecepatan supersonik untuk memisahkan dua isotop, U235 dan U238 dari gas uranium. Proses ini dilakukan berulang-ulang hingga berhasil isotop U235 murni, yang akan dipakai untuk senjata atau pembangkit listrik tenaga nuklir.

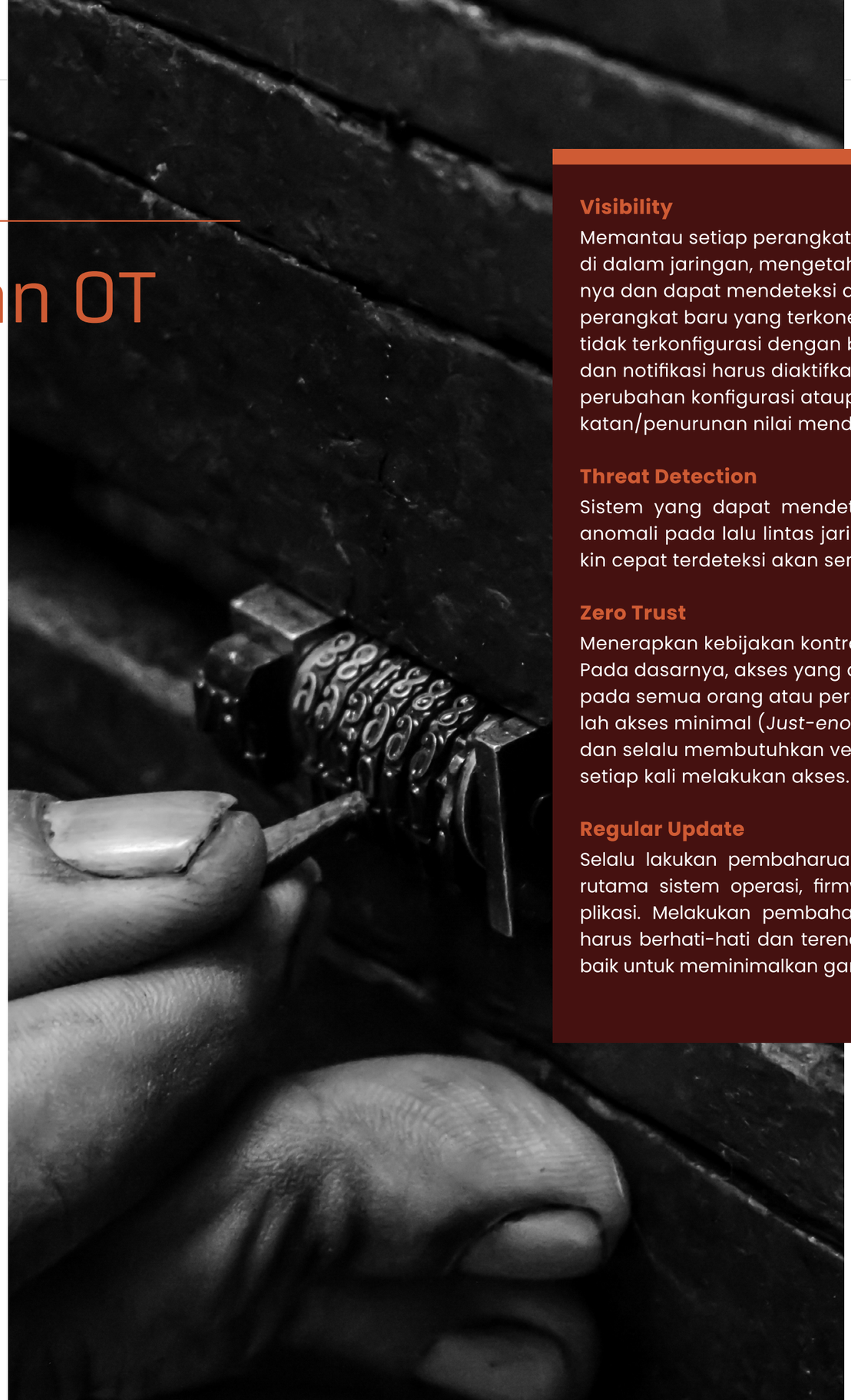
2. Man-in-the-middle Attack

Penyerang datang ke lokasi sistem OT, mengganggu dan memanipulasi komunikasi antara sistem kontrol dan perangkat. Contoh nyata terjadi di Turki tahun 2008. Dua orang berseragam ala militer mendatangi jalur pipa minyak yang membentang dari Baku, Azerbaijan ke Ceyhan, kota tepi laut di Turki. Dua orang itu berhasil menyusup melalui celah keamanan pada sistem CCTV. Setelah mereka mendapatkan akses ke jaringan, mereka menemukan komputer yang mengontrol sistem alarm. Mereka pun mengubah pengaturannya sehingga sistem alarm tidak berfungsi saat mereka meningkatkan tekanan pipa di atas batas normal.

3. Serangan Supply Chain

Kebanyakan OT dibangun atau dipelihara oleh vendor eksternal. Vendor bisa menjadi titik lemah apabila mereka lalai dalam menguatkan keamanan sistem mereka dan terkena serangan malware yang dapat mencuri data ataupun menularkan ke jaringan OT pihak klien. Jenis serangan ini pernah terjadi pada Danish State Railways, operator kereta di Denmark, pada tahun 2022. Insiden terjadi pada Supeo, vendor sistem aplikasi masinis yang mengharuskan mereka untuk menghentikan server selama beberapa waktu dan mengganggu jadwal kereta selama beberapa jam.

Mitigasi Serangan OT



Kolaborasi antara sistem OT (Operational Technology) dan IT (Information Technology) memang menciptakan peluang besar, tetapi juga membuka celah baru bagi ancaman siber. Penjahat siber bisa mencoba menembus sistem IT untuk kemudian melancarkan serangan terhadap sistem OT. Sebaliknya, mereka bisa meretas sistem OT untuk kemudian mengakses sistem IT. Serangan ini menunjukkan betapa pentingnya memiliki solusi keamanan yang komprehensif dan terpadu.

Solusi pengamanan yang efektif harus disesuaikan dengan kondisi lapangan, mengingat setiap lingkungan memiliki tantangan dan kebutuhan yang unik.

Kami mengumpulkan beberapa langkah yang Anda dapat lakukan untuk mengamankan sistem IT dan OT.

Visibility

Memantau setiap perangkat yang ada di dalam jaringan, mengetahui letaknya dan dapat mendeteksi apabila ada perangkat baru yang terkoneksi atau tidak terkonfigurasi dengan benar. Alarm dan notifikasi harus diaktifkan jika ada perubahan konfigurasi ataupun peningkatan/penurunan nilai mendekati batas.

Threat Detection

Sistem yang dapat mendeteksi adanya anomali pada lalu lintas jaringan. Semakin cepat terdeteksi akan semakin baik.

Zero Trust

Menerapkan kebijakan kontrol akses. Pada dasarnya, akses yang diberikan kepada semua orang atau perangkat adalah akses minimal (*Just-enough access*) dan selalu membutuhkan verifikasi ketat setiap kali melakukan akses.

Regular Update

Selalu lakukan pembaharuan sistem, terutama sistem operasi, firmware dan aplikasi. Melakukan pembaharuan ini pun harus berhati-hati dan terencana dengan baik untuk meminimalkan gangguan.

Pengamanan di setiap lapisan

Baik itu pengamanan fisik ataupun pengamanan pada end point dan jaringan seperti antivirus, firewall, protokol, enkripsi data, dll. Segmentasi jaringan juga dapat dipertimbangkan untuk mempersulit penyerang/malware mengakses seluruh sistem.

Pengaplikasian standar keamanan OT

Berikut standar yang paling banyak dipakai menurut suvery SANS OT/ICS Cybersecurity 2019.

1	38.1%	NIST CSF (Cybersecurity Framework)
2	32%	ISO 27000 series
3	31.4%	NIST 800-53
4	30.9%	NIST 800-82
5	30.4%	ISA/IEC 62443
6	29.9%	CIS Critical Security Controls
7	23.7%	NERC CIP
8	15.5%	GDPR
9	10.3%	C2M2 (Cybersecurity Capability Maturity Model)
10	8%	NIS Directive (EU)

Standar Keamanan OT

Cyberattack

Ratusan Hotel Di Indonesia Jadi Korban Peretasan

Ditulis oleh Z. Ananda

Pada 12 Agustus 2024, perhimpunan Hotel dan Restoran Indonesia (PHRI) mengungkapkan adanya peretasan profil Google Bisnis milik ratusan hotel di Indonesia.

