MAGAZINE

PUNGGAWA CYBERSECURITY

PUNGGAWA.COM

NOV 2026 / VOLUME 09



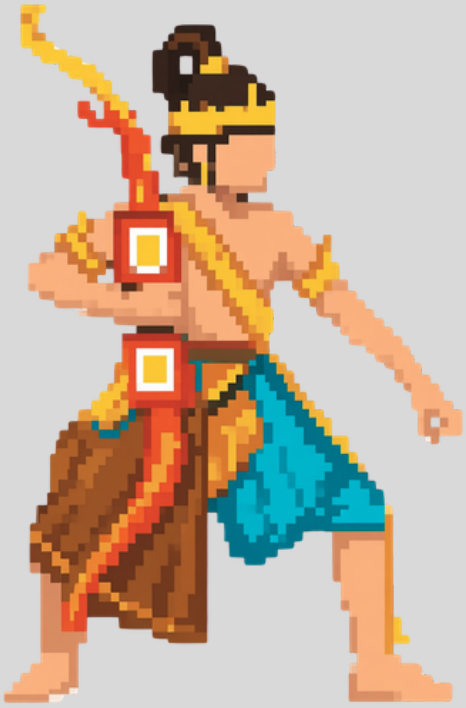
THE MODERN CYBER BATTLEFIELD

How Threats, Attackers, and Defenses are Evolving

Publisher PUNGGAWA cybersecurity

TENTANG KAMI

PUNGGAWA CYBERSECURITY merupakan istilah dari kebudayaan Indonesia yang mengacu pada sosok pemimpin atau figur berwibawa yang terkenal akan kepemimpinannya, tanggung jawabnya, dan arahannya dalam suatu komunitas. Istilah ini melambangkan dedikasi terhadap keunggulan kepemimpinan, praktik etik, atribut kekuatan, kearifan, dan kepercayaan, serta sikap melindungi terhadap mereka yang berada dalam lingkup pengawasannya.



Kami Adalah Tim Punggawa

Tim Punggawa didirikan pada tahun 2018 dan mulai memberikan layanan kepada pelanggan pada tahun 2019, dimulai dengan layanan ***penetration testing***. Kami telah berhasil menembus pasar keamanan siber di Indonesia. Dalam kemitraan dengan klien, kami menyediakan solusi dan layanan keamanan siber yang dirancang untuk meningkatkan postur keamanan secara komprehensif, menutup celah, dan memantau kerentanan secara berkelanjutan melalui operasi dan dukungan yang berkelanjutan dengan mengimplementasikan identifikasi, perlindungan, deteksi, respons, dan pemulihan.

VISI

Menjadi mitra pilihan utama di bidang keamanan siber sebagai bentuk berkontribusi nyata dalam mewujudkan dunia yang lebih aman dalam transformasi digital.

MISI

MENGHADIRKAN HASIL TERBAIK
Dengan dukungan tim yang andal dan dedikasi tinggi pada proses yang tepat, kami menghadirkan solusi yang memberikan kesuksesan nyata bagi klien kami.

MEMBANGUN BUDAYA BELAJAR DAN KESADARAN
Kami senantiasa menumbuhkan budaya untuk terus belajar dan meningkatkan kesadaran (*awareness*) di dalam internal tim kami.

BERBAGI DAN BERKOLABORASI BERSAMA KOMUNITAS
Kami mengedepankan semangat kerja sama yang kuat, baik sebagai satu tim yang solid di dalam organisasi maupun sebagai mitra bagi komunitas yang lebih luas.

CORE VALUE, QALBU



Quick and High Quality Response

Dalam keamanan siber, respons yang cepat terhadap ancaman sangat krusial. Di **PUNGGAWA**, kami mengutamakan aksi cepat untuk mengidentifikasi dan meredakan ancaman siber, memastikan aset digital klien terlindungi secara efisien dan efektif. Respons berkualitas tinggi juga berarti memberikan solusi yang menyeluruh dan berpengetahuan luas terhadap tantangan keamanan siber yang kompleks.

Attitude is Everything

Sikap positif dan proaktif sangat penting di **PUNGGAWA**. Hal ini melibatkan usaha untuk selalu mendahului ancaman potensial, antusiasme untuk belajar tentang tren keamanan baru, dan memelihara ketahanan mental menghadapi ancaman siber yang terus berkembang. Sikap yang berorientasi pada peningkatan berkelanjutan esensial dalam beradaptasi dengan dinamika keamanan siber.

Listen, Learn, Lead & Succeed

Nilai ini menekankan pentingnya pembelajaran berkelanjutan dalam bidang keamanan siber. Dengan mendengarkan secara aktif kebutuhan klien dan perkembangan industri, tim **PUNGGAWA** tetap terdepan dan terinformasi. Pembelajaran ini berujung pada kepemimpinan di bidangnya, yakni pengembangan solusi

Be a Problem Solver

Keamanan siber sering kali tentang memecahkan teka-teki kompleks yang dihadirkan oleh ancaman siber. Di **PUNGGAWA**, kami menekankan pentingnya pendekatan yang berorientasi pada solusi, baik dalam mengatasi serangan siber yang rumit, menavigasi kerentanan jaringan yang kompleks, atau menemukan solusi kreatif untuk tantangan keamanan baru.

Unity is Our Strength

Kami memahami tantangan kewirausahaan dan mengetahui bahwa keamanan siber memerlukan kerja sama tim dan kolaborasi, baik di dalam organisasi maupun dengan klien, mitra, dan komunitas keamanan siber yang lebih luas. Kesatuan dalam tujuan dan aksi menjamin pertahanan yang lebih kuat terhadap ancaman siber dan postur keamanan yang lebih tangguh.

KATA PENGANTAR

Salam hangat para pembaca setia Punggawa Cybersecurity Magazine,

Selamat datang di **Punggawa Cybersecurity Magazine Volume 9.** Melalui tema **"THE MODERN CYBER BATTLEFIELD"**, edisi ini mengajak kita melihat bagaimana ancaman, penyerang, dan pertahanan terus berevolusi. Medan tempur siber kini melintasi identitas digital, aplikasi, layanan cloud, hubungan dengan pihak ketiga, hingga perangkat yang menjaga proses fisik tetap berjalan.

Perubahan tersebut menuntut cara pandang yang lebih menyeluruh. Kepercayaan terhadap sebuah sertifikat, ketepatan distribusi patch, dan **kesiapan menghadapi perkembangan AI** sama pentingnya dengan kemampuan membuktikan sebuah temuan keamanan. Pembahasan tentang eMudhra, krisis PHP2Shell, proyeksi ancaman menuju 2030, dan VulnVerify Skills mengingatkan kita bahwa keputusan pertahanan harus **bertumpu pada konteks serta bukti** yang dapat diperiksa.

Edisi ini juga membawa perhatian kita pada infrastruktur yang sering luput dari pengawasan. Insiden freezer di Prancis serta perbedaan prioritas antara IT dan OT menunjukkan bahwa **dampak serangan tidak berhenti pada kerahasiaan data**. Ketersediaan layanan, keberlangsungan proses, dan keselamatan manusia harus menjadi bagian dari pertimbangan keamanan sejak awal.

Di sisi tata kelola, pelindungan data pribadi dan kisah NusaForm di AWS memperlihatkan pentingnya pengelolaan akses, konfigurasi yang tepat, serta tanggung jawab yang jelas. Teknologi perlu berjalan bersama disiplin operasional agar risiko dapat **dikenali dan ditangani sebelum meluas**.

Sebagai penutup, dua artikel tentang SOC menghubungkan kemampuan mendeteksi dengan ketepatan mengambil tindakan. **Banyaknya perangkat dan notifikasi belum cukup**. Nilai pertahanan terletak pada kemampuan membaca jejak, menghubungkan bukti, memvalidasi ancaman, dan mengoordinasikan respons yang sesuai dengan kebutuhan organisasi.

Kami berharap Volume 9 menjadi bahan refleksi dan diskusi bagi para profesional keamanan, praktisi teknologi, akademisi, serta pengambil kebijakan. Semoga setiap artikel membantu pembaca membangun pertahanan yang lebih tangguh, terukur, dan relevan dengan medan tempur siber modern.

Selamat Membaca!

Iwan Setiawan
CEO PUNGGAWA CYBERSECURITY

DAFTAR ISI

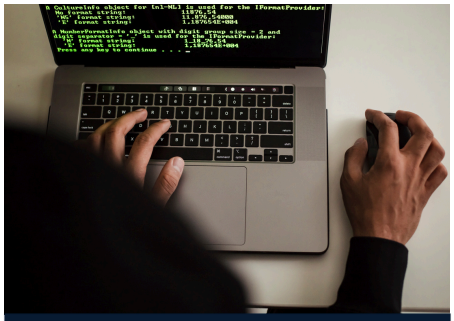
PUNGGAWA
VOLUME 09



IDENTITAS & KEPERCAYAAN



INFRASTRUKTUR & KESELAMATAN



DETEKSI & RESPONS

07 **Medan Tempur Siber Modern:**
Bagaimana Ancaman, Penyerang, dan Pertahanan Terus Berevolusi
Pakde Iwan

12 **Namaste:**
CA-nya eMudhra, Key-nya eMudah Ditebak
Zharfanug

20 **Ketika Patch Jadi Peta Serangan:**
Mengurai Krisis PHP2Shell dan Runtuhnya Embargo CVD
Om Fadhil

24 **The Next Cyber Battlefield:**
What AI Predictions Tell Us About 2030
Alda

29 **Memverifikasi Temuan Pentest dengan VulnVerify Skills**
Kang Ali

36 **Saat Freezer Dipanaskan dari Jauh:**
Serangan Siber di Prancis dan Kerapuhan Infrastruktur yang Terlupakan
Pakde Iwan

42 **IT vs OT:**
Ketika Prioritasnya Bukan Lagi Kerahasiaan Data, tapi Keselamatan Manusia
Pakde Iwan

49 **Dari Insiden Siber ke Kepatuhan:**
Memahami Arah Baru Pelindungan Data Pribadi
Mas Mirza

53 **NusaForm AWS:**
Cerita Startup yang Hampir Kehilangan Data User
Om Tony

61 **Serangan Sudah Masuk, Apakah Kita Menyadarinya?**
Bang Javi

67 **From Alert to Action:**
Seni Membaca Threat di Tengah Banjir Notifikasi Cyber
Farah

EDITORIAL TEAM

Editor-in-Chief
Om Fadhil

Managing Editor
Mba Zakiah

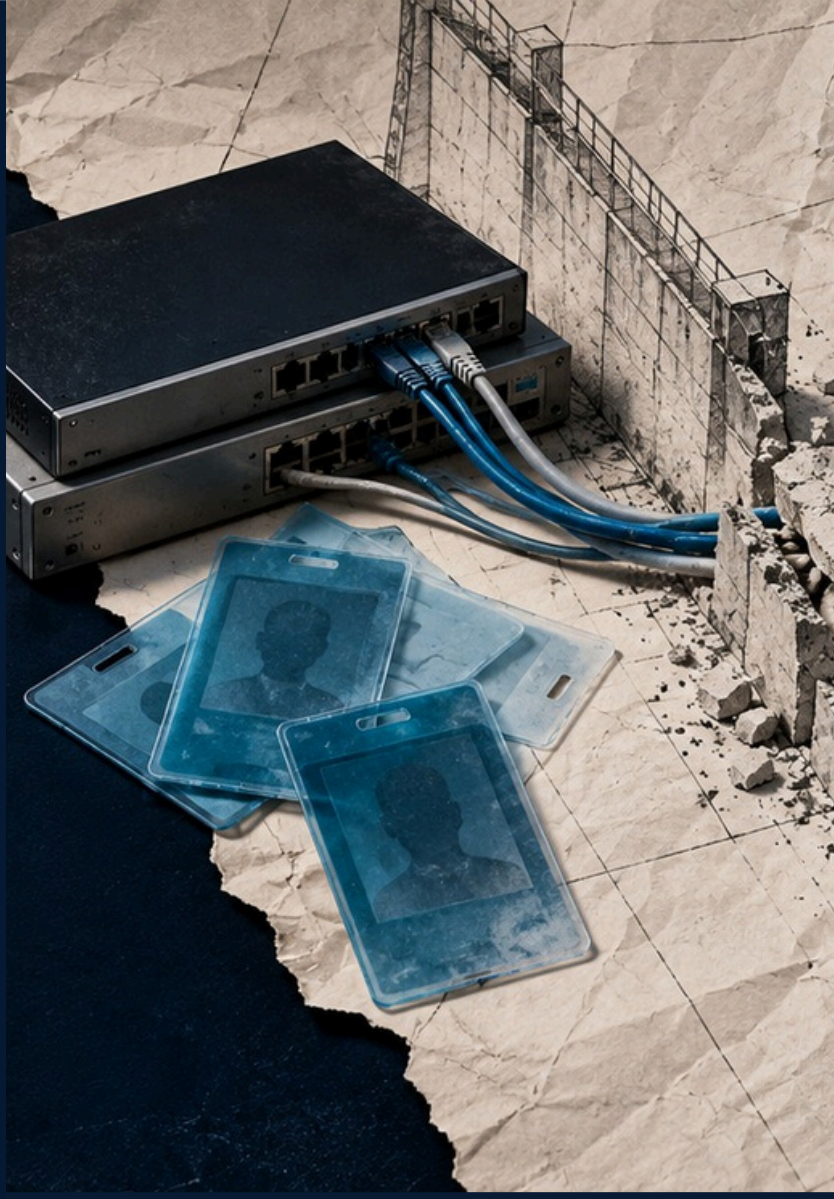
Contributors
Pakde Iwan
Zharfanug
Om Fadhil
Alda
Kang Ali
Mas Mirza
Om Tony
Bang Javi
Farah



MEDAN TEMPUR SIBER MODERN

Bagaimana Ancaman, Penyerang, dan Pertahanan Terus Berevolusi

BY PAKDE IWAN



Ilustrasi konseptual: identitas, perangkat, dan batas kepercayaan.

Ketika Perimeter Lenyap

Selama puluhan tahun, keamanan siber dibayangkan seperti benteng: ada tembok, ada gerbang, ada penjaga. Namun, data tahun ini menunjukkan gambaran tersebut sudah tidak sesuai dengan kenyataan. Untuk pertama kalinya dalam 19 tahun, laporan Verizon menunjukkan bahwa celah (*vulnerability*) pada perangkat lunak yang menjadi awal 31% kasus kebocoran data melampaui password curian sebagai pintu masuk terbanyak. Mandiant mencatat bahwa jeda antara pelaku pertama membuka akses dan menyerahkannya kepada kelompok lain menyusut dari lebih dari delapan jam pada 2022 menjadi 22 detik pada 2025. Menurut **CrowdStrike**, penyerang kriminal rata-rata hanya butuh 29 menit untuk berpindah dari komputer pertama yang mereka kuasai ke komputer lain di jaringan (*breakout time*), dan yang tercepat hanya 27 detik.

Penyerang kini tak perlu meretas benteng. Mereka masuk melalui perangkat yang terlupakan, akun valid, vendor terpercaya, hingga AI agent. **Editorial ini menegaskan satu hal: tembok pertahanan sudah runtuh.** Yang tersisa hanyalah rantai kepercayaan antara identitas, aplikasi, dan pemasok. Pertahanan modern harus berfokus pada ketahanan siber (***cyber resilience)***—mendeteksi ancaman dengan cepat, menekan dampak kerusakan, dan memulihkan sistem secara efektif.



Identitas: Pintu yang Paling Sering Dibuka

Benteng pertahanan modern tak lagi berbentuk fisik, melainkan identitas. Kegagalan mengamankan satu identitas berdampak besar. **Kebocoran satu akun berdampak sangat fatal:** data menunjukkan 52,2% kasus penyusupan melalui akun sah terbukti berlanjut pada pencurian kredensial tambahan secara berantai.

Caranya pun berubah. Penipuan lewat telepon (vishing) kini menjadi cara masuk terbanyak kedua dalam investigasi Mandiant (11%), sementara phishing lewat email turun dari 14% menjadi 6%. Telepon sulit dihadang oleh filter otomatis, dan menurut Microsoft, 93% panggilan vishing berhasil menahan korban cukup lama untuk memulai pengelabuan.

Penyerang juga menyasar prosedur, bukan hanya *password*. *Help desk* dibujuk lewat telepon, lalu token login yang masih berlaku dipanen sehingga *multi-factor authentication* (MFA) tidak pernah diminta. **Bahkan 'karyawan' pun bisa dipalsukan:** CrowdStrike melaporkan kelompok Korea Utara memakai persona buatan AI untuk menyusup ke perusahaan. **Pertanyaannya bukan lagi 'apakah password kita cukup kuat', melainkan 'bisakah kita memastikan orang di seberang sesi memang berhak berada di sana'.**



Celah di Perangkat dan Pemasok yang Terlupakan

Eksploitasi celah bukan hanya soal jumlahnya, tetapi soal lokasinya. Mandiant mencatat kelompok canggih bisa bersembunyi lama di *edge device* seperti *firewall* dan VPN, yang umumnya tidak dipantau. **Pada kasus *backdoor* BRICKSTORM, penyerang bertahan rata-rata 393 hari, jauh melampaui masa simpan log yang lazim, yaitu 90 hari.**

Banyak perangkat juga dibobol sebelum pabrikan sempat merilis patch: CrowdStrike mencatat 42% celah dieksploitasi sebelum diumumkan ke publik. VulnCheck menemukan bahwa 42,5% celah edge device yang dieksploitasi pada 2025 menimpa perangkat yang sudah *end-of-life* (tidak lagi didukung pabrikan), dan hanya 23,7% tercatat di katalog resmi CISA.

Risiko serupa membayangi *cloud* dan *supply chain*. Verizon mencatat kebocoran via pihak ketiga melonjak 60% hingga mencapai 48% dari kasus. Kasus Anthropic membuktikan serangan siber berbasis AI agent mampu memanen 2.100 token Azure AD milik 40 perusahaan hanya dalam 34 jam. **Pelajarannya jelas: kita wajib memetakan izin aplikasi, token, dan kunci akses vendor.**

“Bukan sekadar mendata aset, petakan jejaring kepercayaannya!”

AI: Mempercepat, Namun Belum Mengubah Segalanya

Celah berkembang cepat; audit dan pembaruan patch berkala adalah kuncinya.

Kita perlu realistis. Mandiant menegaskan bahwa peretasan data belum disebabkan langsung oleh AI, melainkan masih dipicu oleh kelalaian manusia dan celah sistem. Data Verizon pun menunjukkan hal serupa, meski CrowdStrike mencatat aktivitas peretas yang memanfaatkan AI telah melonjak 89%.

Bukti terbaru semakin mengkhawatirkan. Pada November 2025, Anthropic melaporkan peretas asal Tiongkok memakai Claude Code untuk mengeksploitasi 30 target, dengan porsi bantuan AI sebesar 80–90% dari operasi. Meski beberapa pakar meragukan klaim ini karena minimnya indikator teknis, laporan September 2026 mengonfirmasi bahwa penggunaan AI oleh peretas individual hingga negara membuat identifikasi pelaku makin kabur. **Poin kuncinya: bukti ini berasal dari pengembang model yang melaporkan produknya sendiri, sehingga belum sepenuhnya diverifikasi oleh pihak independen.**

Di sisi pertahanan, Anthropic menyatakan modelnya mampu melampaui semua manusia kecuali yang paling ahli dalam menemukan celah keamanan, sehingga **hambatan kini ada pada pemeriksaan dan pemasangan patch, bukan penemuan**. Sementara itu, AI agent sendiri menjadi sasaran: **88% perusahaan sudah bereksperimen dengannya, dan Microsoft meminta agar identitas agen dikelola sebelum jumlahnya melampaui jumlah manusia.**



Kejahatan yang Terorganisasi

Kejahatan siber kini bekerja seperti *supply chain*. Hanya dalam 22 detik pasca-infeksi awal, skrip otomatisasi sudah memfasilitasi serangan tahap berikutnya. **Fokus ransomware kini menyasar infrastruktur krusial: sistem identitas, pengelola server virtual, dan backup.** Operasi bersama penegak hukum terbukti menekan ancaman—seperti tumbangnya platform phishing Tycoon2FA hingga 95%. Meski demikian, ancaman spionase negara terus meroket, termasuk pencurian kripto rekor US$1,46 miliar oleh peretas Korea Utara.

Ketika Peretasan Menjadi Kerusakan Fisik

Pada malam 11–12 Oktober 2026, **sistem pendingin di ratusan supermarket Prancis dilumpuhkan dari jarak jauh.** Peretas memaksa suhu freezer melonjak hingga 50°C melalui siklus defrost paksa. **CERT-FR (Computer Emergency Response Team France)** melaporkan pembobolan pada ***controller Danfoss,*** sebelum akhirnya memperluas peringatan ke perangkat Copeland dan Dixell.

Lembaga tersebut menegaskan bahwa membuka antarmuka pengelola langsung ke internet menyalahi best practice. Danfoss menyebut mayoritas unit yang terdampak merupakan produk lama yang tak lagi didukung pembaruan. Hingga 13 Oktober, identitas pelaku maupun metode penyusupan belum diumumkan.



Ilustrasi: Foto alat kontrol suhu di sistem pendingin supermarket

Kasus ini menunjukkan tingginya risiko Operational Technology (OT). Perangkat legacy yang tak lagi didukung sejak 2016 dan 2021 masih digunakan hingga 2026 dengan akses jarak jauh terbuka.



Ilustrasi: Pendingin di supermarket

Pembagian tanggung jawab yang tidak jelas antara peritel, kontraktor, dan pabrikan berujung fatal: pembuangan stok barang hingga kerusakan fisik berupa kebakaran peralatan.

AKSES JARAK JAUH **PENGENDALI** **PROSES FISIK**

Refleksi Lanskap Siber Indonesia

Indonesia berada di tengah arus ini. Dalam data Microsoft untuk Juli 2025 hingga Juni 2026, **Indonesia berada di peringkat ke-24 dunia dan ke-10 di Asia Pasifik untuk negara yang pelanggannya paling sering terdampak ancaman siber.** Badan Siber dan Sandi Negara (BSSN) mencatat sekitar 5,16 miliar anomali lalu lintas data sepanjang 2025, 93,78% di antaranya terkait malware, dengan catatan bahwa anomali tidak sama dengan serangan yang berhasil.

Ujiannya ternyata terjadi pada Juni 2024, ketika ransomware BrainCipher, varian LockBit 3.0, melumpuhkan Pusat Data Nasional Sementara (PDNS) 2 di Surabaya dan mengganggu layanan 239 dari 282 instansi pengguna. Menurut BSSN, backup dimatikan oleh akun baru sekitar tiga menit sebelum ransomware dijalankan, dan Kepala BSSN menyatakan kepada DPR bahwa hanya 2% data di Surabaya yang memiliki salinan di lokasi lain. **Pelajarannya lebih soal tata kelola daripada teknologi: tidak adanya backup adalah keputusan organisasi. Dari sisi hukum, UU Pelindungan Data Pribadi, yang masa transisinya berakhir pada Oktober 2024, mewajibkan pemberitahuan tertulis dalam 3x24 jam setelah terjadi kebocoran data.**



Bertahan Berarti Siap Pulih

Tanpa perimeter, fokus bergeser ke kecepatan deteksi. Meski deteksi mandiri naik ke angka 52%, hampir separuh insiden masih baru teridentifikasi melalui pihak luar. Mengingat peretas bergerak dalam hitungan detik, alert malware sepele tidak boleh diabaikan, dan **pemantauan wajib diperluas ke *edge device, hypervisor*, serta retensi log minimal 90 hari.**

Microsoft menekankan MFA tahan phishing, pembatasan akun admin, dan penilaian berbasis penurunan risiko. Untuk pemulihan insiden, isolasi penuh pada sistem pengelola server serta skema backup yang immutable, terisolasi, dan rutin diuji menjadi syarat mutlak.

Ada tiga pertanyaan strategis yang wajib dijawab oleh dewan direksi:

- Berapa menit rentang waktu dari alert awal hingga insiden terkendali?
- Apakah kita bisa memverifikasi setiap identitas yang mengakses akun berhak akses khusus?
- Jika sistem dan backup lumpuh total besok, seperti apa skenario pemulihannya?

Di era ini, organisasi yang mampu menjawab dengan data konkret—bukan asumsi—lah yang akan selamat.

