

STUDI KASUS • BRUTE FORCE ATTACK

Deteksi *Brute Force Attack* dalam 5 Menit, Risiko *Account Takeover* Turun hingga 95%

Pendekatan pertahanan siber proaktif dalam mendeteksi serangan kredensial dan memutus rantai *account takeover*, berdasarkan sebuah studi kasus penanganan insiden.

Serangan berbasis identitas seperti *brute force* dan *credential stuffing* kini menjadi salah satu metode penyusupan yang paling sering ditemui dalam insiden siber, baik di tingkat global maupun di Indonesia. Namun yang menentukan seberapa besar kerugiannya sering kali bukan kecanggihan serangan itu sendiri, melainkan seberapa cepat insiden tersebut terdeteksi dan dihentikan.

White paper ini membedah satu insiden *brute force* terdistribusi (mulai dari *alert* pertama hingga *containment*) untuk memperlihatkan bagaimana deteksi dini dan respons yang terkoordinasi dapat memutus rantai *account takeover* sebelum kerusakannya meluas.

Ringkasan Eksekutif

Sebuah aplikasi *public-facing* dengan puluhan ribu pengguna harian menjadi sasaran *brute force attack* terdistribusi. Tim SOC Cisometric mendeteksinya hanya dalam 5 menit, menuntaskan *containment* dalam hitungan jam, dan menekan potensi pengambilalihan akun dari yang semula bisa mencapai ratusan hingga ribuan menjadi sangat minim.



Apa artinya untuk bisnis Anda?

Apa yang membedakan *outcome* insiden ini bukan skala serangannya, tetapi **kesiapan untuk mendeteksi dan merespons sebelum kerusakan meluas**. Dokumen ini membahas bagaimana kesiapan tersebut dibangun, dan apa yang harus bisnis Anda persiapkan **sebelum** serangan terjadi.

Daftar Isi

03

Lanskap Ancaman: *Brute Force Attack*

08

Titik Awal Serangan

09

Kronologi Serangan

12

Mekanisme Deteksi Serangan

14

Kecepatan Respons Terhadap Ancaman

15

Respons dan Mitigasi

17

Prasyarat Kapabilitas Deteksi 5 Menit

19

Sebelum vs. Sesudah SOC

20

Kesimpulan

21

Tentang Cisometric

22

Tim Editorial

23

Daftar Pustaka

Serangan Kredensial Global & Nasional

Brute force dan **credential stuffing** adalah metode penyusupan berbasis identitas yang paling mendominasi insiden siber global, dengan efektivitas dampaknya lebih bergantung pada keterlambatan deteksi dibandingkan kompleksitas teknis.¹ Dari **22.052** insiden siber global, **12.195** merupakan *confirmed data breaches*, dan **22%** di antaranya dipicu oleh *compromised credentials* sebagai *initial access vector*.¹

Di Indonesia, BSSN mencatat **16.001.962** aktivitas **brute force** pada akun *database MSSQL* sepanjang 2023, masuk ke dalam 10 anomali lalu lintas jaringan tertinggi nasional.² Pada 2024, BSSN mengkategorikan **Brute Force (T1110)** dan **Exploitation for Credential Access (T1212)** ke dalam *Top 3 Attack Vectors* yang melumpuhkan sistem autentikasi dan memicu kebocoran data berskala besar.³