Google Business Profile adalah fitur dari Google yang membantu pemilik bisnis agar terlihat di Google Search dan Google Maps. Di profil ini, pemilik bisnis dapat menampilkan informasi tentang produk atau layanan mereka, seperti alamat, nomor telepon, situs web, jam operasional, foto, dan video produk. Bahkan, ada fitur untuk berinteraksi dengan pelanggan melalui fitur tanya/jawab dan merespons ulasan.

Anda bisa memandang Google Business Profile seperti etalase toko Anda. Profil ini akan muncul ketika pengguna Google melakukan pencarian atau melihat di Google Maps. Dengan informasi yang lengkap, diharapkan bisnis Anda dapat menarik lebih banyak pelanggan.

Seperti akun lainnya, akun Google Business juga rentan terhadap peretasan. Para penjahat siber semakin canggih dalam menemukan celah keamanan, meskipun penyedia layanan telah memiliki sistem keamanan yang baik. Oleh karena itu, peran pengguna sangat penting agar kontrol keamanan berfungsi maksimal.

Kasus peretasan akun Google Business pada beberapa hotel di Indonesia dapat berdampak buruk dan merusak reputasi bisnis mereka. Banyak korban mengalami kerugian finansial dan, yang lebih serius, menurunnya tingkat kepercayaan pelanggan.

Pada kasus ini, penjahat siber berhasil meretas akun Google Business milik hotel dan menambahkan nomor WhatsApp (WA) palsu ke bagian nama bisnis, deskripsi, atau tanya jawab. Setelah nomor palsu ditambahkan, mereka menunggu hingga ada korban yang menghubungi nomor tersebut. Sayangnya, banyak korban yang tanpa curiga menghubungi nomor tersebut. Dengan diiming-imingi diskon besar, korban akhirnya terjebak hingga melakukan reservasi dan pembayaran.

Bagaimana Peretasan Terjadi?

Ada beberapa taktik dalam mengeksploitasi Google Business, tapi pada kasus ini ada tiga kemungkinan.

1. Meretas akun dan kepemilikan dari profil Google Business.

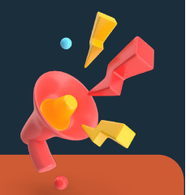
Peretasan akun bisa dilakukan dengan berbagai cara. Mungkin Anda sudah tahu tentang teknik phishing, social engineering, atau masalah keamanan kata sandi yang lemah. Tujuannya adalah mendapatkan nama akun pengguna dan kata sandi dari profil Google Business, lalu mengubah informasinya.

2. Klaim profil.

Ada cara lain untuk mengakses profil Google Business, yaitu dengan mengklaim profil bisnis sebagai milik seseorang. Beberapa skenario yang mungkin terjadi:

Bisnis yang belum memiliki profil Google Business.
Penjahat siber bisa membuat profil bisnis palsu menggunakan akun mereka dan mengklaim sebagai pemiliknya. Kemudian mereka menambahkan informasi sesuai keinginan.

Profil yang sudah ada, tetapi belum berpemilik. Google dapat membuat profil secara otomatis dengan mengumpulkan informasi dari ber-



WhatsApp (WA) adalah aplikasi pesan instan yang sangat populer. Dengan WA, kita bisa mengirim pesan langsung atau melakukan panggilan telepon melalui koneksi data.

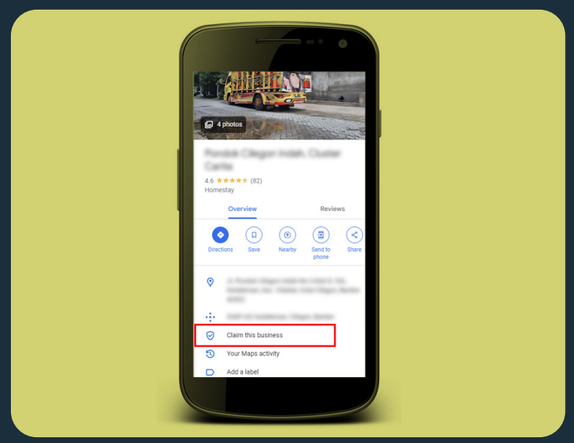
bagai sumber. Namun, karena profil ini bukan dibuat oleh pemilik bisnis, siapa pun bisa mengklaimnya melalui situs Google Business.

Profil yang sudah ada, tetapi belum berpemilik.

Google dapat membuat profil secara otomatis dengan mengumpulkan informasi dari berbagai sumber. Namun, karena profil ini bukan dibuat oleh pemilik bisnis, siapa pun bisa mengklaimnya melalui situs Google Business.

Mengubah kepemilikan.

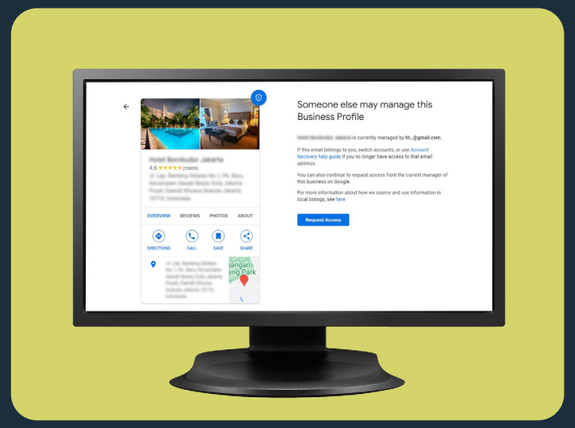
Kepemilikan profil Google Business bisa diubah dengan menekan tombol “Request Access” di situs Google Business. Setelah itu, kita bisa meminta akses sebagai pengelola atau pemilik. Pemilik profil saat ini akan menerima notifikasi untuk menyetujui permintaan akses. Jika pemilik lengah dan menyetujui tanpa konfirmasi, kepemilikan profil bisa berpindah



Menu "Request Access" untuk meminta akses sebagai pengelola/pemilik

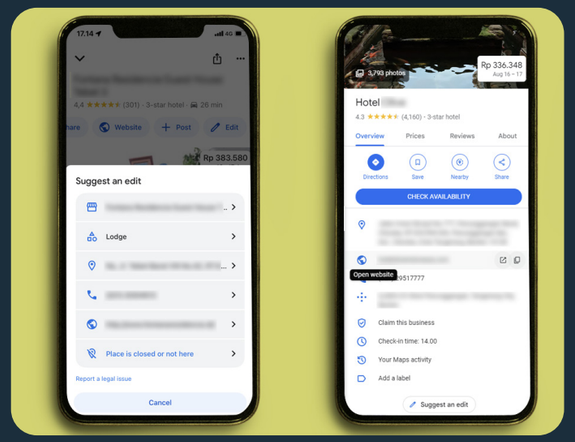
3. Permintaan Perubahan Informasi.

Pada Google Business, ada opsi “Suggest an Edit” yang memungkinkan pengguna mengajukan perubahan pada profil bisnis yang belum diverifikasi oleh pemiliknya. Permintaan perubahan ini akan ditinjau oleh tim Google,



Menu "Request Access" untuk meminta akses sebagai pengelola/pemilik

dievaluasi, dan diverifikasi sebelum diterima atau ditolak. Meskipun kita tidak mengetahui proses review secara detail, ini bisa menjadi celah bagi penjahat siber untuk mengubah informasi pada profil Google Business.



Menu "Suggest an Edit" untuk meminta perubahaan informasi

Pencegahan

Agar terhindar dari serangan siber semacam ini, pemilik bisnis sebaiknya mengambil tindakan proaktif untuk melindungi profil Google Business mereka. Salah satu langkah penting adalah mengaktifkan *two-factor authentication* (2FA). Fitur ini menambah lapisan keamanan untuk mencegah peretasan akun. Selain itu, karena Google masih menggunakan proses yang sama—memperbolehkan orang lain meminta perubahan informasi—pemilik bisnis harus rutin memantau profil Google Business agar dapat mengembalikan informasi yang benar jika terjadi perubahan yang tidak diinginkan.