REFERENSI UTAMA

Verizon— DataBreach Investigations Report 2026
Mandiant — M-Trends 2026: Executive Edition
CrowdStrike — Global Threat Report 2026

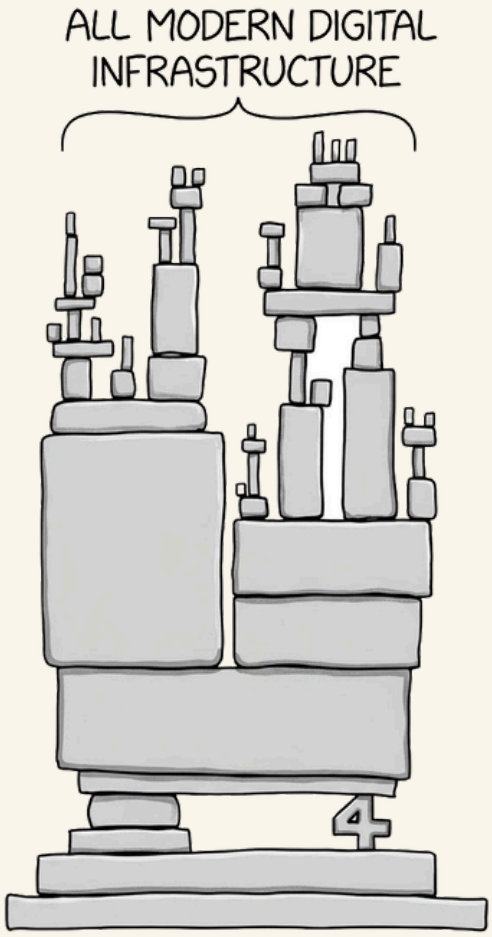
NAMASTE

CA-nya eMudhra, Key-nya eMudah Ditebak

BY ZHARFANUG

Bagi sebagian masyarakat Asia, angka 4 dianggap membawa sial, sehingga lantai empat di banyak gedung sering diubah menjadi "3A".

Selama ini, hal tersebut sekadar **mistifikasi**. Namun, pada 20 Oktober 2026, **angka 4 bergeser dari ranah fengsui ke dunia kriptografi—menjadi sumber masalah yang nyata.** Peneliti keamanan Scott Helme menemukan bahwa salah satu private key milik eMudhra, ***Certificate Authority*** **(CA)** asal India yang mengklaim telah menerbitkan lebih dari 60 juta sertifikat digital, bernilai persis angka 4.



"Salah satu private key eMudhra bernilai persis angka 4—bukan diawali angka 4 atau diikuti ratusan digit acak, hanya 4," *ungkap Helme*. "Kunci lain yang ditemukan bernilai 56 dan 115."

Nyatanya... Angka sial itu benar-benar bisa jadi masalah, bukan hanya tentang takhayul.

Apa Pentingnya Private Key?

Setiap kali Anda membuka situs web yang menampilkan ikon gembok di address bar, **ada "notaris digital" di balik layar yang menjamin keabsahan pemiliknya.** Notaris digital ini disebut ***Certificate Authority*** **(CA)**. eMudhra merupakan satu dari sedikit lembaga di dunia yang memegang kepercayaan penuh dari browser dan sistem operasi raksasa—mulai dari Mozilla, Microsoft, Apple, hingga Google Chrome—untuk menjalankan peran krusial tersebut.



Ilustrasi: Ikon gembok di address bar

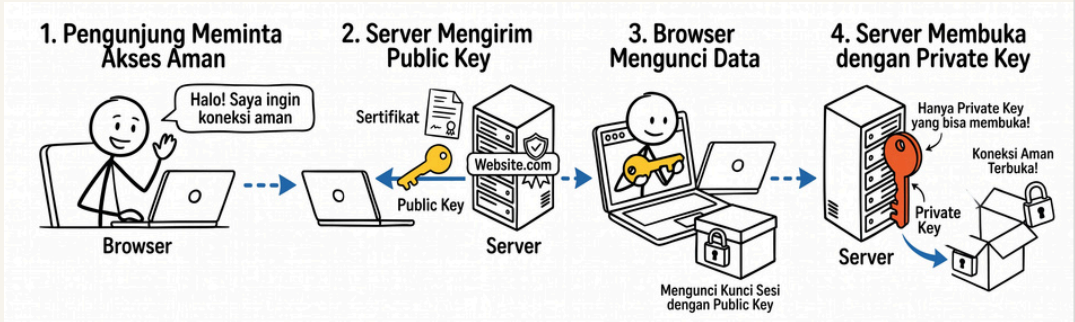
Keamanan CA bertumpu pada private key yang seharusnya dipilih acak dari 10^{115} kemungkinan kombinasi standar kurva P-384. Sayangnya, delapan private key milik eMudhra justru berangka sangat kecil di bawah 256 (seperti angka 4 hingga 237).

Celah ini membuat kunci dapat diretas dari *public key*-nya hanya dalam hitungan milidetik. Akibatnya, peretas dapat menerbitkan sertifikat palsu atas nama domain mana pun. Cloudflare menegaskan bahwa insiden ini memungkinkan penyerang menyamar sebagai server resmi untuk memanipulasi seluruh lalu lintas data.

Kronologi Singkat

- **30 April 2025:** eMudhra menerbitkan 8 sertifikat Intermediate CA via HSM FIPS 140-2 Level 3—perangkat aman yang justru menghasilkan kunci rapuh.
- **Pertengahan 2025:** Sertifikat lolos audit independen dan terintegrasi ke trust store seluruh browser utama.
- **17-18 Oktober 2026:** Peneliti "Wayne" melaporkan celah tersebut pada Big Tech setelah membuktikan dirinya bisa menandatangani pesan memakai private key ke-8 eMudhra.
- **17-20 Oktober 2026:** Chrome, Firefox, Apple, dan Microsoft memblokir sertifikat terkait. eMudhra mencabut (revoke) seluruh kunci terdampak.
- **20-21 Oktober 2026:** Insiden dirilis secara publik; 40+ ekosistem perangkat lunak global mendesak update keamanan darurat.

Cara kerja private key



Kok Bisa Lolos dari HSM Bersertifikat dan 2 Kali Audit?

Pertanyaan yang lebih menarik dari sekadar "angka berapa kuncinya" adalah bagaimana proses yang didesain seketat ini, pakai perangkat keras bersertifikasi, prosedur formal, dua kali audit independen, masih bisa meluluskan kunci yang gampang ditebak.

Menurut penjelasan resmi eMudhra, masalahnya ada di satu langkah teknis bernama key wrap/unwrap, proses membungkus dan membuka kunci kriptografi untuk keperluan backup. Pada langkah ini, tanpa sengaja tercipta sepasang kunci kedua yang lemah, berdampingan dengan kunci asli yang kuat. Karena label kedua pasangan kunci ini mirip, kunci yang lemah itulah yang akhirnya kepakai dan diterbitkan ke daftar kepercayaan browser, bukan kunci aslinya.

Jadi, akar masalahnya sederhana: salah proses dan salah label yang lolos dari dua kali audit formal selama kurang lebih 18 bulan. Nggak perlu hacker jenius buat bikin ini terjadi.

Daftar Lengkap 8 Sertifikat yang Bermasalah

Berikut delapan intermediate CA eMudhra yang terkena revoke. Masing-masing diterbitkan dua kali (cross-signed): sekali lewat root eMudhra sendiri, sekali lewat cross-sign root Sectigo, jadi total 16 entri sertifikat unik kalau dihitung per rantai.

Nama Certificate Authority	Organisasi	Jenis Sertifikat
EM DV TLS CA - G3B	eMudhra BV, Belanda	TLS, Domain Validation
EM DV TLS CA - G3C	eMudhra Inc, Amerika Serikat	TLS, Domain Validation
EM OV TLS CA - G3B	eMudhra BV, Belanda	TLS, Organization Validation
EM OV TLS CA - G3C	eMudhra Inc, Amerika Serikat	TLS, Organization Validation
EM EV TLS CA - G3B	eMudhra BV, Belanda	TLS, Extended Validation
EM EV TLS CA - G3C	eMudhra Inc, Amerika Serikat	TLS, Extended Validation
EM OV CS CA - G3B	eMudhra BV, Belanda	Code Signing
EM OV CS CA - G3C	eMudhra Inc, Amerika Serikat	Code Signing

Dua root yang ikut didistrust browser akibat insiden ini:

- **AAA Certificate Services** (alias "Comodo AAA Services root", dioperasikan Sectigo)
- **emSign ECC Root CA - G3 (**dioperasikan eMudhra)

Serial number dan fingerprint SHA256 lengkap dari seluruh 16 entri sertifikat ini bisa diambil langsung dari **emudhra.we-have-a-problem.com/impacted-intermediates.json** dan **emudhra.we-have-a-problem.com/roots.json**, kalau tim Anda butuh referensi teknis persis untuk audit atau *scripting*.

Jadi, Perlu Panik atau Nggak? Berikut Cara Cek dan Mengatasinya!

Banyak media menulis insiden ini seolah-olah internet akan runtuh. Padahal dari delapan sertifikat yang bermasalah, hanya satu yang pernah benar-benar digunakan, dan yang satu itu pun belum pernah menerbitkan satu sertifikat pun kepada siapa pun, jadi belum ada bukti bahwa kunci-kunci ini sempat disalahgunakan. Semua vendor besar juga sudah memblokir sertifikat bermasalah ini sejak 17–20 Oktober 2026, jadi **jika Anda hanya pengguna biasa dengan browser dan OS yang update otomatis, kemungkinan besar Anda sudah aman tanpa perlu melakukan apa pun.**

Untuk pengguna umum (non-IT):

- Pastikan Chrome, Firefox, Edge, atau Safari Anda sudah versi terbaru.
- Pastikan sistem operasi (Windows, macOS, Android, iOS) sudah update dalam beberapa minggu terakhir.
- Kalau dua hal itu sudah beres, selesai. Lanjut kerja seperti biasa.

Untuk tim IT dan developer, ini panduan lengkapnya, diambil langsung dari situs resmi pelacakan insiden **(emudhra.we-have-a-problem.com)** yang terus diperbarui oleh tim Mozilla dan komunitas:

1. Segera cek status validasi sertifikat pada sistem Anda.

Cara paling gampang: buka emudhra.we-have-a-problem.com/#, cek lewat browser Anda. Terdapat tabel checker otomatis yang dapat langsung memberi tahu status ke-12 kombinasi sertifikat/root yang bermasalah. Untuk cek command-line client atau sistem non-browser, situs resmi menyediakan 12 endpoint uji yang sama (per kombinasi jenis sertifikat dan rantai root). **Jalankan dari command lin**e:

```
curl https://dv-g3b-emudhra.we-have-a-problem.com/
curl https://dv-g3b-aaa-emudhra.we-have-a-problem.com/
```

Jika hasilnya error sertifikat, berarti klien Anda sudah aman (tidak lagi dipercaya). Kalau berhasil konek tanpa error, berarti masih *trust* dan perlu *update*. Untuk mengecek *trust store* secara offline, situs itu juga menyediakan chains.zip. Isinya certificate chain tiap endpoint dalam format PEM lengkap dengan instruksi verifikasi OpenSSL.

2. Workaround per platform

macOS: sistemnya sendiri sudah diblokir, tapi curl, git, python3, perl, ruby, dan openssl bawaan masih memverifikasi lewat /etc/ssl/cert.pem yang belum ikut ter-update otomatis:

macOS – Trust store

```
sudo cp -p /etc/ssl/cert.pem /etc/ssl/cert.pem.bak &&
sudo awk '/^(###|===) /{skip=0}
/^=== .*\/CN=(AAA Certificate Services|emSign ECC Root CA - G3)$/{skip=1}
!skip' /etc/ssl/cert.pem.bak | sudo tee /etc/ssl/cert.pem > /dev/null
```

Jika memakai pip3 bawaan atau virtual environment dari python3 bawaan, tambahkan ini supaya ikut pakai file yang sudah bersih:

macOS – pip dan virtual environment

```
F="$(/usr/bin/python3 -c 'import sysconfig; print(sysconfig.get_path("stdlib"))')/sitecustomize.py" &&
echo 'import os; os.environ.setdefault("PIP_CERT", "/etc/ssl/cert.pem")' | sudo tee -a "$F" > /dev/null &&
sudo chmod 644 "$F"
```

Linux: sambil menunggu distro Anda merilis paket ca-certificates baru, berikut cara distrust manual (untuk *expert*, tidak disarankan untuk pengguna biasa):

Debian / Ubuntu:

```
sed -i \
-e 's|^mozilla/emSign_ECC_Root_CA_-_G3.crt|!&|' \
-e 's|^mozilla/Comodo_AAA_Services_root.crt|!&|' \
/etc/ca-certificates.conf && update-ca-certificates
```

Workaround per platform – lanjutan

Fedora/RHEL/CentOS Stream/Rocky Linux/AlmaLinux /Amazon Linux 2023:

```
d=/etc/pki/ca-trust/source/blocklist; [ -d $d ] || d=/etc/pki/ca-trust/source/blacklist
trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=Comodo%20AAA%20Services%20root;type=cert' \
  $d/Comodo_AAA_Services_root.pem &&
trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert' \
  $d/emSign_ECC_Root_CA_-_G3.pem &&
update-ca-trust
```

Arch Linux:

```
trust extract --format=pem-bundle \
--filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert' \
/etc/ca-certificates/trust-source/blocklist/emSign_ECC_Root_CA_-_G3.pem &&
update-ca-trust
```

Windows: Microsoft sudah mengirim blokir lewat *Automatic Certificate Trust List update,* jadi *device* yang menerima *update* ini tidak perlu langkah tambahan. Untuk *device offline* atau yang auto-update-nya dimatikan, eMudhra & komunitas menyediakan script PowerShell resmi Block-EmudhraCompromisedCA.ps1 yang menambahkan ke-16 sertifikat bermasalah ke LocalMachine\Disallowed :

```
powershell.exe -NoProfile -ExecutionPolicy Bypass -File .\Block-EmudhraCompromisedCA.ps1
```

Catatan: untuk device yang dikelola IT *enterprise*, jangan jalankan sendiri, koordinasikan dulu dengan tim IT karena *rollout* biasanya sudah mereka atur terpusat.

NetBSD (versi 10 ke atas):

```
certctl untrust /usr/share/certs/mozilla/all/emSign_ECC_Root_CA_-_G3.pem &&
certctl untrust /usr/share/certs/mozilla/all/Comodo_AAA_Services_root.pem
```

FreeBSD (versi 14 ke atas):

```
cp /etc/ssl/certs/14bc7599.0 /usr/share/certs/untrusted/14bc7599.pem
cp /etc/ssl/certs/ee64a828.0 /usr/share/certs/untrusted/ee64a828.pem
certctl rehash
```

3. Daftar lengkap *software* yang sudah merilis *patch*

Jika organisasi Anda pakai salah satu dari ini, update ke versi berikut:

Software	Versi yang sudah patch
Ubuntu ca-certificates	20260816ubuntu0.22.04.1 / 0.24.04.1 / 0.26.04.1 / 0.26.10.1
Debian ca-certificates	20250419~deb12u2, 20250419+deb13u1, 20260816+nmu1
Devuan ca-certificates	Sama seperti Debian
Arch Linux ca-certificates-mozilla	3.131.1-1
Gentoo ca-certificates	20260816.3.125
Fedora ca-certificates	2026.2.92_v9.0.319
FreeBSD caroot	15.1-RELEASE-p6, 14.5-RELEASE-p3, 14.4-RELEASE-p12
FreeBSD ca_root_nss	1.131.1
Freedesktop SDK	25.08.19, 26.08.3
Chainguard ca-certificates	20260909-r3
Alpine Linux ca-certificates	20261020-r0
GNU Guix	commit 7608a99
OmniOS web/ca-bundle	r151054by, r151056ay, r151058y
Bottlerocket	belum rilis (pending)
NSS	3.131.1
curl CA bundle	rilis 2026-10-20
Cloudflare CFSSL trust store	2026.10.1
Homebrew ca-certificates	2026-09-25_1
Go	1.27.3, 1.26.10
Java (OpenJDK/Oracle JDK)	27.0.1.0.2, 25.0.5.0.2, 21.0.13.0.2, 17.0.21.0.2, 11.0.33.0.2, 8u511

DAFTAR PATCH / LANJUTAN

Software	Versi yang sudah patch
Node.js	22.23.4, 24.22.1, 26.12.1
Python certifi	2026.10.19
pip	26.2.2
uv	0.13.4
pixi	0.82.1
Rust rustls-webpki	0.103.16
Rust webpki-roots / webpki-root-certs	1.0.10
Rustup	1.29.2
Electron	44.9.1, 43.8.1, 42.11.16
Bun	belum rilis (pending)
Claude Code	2.1.303
Composer ca-bundle	1.4.16, 1.6.0
Elixir castore	1.0.22
Erlang certifi	belum rilis (pending)
mise	2026.10.17
Perl Mozilla::CA	20261020
Deno	2.9.8

Daftar ini terus bertambah di repo resminya, github.com/galadran/we-have-a-problem.com, jika Anda ingin cek versi terbaru.



4. Satu hal yang jangan dilakukan

Jika setelah *update* muncul error sertifikat di dashboard atau log, jangan buru-buru matikan verifikasi sertifikat untuk "menghilangkan" error itu, karena sama dengan mencabut pagar yang baru dipasang. Cari tahu dulu mengapa errornya muncul, karena biasanya itu justru tanda proteksi barunya bekerja.

Jadi, Namaste agak berbeda maknanya bagi tim keamanan eMudhra bulan ini. Bagi kita semua, ini alasan baru untuk skip lantai 4: sekarang ada contoh nyata kenapa detail kecil yang kelihatannya sepele bisa bikin masalah besar.

REFERENSI UTAMA

Tracker Insiden eMudhra

Pernyataan resmi eMudhra Cloudflare — Certificate compromise

KETIKA *PATCH* JADI PETA SERANGAN

Mengurai Krisis PHP2Shell dan Runtuhnya Embargo CVD

BY OM FADHIL

Sebelum membaca artikel ini lebih lanjut berikut adalah penjelasan vulnerability PHP2Shell dan Embargo CVD,

PHP2Shell adalah sebutan untuk sepasang celah keamanan kritis (**CVE-2026-109618 dan CVE-2026-109619)** pada *core runtime* bahasa pemrograman PHP yang memungkinkan penyerang mengeksekusi kode berbahaya dari jarak jauh (*Remote Code Execution*/RCE) tanpa perlu autentikasi. Serangan ini bekerja dengan memicu kerusakan alokasi memori (*heap corruption*) melalui permintaan HTTP khusus, sehingga penyerang dapat mengambil alih kontrol penuh atas server web tanpa bergantung pada celah aplikasi di atasnya.

Embargo CVD (*Coordinated Vulnerability Disclosure*) adalah perjanjian kerahasiaan sementara antara penemu celah, pengembang perangkat lunak, dan vendor terkait untuk menahan rilis detail teknis ke publik sampai *patch* siap didistribusikan secara serentak. Tujuannya adalah memberi waktu bagi tim pertahanan (*defender*) untuk memperbarui sistem sebelum peretas mengetahui cara mengeksploitasi kelemahan tersebut.

BERKAS PHP2SHELL



EMBARGO DALAM TEKANAN

17 OKT

Eksploitasi teramati

20 OKT

Metadata & PoC bocor

21 OKT

Build dan *patch* dirilis

22 OKT

Jadwal asli embargo

KRONOLOGI PECAHNYA EMBARGO

17 Okt 2026
Eksploitasi In-The-Wild
Honeypot AWS diserang

20 Okt 2026
Bocoran CVE ID & PoC
Video Calif bocor

21 Okt / 07:41 UTC
Chainguard rilis build
Embargo pecah

21 Okt / 14:00 UTC
PHP Project resmi rilis
Patch darurat

22 Okt / 14:00 UTC
Jadwal asli embargo
Gagal dipertahankan

ANATOMI TEKNIS & KEGAGALAN SISTEMIK EMBARGO

1. Root Cause & Vektor Eksploitasi

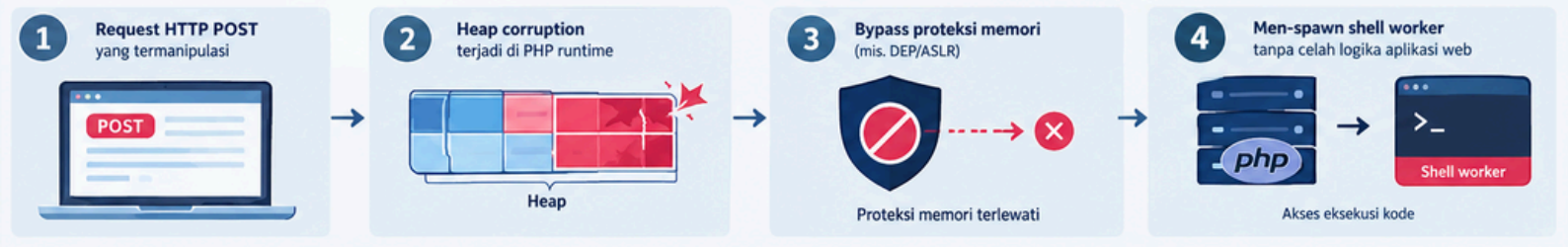
Dua kerentanan kritis, CVE-2026-109618 dan CVE-2026-109619 (CVSS 9.2–9.8) bernama PHP2Shell, memicu krisis *unauthenticated Remote Code Execution* (RCE) pada runtime PHP yang menopang 70–80% web publik. Berikut adalah root cause dan vektor eksploitasi:

Mekanisme Kerentanan:
Celah berakar dari penanganan status Out-Of-Memory (OOM) pada core engine PHP serta manajemen session upload-progress.

Akselerasi AI:
Riset OpenAI, Wiz, dan Calif menunjukkan bahwa AI mampu menemukan teknik eksploitasi yang lebih presisi, sehingga celah keamanan memori yang telah dikenal selama hampir 20 tahun kini dapat dimanfaatkan menjadi serangan nyata.

RCE Bypass:
Pada runtime seperti Apache mod_php, satu **request HTTP POST yang** termanipulasi cukup memicu heap corruption, mem-**Bypass proteksi memori,** dan men-**Spawn shell worker** tanpa bergantung pada celah logika aplikasi web.

Proses RCE Bypass:



2. Mengapa Embargo CVD Kolaps?



Skema *Coordinated Vulnerability Disclosure* (CVD) gagal mencegah penyebaran eksploitasi secara efektif akibat empat faktor yang saling berkaitan, yaitu:

Eksploitasi Sebelum Pengumuman Resmi (*Pre-Disclosure*)
AWS *Threat Intelligence* mendeteksi aktivitas serangan di honeypot sejak 17 Oktober, empat hari sebelum patch dirilis. Temuan ini mengindikasikan bahwa penyerang telah mengeksploitasi kerentanan sebelum perbaikan resmi tersedia.

Kebocoran Informasi dan PoC
Pada 20 Oktober, identitas CVE mulai beredar di publik. Video demonstrasi *Proof of Concept* (PoC) dari Calif juga sempat bocor di media sosial, sehingga meningkatkan kekhawatiran di kalangan pelaku industri.

Rilis *Patch* Terlalu Dini: Pedang Bermata Dua
Chainguard merilis build image yang telah ditambal enam jam sebelum jadwal revisi resmi. Penyerang dapat membandingkan versi sebelum dan sesudah patch melalui teknik *binary diffing* untuk merekonstruksi cara mengeksploitasi celah tersebut, bahkan sebelum Ubuntu, Debian, dan Red Hat merilis pembaruan masing-masing.

AI Mempercepat Rekayasa Balik
AI mempercepat proses analisis dan rekayasa balik (*reverse engineering*) yang sebelumnya dapat memakan waktu berminggu-minggu menjadi hitungan jam. Akibatnya, waktu yang tersedia bagi organisasi untuk mempersiapkan perlindungan semakin sempit, sementara pendekatan kerahasiaan yang melibatkan banyak pihak menjadi kurang efektif.

RESPONS INDUSTRI & BLUE TEAM PLAYBOOK

1. Dampak Operasional Global

Fasilitas Publik

Censys dan VirusTotal mencatat 2,5–5,1 juta host publik terekspos. Sejumlah portal pemerintahan, rumah sakit, dan kampus di Eropa memilih mematikan server (full offline) demi mencegah kompromi web shell massal.

Backport Darurat untuk Versi EOL

AWS dan Google Cloud memperbarui base image mereka. Karena lebih dari 50% server dunia masih menggunakan PHP End-of-Life (<= 8.1), vendor panel seperti cPanel dan Plesk terpaksa merekayasa patch backport non-resmi.

2. Actionable Playbook (SecOps & Security Engineer)

Vektor / Domain	Tindakan Mandatori	Dasar Penanganan
Runtime Patching	Update ke versi PHP 8.5.12, 8.4.27, 8.3.36, atau 8.2.35.	Solusi permanen; versi EOL wajib gunakan patch backport vendor (Sumber: Krebs on Security).
Config Hardening	Ubah php.ini: session.upload_progress.enabled = Off.	Mitigasi cepat memutus heap grooming vector (Sumber: SecurityWeek).
WAF / Virtual Patch	Terapkan rule inspeksi payload POST multipart (Cisco Talos, Cloudflare WAF).	Menahan serangan otomatis saat patching berlangsung (Sumber: SecurityWeek).
EDR Behavioral Rules	Blokir child process dari user web (www-data, apache, nginx).	Alert instan jika spawn /bin/sh, /bin/bash, curl, wget, atau drop file .php baru.
Retroactive Hunting	Periksa histori log server web dan catat crash error memori (OOM/segfault) ke belakang minimal hingga 17 Oktober 2026. Cari tanda penyerang sudah masuk sebelum patch dirilis.	Merespons temuan AWS bahwa serangan liar sudah terjadi 4 hari sebelum patch resmi diumumkan (Sumber: BleepingComputer).

Catatan teknis: mitigasi sementara tidak menggantikan pembaruan PHP resmi.

3. Catatan Strategis CISO

Berikut adalah catatan strategis yang bisa diterapkan,

- **Zero Patching Window:** Asumsikan eksploitasi telah berjalan bersamaan dengan atau mendahului rilis patch resmi.
- **Lacak PHP Tersembunyi:** Audit daftar komponen software (Software Bill of Materials /SBOM) secara menyeluruh untuk mendeteksi versi PHP yang diam-diam tertanam di perangkat firewall/UTM maupun microservices lama.
- **Kewenangan Isolasi:** Tetapkan protokol terotorisasi di awal agar tim teknis dapat mematikan atau mengisolasi layanan tanpa menunggu persetujuan birokrasi di tengah krisis.

REFERENSI UTAMA

PHP — Security advisory, 21 Oktober 2026

AWS — Eksploitasi sebelum pengungkapan di MadPot CSO — PHP2Shell dan coordinated vulnerability disclosure

THE NEXT CYBER BATTLEFIELD 2030

WHAT AI PREDICTIONS TELL US ABOUT



By 2030, will humans still be fast enough to defend the digital world?

BY ALDA



Ilustrasi: Tangan robot mengetik

Perubahan yang perlu diperhatikan bukan hanya kemampuan AI, tetapi juga dampaknya terhadap waktu yang dimiliki organisasi untuk mendeteksi dan menangani ancaman.

Sejumlah penelitian mulai memberikan gambaran tentang perubahan ini. Temuannya menunjukkan bahwa kemampuan AI terus berkembang, tetapi risiko keamanan tetap dipengaruhi oleh faktor lain, mulai dari pengelolaan kerentanan hingga ketergantungan pada teknologi pihak ketiga.

Lalu, apa yang perlu dipersiapkan untuk menghadapi medan perang siber pada 2030?

AI Mulai Mengambil Alih Sebagian Pekerjaan Teknis

Kemampuan AI dalam mengerjakan tugas keamanan siber menunjukkan peningkatan yang cukup signifikan. Hal ini terlihat dalam pengujian UK AI Security Institute (AISI), lembaga pemerintah Inggris yang mengevaluasi kemampuan dan risiko AI.

Dalam Frontier AI Trends Report, UK AI Security Institute (AISI) mencatat peningkatan kemampuan model AI dalam menyelesaikan tugas siber. Pada awal 2024, model yang diuji hanya berhasil menyelesaikan sedikit lebih dari 10% tugas tingkat pemula. Dalam evaluasi yang lebih baru, rata-rata tingkat keberhasilannya mencapai sekitar 50%. Pada 2025, AISI juga melaporkan model yang berhasil menyelesaikan tugas tingkat ahli yang biasanya membutuhkan pengalaman praktisi manusia lebih dari 10 tahun.

AISI turut memperkirakan bahwa durasi tugas siber yang dapat diselesaikan model tanpa bantuan manusia dengan tingkat keberhasilan 50% meningkat dua kali lipat kira-kira setiap delapan bulan. Angka ini menggambarkan tren dalam pengujian AISI, bukan jaminan bahwa kemampuan AI akan terus berkembang dengan laju yang sama.

Temuan ini menunjukkan bahwa AI berpotensi menangani tugas yang semakin kompleks. Namun, hasil pengujian tidak otomatis mencerminkan kemampuan AI dalam kondisi operasional nyata, dan kemajuannya belum tentu berlanjut dengan kecepatan yang sama.

Bagi keamanan siber, peningkatan kemampuan ini dapat membantu pekerjaan teknis, tetapi juga membuka peluang penyalahgunaan. Dampaknya akan bergantung pada bagaimana teknologi digunakan dan seberapa baik hasilnya dikendalikan.



Ilustrasi: *Frontier AI Trends Report*

2027

Saat Serangan Siber Semakin Masif

Dalam laporan Impact of AI on Cyber Threat from Now to 2027, UK National Cyber Security Centre (NCSC) memperkirakan bahwa AI akan meningkatkan efektivitas teknik serangan yang sudah dikenal.

Phishing, misalnya, dapat dibuat lebih personal dengan menyesuaikan isi pesan berdasarkan informasi tentang calon korban. AI juga berpotensi meningkatkan kemampuan penyerang dalam meneliti kerentanan dan mengembangkan eksploitasi (*vulnerability research and exploit development*).

NCSC menilai bahwa hingga 2027, alat berbasis AI hampir pasti meningkatkan kemampuan penyerang memanfaatkan kerentanan yang telah diketahui, terutama pada sistem yang belum diperbarui.

Artinya, organisasi memiliki alasan semakin kuat untuk mempercepat pengelolaan kerentanan. Prioritas perlu ditentukan berdasarkan tingkat risiko, paparan sistem terhadap internet, potensi dampak, dan kemungkinan kerentanan tersebut dieksploitasi. Jika pembaruan belum dapat dilakukan, pembatasan akses dan pemantauan tambahan dapat membantu mengurangi risiko.

AI mungkin mempercepat serangan, tetapi kelemahan mendasar seperti sistem yang tidak diperbarui dan konfigurasi yang keliru tetap menjadi persoalan penting.

2030

Saat AI Mampu Selesaikan Tugas Berhari-hari

Dalam International AI Safety Report 2026, lebih dari 100 pakar AI membahas kemungkinan perkembangan kemampuan AI hingga 2030. Salah satu proyeksinya adalah **kemampuan AI menyelesaikan tugas rekayasa perangkat lunak yang terdefinisi dengan baik dan biasanya membutuhkan beberapa hari kerja seorang engineer, jika tren kemajuan saat ini berlanjut.**

Kemampuan ini relevan bagi keamanan siber. AI dapat membantu meninjau kode, menguji perangkat lunak, dan mencari kelemahan sistem. Namun, kemampuan yang sama juga berpotensi digunakan untuk mengembangkan eksploitasi.

Proyeksi tersebut bukan berarti AI pasti mampu menjalankan serangan kompleks dari awal hingga akhir secara mandiri. AI masih dapat mengalami kesulitan ketika menghadapi informasi yang tidak lengkap, proyek panjang, atau kondisi yang tidak terduga. Kemampuan menyelesaikan tugas teknis yang terdefinisi dengan baik juga tidak otomatis menunjukkan bahwa AI mampu menangani seluruh tahapan serangan siber yang kompleks.

Meski demikian, organisasi perlu bersiap menghadapi kemungkinan meningkatnya otomatisasi pekerjaan teknis. Proses keamanan yang sepenuhnya manual dapat semakin sulit mengejar perubahan jika volume pekerjaan meningkat, sementara waktu untuk merespons semakin terbatas.

Risiko *Software* di *Supply Chain*

Perkembangan AI bukan satu-satunya faktor yang membentuk ancaman siber menuju 2030. Ketergantungan pada teknologi pihak ketiga juga menjadi perhatian penting.

Dalam laporan Foresight Cybersecurity Threats for 2030 – Update 2024, European Union Agency for Cybersecurity (ENISA) menempatkan serangan melalui rantai pasok perangkat lunak sebagai salah satu ancaman yang perlu diwaspadai. Laporan tersebut juga mengidentifikasi risiko lain, termasuk kekurangan tenaga ahli, kesalahan manusia, dan penggunaan sistem lama yang rentan. Penilaian ini didasarkan pada masukan dari 24 ahli.

Risikonya muncul karena organisasi menggunakan berbagai aplikasi, layanan cloud, dan komponen perangkat lunak dari pemasok yang berbeda. Jika salah satu komponen tersebut disusupi, banyak organisasi dapat terdampak sekaligus, termasuk yang bukan target awal penyerang.

Dalam Global Cybersecurity Outlook 2026, World Economic Forum melaporkan bahwa 65% perusahaan yang masuk kategori perusahaan besar berdasarkan pendapatan menganggap kerentanan pihak ketiga dan rantai pasok sebagai tantangan terbesar dalam membangun ketahanan siber. Angka ini naik 11 poin persentase, dari 54% pada 2025 menjadi 65% pada 2026.

Temuan tersebut menunjukkan bahwa keamanan internal saja tidak cukup. Organisasi perlu memahami teknologi yang digunakan, mengevaluasi praktik keamanan pemasok, serta menyiapkan langkah pemulihan jika layanan yang diandalkan mengalami gangguan.

Peran AI dalam Pertahanan

AI juga mulai diuji untuk membantu analis SOC menangani investigasi insiden. Dalam Beyond the Hype: A Benchmark Study of AI Agents in the SOC (2025), Cloud Security Alliance melaporkan bahwa 148 peserta yang menggunakan bantuan Dropzone AI menyelesaikan dua skenario investigasi 45–61% lebih cepat, dengan akurasi 22–29% lebih tinggi dibandingkan dengan kelompok yang bekerja tanpa bantuan AI. **Hasil ini menunjukkan potensi AI dalam mempercepat investigasi, tetapi pengujiannya masih terbatas pada dua skenario.** Karena itu, hasil tersebut belum cukup untuk menyimpulkan bahwa AI akan selalu meningkatkan kecepatan dan akurasi dalam semua jenis investigasi SOC.

Namun, kecepatan investigasi tidak selalu sejalan dengan ketepatan penentuan prioritas. Penelitian yang diterbitkan dalam Expert Systems with Applications pada 2026 menguji delapan model bahasa besar terhadap 178 alert. Hasilnya menunjukkan bahwa meskipun model-model tersebut cukup baik dalam mengklasifikasikan alert, kemampuan menentukan prioritasnya masih terbatas. Jika tidak ditinjau kembali, alert yang salah diprioritaskan dapat menyita waktu analis dan membuat ancaman yang lebih serius luput dari perhatian.

Karena itu, AI di SOC sebaiknya berperan sebagai pendukung investigasi, bukan pengganti pertimbangan analis. Rekomendasi AI perlu dievaluasi berdasarkan konteks insiden sebelum ditindaklanjuti, sementara tindakan otomatis seperti memblokir akses atau menonaktifkan akun perlu dibatasi dengan aturan dan kewenangan yang jelas.



Bersiap Sebelum Medan Perang Berubah

Sejauh mana AI akan berkembang hingga 2030 masih belum dapat dipastikan. International AI Safety Report 2026 membahas berbagai kemungkinan, mulai dari kemajuan yang melambat hingga percepatan yang signifikan. Perkembangan akhirnya akan dipengaruhi oleh kendala teknis, kebutuhan energi, dan kemampuan AI menangani tugas kompleks.

Namun, organisasi tidak perlu menunggu kepastian tersebut untuk memperkuat pertahanan.

Inventarisasi aset, pengelolaan kerentanan, pembaruan sistem, perlindungan identitas, dan pengaturan hak akses tetap menjadi fondasi keamanan. Organisasi juga perlu menetapkan batas penggunaan AI, termasuk data yang boleh diakses dan keputusan yang harus tetap berada di bawah kendali manusia.

Bagi praktisi keamanan siber, tantangannya adalah terus memperbarui keterampilan teknis sekaligus memahami kemampuan dan keterbatasan AI.

Masa depan keamanan siber tidak hanya ditentukan oleh seberapa cepat AI berkembang, tetapi juga oleh seberapa siap manusia beradaptasi dengannya. Teknologi dapat memperluas kemampuan pertahanan, tetapi tanggung jawab untuk mengelola risiko dan mengambil keputusan tetap harus berada di tangan manusia.



Proyeksi bukan kepastian.

REFERENSI UTAMA

AISI — Frontier AI Trends Report 2025

NCSC — Impact of AI on cyber threat, now to 2027 International AI Safety Report 2026

MEMVERIFIKASI TEMUAN PENTEST

dengan VulnVerify Skills

BY KANG ALi



Ilustrasi konseptual: memeriksa bukti di balik klaim laporan.

Laporan pentest dapat memuat *payload*, tangkapan layar, dan penjelasan dampak yang meyakinkan. Namun, setiap temuan tetap perlu diperiksa terhadap perilaku aplikasi yang sebenarnya. Payload yang muncul di halaman belum tentu dieksekusi. Respons HTTP yang berhasil belum tentu membuktikan bahwa akses tidak sah. Kesimpulan yang keliru dapat mengarahkan pekerjaan perbaikan ke masalah yang tidak terbukti.

VulnVerify Skills membantu pemeriksaan tersebut pada laporan kerentanan website dan aplikasi web, termasuk hasil pentest dan bug hunting yang dilakukan secara manual maupun dengan AI agent. Proyek ini memberi agent urutan kerja untuk menilai klaim, memeriksa bukti, lalu menyiapkan reproduksi yang terkontrol. Hasilnya harus menjelaskan apa yang benar-benar terbukti dan informasi apa yang masih kurang.

Dalam demonstrasi lokal untuk artikel ini, dua laporan dengan dugaan eksekusi JavaScript menghasilkan kesimpulan berbeda. Satu klaim terbukti melalui perubahan marker di browser. Klaim lainnya terbantahkan karena input diproses sebagai teks. Perbedaannya dapat ditelusuri dari tindakan pengujian, struktur halaman, dan implementasi yang sesuai dengan build yang diuji.

Bukti perlu menjelaskan efek, jalur input, dan batas kesimpulan.

Mengubah Laporan Menjadi Pertanyaan yang Dapat Diuji

VulnVerify menyediakan tiga skill untuk OpenCode, OpenAI Codex, dan Claude Code. Skill tersebut berupa instruksi dan referensi yang dibaca oleh agen melalui mekanisme klien masing-masing. Agent tetap bergantung pada kemampuan model,akses dokumen, alat yang tersedia, dan kelengkapan konteks. Memasang skill tidak otomatis membuat setiap analisis benar.

01

vulnerability-triage-brocards

Alurnya dimulai dengan vulnerability-triage-brocards.
Agent mengidentifikasi klaim, komponen terdampak, kemampuan awal penyerang, prasyarat, aturan keamanan yang seharusnya berlaku, serta bukti dalam laporan. Tujuh brocard membantu memeriksa apakah klaim memiliki konteks ancaman dan penggunaan yang masuk akal. Keputusan triage mengarahkan penyelidikan; keputusan itu belum merupakan bukti teknis bahwa temuan valid atau salah.

02

fp-check

Berikutnya, fp-check menilai aliran input menuju operasi yang dipersoalkan.
Agent memeriksa kontrol penyerang, transformasi input, batas kepercayaan, perlindungan yang relevan, dan dampak yang benar-benar didukung oleh bukti. Jalur standar digunakan untuk klaim yang jelas dan sederhana. Jalur deep digunakan ketika terdapat ambiguitas, perilaku asinkron, atau kondisi lain yang memerlukan pemeriksaan lebih rinci.

03

poc-builder

Ketika reproduksi diperlukan dan diizinkan, poc-builder menerima klaim yang sama beserta target, kondisi, input, hasil yang diharapkan, dan pembandingnya.
Skill ini menyiapkan prosedur atau artefak yang sesuai, lalu mencatat apakah pengujian direncanakan, dibuat, dijalankan, dan menghasilkan efek yang dimaksud. Hasil reproduksi dikembalikan ke fp-check untuk ditinjau sebelum verdict diterbitkan.

Metodologi utama VulnVerify mengadaptasi pendekatan Trail of Bits, ketika poc-builder yang semula berupa agent terikat fp-check diubah menjadi skill portabel. Penyesuaian juga mencakup verifikasi kelengkapan tertulis, mengingat mekanisme hooks maupun agent pada satu client tidak selalu tersedia di client lain. Seluruh atribusi, revisi sumber, dan lisensi telah dicatat dalam repositori.

Peran Playwright MCP dalam Pembuktian

Untuk temuan yang bergantung pada perilaku browser, **Playwright MCP memungkinkan agent membuka halaman yang diizinkan, mengisi formulir, menekan tombol, dan memeriksa hasilnya.** Agent dapat menyimpan screenshot, snapshot halaman, serta keluaran console dan jaringan yang relevan. Temuan yang cukup diperiksa melalui kode, konfigurasi, atau antarmuka non-browser tidak harus memakai Playwright.

Cara pengiriman input perlu sesuai dengan laporan. Jika klaimnya menyebut formulir tertentu, payload perlu melewati formulir tersebut. Menjalankan JavaScript langsung melalui alat evaluasi lalu menampilkan perubahan halaman tidak membuktikan bahwa input dapat mencapai efek yang sama lewat aplikasi. Identitas halaman, versi, sesi, dan perlindungan browser juga perlu dipertahankan.

Laporan PDF, JSON, atau Markdown dapat menjadi titik awal, mengikuti kemampuan pembacaan client. Source code membantu menjelaskan penyebab internal ketika tersedia. Tanpa source code, perilaku eksternal yang cukup kuat tetap dapat membuktikan pelanggaran tertentu, sementara penyebab yang belum diperiksa harus tetap ditulis sebagai dugaan. VulnVerify tidak menyertakan parser PDF atau OCR universal.

Instalasi Singkat dari GitHub

Kode tersedia di repositori VulnVerify Skills. Siapkan Git, Python3.9 atau lebih baru, shell POSIX, dukungan symlink, dan client yang ingin digunakan. Contoh berikut memasang tiga skill pada akun pengguna untuk OpenCode, Codex, dan Claude Code. Periksa pratinjau perubahan sebelum menjalankan instalasi:

INSTALASI / SHELL POSIX

```
git clone https://github.com/roomkangali/vulnverify-skills.git
cd vulnverify-skills
sh scripts/install.sh install --scope user --client all --dry-run
sh scripts/install.sh install --scope user --client all
sh scripts/install.sh check --scope user --client all
```

Simpan folder repositori di lokasi tetap karena instalasi menggunakan tautan ke file skill di dalamnya. Setelah instalasi, buka sesi client baru dan pastikan ketiga nama skill ditemukan. Installer tidak mengatur koneksi MCP; petunjuk penggunaan dan penyiapan Playwright MCP tersedia dalam GUIDE.md.

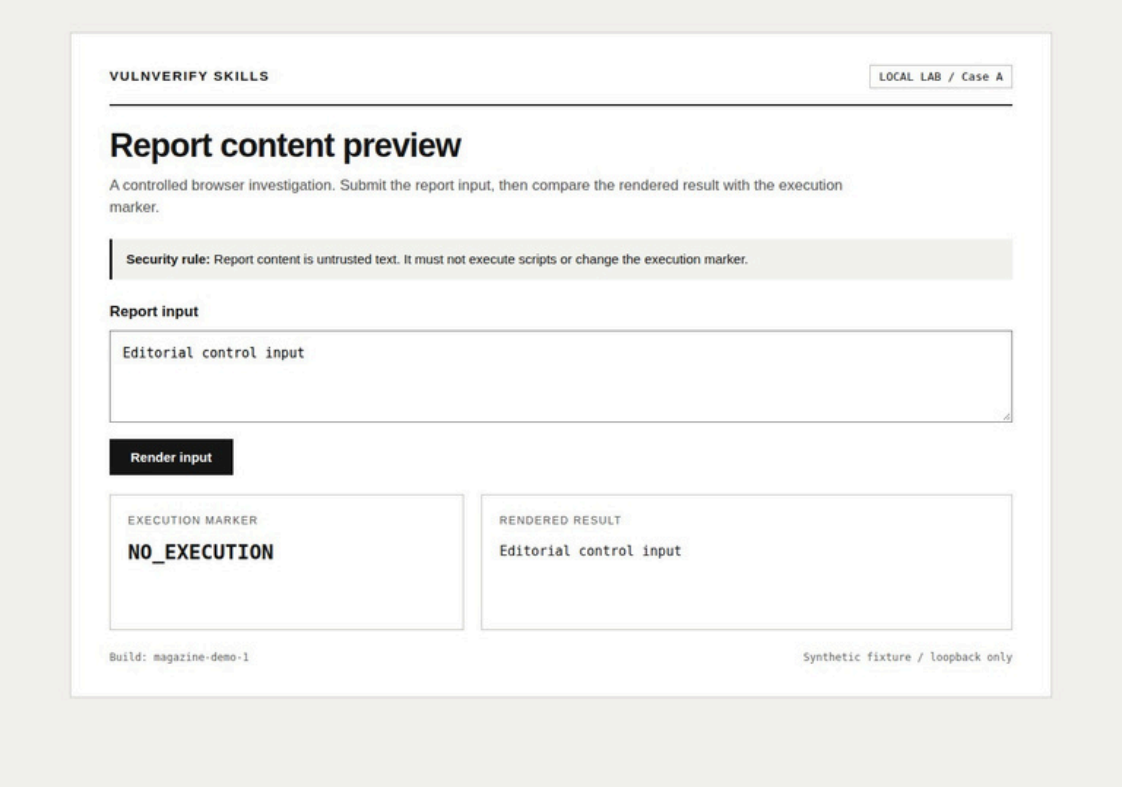
Laboratorium Dua Laporan dengan Klaim Serupa

Contoh dalam artikel ini menggunakan aplikasi sintetis yang berjalan di 127.0.0.1. Target aslinya adalah laboratorium itu sendiri, dengan build magazine-demo-1. Tidak ada website pihak lain, akun nyata, atau data pengguna yang diuji. Laporan A dan B mengajukan klaim sempit: input pada formulir preview dapat menjalankan handler JavaScript dan mengubah marker milik halaman.

Kedua halaman menampilkan aturan yang sama. Isi laporan diperlakukan sebagai teks yang tidak dipercaya dan tidak boleh menjalankan script atau mengubah marker. Penguji hanya diberi kendali atas kolom Report input. Efek payload dibatasi pada perubahan tulisan NO_EXECUTION menjadi DEMO_EXECUTION. Pengujian ini tidak menunjukkan pengiriman payload kepada korban lain atau dampak pada sistem produksi.

Sebelum memakai *payload*, penguji mengirim teks biasa melalui tombol Render input. Halaman harus menampilkan teks yang sama dan marker tetap tidak berubah. Pembanding ini dijalankan terpisah pada A dan B agar keberhasilan satu halaman tidak dianggap membuktikan kesiapan halaman lainnya.