Selain itu, sebisa mungkin, sebarkan informasi tentang risiko ini agar pemilik bisnis dan calon pelanggan lebih berhati-hati. Kasus ini menunjukkan bahwa banyak hotel, termasuk yang bukan berbintang, mengalami peretasan. Ini membuktikan bahwa serangan siber tidak memandang status. Kita harus sadar bahwa siapa pun bisa menjadi target serangan. Kepedulian dalam mengamankan sistem harus menjadi bagian dari rutinitas sehari-hari kita.

Informasi

GDPR: Ketika Hak Data Pribadi Dilindungi

Ditulis oleh Irra Fachriyanthi

Privasi adalah hak, bukan kemewahan

Beberapa hari yang lalu, saya menerima pemberitahuan dari Instagram saat sedang menikmati sore di Copenhagen, Denmark. Pesan tersebut mengumumkan sesuatu yang menarik: mulai 12 November 2024, ***Meta***—perusahaan induk Instagram dan Facebook—memperkenalkan aturan baru bagi pengguna di Uni Eropa. Kami, pengguna di wilayah ini, kini diberikan dua pilihan: Pertama, berlangganan untuk pengalaman tanpa iklan, dengan biaya tertentu. Kedua, menggunakan layanan gratis, tetapi data pribadi kami tetap digunakan untuk menargetkan iklan, meskipun dalam bentuk yang lebih terbatas.

Langkah ini adalah respons langsung Meta terhadap dua regulasi besar Uni Eropa, yaitu GDPR (General Data Protection Regulation) dan DMA (Digital Markets Act). Apabila DMA mengatur perusahaan besar agar lebih transparan dan adil terhadap pengguna, termasuk soal pemrosesan data, maka GDPR menitikberatkan pada perlindungan data pribadi dan memberikan kontrol lebih besar kepada individu atas data mereka. Lebih jelasnya mari kita bahas tentang GDPR dan apa dampaknya di Indonesia, yuk!

Apa itu GDPR?

GDPR atau General Data Protection Regulation adalah peraturan perlindungan data pribadi yang berlaku di Uni Eropa sejak Mei 2018. GDPR bertujuan untuk melindungi privasi individu dengan memberikan kontrol lebih besar terhadap data pribadi mereka, serta menetapkan standar ketat bagi organisasi yang mengumpulkan, menyimpan, dan memproses data. Meski berlaku di Uni Eropa, efek GDPR meluas hingga ke luar Uni Eropa, termasuk Indonesia, terutama bagi perusahaan atau individu yang berurusan dengan data warga Uni Eropa.

Mengapa GDPR Penting untuk Diketahui?

Meskipun GDPR adalah undang-undang Uni Eropa, dampaknya dirasakan secara global karena dua hal utama:

1. Efek Ekstrateritorial

GDPR berlaku untuk semua organisasi yang menawarkan barang atau jasa kepada warga Uni Eropa (baik gratis maupun berbayar). Juga bagi perusahaan yang memproses data warga Uni Eropa, terlepas dari lokasi organisasi tersebut. Contohnya, e-commerce di Indonesia yang menjual produk ke pelanggan di Uni Eropa harus mematuhi GDPR.

2. Standar Perlindungan Data Global

GDPR telah menjadi standar emas untuk perlindungan data di seluruh dunia. Banyak negara, termasuk Indonesia, mulai mengadopsi prinsip serupa dalam undang-undang privasi mereka, seperti UU Perlindungan Data Pribadi (UU PDP) di Indonesia yang mulai berlaku pada 2022.

Kegagalan mematuhi GDPR dapat menyebabkan denda besar, hingga 20 juta euro atau 4% dari pendapatan tahunan global perusahaan, tergantung mana yang lebih besar.

Pada Juli 2021, Amazon menerima denda sebesar 746 juta euro (sekitar 12 triliun rupiah) dari otoritas perlindungan data Luksemburg karena menggunakan data pelanggan untuk sistem iklan tertarget tanpa persetujuan.

Apa dampak GDPR di Indonesia?

Berikut adalah dampak GDPR yang relevan bagi individu dan perusahaan di Indonesia:

1. Untuk Perusahaan di Indonesia

Jika bisnis Anda mengumpulkan data pribadi dari warga Uni Eropa, Anda harus mematuhi GDPR, yaitu memastikan ada dasar hukum untuk memproses data (seperti persetujuan pengguna). Selain itu harus ada transparansi yaitu menjelaskan tujuan pengumpulan data dalam kebijakan privasi yang jelas dan mudah dipahami. Juga menerapkan langkah-langkah teknis untuk melindungi data dari kebocoran atau akses tidak sah. Jangan lupa memberikan hak kepada pengguna seperti mengakses, menghapus, atau mengoreksi data mereka.

2. Untuk Pengguna di Indonesia

Sebagai pengguna layanan dari perusahaan Eropa, Anda mendapatkan hak tambahan:

- **Hak Privasi:** Perusahaan harus meminta persetujuan sebelum mengumpulkan data Anda.
- **Hak Akses:** Anda dapat meminta informasi tentang data apa saja yang dikumpulkan dan untuk tujuan apa.
- **Hak Lupa:** Anda dapat meminta perusahaan untuk menghapus data Anda (right to be forgotten).

Apa yang Bisa Dilakukan Perusahaan di Indonesia?

Mengingat besarnya denda yang diberikan bila melanggar GDPR maka perusahaan di Indonesia yang mengumpulkan data warga Uni Eropa segera melakukan audit data. Identifikasi data pribadi yang Anda kumpulkan, simpan, dan proses. Pastikan data tersebut memiliki dasar hukum sesuai dengan GDPR. Jangan lupa gunakan enkripsi, firewall, dan langkah-langkah keamanan lainnya untuk melindungi data dari kebocoran.

Langkah selanjutnya segera perbarui kebijakan privasi yang harus mencakup detail tentang pengumpulan, penggunaaan, dan perlindungan data pengguna. Dan tidak kalah pentingnya adalah melatih karyawan dengan cara mengedukasi tim tentang pentingnya perlindungan data dan prosedur GDPR untuk mengurangi resiko pelanggaran.

Mengapa GDPR Relevan untuk Masa Depan?

Dengan dunia yang semakin digital dan terhubung, perlindungan data menjadi isu utama. Undang-undang seperti GDPR menetapkan standar untuk menangani data dengan lebih bertanggung jawab, dan tren ini terus berkembang.

Indonesia, melalui UU PDP, mulai mengikuti langkah ini untuk memastikan warga negara terlindungi dari penyalahgunaan data. Oleh karena itu, memahami GDPR bukan hanya relevan bagi perusahaan yang berbisnis lintas negara, tetapi juga membantu masyarakat lebih sadar akan hak privasi mereka.

GDPR adalah langkah besar dalam melindungi data pribadi, dan meskipun diterapkan di Uni Eropa, dampaknya meluas hingga ke Indonesia. Bagi perusahaan di Indonesia yang berurusan dengan data warga Uni Eropa, kepatuhan terhadap GDPR bukanlah pilihan, melainkan kewajiban.

Sebagai individu, memahami GDPR membantu kita mengenali hak-hak privasi kita, bahkan saat menggunakan layanan global. Di era digital ini, privasi adalah aset yang harus kita lindungi bersama.

Cyber Risk

Kisah “Sweet Bobby” dan Bahaya Catfishing di Era Digital

Di balik layar, siapa saja bisa jadi apapun atau siapa pun

Ditulis oleh Irra Fachriyanthi

Bayangkan kamu menjalin hubungan hampir satu dekade dengan seseorang yang tampak sempurna—penuh perhatian, romantis, dan seolah-olah benar-benar “the one.” Kamu berbicara dengannya setiap hari, berbagi cerita, mimpi, dan cinta, hanya untuk suatu hari menyadari... orang itu tidak pernah ada.

Inilah yang terjadi pada Kirat Assi, seperti yang diceritakan dalam podcast dokumenter terkenal “Sweet Bobby” yang kemudian diangkat ke layar Netflix . Selama lebih dari 10 tahun, Kirat percaya bahwa ia menjalin hubungan dengan pria bernama Bobby, seorang dokter sukses yang hangat dan penyayang. Tapi ternyata, Bobby hanyalah identitas palsu yang diciptakan oleh seseorang dalam lingkaran sosialnya sendiri. Pelaku ini dengan sengaja menciptakan narasi rumit untuk memanipulasi Kirat dan mengontrol hidupnya.