Payload menggunakan elemen gambar dengan alamat lokal yang sengaja tidak tersedia. Jika string itu menjadi elemen HTML, kegagalan pemuatan gambar memicu handler onerror. Handler tersebut hanya mencoba mengganti marker. **Kegagalan permintaan gambar sendiri bukan bukti eksekusi; perubahan marker melalui jalur input yang benar menjadi pembeda utamanya.**

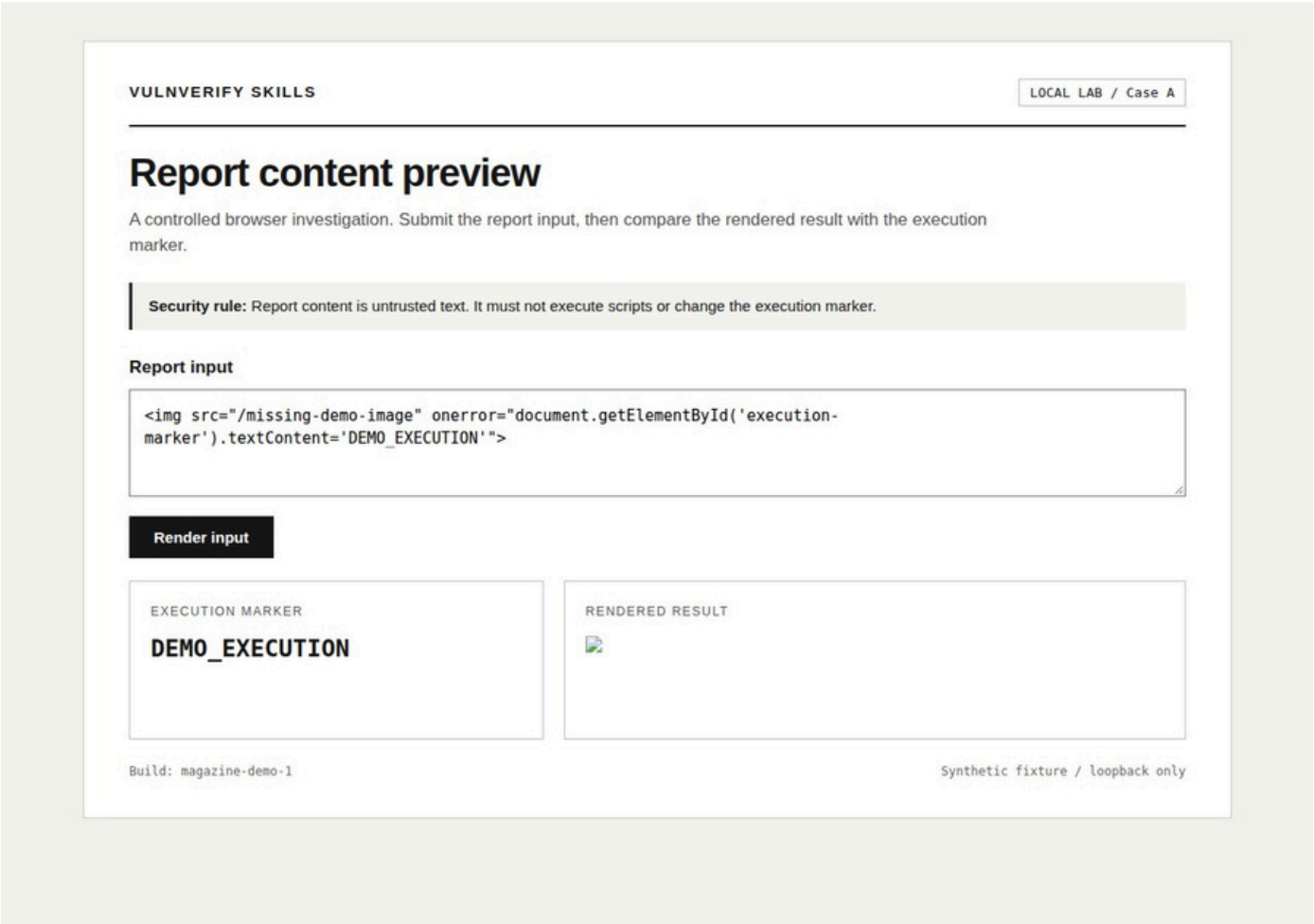


Gambar 1. Input normal pada kasus A tampil sesuai isinya dan marker tetap NO_EXECUTION. Pembanding yang setara juga dijalankan secara terpisah pada kasus B.

KASUS A / CONFIRMED

Kasus A Membuktikan Efek Eksekusi yang Diklaim

Pada kasus A, payload dikirim melalui formulir yang sama setelah navigasi baru. Browser membentuk satu elemen gambar dan marker berubah menjadi DEMO_EXECUTION.Snapshot dan pemeriksaan DOM mencatat input yang diterima serta hasilnya. Screenshot memperlihatkan keadaan halaman setelah tindakan tersebut.



Gambar 2. Payload pada kasus A mengubah marker menjadi DEMO_EXECUTION. Ikon gambar rusak adalah efek samping yang disengaja; perubahan marker menunjukkan handler berjalan.

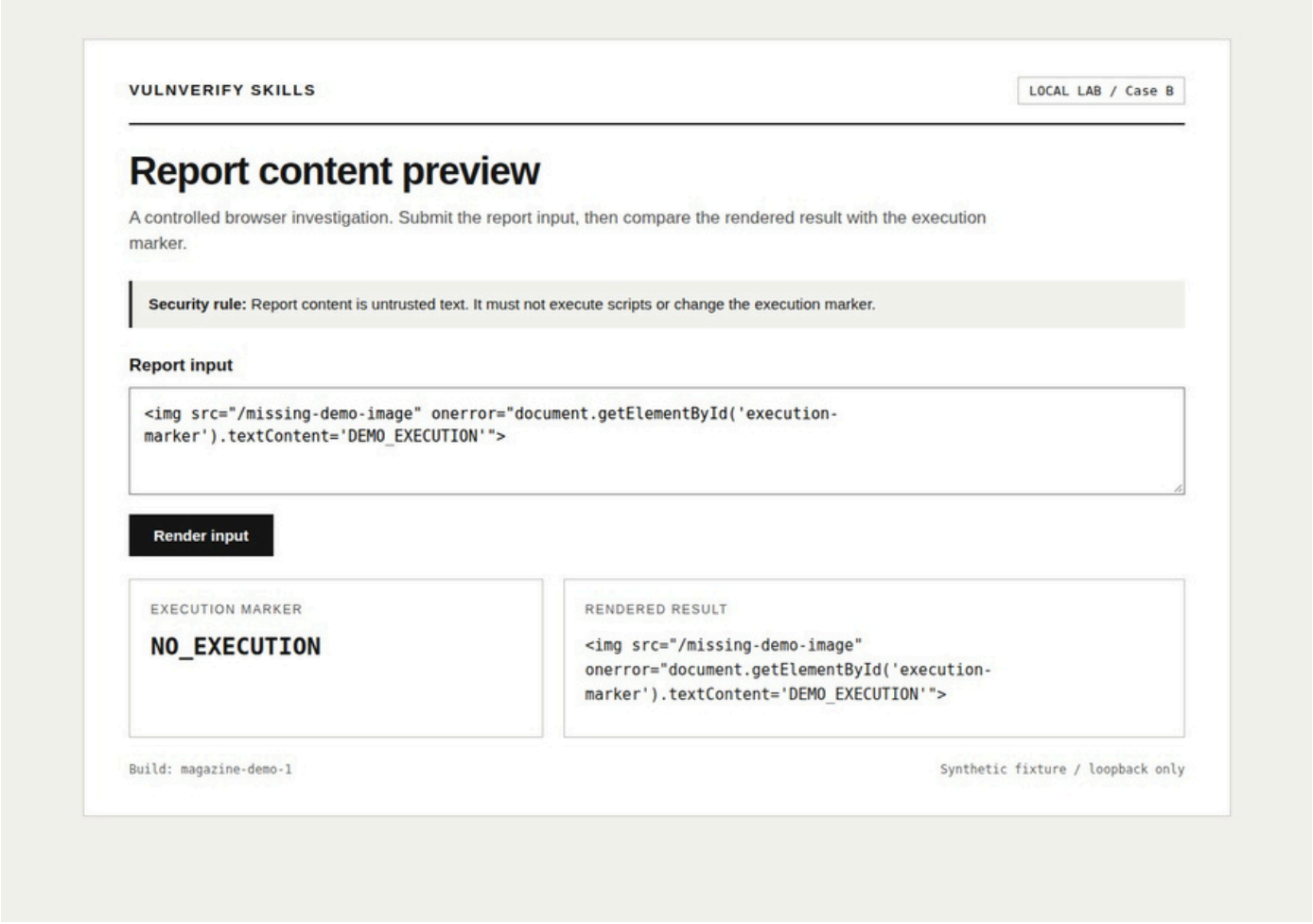
Pemeriksaan implementasi laboratorium menunjukkan bahwa handler A memasukkan string melalui innerHTML. Respons halaman yang disajikan dibandingkan dengan keluaran kode fixture agar penjelasan tersebut terhubung dengan aplikasi yang benar-benar diuji. Temuan ini tidak hanya bergantung pada nama API yang tampak berbahaya: efek eksekusinya diamati melalui formulir asli.

Verdict untuk klaim terbatas tersebut adalah Confirmed. Yang terbukti ialah pelanggaran aturan teks menjadi eksekusi script dan perubahan marker pada fixture A. Bukti ini tidak mendukung klaim tambahan tentang pencurian cookie, pengambilalihan akun, persistensi, atau serangan terhadap pengguna lain.

KASUS B / FALSE POSITIVE

Kasus B Memerlukan Bukti untuk Membantah Klaim

Laporan B menganggap kemunculan string menyerupai HTML di preview sebagai bukti eksekusi. Pengujian tidak menerima anggapan itu sebagai kesimpulan. Teks biasa terlebih dahulu berhasil diproses pada halaman B. Sesudah navigasi baru, payload yang sama dikirim melalui formulir B.



Gambar 3. Kasus B menampilkan payload sebagai teks. Bukti struktur DOM dan handler yang sesuai dengan build mendukung pembantahan klaim eksekusi pada jalur ini.

Marker tetap NO_EXECUTION. Pemeriksaan tidak berhenti pada tidak adanya efek tersebut. Preview berisi string payload secara literal, jumlah elemen anaknya nol, dan tidak ada elemen gambar yang terbentuk. Implementasi yang sesuai dengan respons halaman memakai textContent untuk penempatan string itu, sehingga input tidak diproses menjadi markup pada jalur yang diperiksa.

Verdict untuk klaim B adalah False Positive. Dasarnya ialah bukti bahwa kondisi yang dibutuhkan untuk menjalankan handler tidak terbentuk, ditambah pembanding yang berhasil dan pemeriksaan implementasi. Kesimpulan ini berlaku untuk input, halaman, dan build yang diperiksa. Keamanan semua halaman atau payload lain belum dinilai.

Membaca Verdict Bersama Batas Buktinya

VulnVerify menggunakan tiga hasil akhir: **Confirmed** ketika bukti memadai mendukung pelanggaran yang diklaim; **False Positive** ketika bukti afirmatif membantah kondisi penting klaim; dan **Inconclusive** ketika masih ada informasi penting yang belum terselesaikan. Reproduksi yang gagal, timeout, atau lingkungan yang tidak tersedia tidak otomatis menghasilkan False Positive.

CONFIRMED

FALSE POSITIVE

INCONCLUSIVE

Sebelum verdict, fp-check meninjau enam gate: *Process*, *Reachability*, *Real Impact*, *PoC Validation*, *Math Bounds*, dan *Environment*. Pemeriksaan yang tidak relevan perlu diberi alasan. Dalam contoh ini, tidak ada klaim *overflow* atau pelanggaran batas memori, sehingga *Math Bounds* diberi N/A. *Callback* gambar yang asinkron juga tidak otomatis berarti ada race condition.

Empat perbandingan perilaku pada laboratorium ini berhasil dijalankan melalui Playwright MCP langsung menggunakan konteks browser terisolasi. Hasilnya adalah bukti fixture, bukan pengukuran akurasi model. Sesi model melalui OpenCode, Codex, atau Claude Code tidak dijalankan untuk pengambilan gambar ini. Screenshot panel klien dan kepatuhan agen terhadap seluruh langkah perlu diperiksa pada pengujian klien yang sebenarnya.

Paket pendamping menyediakan dua laporan PDF dengan nama netral, prompt terpisah, kode laboratorium, empat screenshot asli, dan kunci investigasi. Untuk mencoba sendiri, jalankan lab/server.py, pastikan tiga skill dan Playwright MCP tersedia, lalu berikan satu laporan beserta prompt kasusnya pada sesi baru. Simpan kunci evaluasi dan hasil referensi sampai pengujian mandiri selesai agar jawaban tidak bocor ke agent.

Pada laporan nyata, pola kerjanya tetap sama: pertahankan klaim yang diuji, periksa kondisi aplikasi, dan hubungkan kesimpulan dengan bukti yang dapat ditelusuri. Manusia tetap perlu menilai hasil agent, terutama ketika bukti bertentangan atau dampak yang diklaim lebih luas daripada yang berhasil direproduksi.

Bukti demonstrasi: evidence/run-summary.json, snapshot, rekaman alat MCP, screenshot, dan REVIEWER-KEY.md dalam paket pendamping. Pengujian dilakukan pada 22 Oktober 2026 menggunakan Playwright MCP 0.0.83 dan Google Chrome 156.0.8078.47.

REFERENSI UTAMA

VulnVerify Skills — repositori dan panduan

Trail of Bits — poc-builder, revisi yang diadaptasi

Microsoft — Playwright MCP





SAAT FREEZER DIPANASKAN DARI JAUH

Serangan Siber di Prancis dan Kerapuhan Infrastruktur yang Terlupakan

BY PAKDE IWAN

Dalam satu malam, ratusan supermarket Prancis kehilangan stok pangan bukan karena data dicuri, melainkan karena freezer mereka diperintah untuk memanas. Pelajarannya melampaui dunia ritel: perangkat paling sederhana di gedung kita dapat menjadi titik lemah yang paling mahal.

Kegagalan Sistem Cold Chain

Pada malam Minggu, 11 Oktober 2026, sistem pendingin di ratusan supermarket Prancis menerima perintah yang tidak pernah dikehendaki pemiliknya: masuk ke mode defrost. Mode ini biasanya dipakai sebentar untuk mencairkan es, tetapi kali ini ia terus menyala dan memanaskan ruang pendingin. Reuters melaporkan suhu freezer dan lemari pendingin naik hingga 50°C, menimbulkan kebakaran di sejumlah toko dan merusak stok makanan. Les Mousquetaires, induk Intermarché, menyebut pemanasan berlangsung sekitar enam jam semalaman.

Skala dampaknya baru terlihat sepanjang Senin. Menurut AFP, sedikitnya 300 toko Intermarché dan Netto, kurang dari seratus toko Coopérative U, 80 supermarket Carrefour, sekitar 30 toko Monoprix, dan beberapa toko E.Leclerc terkena. Menteri Keuangan Roland Lescure kemudian menyampaikan kepada parlemen bahwa sekitar 700 dari 10.000 supermarket di Prancis terdampak.

Yang membedakan insiden ini: tidak ada data yang dicuri. Kerugiannya berupa makanan segar dan beku yang harus dibuang agar standar cold chain (rantai dingin) tetap terjaga. Intermarché menyatakan semua produk terdampak harus dimusnahkan, dan memperkirakan salah satu soal tersulit adalah asuransi yang tidak menanggung kejadian seperti ini. CEO Coopérative U, Dominique Schelcher, menyebut serangan terhadap peralatan penjaga kesegaran sebagai serangan terhadap rantai pasok pangan warga Prancis.

Pemerintah memperlakukannya sebagai isu keamanan nasional. Perdana Menteri Sébastien Lecornu meminta ANSSI, badan keamanan siber Prancis, menangani kasus ini, dan kejaksaan Paris membuka penyelidikan. Pelaku belum diketahui secara resmi.

Bukan Ransomware, Tapi Remote Control

Banyak orang mengira serangan siber selalu berupa ransomware: data dikunci, lalu tebusan diminta. Kasus Prancis berbeda. Tidak ada yang dikunci dan tidak ada tebusan yang dilaporkan. Penyerang mengambil alih panel kendali pendingin, lalu menyalakan fitur defrost yang memang sudah ada di perangkat.

Panel kendali ini disebut *controller*. Di toko modern, satu controller mengatur seluruh freezer, lemari pajang, dan ruang pendingin. Controller biasanya punya halaman web sehingga teknisi bisa memantau dan mengubah pengaturan dari jauh tanpa datang ke toko. Perangkat seperti ini termasuk Operational Technology (OT), yaitu teknologi yang menjalankan proses fisik, berbeda dari IT yang mengelola data dan aplikasi. CERT-FR, tim tanggap insiden siber Prancis, mengonfirmasi bahwa dua seri controller Danfoss, AK-SM dan AK-SC, telah dibobol. Belakangan, sistem XWEB buatan Copeland dan Dixell juga terdampak.

Masalahnya jelas: bila controller bisa dijangkau dari internet, siapa pun yang berhasil masuk memegang kendali atas proses fisik. Pada 13 Oktober, peneliti SOCRadar menemukan 4.481 halaman web controller Danfoss yang terlihat di Shodan, mesin pencari untuk perangkat yang terhubung ke internet. Sebanyak 2.898 di antaranya berada di Prancis. Kepala ANSSI, Vincent Strubel, mengimbau agar controller tersebut segera diputus dari internet, atau setidaknya dibatasi aksesnya dengan sangat ketat.

Satu catatan: otoritas belum mengumumkan bagaimana penyerang masuk. Beberapa laporan menyebut password lemah, termasuk password yang mengikuti tanggal hari itu. Namun The Register menegaskan bahwa titik masuk belum dikonfirmasi, dan celah yang pernah diungkap peneliti belum terbukti dipakai dalam serangan ini.

Celah yang Sudah Diketahui, tetapi Belum Ditutup

Ironisnya, kelemahan perangkat ini bukan rahasia. Tim peneliti Claroty Team82 menemukan tiga celah pada halaman web Danfoss AK-SM 800A. Salah satunya adalah mekanisme "code-of-the-day" tersembunyi: perangkat menerima kode yang dihitung dari tanggal hari itu dan melewati kata sandi administrator. Celah lainnya adalah command injection yang memungkinkan penyerang menjalankan perintah dari jauh. Danfoss menerbitkan advisory keamanan pada Maret 2025, dan badan siber Amerika Serikat, CISA, mengeluarkan peringatan pada Mei 2025. Claroty juga mencatat 2.765 controller seri ini terbuka ke internet.

Mengapa celah yang sudah diperbaiki tetap berujung bencana? Karena banyak perangkat di lapangan tidak diperbarui. Danfoss menyatakan toko yang terdampak memakai firmware lama, dan sebagian unit adalah model yang tidak lagi menerima pembaruan keamanan. SOCRadar mencatat AK-SM 800 berstatus end-of-life (tidak lagi didukung produsen) sejak Mei 2021, dan AK-SC 355 dihentikan sejak 2016. Untuk perangkat seperti itu, patching tidak mungkin dilakukan, sehingga satu-satunya pertahanan adalah menata jaringan: memutus atau mengisolasi akses dari internet.

Skema fungsi pengendalian; tidak menetapkan jalur masuk serangan.



Pola serupa pernah terjadi. Buletin Danfoss pada Oktober 2025 mencatat serangan terhadap controller AK-SM 800 di 16 supermarket Rusia dan 40 toko Israel pada 2022. Seluruh toko Israel itu tidak memiliki firewall (penyaring lalu lintas jaringan) atau VPN (jalur akses jarak jauh yang terenkripsi) yang memadai. Reuters juga mencatat kemiripan insiden ini dengan gangguan pendingin di sekitar selusin toko militer AS pada akhir Agustus, meski belum terbukti ada kaitannya.

Siapa pelakunya masih terbuka. Beberapa ahli yang dikutip BetaNews menilai ini tampak seperti aksi sederhana yang dimungkinkan oleh *update* yang dilewatkan dan halaman web yang terbuka, bukan operasi negara yang canggih. Gambarannya juga belum rapi: CEO Coopérative U mengatakan perusahaannya bukan pelanggan Danfoss, dan serangan dilaporkan berlanjut ke toko berperangkat Dixell serta ke Belgia dan Spanyol. Penyelidikan masih berjalan.



Empat Implikasi Bagi Keamanan Bisnis

Siapapun pelakunya, kasus ini memberi empat pelajaran bagi perusahaan di sektor apa pun yang memakai perangkat terhubung. **Urgensinya meningkat: Claroty memperingatkan bahwa kecerdasan buatan (AI) mempercepat pemindaian sistem yang rentan, sehingga serangan serupa bisa dilakukan lebih luas dan lebih cepat.**

1. Risiko OT adalah risiko bisnis: Dampaknya berupa stok yang dimusnahkan, toko yang terhenti, dan kebakaran, bukan kebocoran data. Asuransi yang ada juga belum tentu menanggungnya, seperti diingatkan Intermarché. Karena itu, pertanyaan tentang ketahanan OT perlu sampai ke direksi, bukan berhenti di manajer fasilitas.

2. Anda tidak bisa melindungi apa yang tidak Anda lihat: Ribuan *controller* terlihat di internet. Langkah pertama yang paling murah adalah mendaftar aset yang jujur: perangkat apa saja di setiap lokasi, versi firmware-nya, siapa vendornya, dan apakah bisa dijangkau dari luar.

3. Akses jarak jauh vendor harus dijaga: *Controller* dibuka ke internet karena teknisi ingin memecahkan masalah dari jauh. Kemudahan itu perlu diimbangi dengan network segmentation (memisahkan jaringan agar satu gangguan tidak merambat), VPN, autentikasi yang kuat, dan pencatatan siapa yang masuk. Danfoss mencatat bahwa semua toko Israel yang diserang pada 2022 tidak punya firewall atau VPN yang memadai.

4. Siapkan rencana untuk perangkat yang tidak bisa di-patch, dan jangan percaya pada satu layar: Perangkat *end-of-life* perlu perlindungan tambahan: isolasi, penggantian terjadwal, dan pemantauan. Riset Claroty bahkan mendemonstrasikan bahwa controller yang sudah dikuasai dapat mematikan pendingin sambil memalsukan suhu yang tampil di layar. Oleh karena itu, sensor suhu independen dan prosedur manual saat ada anomali sama pentingnya dengan patching.

Bagaimana dengan Indonesia?

Artikel ini tidak menyatakan bahwa perangkat yang sama banyak dipakai di Indonesia; data publik untuk itu belum tersedia. Pertanyaan yang lebih mendasar: **Apakah organisasi tahu perangkat apa saja yang mengendalikan proses fisik mereka dan siapa yang bisa mengaksesnya?**

Menurut penilaian **Punggawa Cybersecurity,** struktur risikonya mirip di dalam negeri. Jaringan ritel dengan ribuan gerai, industri perikanan dan pengolahan makanan, distribusi obat dan vaksin, hingga pusat data dan pabrik bergantung pada sistem yang dikelola dari jauh oleh kontraktor atau vendor. Di negara tropis, pendinginan bukan kemewahan, melainkan syarat operasional. Sebuah studi akademik 2025 mengkaji hambatan yang dihadapi organisasi Indonesia dalam mengadopsi *cyber resilience*, dengan latar belakang bahwa Indonesia menghadapi serangan yang semakin canggih.

Kabar baiknya, pelajaran dari Prancis tidak menuntut anggaran besar. Daftar aset, pemisahan jaringan, kontrol akses vendor, dan latihan respons insiden adalah langkah yang bisa dimulai bulan ini.

KETERGANTUNGAN DI BALIK OPERASI



Dari Kesadaran Menuju Ketahanan: Pendekatan Punggawa Cybersecurity

Kasus Prancis menunjukkan bahwa ketahanan siber tidak berhenti di jaringan kantor. Oleh karena itu, **Punggawa Cybersecurity memperluas layanannya ke OT/Industrial Security, yaitu keamanan untuk sistem yang mengendalikan proses fisik, seperti ICS dan SCADA (sistem pengendali industri)**. Layanan ini melengkapi Punggawa Cyber Resilience Framework. **Alasannya sederhana: di fasilitas yang bergantung pada ICS dan SCADA, kegagalan keamanan berarti kegagalan fisik, bukan sekadar gangguan data.** Empat kapabilitas berikut menjawab langsung pelajaran dari Prancis, sebagai berikut.

DARI PELAJARAN KE KAPABILITAS OT/ICS

Pelajaran dari Prancis	Kapabilitas OT/ICS Punggawa Cybersecurity	Hasil yang diinginkan
Perangkat tak terlihat dan terbuka ke internet	OT Asset Visibility & Network Segmentation	Daftar aset OT dan pemisahan jaringan yang memutus jalur dari internet
Celah lama yang tak kunjung ditutup	ICS/SCADA Vulnerability Assessment & Penetration Testing	Daftar celah yang diprioritaskan, termasuk perangkat yang tidak bisa lagi di-patch
Anomali yang tak terdeteksi	OT-Specific Threat Detection (CSOC Integration)	Perilaku tidak wajar pada perangkat OT terpantau oleh tim keamanan yang sama dengan IT
Respons yang lambat dan stok yang terbuang	OT Incident Response & Forensics	Prosedur pemulihan yang teruji, bukti forensik, dan bahan perbaikan

Layanan ini berpijak pada dua rujukan yang diadopsi Punggawa Cybersecurity. IEC 62443 adalah rangkaian standar internasional untuk keamanan sistem otomasi dan kontrol industri. NIST SP 800-82 adalah panduan keamanan OT dari lembaga standar Amerika Serikat. Keduanya memberi bahasa yang sama bagi tim keamanan, tim teknik, dan vendor, sesuatu yang sering tidak ada justru saat insiden terjadi.

Urutan kerjanya sengaja sederhana: lihat dulu, baru lindungi. Dengan *asset visibility* (mengetahui perangkat apa saja yang ada dan siapa yang bisa mengaksesnya), kita tahu bagian jaringan mana yang harus dipisahkan. Hasil pengujian menentukan prioritas perbaikan. Deteksi yang terhubung ke CSOC (pusat pemantauan keamanan) memastikan sinyal dari pabrik atau ruang mesin toko tidak berhenti di layar teknisi. Pengujian di lingkungan OT juga harus dirancang berbeda dari IT, karena proses yang sedang berjalan tidak boleh terganggu oleh pengujinya sendiri.

Tidak semua organisasi memakai *controller* Danfoss, tetapi hampir semua punya perangkat serupa: bekerja diam-diam, dikelola vendor, dan jarang masuk daftar aset. Di situlah percakapan tentang ketahanan sebaiknya dimulai, dan tim **Punggawa Cybersecurity** terbuka untuk berdiskusi dengan para pemimpin bisnis dan teknologi yang ingin memulainya.

5 Pertanyaan Kritis Sebelum Terjadi Insiden!

Pertanyaan berikut ditujukan bagi pembaca untuk diajukan di rapat direksi perusahaannya sendiri. Jawaban yang ragu-ragu atas pertanyaan tersebut bukan tanda kegagalan, melainkan daftar pekerjaan pertama yang paling berguna.

- **Apakah kita memiliki daftar lengkap perangkat OT di setiap lokasi, termasuk yang dipasang vendor, beserta versi firmware-nya?**
- **Apakah perangkat *interface* tersebut dapat dijangkau langsung dari internet dan kapan terakhir kali hal itu diperiksa?**
- **Siapa saja yang memiliki akses jarak jauh, melalui jalur apa, dan apakah akses itu dibatasi serta dicatat?**
- **Berapa banyak perangkat yang sudah *end-of-life*, dan apa rencana penggantian atau kontrol kompensasinya?**
- **Jika suhu atau proses menyimpang malam ini, siapa yang akan tahu, seberapa cepat, dan apakah asuransi kita menanggung kerugiannya?**

REFERENSI UTAMA

Reuters — insiden pendingin Prancis
Claroty Team82 — riset controller
NIST SP 800-82 Rev. 3 — keamanan OT

IT vs OT

Ketika Prioritas Bukan Lagi Kerahasiaan Data, tapi Keselamatan Manusia

BY PAKDE IWAN



Satu *Scan*, Satu Lini Produksi Berhenti

Bayangkan sebuah Jumat sore di pabrik. Tim IT menjalankan vulnerability scan rutin, persis seperti yang mereka lakukan setiap bulan di jaringan kantor. Beberapa menit kemudian, sebuah PLC di lini produksi tiba-tiba restart, dan mesin-mesin berhenti di tengah proses.

Bagi tim IT, itu hanya pemindaian biasa. Bagi tim OT, itu insiden: produksi terhenti, bahan baku terancam terbuang, dan operator di lapangan harus memastikan tidak ada yang terluka. Skenario seperti ini sering dibahas di kalangan praktisi, sebab banyak perangkat industri lama memang tidak dirancang untuk menerima lalu lintas pemindaian yang agresif.

Lalu siapa yang salah? Sebenarnya tidak ada. Kedua tim bekerja dengan benar menurut aturan di dunianya masing-masing. Persoalannya, aturan itu berbeda, dan jarak di antara dua dunia itulah yang ingin kita telusuri dalam tulisan ini.

Tujuannya sama: Semua orang pulang dengan selamat.

Dua Dunia, Dua Budaya

Untuk memahami mengapa dua tim yang sama-sama pintar bisa berselisih, kita perlu melihat dunia tempat mereka bekerja. IT, singkatan dari *Information Technology*, mengurus server, laptop, aplikasi, dan database. Tugas utamanya adalah menjaga data tetap aman dan layanan digital tetap hidup. **OT**, atau *Operational Technology*, mengurus mesin dan proses fisik: PLC yang mengatur motor dan katup, sensor yang membaca suhu dan tekanan, sistem SCADA dan layar HMI tempat operator memantau seluruh proses, serta panel kontrol yang dijaga oleh insinyur dan teknisi.

Kebiasaan kerja keduanya pun berbeda. Orang IT hidup dengan *update* rutin, *reboot*, dan penggantian perangkat setiap beberapa tahun. Orang OT hidup dengan prinsip yang hampir kebalikannya: kalau sudah jalan, jangan diutak-atik. Sistem mereka dirancang untuk beroperasi belasan hingga puluhan tahun, dan berhenti sebentar saja bisa merugikan, bahkan membahayakan. **Menambal sistem di dunia IT berarti menjadwalkan reboot di malam hari; di dunia OT, itu bisa berarti menunggu jendela perawatan yang datang setahun sekali.**

Bahasa sehari-hari mereka juga berlainan. Apa yang di kantor disebut server, di lantai produksi kurang lebih adalah HMI atau server SCADA. Apa yang di kantor disebut endpoint, di lapangan adalah PLC atau RTU yang langsung menggerakkan mesin. Kebijakan password ketat yang masuk akal bagi karyawan kantor bisa menjadi masalah bagi operator yang butuh akses cepat saat keadaan darurat. Dan pemindaian aktif yang lumrah di IT berubah menjadi hal yang harus dihindari di OT, digantikan pemantauan pasif yang hanya mendengarkan lalu lintas jaringan.

Kedua kebiasaan itu sama-sama masuk akal di habitatnya. Perbedaan yang paling dalam ternyata bukan pada alat, melainkan pada apa yang paling ditakuti.

Prioritas yang Terbalik

Apa yang paling ditakuti orang IT? Jawabannya tercermin dalam urutan prioritas yang dikenal sebagai CIA: *Confidentiality* (kerahasiaan), *Integrity* (keutuhan), lalu *Availability* (ketersediaan). Pertanyaan yang selalu mereka ajukan adalah apakah data kita bocor atau berubah tanpa izin.

Di dunia OT, urutan itu cenderung terbalik, dan ada satu unsur tambahan yang hampir tidak dikenal dunia IT: Safety, atau keselamatan. Pertanyaannya berbeda. Apakah proses tetap berjalan dengan aman? Apakah semua orang tetap selamat? Setelah keselamatan, barulah ketersediaan (proses terus berjalan), keutuhan (perintah dan data proses tidak berubah), dan terakhir kerahasiaan. Urutan ini adalah pola
umum di kalangan praktisi, bukan aturan baku, tetapi cukup menggambarkan cara berpikir tim OT.

Perbedaan urutan itu muncul dalam keputusan sehari-hari. **Bagi tim IT, *downtime* adalah ketidaknyamanan; bagi tim OT, *downtime* bisa berarti kerugian besar atau situasi berbahaya. Insiden di IT biasanya berujung pada kebocoran data dan kerugian finansial, sedangkan insiden di OT bisa berujung pada cedera, kerusakan lingkungan, atau layanan publik yang terhenti.** Itulah sebabnya tim OT sering terlihat keras kepala soal patch dan perubahan.

Perlu dipahami, tim OT tidak menganggap data tidak penting. Mereka hanya menghitung bahwa proses yang salah arah bisa melukai orang, sedangkan data yang bocor tidak. **Dan karena dampak serangan OT tidak berhenti di layar, pertanyaan berikutnya menjadi relevan bagi siapa saja: siapa sebenarnya yang bergantung pada sistem-sistem ini?**

IT: Kerahasiaan Ketersediaan → Keutuhan

OT: Keselamatan → Keutuhan → Ketersediaan Kerahasiaan

OT di Luar Lantai Produksi: Menopang Infrastruktur dan Aktivitas Harian

Jika Anda bekerja di bank, startup, rumah sakit, atau kantor pemerintahan, mungkin OT terasa seperti urusan orang pabrik dan kilang. Coba ikuti satu hari biasa dan lihat seberapa sering Anda bersentuhan dengannya.

Pagi hari, lampu menyala dan air mengalir dari keran. Keduanya hasil kerja sistem kontrol di pembangkit listrik dan instalasi pengolahan air, yang mengatur aliran daya, tekanan pipa, dan dosis bahan kimia tanpa kita sadari. Dalam perjalanan ke kantor, kereta, lampu lalu lintas, dan pelabuhan yang memasok barang ke toko-toko bergantung pada sistem sejenis. Di gedung kantor, lift, pendingin udara, dan kontrol akses digerakkan oleh building automation. Makanan yang kita santap siang hari melewati lini produksi dan rantai dingin yang suhunya dijaga ketat, dan kalau jatuh sakit, ventilator serta pompa infus di rumah sakit bekerja dengan prinsip yang sama. Bahkan aplikasi yang kita buka sepanjang hari tetap hidup berkat pendingin dan pasokan listrik di data center.

Semua itu ditopang OT. Artinya, hampir setiap sektor punya ketergantungan tersembunyi pada sistem kontrol industri, dan ketergantungan itu saling terhubung. Listrik yang padam bukan hanya membuat lampu mati: bank, rumah sakit, dan operator telekomunikasi ikut terganggu, dan efeknya menjalar dari satu sektor ke sektor lain seperti domino. Pelanggan, pasien, dan pengguna layanan bisa menjadi korban tidak langsung meskipun bukan target serangan. Perusahaan retail atau e-commerce pun bisa lumpuh hanya karena pemasok atau pelabuhan langganannya terganggu.

Itu sebabnya batas antara IT dan OT makin terasa tipis. Dalam beberapa kasus yang akan kita bahas sebentar lagi, serangan bermula dari sisi IT, tetapi ujungnya menghentikan operasi di lapangan. Edisi ini pun sudah menyinggung sisi lain dari kerapuhan itu lewat artikel tentang serangan siber di Prancis yang menyasar freezer, contoh bagaimana infrastruktur yang sering terlupakan bisa menjadi titik lemah.

OT MENOPANG LAYANAN SEHARI-HARI:



Air bersih **Transportasi** **Gedung** **Kesehatan** **Pusat data**

Bagaimana dengan Indonesia?

Pertanyaan yang wajar muncul: seberapa dekat semua ini dengan kita? Gambaran yang tersedia saat ini menunjukkan dua hal sekaligus. Di satu sisi, sistem kontrol industri di Indonesia ikut menjadi sasaran ancaman. Di sisi lain, kerangka hukum untuk melindunginya mulai terbentuk, meski belum lengkap.

Mulai dari datanya. Menurut Kaspersky ICS CERT, 21,81% komputer ICS di Indonesia memblokir objek berbahaya pada kuartal I/2026, sedikit di atas rata-rata global sebesar 19,6%. Sektor migas paling menonjol: 28% komputer ICS di sektor itu mendeteksi dan memblokir objek berbahaya pada Januari–Maret 2026. Kaspersky menilai masih banyak perusahaan industri yang menjalankan sistem OT yang sudah lama sehingga mudah dieksploitasi. Sebagai latar yang lebih luas, BSSN mencatat lebih dari 5,16 miliar anomali trafik di Indonesia sepanjang 2025.

Angka-angka ini perlu dibaca dengan hati-hati. Yang diukur adalah komputer ICS yang berhasil memblokir *malware*, bukan serangan yang berhasil mengganggu operasi, dan datanya berasal dari satu vendor keamanan. Fungsinya lebih sebagai penunjuk tekanan ancaman daripada penghitung insiden.

21,81 %

Komputer ICS di Indonesia yang memblokir objek berbahaya pada Q1/2026, menurutKaspersky ICS CERT.

Dari sisi regulasi, fondasinya adalah Perpres 82/2022 tentang Perlindungan Infrastruktur Informasi Vital (IIV), yang ditetapkan pada 24 Mei 2022 dengan BSSN sebagai koordinator. Sektor yang dicakup terbagi menjadi delapan sektor strategis nasional, antara lain administrasi pemerintahan, energi dan sumber daya mineral, transportasi, keuangan, pangan, dan pertahanan. Bagian yang paling relevan bagi pembahasan kita ada di Peraturan BSSN Nomor 8 Tahun 2023: IIV didefinisikan sebagai sistem elektronik yang memanfaatkan teknologi informasi dan/atau teknologi operasional. Dengan kata lain, OT secara hukum sudah ikut dilindungi. Peraturan itu juga menetapkan bahwa target penerapan kontrol keamanan ditentukan dari pengukuran tingkat kematangan keamanan siber, dengan target paling rendah pada level tiga dari lima level, dan hasil pengukurannya diverifikasi oleh BSSN.

Di level undang-undang, pembahasannya masih berjalan. Komisi I DPR dan pemerintah sepakat memulai pembahasan RUU Keamanan dan Ketahanan Siber pada 29 Juni 2026, dan per awal Juli RUU itu masih dibahas melalui sejumlah rapat di Komisi I.

Masih ada pekerjaan rumah. Skor National Cybersecurity Index Indonesia turun dari 63,64 (peringkat 48 dari 136 negara) pada 2023 menjadi 47,50 (peringkat 84) pada 2025. Dalam Rakornas BSSN 2025, Kementan juga menyampaikan bahwa regulasi turunan Perpres 82/2022 masih dibutuhkan, khususnya untuk sektor pertahanan dan transportasi.

Maka ada satu pertanyaan yang layak dibawa pulang oleh siapa pun, apa pun profesinya. **Jika listrik di kota Anda mati 24 jam karena serangan siber, layanan apa di tempat Anda bekerja yang ikut berhenti?**

Ketika Dunia Digital Menyentuh Dunia Fisik

Risiko OT bukan sekadar teori. Sejarah serangan siber ke sistem industri punya beberapa kasus yang memperlihatkan dengan jelas seperti apa wujudnya, dan masing-masing menunjukkan wajah yang berbeda.

2015

Operasi manual menjadi cadangan.

Kasus yang paling sering menjadi rujukan terjadi di Ukraina. Pada 23 Desember 2015, perusahaan listrik di Ukraina mengalami pemadaman tidak terjadwal yang berdampak pada banyak pelanggan, dan investigasi menyimpulkan bahwa penyebabnya adalah penyerang dari luar. Sekitar 225.000 pelanggan di tiga wilayah kehilangan listrik, dengan pemadaman yang berlangsung hingga sekitar enam jam. Di pusat kontrol, layar HMI mulai membuka dan menutup pemutus sirkuit tanpa perintah operator. Kasus ini disebut sebagai serangan siber berhasil pertama yang terdokumentasi secara publik terhadap sistem kontrol jaringan listrik. Yang menyelamatkan keadaan adalah hal yang sederhana: operator masih bisa menjalankan pemutus secara manual, sehingga listrik pulih. Kemampuan beroperasi tanpa otomasi ternyata menjadi cadangan yang sangat berharga.

2017

Sistem keselamatan menjadi sasaran.

Dua tahun kemudian, sasaran serangan bergeser ke sesuatu yang jauh lebih mengkhawatirkan. Pada 2017, *malware* yang dikenal sebagai TRITON (atau TRISIS) menyerang sistem keselamatan di sebuah pabrik petrokimia di Timur Tengah. Yang diincar adalah Triconex, sistem yang bertugas memicu penghentian darurat ketika kondisi menjadi berbahaya, ibarat lapisan pertahanan terakhir bagi manusia di dalam pabrik. Penyerang masuk lewat jaringan IT, lalu bergerak ke jaringan OT sampai ke sistem keselamatan itu. Ironisnya, mereka ketahuan karena cacat pada kode malware yang memicu sistem pengaman dan menghentikan pabrik dua kali. TRITON dikenal sebagai *malware* pertama yang dirancang untuk menargetkan sistem keselamatan industri. Menjadikan lapisan pelindung nyawa sebagai sasaran mengubah sifat ancaman dari kerugian bisnis menjadi risiko keselamatan manusia.

Serangan Colonial Pipeline (2021)

Kasus ketiga memperlihatkan hal yang berbeda lagi: serangan yang bermula dari IT tetapi berdampak fisik. Pada Mei 2021, *ransomware* DarkSide menyerang jaringan IT Colonial Pipeline, termasuk sistem penagihan, sedangkan sistem OT yang menggerakkan minyak tidak dikompromikan secara langsung. Meski begitu, perusahaan memilih menghentikan operasi pipa sebagai langkah pencegahan, dan akibatnya terlihat di jalanan: pembelian panik dan antrean panjang di SPBU. Menurut laporan CNN, salah satu pertimbangannya adalah kekhawatiran perusahaan tidak bisa menagih pelanggan untuk bahan bakar yang tersalurkan. **Pelajarannya, batas antara IT dan OT bukan tembok kedap. Ketika sistem bisnis lumpuh dan perusahaan tidak yakin seberapa jauh penyusupan terjadi, operasi fisik ikut berhenti.**

Kasus lain yang kerap memicu diskusi adalah insiden pengolahan air di Oldsmar, Florida, pada Februari 2021. Laporan awal menyebut peretas mengakses komputer kontrol via perangkat lunak remote untuk mengacak dosis sodium hidroksida. Namun, pejabat kota belakangan mengklarifikasi bahwa insiden tersebut bukanlah hasil dari serangan siber. Mengingat kronologi resminya masih diperdebatkan, kasus ini lebih tepat dipandang sebagai catatan kritis ketimbang preseden utama.

Dari ketiga kasus utama tadi tampak pola yang sama: celah sering kali bukan di mesinnya, melainkan di cara organisasi mengelola sambungan antara dua dunia itu.

Pola Kesalahan Berulang

Dari kasus-kasus tadi dan pengalaman para praktisi, terlihat beberapa kesalahan yang berulang di banyak organisasi. Yang paling umum adalah menerapkan kebijakan IT mentah-mentah ke dunia OT: password *lockout* yang mengunci operator justru saat kondisi darurat, pembaruan otomatis yang membuat mesin restart pada waktu yang salah, atau pemindaian agresif yang menjatuhkan perangkat lama, seperti dalam skenario di awal tulisan ini.

Kesalahan kedua lebih halus, yaitu mengira OT aman karena "terisolasi". Pada praktiknya, selalu ada jalur yang menghubungkan, entah laptop teknisi, USB, akses remote dari vendor, atau koneksi ke jaringan kantor. Kasus TRITON mengingatkan kita bahwa penyerang justru masuk lewat IT lalu menyeberang ke OT. Berkaitan dengan itu, banyak organisasi tidak benar-benar tahu apa saja yang mereka miliki. Tanpa inventaris aset, sulit memantau, menambal, atau bahkan menyadari ada perangkat yang terhubung ke internet.

K**esalahan terakhir muncul setelah insiden. Tim IT menunjuk OT yang "tidak mau di-patch", tim OT menunjuk IT yang "mengganggu produksi", padahal keduanya tidak pernah berlatih menghadapi insiden bersama.** Dan di balik semua itu sering ada satu alasan yang menenangkan sekaligus menyesatkan: "belum pernah ada kejadian". Kalimat itu sering kali berarti belum pernah ada yang mengamati.

ASUMSI YANG PERLU DIUJI

“Belum pernah ada kejadian”

Membangun Jembatan IT-OT

Kabar baiknya, kedua tim tidak perlu saling mengalah. Yang dibutuhkan adalah bahasa dan kebiasaan kerja bersama. Titik awal yang paling praktis adalah inventaris aset yang disusun bersama, karena tidak ada yang bisa dilindungi kalau keberadaannya belum diketahui. Dari situ, insinyur OT perlu dilibatkan sejak awal dalam setiap keputusan keamanan di lantai produksi, sebab merekalah yang paling paham dampak sebuah perubahan terhadap keselamatan proses.

Berikutnya, kedua tim perlu memakai bahasa risiko yang sama. Alih-alih hanya berdebat soal skor kerentanan, ukur dampaknya dalam hal keselamatan, kelangsungan produksi, dan layanan kepada masyarakat. Dalam praktik teknis, ini berarti memantau secara pasif lebih dulu untuk mengenali lalu lintas jaringan, dan menguji setiap perubahan di lingkungan percobaan sebelum menyentuh sistem yang berjalan. Pintu belakang pun perlu dikunci: akses remote vendor dibatasi dan diawasi, dan jaringan IT dipisahkan dari OT lewat segmentasi yang jelas.

Namun, semua itu tidak akan berjalan tanpa kepercayaan, dan kepercayaan dibangun sebelum krisis datang. Simulasi insiden lintas tim serta pertukaran peran, misalnya orang IT turun ke lapangan dan orang OT belajar dasar siber, membuat kedua pihak saling mengenal cara berpikir satu sama lain.

Untuk acuan teknis, ada seri standar IEC 62443 yang dikembangkan karena langkah keamanan IT tidak selalu cocok untuk sistem otomasi dan kontrol industri. Bagi penyelenggara infrastruktur vital di Indonesia, peraturan BSSN juga mengatur pengukuran tingkat kematangan keamanan siber, sehingga kerja sama IT-OT relevan dengan kepatuhan, bukan sekadar niat baik.

Apa yang Bisa Anda Lakukan?

Anda tidak perlu bekerja di pabrik untuk mulai peduli, hanya saja langkah pertamanya berbeda menurut peran. **Bagi praktisi IT dan SOC, langkah awalnya adalah mempelajari protokol dan prioritas OT, serta tidak menjalankan pemindaian aktif di jaringan industri tanpa berkoordinasi dengan tim operasi.** Bagi insinyur dan operator OT, yang terpenting adalah mengenali tanda anomali, seperti layar yang bergerak sendiri atau perubahan pengaturan yang tidak dikenal, melaporkannya, dan menghindari pemasangan USB atau perangkat yang tidak dikenal.

Di level manajemen dan kepatuhan, pekerjaannya adalah memetakan layanan mana yang bergantung pada OT dan pemasok mana yang menjalankannya, lalu mengadakan latihan simulasi krisis. Pembahasan tentang kepatuhan dan perlindungan data pribadi di artikel lain pada edisi ini bisa menjadi pelengkap yang baik. Adapun bagi pembaca umum, kontribusinya dimulai dari kesadaran bahwa layanan dasar yang kita pakai setiap hari, dari listrik sampai air bersih, bergantung pada sistem yang bisa diserang, dan dari dukungan terhadap transparansi penyedia layanan publik.

Penutup: Pulang dengan Selamat

Di dunia IT, tolok ukur keberhasilan keamanan adalah data yang tetap aman. **Di dunia OT, tolok ukurnya lebih sederhana dan lebih berat: semua orang pulang dengan selamat dan layanan yang menopang hidup banyak orang tetap berjalan.**

IT dan OT tidak harus menjadi sama. Yang perlu mereka miliki adalah pemahaman bahwa mereka menjaga hal yang sama dari sisi yang berbeda.

Jadi, sekali lagi: jika listrik di kota Anda mati 24 jam karena serangan siber, layanan apa di tempat Anda bekerja yang ikut berhenti, dan siapa yang akan Anda hubungi lebih dulu, tim IT atau tim OT?

REFERENSI UTAMA

CISA — serangan infrastruktur Ukraina
Peraturan BSSN No. 8 Tahun 2023
Schneider Electric — standar IEC

DARI INSIDEN SIBER KE KEPATUHAN

Memahami Arah Baru Pelindungan Data Pribadi

BY MAS MIRZA

Pada September 2026, perusahaan teknologi kesehatan Veradigm di Amerika Serikat mengungkap insiden kebocoran data yang melibatkan kredensial milik vendor pihak ketiga.

Kredensial tersebut digunakan untuk mengakses API dan mengunduh sebagian data pribadi pasien. Insiden ini menjadi pengingat bahwa keamanan data tidak hanya bergantung pada sistem internal, tetapi juga pada bagaimana akses dan hubungan dengan pihak ketiga dikelola.

Akses pihak ketiga tetap bagian dari tata kelola data.



Ilustrasi konseptual: identitas, akses, dan jejak pertanggungjawaban.

Di Indonesia, persoalan seperti ini semakin relevan dengan hadirnya Peraturan Pemerintah (PP) Nomor 33 Tahun 2026 tentang Peraturan Pelaksanaan UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Ditetapkan pada 16 Juli 2026, PP ini mulai berlaku pada 16 Januari 2027 dan memperjelas pelaksanaan berbagai kewajiban pelindungan data pribadi.

Lantas, apa saja poin penting yang perlu diperhatikan organisasi?

1. Perketat Pengawasan Vendor

Penggunaan vendor atau penyedia layanan pihak ketiga tidak serta-merta memindahkan tanggung jawab pelindungan data dari perusahaan. PP 33/2026 mengatur penunjukan prosesor melalui perjanjian yang mencakup ruang lingkup pemrosesan, tujuan, hak dan kewajiban para pihak, serta mekanisme pengawasan dan audit. Tanggung jawab atas pemrosesan yang dilakukan prosesor tetap berada pada pengendali data.