Kisah ini bukan sekadar cerita sedih, tetapi pengingat betapa bahayanya catfishing—praktik menipu orang dengan identitas palsu secara daring.

Apa Itu Catfishing?

Catfishing adalah ketika seseorang menciptakan persona palsu untuk menipu orang lain secara online. Tujuannya bisa macam-macam: dari kepuasan emosional, manipulasi psikologis, sampai keuntungan finansial. Modus ini sering terjadi di media sosial, aplikasi kencan, atau bahkan dalam percakapan pribadi seperti chat atau email.

Yang bikin ngeri, pelaku catfishing biasanya sangat pintar memanfaatkan emosi korban. Mereka bisa menciptakan cerita yang meyakinkan, sehingga sulit bagi korban untuk melihat kebenarannya—seperti yang dialami Kirat di “Sweet Bobby”.

Kenapa Catfishing Bisa Terjadi?

Ada beberapa alasan kenapa orang bisa terjebak dalam catfishing:

Kepercayaan pada Identitas Digital
Di zaman sekarang, kita sering kali terlalu percaya pada apa yang kita lihat di layar, tanpa berpikir untuk memverifikasi.

Eksploitasi Emosi
Pelaku tahu cara memanfaatkan kerentanan korban, misalnya kesepian atau keinginan untuk merasa dicintai.

Kurangnya Pertemuan Langsung
Kalau semua komunikasi hanya terjadi secara online, lebih mudah bagi pelaku untuk terus menyembunyikan kebohongannya.

Dampak Catfishing?

Seperti yang dialami Kirat, dampak catfishing itu tidak main-main. Selain kehilangan waktu dan energi emosional, korban sering merasa trauma, malu, dan kesulitan mempercayai orang lain. Bahkan, hubungan sosial dan profesional mereka juga bisa terganggu.

Pelajaran dari Kisah “Sweet Bobby”

Kisah ini mengajarkan beberapa hal penting yang bisa jadi tameng kita dari catfishing:

Skeptis Itu Penting
Jangan langsung percaya pada seseorang yang kamu kenal secara online, apalagi kalau ada hal-hal yang terasa tidak masuk akal.

Waspadai Red Flags
Misalnya, kalau mereka selalu punya alasan untuk tidak bisa video call atau ketemu langsung. Cerita yang tidak konsisten atau permintaan uang juga patut dicurigai.

Verifikasi Itu Perlu
Misalnya, pakai pencarian gambar terbalik untuk mengecek apakah foto mereka asli atau hanya diambil dari internet.

Bagaimana Melindungi Diri?

Platform digital sebenarnya punya peran besar untuk membantu memerangi catfishing, misalnya dengan sistem verifikasi identitas. Tapi di sisi lain, kita juga harus lebih waspada. Jangan gampang percaya, selalu cross-check informasi, dan tidak ada salahnya minta pendapat orang terdekat kalau kamu mulai merasa ada yang janggal.

Kasus “Sweet Bobby” adalah contoh nyata betapa bahayanya hubungan online kalau kita tidak hati-hati. Dunia digital itu mempermudah banyak hal, tapi juga membuka peluang untuk manipulasi seperti ini. Jadi, selalu ingat untuk skeptis, waspada, dan tidak segan-segan mengecek ulang kalau ada yang terasa tidak beres. Karena di balik layar, siapa pun bisa menjadi apa saja.

Cyber Fact!

Salah satu contoh catfishing yang terkenal lainnya adalah kasus Manti Te’o, seorang pemain sepak bola dari Universitas Notre Dame. Pada tahun 2012, terungkap bahwa Te’o telah terlibat dalam hubungan online dengan seorang wanita bernama Lennay Kekua, yang dia klaim sebagai kekasihnya. Namun, setelah penyelidikan, terungkap bahwa Lennay Kekua sebenarnya tidak ada. Identitasnya adalah seorang pria yang menciptakan persona palsu untuk memanipulasi Te’o secara emosional. Kasus ini menjadi sorotan besar di media dan dianggap sebagai salah satu contoh catfishing yang paling terkenal.

Teknologi

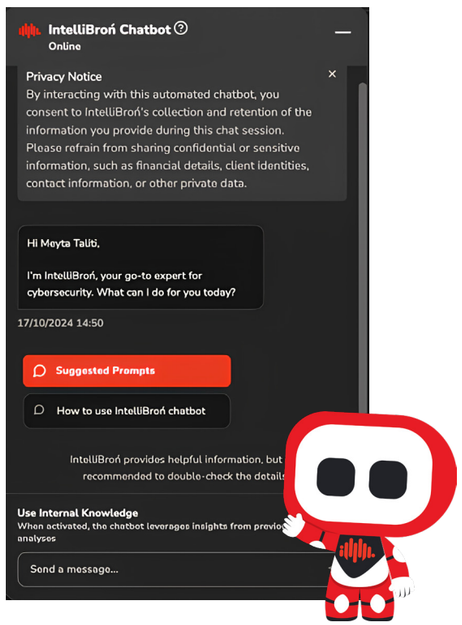
Chatbot Sebagai Pendamping Keamanan

Dapatkah mesin bekerja lebih baik daripada kita?

Ditulis oleh :
Meyta Zenis (Researcher, LinkedIn)
M. Alif R. (Researcher, LinkedIn)
M. Adamy Rayeuk (Backend Developer, LinkedIn)

Meskipun ramalan ini mungkin terdengar menakutkan, saya yakin bahwa mesin memiliki potensi luar biasa untuk mengungguli manusia dalam pekerjaan tertentu. Kata "tertentu" perlu digaris-bawahi. Menurut saya, Mesin dapat mengungguli manusia pada jenis tugas-tugas yang memerlukan penilaian obyektif berdasarkan parameter yang telah ditentukan sebelumnya. Salah satu pekerjaan yang sesuai kriteria tersebut adalah pekerjaan yang memerlukan repetisi. Sebagai contoh, chatbot customer service, dimana fitur chatbot dipakai untuk menjawab pertanyaan-pertanyaan yang sering ditanyakan oleh pelanggan. Chatbot dapat menjawab pertanyaan karena sudah dilatih dengan dataset yang dikumpulkan sebelumnya oleh manusia.

Chatbot ini memiliki berbagai fungsi yang dapat diterapkan di berbagai bidang. Dalam artikel ini, kita akan menjelajahi pengembangan AI percakapan atau chatbot, yang dirancang khusus untuk mendukung keamanan siber. Chatbot ini bertujuan untuk memberikan dukungan penting dalam menjaga aset digital tetap aman.



Retrieval-Augmented Generation (RAG) Chatbot

LLM

(Large Language Model) adalah jenis model kecerdasan buatan yang dirancang untuk memahami, menghasilkan, dan memproses bahasa manusia dalam skala besar.

Ada banyak jenis chatbot yang didukung oleh AI, namun kali ini kita akan membahas tentang Retrieval-Augmented Generation (RAG) Chatbot. RAG adalah teknik inovatif yang menggabungkan metode berbasis pencarian (retrieval) dan generatif untuk menghasilkan respons yang lebih akurat dan relevan. Metode berbasis retrieval menelusuri database teks yang ada untuk menemukan informasi yang sesuai dengan kueri tertentu. Sementara itu, model generatif menciptakan konten baru berdasarkan input pengguna menggunakan teknik seperti pra-pelatihan dan pembelajaran mendalam. Dengan memanfaatkan sumber pengetahuan eksternal, RAG mampu memberikan tanggapan yang lebih komprehensif dan informatif.

Ada tiga komponen penting dari RAG yang akan bahas lebih dalam pada artikel ini.

1. Embedding

Mari kita mulai dengan Embedding, salah satu bagian penting dari Large Language Models (LLM). Embeddings adalah proses mengubah teks menjadi vektor numerik atau angka-angka yang merepresentasikan maknanya. Angka-angka ini ditempatkan dalam "ruang" besar di mana kata-kata dengan makna serupa akan diletakkan berdekatan. Misalnya pada gambar Figure 2 dijelaskan ada kata 'man' dan 'woman.' Meskipun kedua kata ini tidak sama, mereka memiliki konotasi yang sebanding. Oleh karena itu, dalam dunia vector embedding, representasi vektor kedua kata tersebut dapat ditempatkan di ruang vektor yang berdekatan. Inilah yang disebut dengan 'semantic retrieval' —proses menemukan makna yang terkait dalam ruang semantik yang luas.

Kami menggunakan model Embedding untuk membantu model LLM (Large Language Model) memahami dan memproses data yang kompleks. Model Embedding ini adalah algoritma yang dirancang untuk mengompresi informasi menjadi representasi yang padat dalam ruang

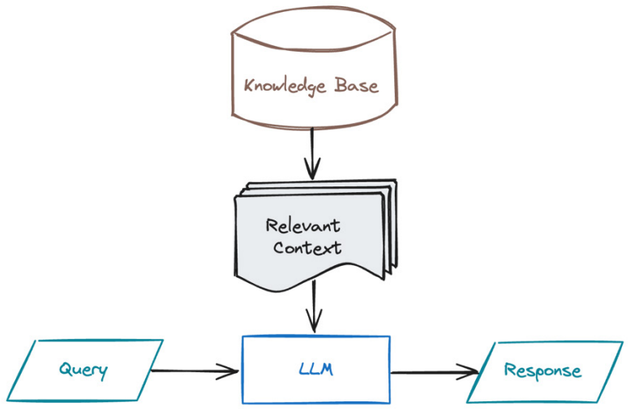


Figure 1. Diagram RAG workflow

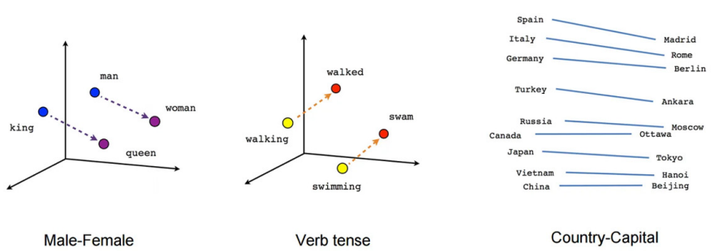


Figure 2. Word2Vec embeddings, Hubungan linear

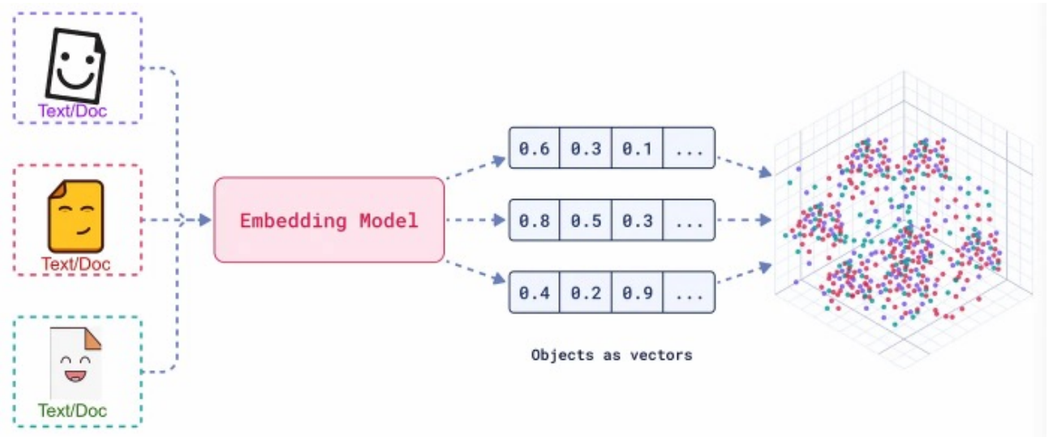


Figure 3. Bagaimana embedding bekerja

multidimensi.

Dengan kata lain, model Embedding membuat vektor berukuran tetap yang merepresentasikan teks dan berfokus pada makna semantik dari pekerjaan atau tugas, terutama membandingkan teks guna menemukan kesamaan arti.

2. Database

Nah, data vektor ini kan banyak sekali. Pastinya perlu database untuk menyimpannya. Disinilah bantuan Database Vektor dibutuhkan.

Vector Database

Dirancang khusus untuk menyimpan dan mencari vektor secara efisien. Vektor adalah representasi numerik dari data yang memiliki dimensi tertentu. Database ini memungkinkan model pembelajaran mesin untuk mengingat dan memproses masukan sebelumnya, mendukung berbagai kasus penggunaan seperti penelusuran, rekomendasi, dan pembuatan teks. Dengan mengidentifikasi data berdasarkan metrik kesamaan daripada pencocokan persis, model komputer dapat memahami data secara kontekstual dan memberikan hasil yang lebih relevan.

> **Database**
>
> adalah kumpulan data yang terstruktur dan terorganisir sehingga mudah diakses, dikelola, dan diperbarui. Data dalam database biasanya disusun dalam tabel, yang memungkinkan penyimpanan informasi dalam format yang teratur.

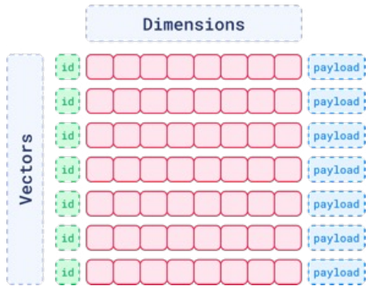


Figure 4.Representasi vector pada database.

No SQL Database

Database vektor dioptimalkan untuk menyimpan dan mengambil data vektor dengan efisien, sedangkan database tanpa SQL dirancang untuk menangani data tidak terstruktur. Data tidak terstruktur adalah informasi yang tidak memiliki model atau format tetap, membuatnya sulit dikelola oleh database konvensional. Namun, data tidak terstruktur memiliki potensi besar untuk aplikasi AI, pembelajaran mesin, dan mesin pencari modern. Dalam kasus penggunaan kami, kami menggabungkan berbagai data teks tidak terstruktur ke dalam basis pengetahuan kami, termasuk laporan, faktur, catatan, email, dan keluaran dari berbagai aplikasi produktivitas. Tantangan berikutnya adalah mengambil informasi relevan yang berbasis konteks sebagai jawaban atas pertanyaan pengguna.

3. Metode Retrieval Relevant Context

Metode Relevant Context Retrieval memungkinkan model RAG menghasilkan respons yang lebih relevan secara kontekstual. Hal ini memungkinkan model untuk memahami perintah secara lebih holistik, sehingga menghasilkan respon yang lebih akurat dan koheren.

Mari kita lihat cara kerjanya di figure 5.

Setelah memiliki cukup pengetahuan, kami ingin mesin ini menjawab pertanyaan kami berdasarkan informasi yang telah kami berikan.
Pertama, kami mencari database NoSQL kami untuk menemukan 5 dokumen paling relevan dengan permintaan pengguna. Setelah itu, kami mengonversi perintah pengguna dan kelima dokumen tersebut menjadi representasi vektor. Dengan menggunakan vektor-vektor ini,

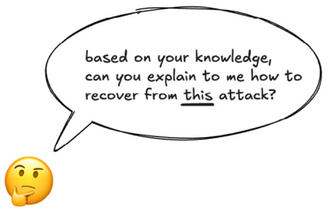


Figure 5. Contoh user prompt

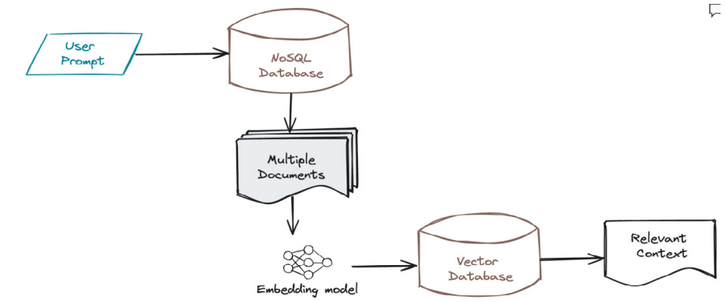


Figure 6. Metode Retrieval Relevant Context

kami menelusuri basis data vektor kami untuk memfilter hasil dan mengambil konteks yang paling relevan lihat figure 7.