Artinya, perusahaan perlu memastikan bahwa akses vendor dibatasi sesuai kebutuhan, aktivitasnya diawasi, dan tanggung jawab ketika terjadi insiden telah ditetapkan dengan jelas.

2. Evaluasi Risiko Lebih Dini

PP 33/2026 mewajibkan penilaian dampak sebelum pemrosesan yang berpotensi menimbulkan risiko tinggi terhadap subjek data. Hal ini mencakup, antara lain, pemrosesan data pribadi spesifik atau dalam skala besar serta penggunaan teknologi baru.

Penilaian tersebut membantu organisasi memahami tujuan pemrosesan, menilai risiko terhadap individu, dan menentukan langkah pengamanan yang diperlukan sebelum risiko berubah menjadi insiden.



BATASI AKSES



AWASI AKTIVITAS



BERTANGGUNG JAWAB

3. Batas Waktu Respons Insiden

3 × 24 JAM

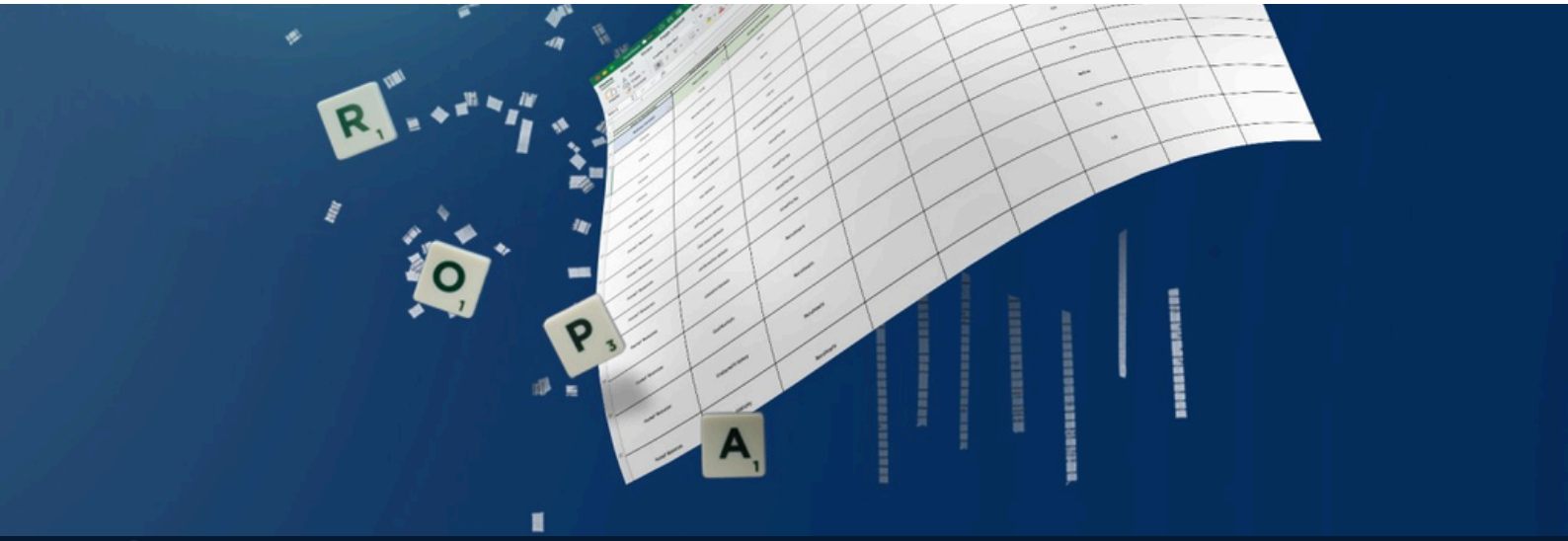
Pemberitahuan kegagalan pelindungan data

Apabila terjadi kegagalan pelindungan data pribadi, pengendali wajib menyampaikan pemberitahuan tertulis kepada subjek data pribadi dan lembaga terkait paling lambat 3 × 24 jam sejak kegagalan diketahui secara pasti, patut, dan wajar. Pemberitahuan tersebut mencakup data yang terungkap, waktu dan cara terjadinya insiden, serta upaya penanganan dan pemulihan. Organisasi juga wajib mendokumentasikan insiden dan memiliki prosedur pencegahan serta penanganan yang jelas. Jika insiden terjadi dalam pemrosesan oleh prosesor, prosesor wajib melaporkannya kepada pengendali pada kesempatan pertama.

Karena itu, perusahaan tidak cukup hanya memiliki perangkat keamanan. Prosedur eskalasi, pembagian tanggung jawab, dokumentasi bukti, dan koordinasi dengan pihak ketiga juga perlu disiapkan agar penanganan tidak terlambat. Salah satu langkah konkret yang perlu dilakukan organisasi adalah menyusun ***Record of Processing Activities*** **(ROPA) atau Rekam Aktivitas Pemrosesan Data Pribadi.** Mengacu pada Pasal 74 PP No. 33 Tahun 2026, **ROPA** berfungsi sebagai inventaris seluruh aktivitas pemrosesan data pribadi, mulai dari jenis data yang dikumpulkan, tujuan dan dasar pemrosesannya, pihak yang memiliki akses, alur perpindahan data, masa retensi, hingga langkah pengamanan yang diterapkan. **Dengan ROPA, organisasi dapat memahami bagaimana data pribadi dikelola sekaligus mengidentifikasi risiko yang perlu ditangani. Dokumen ini juga harus diperbarui ketika terdapat perubahan dan tersedia untuk keperluan pengawasan sesuai ketentuan yang berlaku.**

RoPA (*Record of Processing Activities*)

DATA	TUJUAN	AKSES	RETENSI



Kepatuhan Bukan Sekadar Kelengkapan Dokumen

PP 33/2026 juga mengatur sanksi administratif atas pelanggaran terhadap ketentuan yang relevan. Bentuknya dapat berupa peringatan tertulis, penghentian sementara pemrosesan data, penghapusan atau pemusnahan data, dan/atau denda administratif. Berdasarkan Pasal 185, denda dapat mencapai maksimal 2% dari pendapatan atau penerimaan tahunan, dengan perhitungan sesuai faktor yang ditentukan oleh peraturan. **Sanksi tidak otomatis dikenakan hanya karena suatu insiden terjadi; penerapannya bergantung pada pelanggaran dan ketentuan yang berlaku.**

Pada akhirnya, kehadiran **PP 33/2026** menjadi momentum bagi organisasi untuk mengevaluasi kembali tata kelola data, pengelolaan vendor, penilaian risiko, dan kesiapan respons insiden. Tujuan pelindungan data bukan sekadar memenuhi kewajiban regulasi, tetapi memastikan bahwa data yang dipercayakan kepada organisasi benar-benar dikelola secara bertanggung jawab.

KOMITMEN PUNGGAWA CYBERSECURITY

Sebagai bentuk komitmen terhadap pelindungan data pribadi, **Punggawa Cybersecurity** akan mendukung penerapan tata kelola pelindungan data pribadi di seluruh lingkungan organisasi melalui penyusunan kebijakan dan prosedur yang relevan, pemetaan aktivitas pemrosesan data pribadi melalui ***Record of Processing Activities*** **(ROPA),** serta peningkatan kesadaran seluruh pihak terkait. Langkah ini diharapkan dapat membantu organisasi mengidentifikasi dan mengelola risiko pemrosesan data, memperkuat kepatuhan terhadap peraturan yang berlaku, serta memastikan bahwa perlindungan data pribadi menjadi bagian penting dalam membangun kepercayaan dan keberlangsungan bisnis.

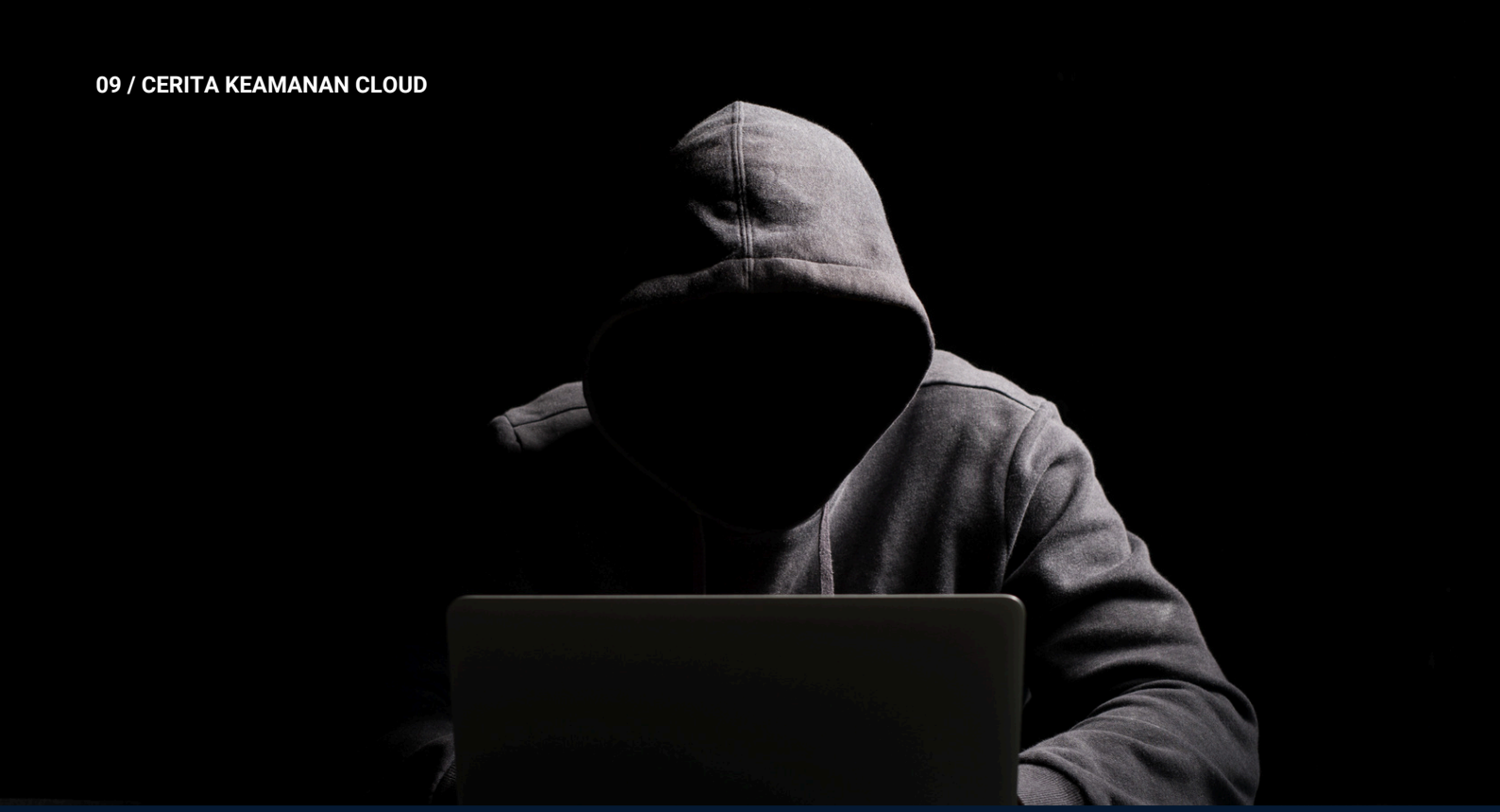


REFERENSI UTAMA

UU No. 27 Tahun 2022 — Pelindungan Data Pribadi

PP No. 33 Tahun 2026 — salinan naskah Bahasa Indonesia

Veradigm — pengungkapan insiden, SEC Form 8-K



NUSAFORM* AWS

*Perusahaan fiksi dalam artikel ini

Cerita *Startup* yang Hampir Kehilangan Data User

BY OM TONY

Empat orang, satu produk, satu AWS account

NusaForm lahir dari kebutuhan sederhana: banyak UMKM di Indonesia masih mengirim kontrak, invoice, dan foto KTP lewat WhatsApp. File tercecer, versi dokumen tertukar, dan bank partner sering meminta kirim ulang berkas yang sama.

Contoh ilustrasi:

Raka (technical founder), Dina (backend), Yoga (full-stack), dan Sinta (customer success) membangun web portal untuk mengunggah dokumen. Stack awalnya sengaja dibuat sesederhana mungkin: satu EC2 t3.small , RDS PostgreSQL, S3, Route 53 plus ACM, dan deploy via GitHub Actions (SSH ke EC2 plus upload static assets ke S3). Malam setelah first deploy, Raka menulis di grup WhatsApp "NusaForm Core Team":

“AWS-nya aman kan ya. Kan Amazon yang jaga”

Asumsi itu yang bermasalah. Dalam Shared Responsibility Model, AWS menjaga data center, hypervisor, dan infrastruktur layanan. Bucket policy, IAM role, security group, dan access key tetap merupakan tanggung jawab user. NusaForm belum sempat membedakan keduanya.

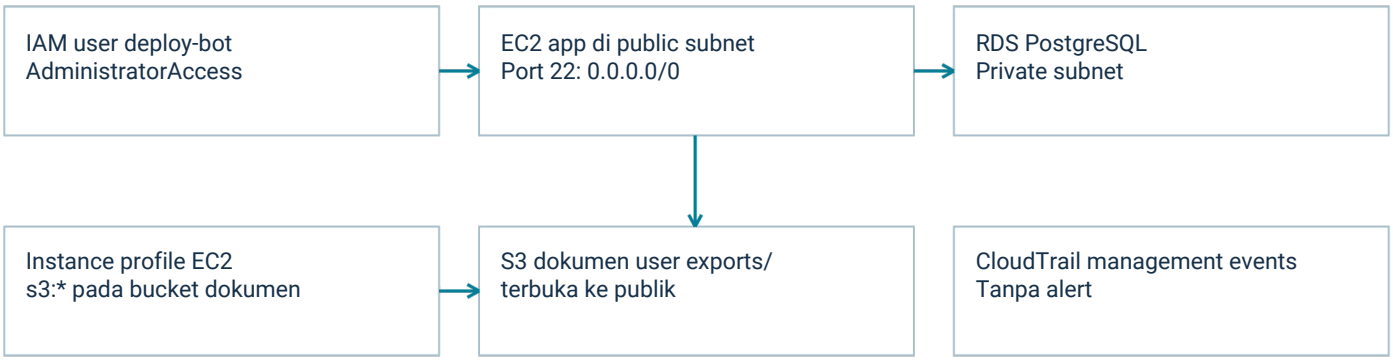
Tiga Shortcut yang Terasa Wajar, Lalu Tertinggal

Minggu pertama, yang penting tombol upload hidup. RDS ditaruh di private subnet. EC2 ditaruh di public subnet supaya hemat Application Load Balancer. Port 22 ikut dibuka ke 0.0.0.0/0 karena Raka dan Yoga sering debug dari kafe berbeda. Yoga sempat menulis TODO: restrict ke IP kantor / VPN di Notion. TODO itu tidak pernah diganti.

Untuk CI/CD, Raka membuat IAM user deploy-bot . Least privilege terasa ribet, sementara demo investor tinggal dua hari. Ia memilih AdministratorAccess , membuat static access key, lalu menyalinnya ke GitHub Actions secrets.

Mereka menyalakan CloudTrail karena muncul di checklist "AWS untuk pemula". Log masuk ke bucket nusaform-cloudtrail , tanpa EventBridge dan tanpa alert ke Telegram atau WhatsApp. Mereka belum tahu CloudTrail default hanya mencatat management events, bukan data events seperti download file di S3. Untungnya Dina sempat mengaktifkan S3 Server Access Logging pada bucket nusaform-docs-prod untuk melacak upload yang gagal.

SEBELUM / SATU AWS ACCOUNT: nusaform-prod



Prefix Publik untuk Bank, Label Temporary

Bank partner minta 12 kontrak sebelum meeting pukul empat. Fitur file sharing belum siap. Yoga membuat prefix exports/bank-bima/ , mengunggah ZIP, lalu membuka akses publik:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "TempPublicExportRead",
   "Effect": "Allow",
   "Principal": "*",
   "Action": "s3:GetObject",
   "Resource": "arn:aws:s3:::nusaform-docs-prod/exports/*"
  }
 ]
}
```



Link dikirim lewat WhatsApp. Tiket Jira ditutup dengan label temporary . Dua minggu kemudian prefix itu masih publik, dan Sinta terus menaruh file baru di sana.

Pola ini pernah muncul di skala jauh lebih besar. UpGuard pernah melaporkan bucket S3 Accenture yang publicly accessible dan berisi data client serta kredensial. Skala NusaForm jauh lebih kecil. Tipe kesalahannya sama: akses publik dibuka karena dikejar deadline, lalu terlupakan.

Access Key Admin di CI

Satu malam pip eline gagal. Yoga menambahkan environment variables untuk debug dan lupa menghapusnya. Potongan config sempat muncul di job log yang bisa dilihat oleh anggota GitHub organization. Key deploy-bot memang tidak tertulis di repository, tetapi hidup di CI dengan AdministratorAccess .

Dua minggu kemudian prefix itu masih publik

PDF Preview Tanpa Filter IP

Menjelang *pitching*, Raka ingin PDF bisa di-preview di browser. Yoga membuat endpoint fetch Remote Preview yang menerima parameter url , fetch file dari URL tersebut, lalu me-render halaman pertama. Untuk memudahkan debug, endpoint mengembalikan raw response body jika file bukan PDF yang valid.

Tidak ada allowlist. Tidak ada pemblokiran ke IP internal atau alamat link-local 169.254.169.254 .

Setiap EC2 punya Instance Metadata Service (IMDS) di 169.254.169.254 . Dari dalam instance, **request HTTP** ke alamat itu bisa membaca informasi instance, termasuk temporary IAM *credentials* jika EC2 punya instance profile.

Dina sempat bertanya, *"Kalau url -nya diisi IP internal?"*
"Siapa mau iseng begitu ke kita," jawab Yoga.

Bulan kedua, user aktif sudah ratusan. Bucket berisi KTP, kontrak, dan invoice. Instance profile EC2 makin longgar karena Yoga mengubah izin menjadi s3:* sewaktu menambal bug upload. Tidak ada yang membutuhkan zero-day. **Semua konfigurasi yang mereka pilih sendiri.**

Lonjakan Tagihan di Kamis Malam

Pukul 22.40, Raka membuka Cost Explorer. Grafik S3 Data Transfer Out melonjak tajam. Ia membuka CloudTrail Event history dan memfilter GetObject . Hasilnya kosong. Dina mengingatkan: CloudTrail default tidak mencatat download S3 kecuali S3 Data Events diaktifkan. Mereka beralih ke S3 Server Access Logs. Di situ terlihat puluhan REST.GET.OBJECT dan REST.GET.BUCKET dari IP asing ke exports/bank-bima/ dan sejumlah objek di luar prefix itu.

Raka menulis di grup WhatsApp:
"Teman-teman, ada yang lagi menjalankan script mass download S3?"

Dalam dua jam mereka menutup pintu yang paling berisiko: Block Public Access di level akun, hapus statement TempPublicExportRead , cabut SSH dari 0.0.0.0/0 , deactivate access key deploy-bot , rotate password RDS dan app secret, serta blokir route /fetchRemotePreview di Nginx. Menjelang pukul satu dini hari, trafik unduhan berhenti.



Ilustrasi: Investigasi kebocoran data S3

Bukti Mengubah Dugaan Menjadi Kesimpulan

Akhir pekan mereka mencocokkan timestamp S3 access log dengan log Nginx. Tiga hipotesis muncul, dan yang ketiga terbukti: seseorang memanfaatkan celah SSRF di fetchRemotePreview dengan mengirim:

url=http://169.254.169.254/ latest/meta-data/iam/security-credentials/app-instance-role.

Karena respons metadata berupa JSON bukan PDF, endpoint mengembalikan AccessKeyId , SecretAccessKey , dan Token sementara milik EC2. Kredensial itu lalu dipakai untuk ListBucket dan mengunduh objek.

Raka juga khawatir tentang skenario yang lebih buruk: jika key deploy-bot yang bocor dan snapshot ikut dihapus. Code Spaces pernah berhenti beroperasi setelah control panel diambil alih dan data beserta backup dihapus dalam waktu singkat. NusaForm menyimpan snapshot RDS di akun yang sama dengan production.

Pemeriksaan CloudTrail menunjukkan key deploy-bot tidak pernah dipanggil dari luar IP runner GitHub Actions. Pelaku masuk lewat SSRF dan memakai instance profile dengan izin s3:* . Database RDS di private subnet tidak terlihat ikut diakses.

Log Nginx mencatat request ke 169.254.169.254 empat menit sebelum rentetan ListBucket. Pola ini dekat dengan kasus Capital One 2019: komponen tepi yang salah konfigurasi, jalur SSRF ke metadata, role dengan izin storage terlalu luas, lalu data di S3 terbaca. Skala NusaForm tidak sebanding. Mekanismenya bisa sangat dekat.

Langkah Perbaikan Utama

Tanpa anggaran untuk platform keamanan mahal yang sudah tergerus biaya Data Transfer, mereka fokus pada perbaikan mendasar—ibarat merapikan rumah setelah hampir kemalingan.

Masalah	Perbaikan
Prefix S3 publik	Block Public Access di level akun + Presigned URL 15 menit untuk bank partner
SSH terbuka ke internet	Cabut port 22, masuk server lewat SSM Session Manager (agen SSM keluar via HTTPS 443, bukan buka inbound SSH)
SSRF ke metadata	IMDSv2 (--http-tokens required) + refactor fetchRemotePreview agar hanya menerima objectKey internal
Static key CI dengan admin	Hapus deploy-bot, ganti GitHub Actions ke OIDC (short-lived token per job)
Instance profile s3:*	Batasi ke GetObject / PutObject pada prefix uploads/* dan previews/*, tanpa ListBucket
CloudTrail tanpa orang yang jaga	Aktifkan S3 Data Events, EventBridge + Lambda ke grup Telegram / WhatsApp
Backup di akun yang sama	Akun AWS kedua untuk snapshot dan log, plus restore test yang benar-benar dijalankan

Perbaikan yang Dijalankan

Dua pengaturan yang paling sering ditanyakan pemula:

```
# Tutup akses publik di level akun
aws s3control put-public-access-block \
  --account-id 123456789012 \
  --public-access-block-configuration
"BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true"
```