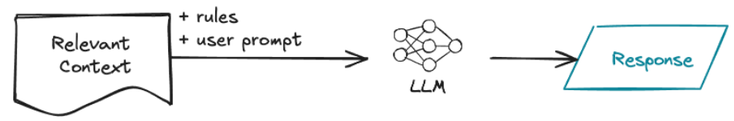
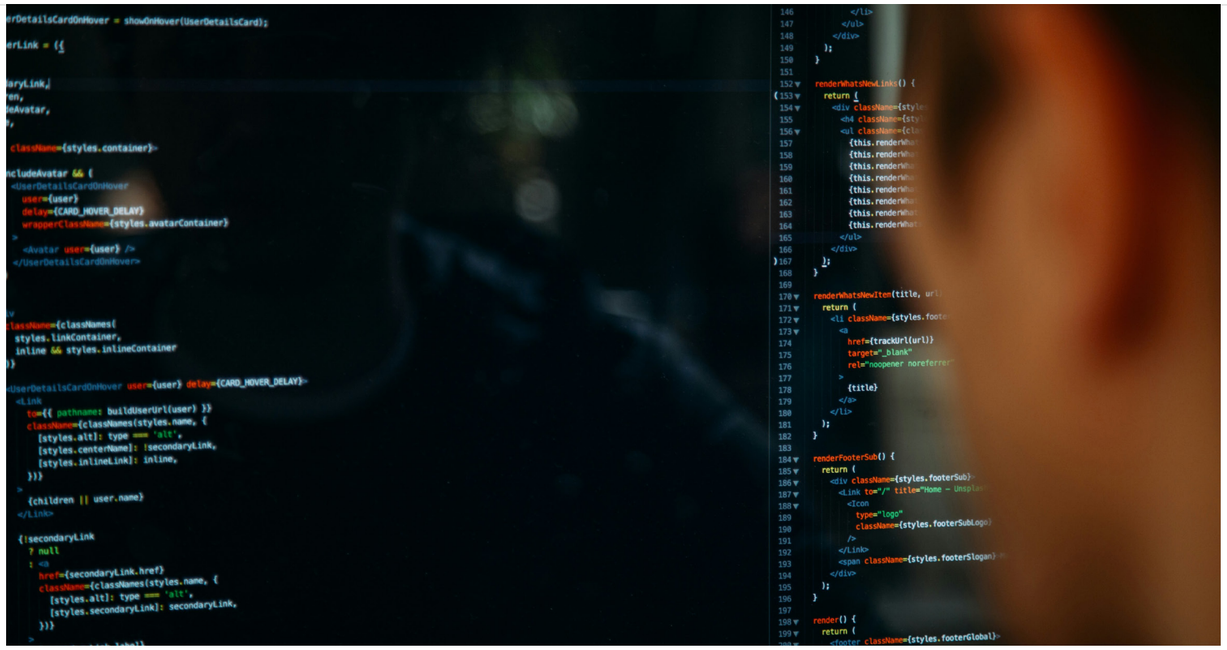


Figure 7. Menghasilkan respon berdasarkan konteks yang relevan

> ***Chatbot Sebagai Pendamping Keamanan***
>
> Dengan kemampuan AI chatbot, kita dapat memperoleh informasi dengan cepat dan tepat terkait topik yang kita butuhkan. Bayangkan jika AI chatbot digunakan untuk keperluan khusus seperti keamanan siber dalam lingkungan Security Operation Center (SOC).
>
> Saat seorang analis SOC menerima peringatan, AI chatbot dapat memberikan panduan langsung tentang cara merespons serangan siber menggunakan strategi Mitre Attack, atau membekali mereka dengan pembelajaran dari skenario serangan siber di dunia nyata. Dengan demikian, AI chatbot secara signifikan meningkatkan kemampuan kita dalam menangani ancaman keamanan lebih efektif, sekaligus membantu analis keamanan memahami dan menanggulangi ancaman tersebut dengan lebih baik.



DevSecOps

Peran Penting Frontend Developer Dalam Keamanan Siber

Ditulis oleh Muhamad Fatah

Dalam dunia yang semakin terhubung secara digital, keamanan IT mulai menjadi prioritas utama dan menjadi tanggung jawab semua pihak. Keamanan IT melibatkan berbagai jenis perlindungan untuk menjaga integritas, kerahasiaan, dan ketersediaan sistem dan data dari ancaman. Beberapa jenis keamanan IT yang cukup sering kita temukan adalah keamanan jaringan, keamanan data, keamanan endpoint dan keamanan aplikasi.

Penggunaan firewall dan sistem deteksi intrusi adalah salah satu cara melindungi jaringan. Access control dan enkripsi data cukup sering kita temukan untuk melindungi data. Untuk melindungi endpoint, kita biasanya menggunakan antivirus agar komputer dan handphone kita aman dari ancaman siber. Untuk keamanan aplikasi, pengamanan dilakukan sejak developer melakukan pengkodean.

Keamanan dari sisi Frontend Developer

Dunia pemrograman terdiri dari berbagai jenis developer yang masing-masing memiliki keahlian khusus dalam ber-

UI (User Interface) adalah bagian dari aplikasi yang berinteraksi lansung dengan pengguna.

bagai aspek pengembangan aplikasi. Salah satu peran yang krusial adalah Frontend Developer, yang bertanggung jawab untuk mengembangkan User Interface (UI) dari sebuah aplikasi atau situs web. Namun, peran mereka tidak hanya terbatas pada menciptakan tampilan yang menarik dan interaktif.

Peran frontend developer dalam menjaga keamanan aplikasi sangat vital. Mereka berfungsi sebagai benteng pertama dalam melindungi aplikasi dari berbagai serangan siber. Frontend developer memastikan bahwa semua input dari pengguna divalidasi dan disanitasi dengan benar. Ini adalah langkah penting untuk mencegah serangan injeksi seperti SQL Injection dan Cross-Site Scripting (XSS), yang dapat membahayakan data dan sistem aplikasi.

Dengan pengetahuan dan keterampilan yang tepat, frontend developer dapat mengenali potensi celah keamanan dan mengimplementasikan langkah-langkah untuk menutup celah tersebut.

Sebagai contoh, kita ingin membuat sebuah situs web dengan fitur forum, di mana pengguna bisa mengetik dan mengubah gaya penulisan mereka, seperti menggunakan huruf tebal, miring, atau membuat judul. Katakanlah kita hanya menggunakan kode seperti berikut:

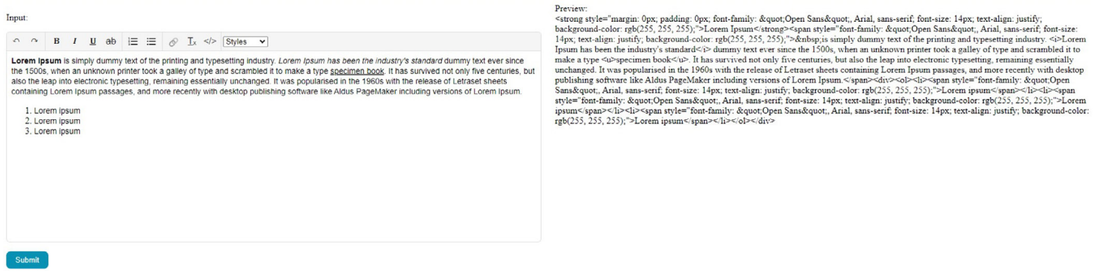


Figure 1

XSS, atau Cross-Site Scripting

adalah jenis serangan keamanan web di mana penyerang menyisipkan kode berbahaya ke dalam situs web yang kemudian dieksekusi oleh browser pengguna. Serangan ini memungkinkan penyerang untuk mencuri data, mencuri sesi, mengubah konten, atau melakukan tindakan berbahaya lainnya.

(html)

Setelah pengguna mengetik di kotak komentar dan mengirimkan hasil ketikannya untuk diposting, tampilan yang muncul terlihat seperti pada figure 1.

Sangat berantakan sekali bukan? Tidak hanya teks yang diketik oleh pengguna yang muncul, tetapi juga potongan kode pemformatan teks ber-

campur. Jadi, bagaimana solusinya agar teks yang diketik oleh pengguna dapat ditampilkan sesuai dengan format yang mereka inginkan? Salah satu solusinya adalah dengan menggunakan atribut ***dangerouslySetInnerHTML*** dari HTML. Atribut ini memungkinkan kita menyuntikkan markup HTML secara langsung ke dalam output yang dirender oleh komponen."

```
<div dangerouslySetInnerHTML={{__html:
html}} />
```

hasil yang didapat dari penggunaan atribut diatas lihat figure 2:

Sudah sesuai kan? Tapi sayangnya jika kita menggunakan ***dangerouslySetInnerHTML*** website yang kita buat juga menjadi rentan terhadap serangan XSS (Cross Site Scripting). XSS adalah eksploitasi keamanan di mana penyerang menempatkan malicious client-end code ke laman web. Sebagai contoh, seorang hacker dapat memasukkan skrip untuk memunculkan notifikasi palsu di halaman tersebut lihat pada figure 3.

Anda pasti pernah menemukan pop-up alert yang muncul ketika membuka situs. Sangat mengganggu kan? Dengan skrip yang dimasukkan oleh peretas, apakah mereka hanya sebatas memunculkan pop-up error? Tentu tidak. Seperti di figure 4, peretas juga bisa menambahkan "perintah" untuk membuka tab baru yang mengarah ke alamat situs yang mereka inginkan. Dari situs tersebut, peretas bisa menyusupkan malware ke dalam komputer Anda.

Untuk mengamankan atribut ***dangerouslySetInnerHTML*** kita harus menyaring output website dengan menghapus atau mengganti karakter atau elemen yang bisa berpotensi menimbulkan bahaya. Hal ini dapat dilakukan dengan menggunakan fungsi atau library yang tersedia, seperti ***DOMPurify*** yang dirancang untuk mencegah serangan XSS dengan "membersihkan" kode HTML dari elemen yang berbahaya, seperti <, >, “, ‘, &, script, img, iframe, dan lain-lain.

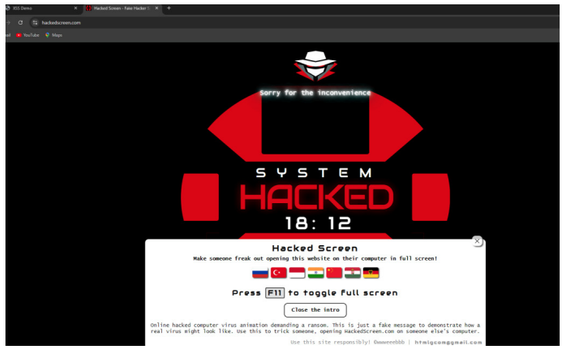


Figure 4

Mari kita coba menggunakan ***DomPurify*** (lihat pada figure 5).

```
<div dangerouslySetInnerHTML={{__html:
DOMpurify.sanitize(html)}} />
```

Setelah berhasil menerapkan ***DOMPurify***, setiap input berbahaya dari pengguna akan difilter seperti contoh pada figure 6, tanpa merusak input yang tidak berbahaya. Jika kita lihat pada Inspect Element, ***DOMPurify.sanitize*** menghapus onError didalam tag <img /> tersebut sehingga input berbahaya tidak di eksekusi oleh browser

Figure 7. Hasil dalam Inspect Element

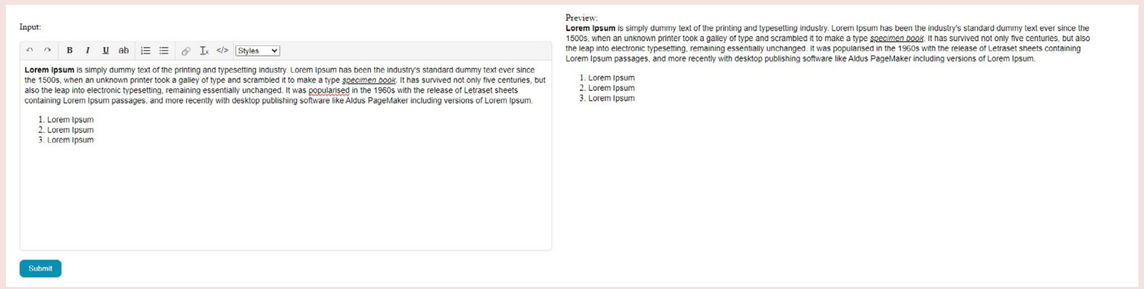


Figure 2

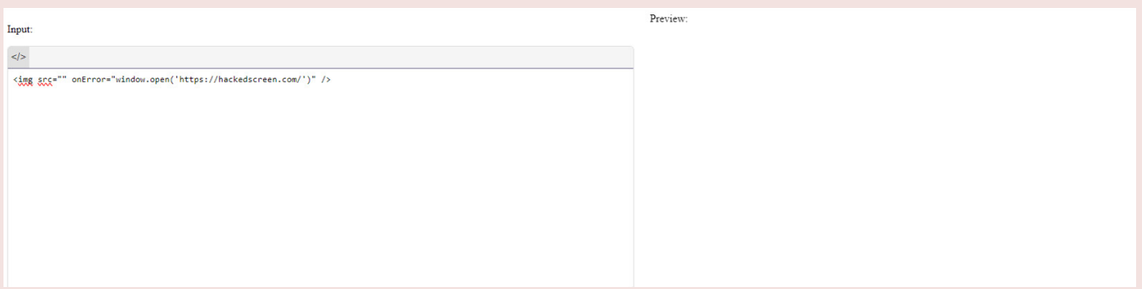


Figure 5

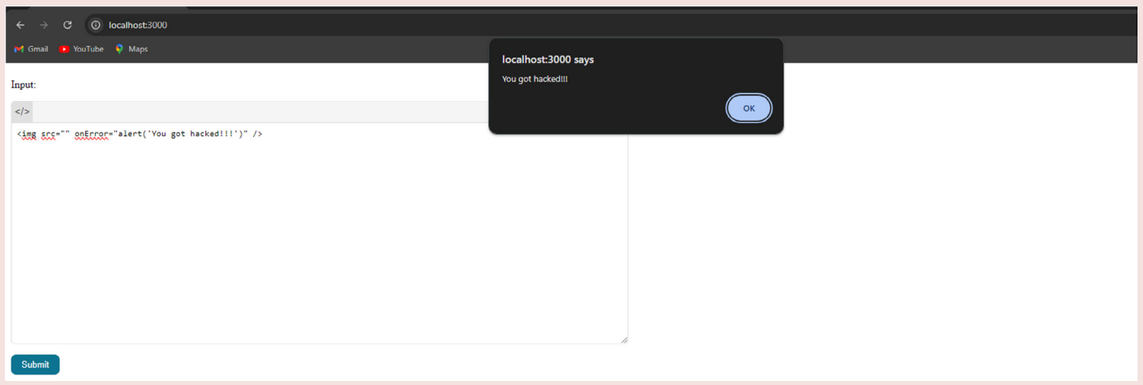


Figure3

Figure 6

Inspect Element

Adalah alat yang tersedia pada browser yang memungkinkan pengembang web dan pengguna untuk melihat dan mengedit HTML dan CSS dari sebuah halaman web secara langsung serta melakukan debugging javascript.

Penutup

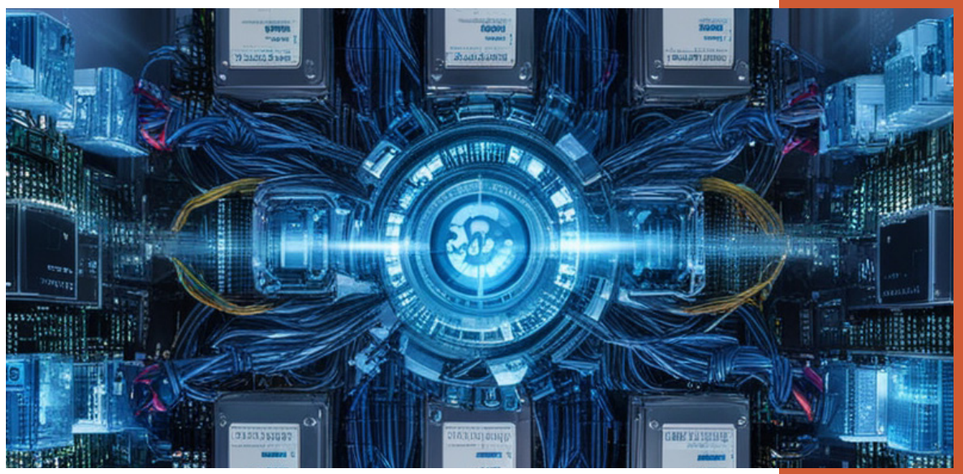
Dalam dunia pengembangan aplikasi, memiliki pengetahuan mendalam tentang keamanan IT adalah aset yang sangat berharga bagi setiap developer. Memastikan keamanan aplikasi sejak tahap awal pengkodean tidak hanya mencegah kerugian besar di kemudian hari, tetapi juga membangun kepercayaan pengguna terhadap produk yang dihasilkan.