```
# Paksa IMDSv2: request GET biasa ke metadata tidak cukup,
# peminta harus PUT dulu untuk dapat session token
aws ec2 modify-instance-metadata-options \
 --instance-id i-0nusaformapp \
 --http-tokens required \
 --http-put-response-hop-limit 1
```

Satu minggu kemudian, verifikasi log selesai. Mayoritas unduhan massal adalah sampel di exports/bank-bima/. Beberapa objek di luar prefix itu yang terbaca lewat SSRF ternyata invoice dummy dari akun uji. Mereka beruntung bukan karena arsitektur awalnya bagus, melainkan karena pintu ditutup sebelum prefix client yang lebih dalam ikut tersalin.

Lalu, Raka mem-pin satu pesan di grup WhatsApp:

> ***“Menggunakan cloud tidak otomatis aman. Amazon mengamankan server fisik, tetapi kita yang wajib menjaga bucket, role, dan access key.”***

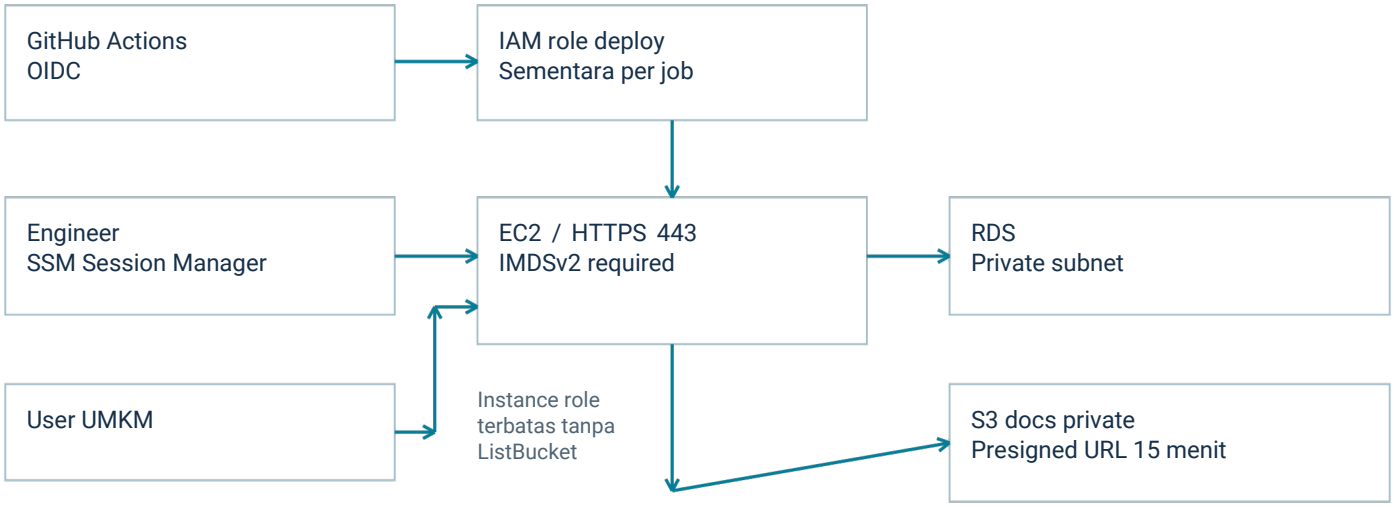
Checklist dan Arsitektur Sesudahnya

Untuk tim empat orang di satu atau dua akun AWS, daftar ini sering lebih berguna daripada *framework* yang tidak pernah dibuka:

1. S3 Block Public Access aktif di level akun?
2. Berbagi file memakai Presigned URL berumur pendek, bukan anonymous read?
3. Static access key CI sudah diganti OIDC atau short-lived role?
4. Role aplikasi dan CI memakai least privilege tanpa wildcard di production?
5. Port 22 / 3389 / database tertutup dari internet, diganti SSM?
6. IMDSv2 diwajibkan pada EC2?
7. Endpoint yang fetch URL dari user memblokir IP internal dan 169.254.169.254?
8. CloudTrail (plus S3 Data Events) aktif dan ada alert yang dibaca manusia?
9. Backup di akun terpisah, dan restore sudah pernah diuji?
10. Setiap pintasan temporary punya PIC dan tanggal kadaluarsa?

Arsitektur Setelah Perbaikan

PRODUKSI: AKSES DIPERKECIL, JALUR DIKENDALIKAN



CloudTrail + S3 Data Events → EventBridge + Lambda → Telegram / WhatsApp alert

AKUN BACKUP TERPISAH / Cross-account RDS snapshot, CloudTrail dan S3 access log ; disertai restore test.

Perbedaannya bukan pada jumlah layanan baru yang dibeli. Perbedaannya pada hak akses yang diperkecil, pintu yang ditutup, dan orang yang bersedia bangun ketika alert berbunyi.

Pola di NusaForm	Kasus publik yang mirip	Pelajaran praktis
Prefix S3 publik yang dilupakan	Accenture S3 (UpGuard, 2017)	Block Public Access + Presigned URL berumur pendek
Role terlalu kuat plus jalur ke metadata	Capital One (2019)	Least privilege + IMDSv2
Backup di batas administratif yang sama	Code Spaces (2014)	Akun backup terpisah + restore test

Bagi tim kecil, keamanan cloud jarang berarti membangun pusat operasi keamanan pada hari pertama. Lebih sering berarti menolak pintasan yang membuat satu key, satu bucket, atau satu port menjadi pintu masuk ke seluruh bisnis.

REFERENSI UTAMA

AWS — Shared Responsibility Model

Amazon S3 — Security & Block Public Access

Amazon EC2 — Instance metadata options

SERANGAN SUDAH MASUK, APAKAH KITA MENYADARINYA?

BY BANG JAVI



Membongkar Kesenjangan Deteksi dan Tantangan Operasional Pusat Operasi Keamanan

Dari jejak digital yang tersembunyi hingga strategi deteksi dan respons insiden yang lebih efektif.

Ancaman Tak Selalu Terlihat

Suatu perusahaan boleh saja memiliki *firewall*, antivirus, *endpoint detection and response* (EDR), serta sistem *Security Information and Event Management* (SIEM), tetapi ternyata tetap gagal menyadari serangan yang sedang berlangsung. Banyaknya perangkat keamanan tidak otomatis menjamin perlindungan. Pertanyaan pentingnya bukan hanya *"Apakah sistem kita aman?"*, melainkan ***"Kalau penyerang berhasil masuk, seberapa cepat kita mengetahuinya?"***

Serangan modern tidak selalu hadir sebagai *malware* yang langsung memicu alarm. Pelaku dapat menggunakan kredensial curian, memanfaatkan perangkat administrasi yang sah, atau bergerak perlahan agar aktivitasnya menyerupai pekerjaan rutin. Login dari akun yang valid, penggunaan PowerShell, perubahan konfigurasi, dan pemindahan data bisa saja merupakan aktivitas normal atau bagian dari rangkaian serangan. Konteks menjadi pembeda utama.

Karena itu, pertahanan siber perlu dilihat sebagai rangkaian kemampuan: mencegah serangan, merekam aktivitas, mendeteksi penyimpangan, menyelidiki bukti, merespons insiden, lalu memperbaiki kontrol yang gagal. Tujuannya bukan menjanjikan bahwa semua serangan dapat dicegah, melainkan mengurangi peluang penyerang beroperasi tanpa diketahui.

PERTANYAAN KUNCI SOC:

Kalau penyerang sudah berada di dalam jaringan, jejak apa yang akan terlihat–dan siapa yang akan menyadarinya?

Dari Satu Jejak Menjadi Gambaran Serangan

Sebuah insiden dapat bermula dari email *phishing*, kata sandi yang bocor, perangkat yang belum diperbarui, atau layanan yang terekspos ke internet. Setelah memperoleh akses awal, pelaku mungkin mencoba memperluas hak akses, mencari sistem lain, mengambil kredensial tambahan, mempertahankan akses, lalu mengakses atau mencuri data. Tidak semua serangan mengikuti urutan yang sama, tetapi setiap tahap berpotensi meninggalkan jejak pada *endpoint*, autentikasi, jaringan, aplikasi, dan layanan cloud.

Tantangannya, bukti tersebut tersebar di banyak sumber. Log autentikasi mungkin tersimpan di domain *controller*, aktivitas proses berada di endpoint, koneksi jaringan tercatat pada *firewall*, sedangkan aktivitas cloud ada di portal audit terpisah. Jika sumber-sumber itu tidak dikumpulkan dan dikorelasikan, setiap kejadian terlihat kecil dan tidak berkaitan. Ketika digabungkan berdasarkan waktu, akun, *host*, alamat IP, dan perilaku, rangkaian yang tadinya samar dapat menunjukkan pola serangan.

Mengapa Deteksi Bisa Terlambat?

Titik buta sering muncul bukan karena organisasi sama sekali tidak memiliki teknologi, melainkan karena telemetri tidak lengkap atau tidak dapat digunakan. Sumber log penting mungkin belum diaktifkan; waktu antarsistem tidak sinkron; retensi terlalu singkat; atau data gagal dikirim ke SIEM. Normalisasi yang keliru juga dapat membuat field penting seperti nama pengguna, alamat IP, dan nama proses sulit dibandingkan.

Di sisi lain, terlalu banyak *alert* dapat menenggelamkan sinyal penting. Aturan yang terlalu sensitif menghasilkan *false positive*, sedangkan aturan yang hanya mencari satu indikator sederhana dapat melewatkan serangan yang berubah-ubah. Kualitas deteksi tidak ditentukan oleh banyaknya notifikasi, tetapi oleh relevansi, konteks, keterujian, dan kejelasan tindakan yang harus dilakukan analis.

Mulai dari Risiko, Bukan Jumlah *Alert*

Prioritaskan skenario yang paling berdampak terhadap organisasi: penyalahgunaan akun istimewa, serangkaian login gagal yang diikuti login berhasil, eksekusi proses mencurigakan, perubahan mekanisme persistensi, atau transfer data yang tidak biasa. Tentukan aset dan identitas yang penting, bukti yang diperlukan, serta keputusan yang harus diambil jika perilaku tersebut terdeteksi.



Dari Log Menjadi Intelijen

***Windows Security Logs* dapat membantu mengungkap aktivitas autentikasi, sementara Sysmon menambah visibilitas atas pembuatan proses, koneksi jaringan, dan perubahan tertentu pada sistem.** *Event* ID 4625, misalnya, merekam kegagalan login; *Event* ID 4624 merekam login berhasil. Rangkaian kegagalan yang diikuti oleh keberhasilan pada akun atau perangkat yang sama dapat menjadi sinyal untuk ditinjau, terutama bila terjadi di luar pola normal. Namun, satu *event* saja tidak cukup untuk menyimpulkan bahwa serangan sedang berlangsung.

Platform seperti **IBM QRadar** dan **Elastic Security** membantu mengumpulkan, menormalisasi, mencari, serta menghubungkan kejadian dari berbagai sumber. **MITRE ATT&CK** menyediakan taksonomi teknik penyerang untuk memetakan skenario ancaman dan mengevaluasi cakupan deteksi. Sigma menyediakan format aturan yang dapat diadaptasi ke berbagai *platform*. *Tools* seperti **Wireshark** dan **Zeek** membantu analisis jaringan, sedangkan **Velociraptor** dapat mendukung pengumpulan artefak *endpoint* untuk investigasi.

4625 / LOGIN GAGAL **4624 / LOGIN BERHASIL**

Alur Praktis Membangun *Use Case* Deteksi:

01 **Definisikan skenario:** Jelaskan perilaku yang ingin ditemukan, alasan risikonya, dan aset yang mungkin terdampak.

02 **Pastikan telemetri tersedia:** Periksa apakah log yang dibutuhkan aktif, lengkap, memiliki *timestamp* yang benar, dan tersimpan cukup lama.

03 **Susun logika deteksi:** Gunakan kombinasi perilaku, identitas, *host*, waktu, dan konteks; hindari bergantung pada satu indikator saja.

04 **Uji sebelum digunakan:** Evaluasi dengan data atau simulasi yang aman. Catat kondisi yang memicu alert.

05 **Siapkan tindakan analis.** Sertakan bukti yang perlu diperiksa, langkah triase, prioritas, jalur eskalasi, dan opsi respons.

06 **Tinjau hasilnya.** Ukur *false positive* dan *false negative* yang ditemukan, lalu perbarui aturan saat sistem atau pola ancaman berubah.

Contoh sederhana: Korelasikan kegagalan autentikasi dengan login berhasil, lalu perjelas *alert* lewat konteks hak akses, aset, dan aktivitas lanjutan. Pastikan query divalidasi terhadap skema SIEM sebelum dipakai di produksi.

Threat Hunting dan Respons Insiden

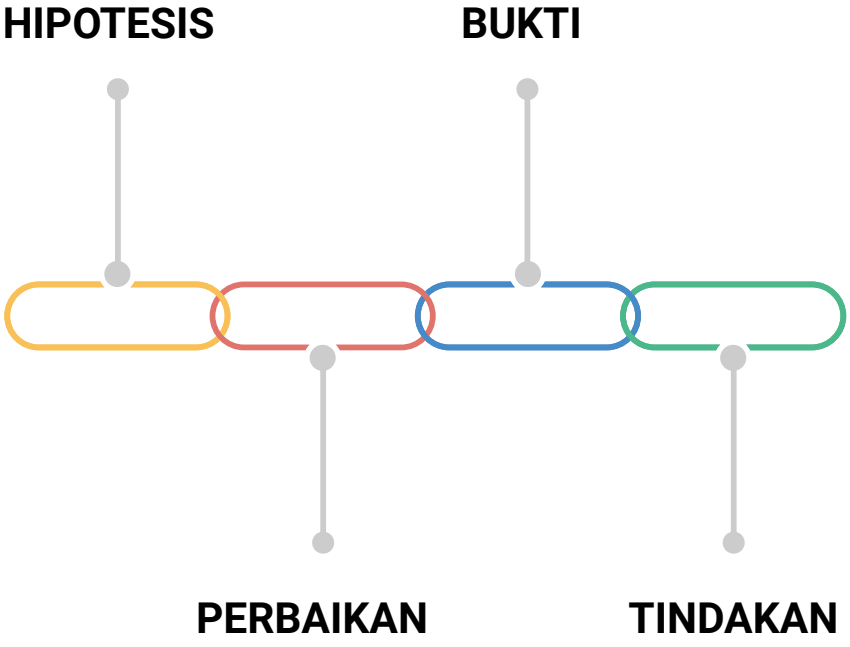


Jejak perlu ditelusuri. Bukti perlu dijaga.

***Threat hunting* melengkapi deteksi otomatis dengan pencarian proaktif terhadap aktivitas yang mungkin belum memicu *alert*.** Mulailah dari hipotesis yang jelas, misalnya: "Apakah ada akun yang melakukan autentikasi tidak lazim lalu menjalankan proses mencurigakan?" Telusuri rentang waktu, identitas, *host*, hubungan proses induk-anak, koneksi jaringan, dan perubahan akun. Catat alasan setiap keputusan agar temuan dapat diulang dan, bila relevan, dikembangkan menjadi aturan deteksi baru.

Ketika *alert* terkonfirmasi, SOC harus bergerak dari sekadar memberi label menuju tindakan terkoordinasi. Validasi bukti, tentukan cakupan, nilai dampak terhadap layanan dan data, lalu eskalasikan sesuai prosedur. Bergantung pada situasi dan kewenangan, tim dapat mengisolasi endpoint, mengamankan atau menonaktifkan akun terdampak, memblokir indikator berbahaya, dan melindungi bukti forensik. **Tindakan harus mempertimbangkan dampak operasional serta kebutuhan untuk menjaga bukti.**

Setelah ancaman terkendali, lakukan pemulihan secara terukur dan cari akar masalahnya. Periksa bagaimana akses awal terjadi, mengapa deteksi terlambat, kontrol apa yang gagal, dan apakah ada sistem lain yang ikut terdampak. **Pelajaran dari insiden perlu diterjemahkan menjadi perubahan nyata, misalnya memperbaiki konfigurasi logging, menambah cakupan deteksi, memperketat akses, atau memperbarui *playbook*.**



Mengukur Efektivitas SOC

Efektivitas SOC tidak cukup diukur dari banyaknya alert yang ditangani. Gunakan metrik yang membantu perbaikan:

Mean Time to Detect (MTTD):

Waktu yang dibutuhkan untuk menemukan aktivitas berbahaya, dengan definisi awal dan akhir pengukuran yang konsisten.

Mean Time to Respond (MTTR):

Waktu untuk memulai atau menyelesaikan respons, sesuai definisi yang disepakati tim.

Detection coverage:

Cakupan skenario prioritas oleh sumber data dan aturan deteksi yang telah diuji.

Latihan *tabletop* dan simulasi terkontrol dapat menguji alur kerja tanpa menunggu insiden nyata. Pengujian harus direncanakan, disetujui, dan dilakukan dalam ruang lingkup yang aman.

False-positive rate:

Proporsi alert yang setelah ditinjau tidak relevan atau tidak terbukti.

Log-source health:

Status kelengkapan, ketepatan waktu, dan keberlangsungan sumber log penting.

Checklist Kesiapan SOC:

- Log kritis tersedia, *timestamp* tersinkron, dan retensi sesuai kebutuhan investigasi.
- *Use case* prioritas memiliki pemilik, dokumentasi, hasil pengujian, dan jadwal peninjauan.
- *Playbook*, kontak eskalasi, dan kewenangan respons masih berlaku.
- Hasil *threat hunting* dan investigasi digunakan untuk memperbaiki deteksi.

Penutup

Tidak ada kontrol yang mampu menjamin bahwa seluruh serangan akan dicegah. Ketahanan dibangun dari kemampuan melihat sinyal, menghubungkan bukti, mengambil keputusan, dan belajar setelah kejadian. Ketika organisasi memperlakukan log sebagai sumber intelijen, bukan sekadar arsip, SOC dapat bergerak dari reaktif menjadi lebih proaktif. Serangan mungkin sudah masuk; yang menentukan adalah apakah kita mampu menyadarinya sebelum dampaknya meluas.

REFERENSI UTAMA

MITRE ATT&CK — Teknik & deteksi
Microsoft — Sysmon
SigmaHQ — Aturan deteksi

FROM ALERT TO ACTION

Seni Membaca Threat di Tengah Banjir Notifikasi Cyber

By Farah



Satu Serangan, Banyak Jejak

Mendeteksi aktivitas adalah awal.
Memahami rangkaiannya menentukan respons.

Satu Serangan, Banyak Jejak

Sebuah serangan *siber* jarang terjadi dalam satu kali aksi saja. Attacker bisa memulai aksinya dari email *phishing*, mencuri *credentials*, lalu memanfaatkan akun tersebut untuk mengakses sistem dan melakukan lateral *movement*.

Setiap tahap dapat meninggalkan jejak yang berbeda. Aktivitas login tercatat pada *authentication* log, eksekusi perintah terlihat pada *endpoint*, sedangkan *network communication* dapat ter-record pada *firewall*.

M**asalahnya, jejak-jejak tersebut tidak selalu terlihat saling berkaitan jika dianalisis secara terpisah.** Di sinilah *struggle* yang dialami tim SOC. Bukan hanya mendeteksi aktivitas mencurigakan, tetapi juga memahami apa yang sebenarnya terjadi, sejauh mana aktivitas tersebut berkembang, dan tindakan apa yang perlu dilakukan.

Mendeteksi aktivitas hanya awalan saja, justru memahami rangkaian serangan adalah langkah untuk menentukan response yang tepat.

The Signal in the Noise

***Modern security system* dapat menghasilkan banyak alert berdasarkan aturan, indikator, dan pola kebiasaan. Namun, tidak semua *alert* menunjukkan serangan yang nyata.**

Sebagai contoh, PowerShell dapat digunakan untuk administrasi sistem yang sah, tetapi juga dapat disalahgunakan oleh *attacker* untuk menjalankan perintah berbahaya. Begitu pula dengan percobaan login berulang yang bisa mengindikasikan *brute force,* tetapi mungkin juga disebabkan oleh kesalahan konfigurasi.

Aktivitas yang sah tetapi terdeteksi sebagai ancaman disebut *false positive*. Sebaliknya, false negative terjadi ketika *threat* tidak terdeteksi oleh mekanisme keamanan. Terlalu banyak *false positive* dapat membuat analis kewalahan dan meningkatkan risiko *alert fatigue.* Di sisi lain, *threat* yang tidak terdeteksi dapat memberikan *attacker* lebih banyak waktu untuk melanjutkan aksinya.

Oleh karena itu, *alert* perlu dianalisis berdasarkan konteksnya. *Severity* yang ditampilkan sistem memang penting, tetapi belum tentu cukup untuk menentukan apakah suatu aktivitas benar-benar berbahaya.

One Alert Is Not the Whole Story



Bayangkan sebuah sistem mendeteksi beberapa percobaan login gagal dari satu sumber IP.
Apakah ini *brute force* biasa, atau bagian dari serangan yang lebih besar? Analis perlu memeriksa apakah ada login yang berhasil setelahnya, apakah akun lain juga menjadi target, dan apakah terdapat aktivitas mencurigakan setelah autentikasi berhasil.

CONTOH KORELASI / PERLU VALIDASI



LOGIN GAGAL → **LOGIN BERHASIL** → **PERINTAH TAK BIASA** → **KONEKSI EKSTERNAL**

Untuk mendapatkan gambaran yang lebih jelas, tim SOC biasanya melakukan korelasi terhadap berbagai data *source*, mulai dari *authentication log, endpoint telemetry, firewall log, network traffic*, hingga aktivitas cloud jika tersedia. Sebagai contoh, login yang berhasil setelah beberapa kali gagal akan menjadi lebih signifikan jika diikuti oleh eksekusi perintah yang tidak biasa atau koneksi ke IP eksternal yang mencurigakan. **Meski demikian, setiap indikasi tetap perlu divalidasi sebelum disimpulkan sebagai insiden.**

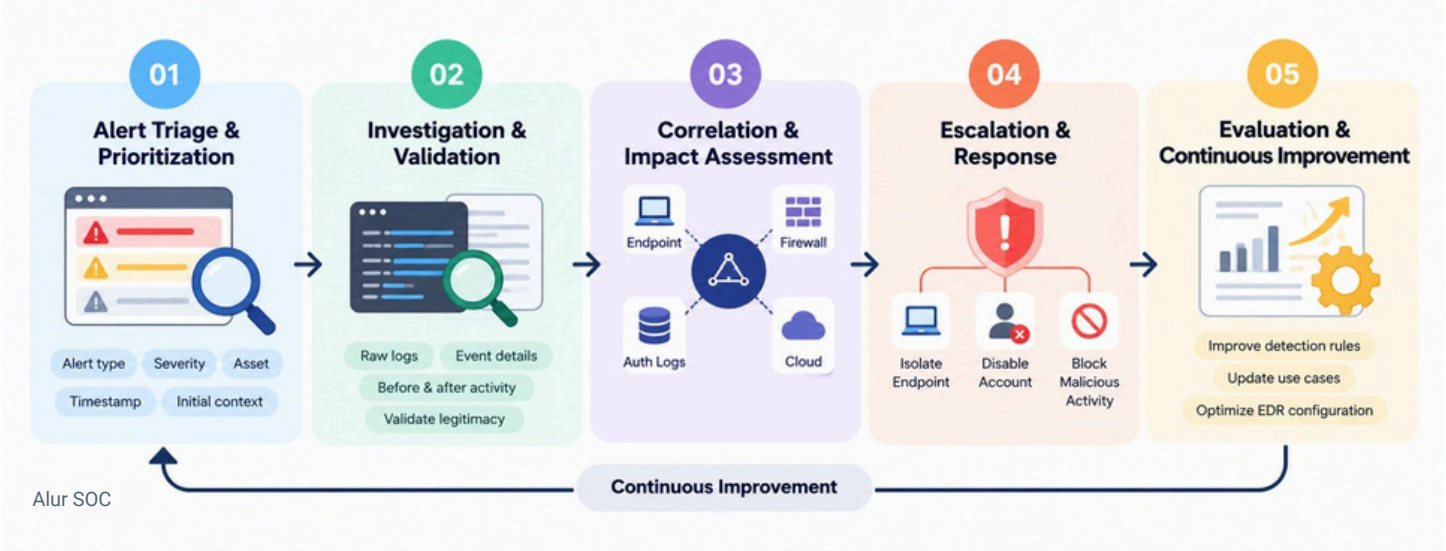
Dengan menghubungkan berbagai temuan berdasarkan *timestamp, user, hostname, IP address,* dan *behavioral patterns,* SOC dapat memahami bukan hanya apa yang terdeteksi, tetapi juga bagaimana suatu aktivitas berpotensi menjadi serangan.

TIMESTAMP / USER / HOSTNAME / IP / PERILAKU

Hubungkan konteks sebelum menyimpulkan insiden.

From Alert to Action:

Bagaimana SOC Bekerja?



Alur SOC

1. *Alert Triage* dan *Prioritization*

Analis menilai jenis *alert*, aset yang terdampak, *severity*, *timestamp*, dan konteks awal untuk menentukan prioritas investigasi. *Alert* dengan severity tinggi tidak otomatis berarti insiden telah terkonfirmasi.

2. *Investigation* dan *Validation*

Analis memeriksa *raw* log, detail *event*, serta aktivitas sebelum dan sesudah kejadian. Tujuannya adalah membedakan aktivitas yang legitimate dari indikasi *threat* yang membutuhkan tindak lanjut.

3. *Correlation* dan *Impact Assessment*

Event dari berbagai *data source* dihubungkan untuk melihat kemungkinan rangkaian serangan,sistem yang terlibat, dan cakupan dampaknya.

4. *Escalation* dan *Response*

Jika ditemukan indikasi threat yang membutuhkan penanganan lebih lanjut, *case* diekskalasikan kepada tim terkait. Tindakan dapat mencakup *endpoint isolation*, penonaktifan akun yang terkompromi, atau pemblokiran terhadap aktivitas berbahaya sesuai hasil investigasi.

5. *Evaluation* dan *Continuous Improvement*

Setelah kasus ditangani, hasil investigasi dapat digunakan untuk meningkatkan *detection rules*, menyesuaikan SIEM *use cases*, atau mengoptimalkan konfigurasi EDR agar aktivitas serupa dapat dikenali dengan lebih baik.

Tutup *alert* bukan akhir kerja SOC, tapi bahan evaluasi pertahanan.

Beyond Technology: Peran Analis Tetap Penting



Ilustrasi: Foto *Automation Supporting the SOC Analyst*

Teknologi keamanan dan *automation* dapat membantu melakukan *alert enrichment*, menghubungkan beberapa indikator, hingga menjalankan respons tertentu. Namun, keputusan yang tepat tetap membutuhkan konteks.

Sistem mungkin mendeteksi aktivitas yang tidak biasa, tetapi analis perlu mempertimbangkan apakah aktivitas tersebut sesuai dengan pekerjaan user, bagaimana kondisi aset yang terdampak, dan apa risikonya jika tindakan mitigasi dilakukan.

Di sinilah pentingnya kombinasi antara teknologi dan *analytical skills*. Automation membantu menangani pekerjaan berulang, sementara analis berfokus pada *evidence validation*, *risk assessment*, *correlation* yang lebih kompleks, dan *decision-making*.

Kolaborasi dengan tim *Incident Response*, IT *Operations/Support*, dan pemilik sistem juga diperlukan agar temuan teknis dapat ditindaklanjuti secara tepat tanpa mengabaikan kebutuhan operasional bisnis.

From Detection to Resilience

Lanskap cybersecurity semakin lama terus berubah. Penyerang dapat memanfaatkan valid *credentials*, *legitimate tools*, dan infrastruktur cloud untuk menjalankan aktivitas yang sulit dibedakan dari operasional normal. Di saat yang sama, organisasi harus mengelola semakin banyak data *sources* dan *security technologies.*

Karena itu, memiliki *security tools* yang canggih saja tidak cukup. Organisasi juga membutuhkan proses analisis yang terstruktur, korelasi yang efektif, dan respons yang terkoordinasi.