Dengan pemahaman tentang keamanan IT, para developer dapat memilih skrip dan atribut yang tepat untuk menutup celah kerentanan yang mungkin muncul dari source code yang mereka buat. Misalnya, mereka bisa menerapkan teknik validasi input yang ketat untuk mencegah serangan seperti SQL Injection dan *Cross-Site Scripting* (XSS).

Lebih dari itu, praktik terbaik dalam pengembangan aplikasi melibatkan pengujian keamanan pada setiap tahap pengembangan, mulai dari tahap perencanaan hingga sebelum aplikasi dirilis ke publik. Melakukan penilaian keamanan secara berkala memastikan bahwa tidak ada titik lemah yang dapat dieksploitasi oleh penjahat siber. Pengujian ini bisa melibatkan teknik seperti penetration testing dan code review untuk mengidentifikasi dan memperbaiki kerentanan keamanan.

Akhirnya, dengan melakukan pendekatan keamanan yang proaktif, developer tidak hanya melindungi data dan privasi pengguna, tetapi juga menjaga integritas dan reputasi organisasi. Langkah-langkah ini memastikan aplikasi tidak hanya fungsional dan menarik, tetapi juga aman dari ancaman yang semakin canggih di dunia maya.

Penulis adalah seorang frontend developer di divisi R&D, ITSEC Asia.



Profil

UX Writer: Menjembatani Teknologi dengan Pengguna Awam

"Perspektif awam saya menjadi kekuatan, bukan kelemahan. Justru itu yang membantu saya memahami kebutuhan pengguna"

Ditulis oleh Hutri Cika A. B (LinkedIn) & Irra Fachriyanthi

Masuk ke dunia cybersecurity untuk pertama kalinya adalah pengalaman yang menantang bagi Hutri Cika. Sebagai seseorang dengan latar belakang komunikasi dan media - Cika adalah lulusan dari UGM (Universitas Gadjah Mada) jurusan Ilmu Komunikasi - dia merasa seperti "atlet lari yang tiba-tiba dilempar ke ring tinju." Dunia ini terasa asing, penuh dengan istilah teknis, dan dikelilingi oleh para profesional yang sudah sangat paham dengan ekosistemnya. Namun, tantangan itu justru menjadi peluang bagi Cika untuk memberikan kontribusi dengan caranya sendiri sebagai seorang UX Writer.

Bekerja di Industri yang Didominasi Laki-Laki

Salah satu hal yang langsung mencolok bagi Cika saat bergabung dengan tim Research & Development (R&D) di ITSEC Asia adalah dominasi laki-laki. "Rasanya seperti tersesat di sekolah khusus laki-laki, di mana obrolan dan interaksi sehari-hari memiliki nuansa yang maskulin," kenangnya. Data dari Linkedin per Mei 2024 menunjukkan hanya 17,9% tenaga kerja di industri ini adalah perempuan, sementara 82,1% lainnya laki-laki.

Sebagai seorang woman in tech, Cika mengakui ada perasaan terintimidasi yang

sulit dihindari, terutama di bidang cybersecurity yang masih sangat teknis. “Istilah women in tech memang semakin sering terdengar, tapi kalau kita bicara women in cybersecurity, bebannya terasa jauh lebih berat,” ungkapnya.

Menghadapi Kendala Bahasa Teknologi

Sebagai UX Writer, tugas utama Cika adalah menyederhanakan bahasa teknis agar mudah dipahami oleh pengguna. Tantangan ini menjadi nyata saat ia harus memahami istilah-istilah seperti “XDR”(Extended Detection and Response) atau “alerts” yang digunakan oleh para engineer di timnya.

“Diskusi dengan tim R&D sering kali membuat saya bingung. Otak saya seperti kamus yang harus menambah entri baru setiap hari,” ujarnya sambil tertawa. Namun, justru di sinilah peran kreatifnya menjadi sangat penting: menyeimbangkan pemahaman teknis dengan kreativitas untuk menciptakan pesan yang intuitif bagi pengguna awam.

Contohnya, alih-alih menulis pesan seperti “Unauthorized access detected: Error code 0x800...”, Cika akan memilih pendekatan yang lebih manusiawi, seperti “Kami mendeteksi upaya akses tidak valid. Jangan khawatir, semua langkah keamanan telah diaktifkan.”

“Apakah Kamu Hacker?”

Sebagai seseorang yang bekerja di dunia cybersecurity, Cika sering menghadapi reaksi kekaguman sekaligus kebingungan dari orang-orang sekitarnya. Biasanya akan terlontar kalimat “Wah, cybersecurity? Keren!” Lalu diikuti pertanyaan seperti, “Kamu hacker, ya?” atau “Bisa bantu pulihkan akun media sosial saya yang diretas?” Dengan senyuman, Cika akan menjelaskan bahwa perannya bukan sebagai hacker, melainkan sebagai UX Writer.

“Tugas saya adalah memastikan alat-alat keamanan siber ini terasa ramah dan mudah digunakan oleh siapa saja,” katanya menjelaskan kerjanya sebagai UX Writer di dunia cybersecurity. Ia mencontohkan bagaimana desain komunikasi yang baik bisa membuat sistem yang rumit menjadi lebih intuitif, membantu profesional cybersecurity bekerja lebih cepat dalam merespons ancaman.

Belajar Beradaptasi di Dunia Baru

Pengalaman hadir di acara cybersecurity menjadi tantangan tersendiri bagi Cika. Berada di tengah-tengah para pemain besar di industri ini sering kali membuatnya bertanya, “Harus mulai dari mana?” Namun, ia tidak menyerah. Ia terus belajar, bertanya, dan perlahan menemukan cara untuk memahami konteks yang ada.

Cika percaya bahwa meskipun ia datang dari latar belakang non-teknis, perspektifnya yang berbeda justru menjadi kekuatan. “Cybersecurity bukan hanya tentang melindungi jaringan atau menghentikan peretas. Ini juga tentang menciptakan alat yang membuat pekerjaan lebih mudah bagi profesional di bidang ini,” jelasnya.

Pesan untuk Pemula

Bagi Cika yang meniti karirnya dari SEO (Search Engine Optimization) writer, berada di dunia cybersecurity sebagai orang dengan latar belakang non-teknis memang menantang, tetapi juga penuh potensi. Ia percaya bahwa siapa pun bisa berkontribusi di industri ini, asalkan mau belajar dan tidak takut untuk bertanya.

“Jangan merasa kecil hati kalau kamu tidak berasal dari jalur yang sama. Justru perspektif unik kita yang akan membawa inovasi baru di industri ini,” pesannya.

Hutri Cika adalah bukti bahwa bahkan di industri yang rumit seperti cybersecurity, ada ruang bagi mereka yang memiliki tekad untuk belajar dan berkontribusi. Melalui perannya sebagai UX Writer, ia terus menjembatani teknologi dengan pengguna, memastikan bahwa setiap orang merasa aman dan percaya diri dalam menggunakan alat-alat keamanan digital.

Apa itu UX Writing?

UX writing adalah penulisan teks pada antarmuka digital untuk memandu dan memudahkan pengguna dalam berinteraksi dengan produk. Teks ini mencakup tombol, menu, notifikasi, pesan error, dan elemen lainnya.

Contoh Microcopy di dunia cybersecurity:

“Add IP addresses to map into network segments.”

“Case submitted as Completed and ready to be closed!”

ITSEC™
SECURITY DELIVERED

PT. ITSEC Asia
Noble House, Level 11
jakarta, Indonesia 12950

+62 (21) 29783050

contact@itsecasia.com

itsec.asia