Keberhasilan SOC bukan hanya tentang berapa banyak alert yang ditangani atau seberapa cepat *case* atau tiket ditutup. Adapun hal yang lebih penting adalah apakah tim mampu memahami risiko, menentukan tindakan yang tepat, dan menggunakan hasil investigasi untuk meningkatkan kemampuan deteksi. Pada akhirnya, nilai SOC bukan sekadar menemukan aktivitas mencurigakan, melainkan mengubah data/aktivitas/log menjadi *insight*, kemudian menjadi *action* yang memperkuat pertahanan organisasi.



INSIGHT MENJADI ACTION

REFERENSI UTAMA

NIST SP 800-61 Rev. 3 (2025) MITRE ATT&CK — Analytics NIST — Incident Response

DAFTAR PUSTAKA

01/MEDAN TEMPUR SIBER MODERN

1. **Verizon**. 2026. Vulnerability exploitation top breach entry point, 2026 industry-wide DBIR finds. Siaran pers, 19 Mei. https://www.verizon.com/about/news/breach-industry-wide-dbir-finds ; halaman DBIR 2026: https://www.verizon.com/business/resources/reports/dbir/
2. **Mandiant** (Google Cloud). 2026. M-Trends 2026 Report: Executive Edition. https://cloud.google.com/security/resources/m-trends-executive-edition
3. **CrowdStrike**. 2026. 2026 CrowdStrike Global Threat Report. Siaran pers, 24 Februari. https://www.crowdstrike.com/en-us/press-releases/2026-crowdstrike-global-threat-report/
4. **Microsoft**. 2026. Microsoft Digital Defense Report 2026. https://www.microsoft.com/en-us/corporate-responsibility/topics/cybersecurity/reports/microsoft-digital-defense-report/
5. **VulnCheck**. 2026. 2026 State of Exploitation: Exploiting the Network Edge. 23 Maret. https://www.vulncheck.com/blog/network-edge-device-report-2026
6. **Anthropic**. 2026. Detecting and countering misuse of AI: September 2026. https://www.anthropic.com/threat-intelligence-report-september-2026
7. **Anthropic**. 2025. Disrupting the first reported AI-orchestrated cyber espionage campaign. 13 November. https://www.anthropic.com/news/disrupting-AI-espionage
8. **The Conversation**. 2025. An AI lab says Chinese-backed bots are running cyber espionage attacks. Experts have questions. (sekunder) https://theconversation.com/an-ai-lab-says-chinese-backed-bots-are-running-cyber-espionage-attacks-experts-have-questions-269815
9. **Anthropic**. 2026. Project Glasswing: https://www.anthropic.com/glasswing ; Expanding Project Glasswing, 2 Juni: https://www.anthropic.com/news/expanding-project-glasswing
10. **CERT-FR (ANSSI)**. 2026. Incident de sécurité ciblant les contrôleurs à distance des installations de réfrigération (CERTFR-2026-ALE-012). 12-13 Oktober. https://www.cert.ssi.gouv.fr/alerte/CERTFR-2026-ALE-012/
11. **The Hacker News**. 2026. Attackers Heat French Supermarket Fridges Up to 50°C by Hijacking Danfoss Controllers. 13 Oktober. (sekunder) https://thehackernews.com/2026/10/attackers-heat-french-supermarket.html
12. **Dragos**. 2026. Dragos OT Cybersecurity Report: Adversaries Increase Real-World Impact, Map Control Loops Across Industrial Infrastructure. Siaran pers, 17 Februari. https://www.businesswire.com/news/home/20260217364132/en/Dragos-OT-Cybersecurity-Report-Adversaries-Increase-Real-World-Impact-Map-Control-Loops-Across-Industrial-Infrastructure
13. **CISA**. 2026. Internet Exposure Reduction Guidance. https://www.cisa.gov/resources-tools/resources/exposure-reduction
14. **Microsoft Asia**. 2026. Microsoft Digital Defense 2026 Report Highlights New Cybersecurity Challenges Amid Rapid AI Adoption. 13 Oktober. https://news.microsoft.com/source/asia/2026/10/13/microsoft-digital-defense-2026-report-highlights-new-cybersecurity-challenges-amid-rapid-ai-adoption/
15. **Periskop**. 2026. BSSN Catat 5,16 Miliar Anomali Siber Sepanjang 2025. 6 Agustus. (sekunder) https://periskop.id/teknologi/20260806/bssn-catat-516-miliar-anomali-siber-sepanjang-2025-perbankan-diminta-tak-pelit-investasi-keamanan-digital
16. **Kementerian Komunikasi dan Digital.** 2024. Siaran Pers: Percepat Pemulihan, Kominfo, BSSN dan Telkom Operasikan Server Baru Pengganti. https://www.komdigi.go.id/berita/pengumuman/detail/siaran-pers-np-tentang-percepat-pemulihan-kominfo-bssn-dan-telkom-operasikan-server-baru-pengganti
17. **CNN Indonesia**. 2024. Klaim Brain Cipher Betapa Mudahnya Mengacak-acak PDNS 2. 4 Juli. (sekunder) https://www.cnnindonesia.com/teknologi/20240704060658-192-1117341/klaim-brain-cipher-betapa-mudahnya-mengacak-acak-pdns-2
18. **Liputan6**. 2024. PDNS Diserang Ransomware, BSSN Sentil Kominfo Tidak Ada Backup Data. 28 Juni. (sekunder) https://www.liputan6.com/news/read/5630032/pdns-diserang-ransomware-bssn-sentil-kominfo-tidak-ada-backup-data
19. **Republik Indonesia**. 2022. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pasal 46 dan Pasal 74. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

02/Namaste: CA-nya eMudhra, Key-nya eMudah Ditebak

1. **Situs Pelacakan Insiden Komunitas**. (2026). eMudhra Incident Tracker. emudhra.we-have-a-problem.com
2. **eMudhra**. (2026). Official Statement: Certificate Security Incident. [emudhra.com/en/post/certificate-security-incident] (https://emudhra.com/en/post/certificate-security-incident)
3. **Scott Helme**. (2026). Eight Bits of Trust: eMudhra's CA Keys Cracked in Milliseconds.scotthelme.co.uk/eight-bits-of-trust-emudhras-ca-keys-cracked-in-milliseconds
4. **Cloudflare Blog.** (2026). eMudhra Certificate Compromise: Analysis and Response blog.cloudflare.com/emudhra-certificate-compromise
5. **The Register.** (2026). Indian Certification Authority eMudhra's Private Keys Compromised: One of Them Was the Number 4. 20 October. [theregister.com/2026/10/20/indian-certification-authority-emudhras-private-keys-compromised] (https://theregister.com/2026/10/20/indian-certification-authority-emudhras-private-keys-compromised)
6. **The Hacker News**. (2026). Eight eMudhra CA Keys Compromised Due to Small Integer Values [thehackernews.com/2026/10/eight-emudhra-ca-keys-compromised.html] (https://thehackernews.com/2026/10/eight-emudhra-ca-keys-compromised.html)
7. **Help Net Security.** (2026). eMudhra Certificates' Private Keys Compromised. 21 Oktober [helpnetsecurity.com/2026/10/21/emudhra-certificates-private-keys-compromised] (https://helpnetsecurity.com/2026/10/21/emudhra-certificates-private-keys-compromised)

03/Ketika Patch Jadi Peta Serangan: Mengurai Krisis PHP2Shell dan Runtuhnya Embargo CVD

1. **Krebs on Security**. (2026). Widespread PHP Flaw May Cause Many Site Outages Today [krebsonsecurity.com/2026/10/widespread-php-flaw-may-cause-many-site-outages] (https://krebsonsecurity.com/2026/10/widespread-php-flaw-may-cause-many-site-outages)
2. **CSO Online.** (2026). PHP2Shell Exposes the Weakness in Coordinated Vulnerability Disclosure [csoonline.com/article/php2shell-exposes-weakness-in-cvd] (https://csoonline.com/article/php2shell-exposes-weakness-in-cvd)
3. **SecurityWeek**. (2026). Tech and Security Companies Respond to PHP2Shell Vulnerabilities [securityweek.com/tech-and-security-companies-respond-to-php2shell] (https://securityweek.com/tech-and-security-companies-respond-to-php2shell)
4. **BleepingComputer.** (2026). Amazon Says PHP2Shell Exploitation Began 4 Days Before Patches [bleepingcomputer.com/news/security/amazon-php2shell-exploitation-began-4-days-before-patches] (https://bleepingcomputer.com/news/security/amazon-php2shell-exploitation-began-4-days-before-patches)
5. **The Register.** (2026). PHP2Shell Exploit Bypasses Protections Designed to Stop Remote Code Execution theregister.com/2026/10/php2shell-exploit-bypasses-rce-protections

04/The Next Cyber Battlefield: What AI Predictions Tell Us About 2030

1. **AI Security Institute (AISI).** (2025). Frontier AI Trends Report. Link: Laporan resmi AISI.
2. **National Cyber Security Centre (NCSC).** (2025). Impact of AI on Cyber Threat from Now to 2027. Link: Laporan resmi NCSC.
3. **Bengio, Y., et al.** (2026). International AI Safety Report 2026. Link: Laporan resmi International AI Safety Report.
4. **European Union Agency for Cybersecurity (ENISA).** (2024). Foresight Cybersecurity Threats for 2030 – Update 2024. Link: Laporan resmi ENISA.
5. **World Economic Forum (WEF).** (2025). Global Cybersecurity Outlook 2025. Link: Laporan WEF 2025.
6. **World Economic Forum (WEF).** (2026). Global Cybersecurity Outlook 2026. Link: Laporan WEF 2026.
7. **Cloud Security Alliance (CSA).** (2025). Beyond the Hype: A Benchmark Study of AI Agents in the SOC. Link: Studi benchmark AI di SOC.
8. **Rieger, M., Shah, A., Abu Alam, & Hossain, M. J.** (2026). Possibilities and limitations of using large language models (LLMs) for alert classification and prioritisation in security operations centers (SOCs). Expert Systems with Applications, 331, Article 133194. DOI: https://doi.org/10.1016/j.eswa.2026.133194

05/Memverifikasi Temuan Pentest dengan VulnVerify Skills

1. **VulnVerify Skills. (**2026). Dokumentasi Repositori, Metodologi, dan Panduan Pengguna (README.md & GUIDE.md). [github.com/roomkangali/vulnverify-skills] (https://github.com/roomkangali/vulnverify-skills)
2. **Trail of Bits.** (2026). poc-builder: Automated Proof-of-Concept Generation (Revisi Adaptasi) [github.com/trailofbits/poc-builder] (https://github.com/trailofbits/poc-builder)
3. **Microsoft**. (2026). Playwright Model Context Protocol (MCP) Integration. [github.com/microsoft/playwright-mcp] (https://github.com/microsoft/playwright-mcp)
4. **Paket Pengujian & Bukti Demonstrasi.** (2026). Artefak Investigasi Terkontrol (evidence/run-summary.json, Snapshot, Rekaman MCP, Screenshot, & REVIEWER-KEY.md). Pengujian independen pada 22 Oktober 2026 (Playwright MCP v0.0.83, Google Chrome v156.0.8078.47).

DAFTAR PUSTAKA

06/Saat Freezer Dipanaskan dari Jauh

1. **Reuters (via ARY News).** "Hackers heat French supermarket fridges, sparking fires and spoiling food". 13 Oktober 2026. https://arynews.tv/hackers-heat-french-supermarket-fridges-sparking-fires-and-spoiling-food
2. **AFP (via Le Petit Journal).** "Des supermarchés français touchés par une cyberattaque inédite de leurs installations frigorifiques". 12-13 Oktober 2026. https://lepetitjournal.com/expat-mag/societe/des-supermarches-francais-touches-par-une-cyberattaque-inedite-de-leurs-installations-frigorifiques
3. **ClickOnDetroit.** "Cyberattack targeting refrigeration systems hits 700 supermarkets, French government says". 13 Oktober 2026. https://www.clickondetroit.com/business/2026/10/13/cyberattack-targeting-refrigeration-systems-hits-700-supermarkets-french-government-says/
4. **OCCRP.** "Hackers Turn French Supermarket Refrigerators Into Furnaces". https://www.occrp.org/en/news/hackers-turn-french-supermarket-refrigerators-into-furnaces
5. **Sud Radio.** "Cyberattaque des supermarchés : la vague se poursuit en France et s'étend en Europe". 13 Oktober 2026. https://www.sudradio.fr/sud-radio/cyberattaque-des-supermarches-la-vague-se-poursuit-en-france-et-s'étend-en-europe
6. **BleepingComputer**. "Cyberattack shuts down refrigerators at French supermarkets". 12 Oktober 2026. https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-refrigerators-at-french-supermarkets/
7. **The Register.** "Cyberattacks crank French supermarket refrigeration systems up to 50°C". https://www.theregister.com/a/5302784
8. **The Hacker News.** "Attackers Heat French Supermarket Fridges Up to 50°C by Hijacking Danfoss Controllers". 13 Oktober 2026. https://thehackernews.com/2026/10/attackers-heat-french-supermarket.html
9. **Hard2bit** (mengutip data SOCRadar). "How a cyberattack on Danfoss refrigeration controllers hit hundreds of French supermarkets". 14 Oktober 2026. https://hard2bit.com/en/blog/french-supermarket-cyberattack-refrigeration-danfoss/
10. **Claroty Team82.** "Freeze the Controller, Defrost the Food: Uncovering Vulnerabilities in Danfoss Refrigeration Controllers". https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers
11. **Danfoss.** "Security Advisory DSA-2025-03-01". https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/dsa-2025-03-01/
12. **CISA.** "ICS Advisory ICSA-25-140-03: Danfoss AK-SM 8xxA Series". https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-03
13. **BetaNews**. "Attack on French supermarket fridges hit outdated Danfoss controllers". https://betanews.com/article/danfoss-fridge-attack-france-supermarket/
14. **SOCRadar**. "French supermarket cyberattack: OT analysis". https://socradar.io/blog/french-supermarket-cyberattack-ot/
15. **IT-Connect**. "Cyberattaque supermarchés : froid Danfoss". 12 Oktober 2026. https://www.it-connect.fr/cyberattaque-supermarches-froid-danfoss/
16. **PACIS 2025.** "Barriers to Cyber Resilience Adoption: The Indonesian Context". https://aisel.aisnet.org/pacis2025/security/security/8
17. **NIST. "SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security".** https://csrc.nist.gov/pubs/sp/800/82/r3/final

07/IT vs OT: Ketika Prioritasnya Bukan Lagi Kerahasiaan Data, tapi Keselamatan Manusia

1. **Pasardana**. "Sektor Minyak dan Gas RI Jadi Sasaran Empuk Serangan Siber, Kaspersky Blokir Ribuan Malware". 15 Juni 2026. https://pasardana.id/news/2026/6/15/sektor-minyak-dan-gas-ri-jadi-sasaran-empuk-serangan-siber-kaspersky-blokir-ribuan-malware
2. **Bisnis.com.** "Sektor Migas Jadi Sasaran Empuk Serangan Siber pada Kuartal I/2026". 15 Juni 2026. https://teknologi.bisnis.com/read/20260615/84/1980924/sektor-migas-jadi-sasaran-empuk-serangan-siber-pada-kuartal-i2026
3. **Selular.ID.** "Pemimpin Industri Harus Siap Hadapi Ancaman Keamanan Siber, BSSN Minta Waspadai Hal Ini". Juni 2026. https://selular.id/2026/06/pemimpin-industri-harus-siap-hadapi-ancaman-keamanan-siber-bssn-minta-waspadai-hal-ini/
4. **Sekretariat Kabinet RI.** "Presiden Terbitkan Perpres 82/2022 tentang Pelindungan Infrastruktur Informasi Vital". 15 Juni 2022. https://setkab.go.id/presiden-terbitkan-perpres-82-2022-tentang-pelindungan-infrastruktur-informasi-vital/
5. **Infobanknews.** "BSSN Tegaskan Blueprint Nasional Keamanan Siber Bisa Diadopsi Seluruh Industri". Mei 2026. https://infobanknews.com/bssn-tegaskan-blueprint-nasional-keamanan-siber-bisa-diadopsi-seluruh-industri

08/Dari Insiden Siber ke Kepatuhan: Memahami Arah Baru Pelindungan Data Pribadi

1. **National Institute of Standards and Technology (NIST).** (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST SP 800-61 Rev. 3). csrc.nist.gov/pubs/sp/800/61/r3/final
2. **MITRE ATT&CK.** (2026). Detection Analytics and Behavioral Mapping. attack.mitre.org/analytics/
3. **National Institute of Standards and Technology (NIST).** (2026). Computer Security Resource Center: Incident Response Project. csrc.nist.gov/projects/incident-response

09/NusaForm AWS: Cerita Startup yang Hampir Kehilangan Data User

1. **Amazon Web Services (AWS).** Shared Responsibility Model & Security Best Practices. aws.amazon.com/compliance/shared-responsibility-model
2. **Amazon Web Services (AWS).** Amazon S3 Security: Block Public Access Configuration. [docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html] (https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html)
3. **Amazon Web Services (AWS).** Best Practices for Managing AWS Access Keys & IAM Credentials. [docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html] (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html)
4. **Amazon Web Services (AWS).** Configure Instance Metadata Options (IMDSv2). [docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html] (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html)
5. **Amazon Web Services (AWS).** Logging S3 API Calls Using AWS CloudTrail Data Events. [docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html] (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html)
6. **UpGuard**. (2017). Accenture S3 Bucket Data Exposure Analysis.[upguard.com/breaches/cloud-leak-accenture] (https://upguard.com/breaches/cloud-leak-accenture)
7. **US Department of Justice.** (2019). Capital One Cyberattack Case Facts and Findings.justice.gov/usao-wawd/pr/former-tech-worker-convicted-wire-fraud-and-data-theft-capital-one-breach
8. **Ars Technica.** (2014). Code Spaces Shuts Down After Cyberattack Erases AWS Infrastructure. [arstechnica.com/information-technology/2014/06/aws-console-breach-forces-code-spaces-out-of-business] (https://arstechnica.com/information-technology/2014/06/aws-console-breach-forces-code-spaces-out-of-business)

10/Serangan Sudah Masuk, Apakah Kita Menyadarinya?

1. **MITRE ATT&CK.** (2026). Enterprise Matrix and Threat Detection Analytics. attack.mitre.org
2. **Microsoft Sysinternals.** (2026). Microsoft System Monitor (Sysmon) Documentation [learn.microsoft.com/sysinternals/downloads/sysmon (https://learn.microsoft.com/sysinternals/downloads/sysmon)
3. **SigmaHQ**. (2026). Generic Rule Format for Security Information and Event Management Systems. [github.com/SigmaHQ/sigma] (https://github.com/SigmaHQ/sigma)
4. **IBM Documentation.** (2026). IBM QRadar SIEM Architecture and Administration Guide. [ibm.com/docs/en/qradar-common] (https://ibm.com/docs/en/qradar-common)
5. **CISA**. (2026). Best Practices for Event Logging and Threat Detection in Enterprise Networks.cisa.gov/resources-tools/resources/event-logging-guidance

11/From Alert to Action: Seni Membaca Threat di Tengah Banjir Notifikasi Cyber

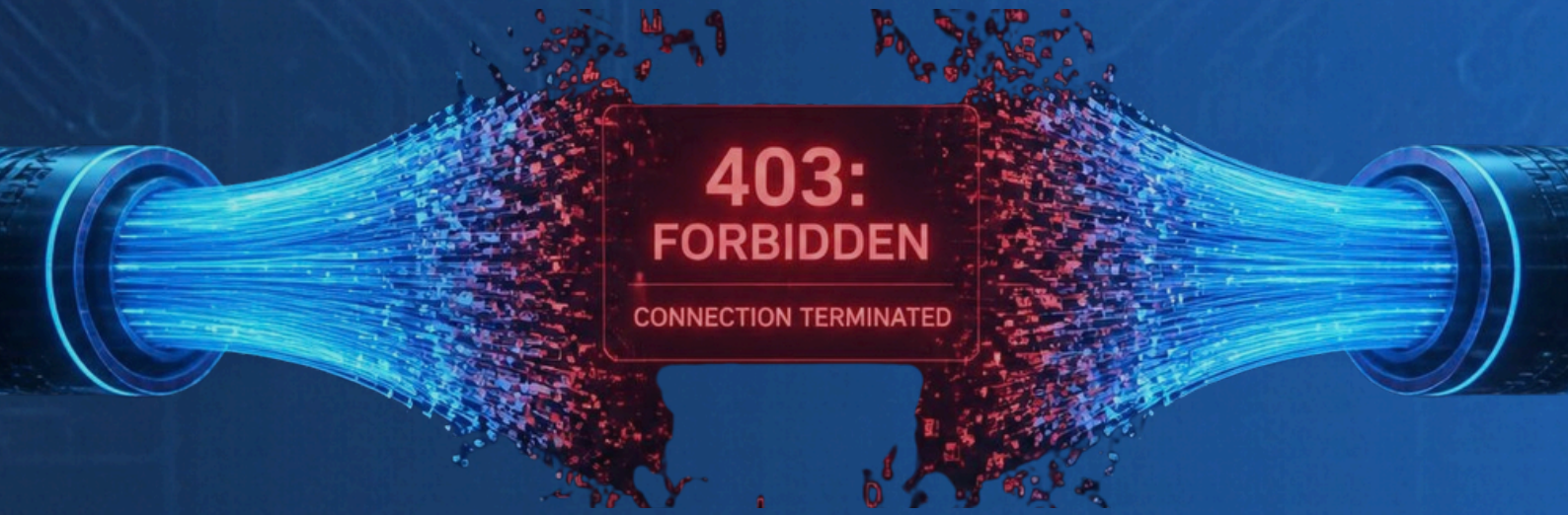
1. **National Institute of Standards and Technology (NIST).** (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST SP 800-61 Rev. 3). csrc.nist.gov/pubs/sp/800/61/r3/final
2. **MITRE ATT&CK.** (2026). Detection Analytics and Behavioral Mapping. attack.mitre.org/analytics/
3. **National Institute of Standards and Technology (NIST).** (2026). Computer Security Resource Center: Incident Response Project. csrc.nist.gov/projects/incident-response

PUNGGAWA cybersecurity

Cyber Awareness & Resilience Education

Cut the Cord

The project is over, but VPNs and database accounts remain active?
In the modern cyber battlefield, dormant third-party accounts are a paved highway for advanced threat actors. It's time to shrink the attack surface



Identity is the New Perimeter. Access Isn't a Souvenir

Be Proactive, Not Reactive

Organizations can no longer rely solely on automated revocations. Both clients and contractors must proactively destroy shared credentials to prevent supply-chain exploitations

Erase Virtual Keys

Revoke all API keys, tokens, and automation scripts post-deployment. Unmonitored machine-to-machine access is a critical blind spot frequently exploited by automated attacks

Offboard Your Team

Strict offboarding is not just an administrative checklist; it is a vital defense mechanism. Human error and forgotten access remain the weakest links in modern cyber defenses



Scan for download

MAGAZINE PUNGGAWA VOLUME 9

NOV 2026

ask.sales@punggawa.com
punggawacyber
PunggawaCyber
Punggawa Cybersecurity