Attack Success Rate vs. Exposure Scale

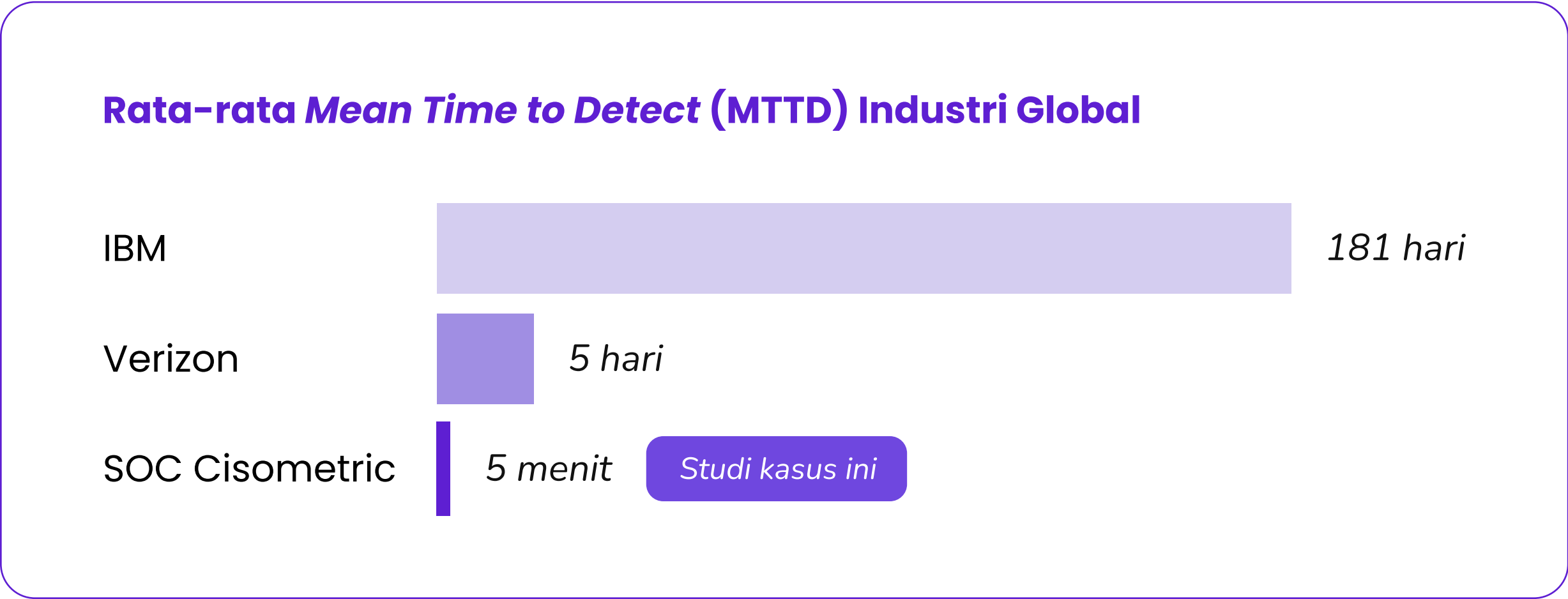
Tanpa kontrol pertahanan aktif, *credential stuffing* global mencatat tingkat keberhasilan 0,1%–4% *per tested credential*.⁴ **Data exposure di Indonesia** meningkat sebesar 33 kali lipat dalam satu tahun, dari 1.674.185 (429 *stakeholders*) pada 2023 menjadi 56.128.160 (461 *stakeholders*) pada 2024.^{2,3} Pada skala 56 juta total kredensial yang bocor, batas bawah 0,1% secara teoritis berdampak pada pengambilalihan puluhan ribu akun valid secara nasional.^{3,4}

Risiko dari insiden ini pun dapat menyebar lintas sektor. **Sektor Administrasi Pemerintahan** menyumbang **39,78%** dari *total data exposure* pada **2023**, meningkat menjadi **58,34%** pada **2024**.^{2,3} Konsentrasi ini menimbulkan *spillover risk* bagi sektor strategis lain, khususnya *financial services*, karena kebocoran sektor publik terus memperkaya basis data kredensial yang dimanfaatkan untuk *automated testing* terhadap target bernilai tinggi.³



Detection Latency & Attack Duration

Berdasarkan data IBM, rata-rata *Mean Time to Detect* (MTTD) industri global adalah 181 hari, sementara *cross-sectional median* di berbagai organisasi berdasarkan riset Verizon adalah 5 hari.^{5,6} Divergensi ini mencerminkan *long right tail* dari organisasi tanpa *real-time correlation* dan SOC.^{7,8}



Brute force yang tidak terdeteksi umumnya mempertahankan *high-velocity automated probing* selama 2–3 hari, dengan ~90% berakhir dalam satu minggu.⁷ Secara regional, dugaan insiden kebocoran data BSSN meningkat lebih dari dua kali lipat dari 103 (2023) menjadi 241 (2024), menunjukkan volume serangan telah melampaui standar pemantauan infrastruktur organisasi.^{2,3}



Apa artinya untuk bisnis Anda?

Setiap menit yang berhasil dipangkas dari waktu deteksi langsung berubah menjadi penghematan biaya. Semakin cepat aktivitas mencurigakan terdeteksi, semakin kecil ruang bagi *attacker* untuk melanjutkan serangan dan memperluas akses. **Memangkas *dwell time* memberi tim lebih banyak kesempatan untuk melakukan investigasi dan *containment* sebelum dampaknya berkembang lebih jauh.**

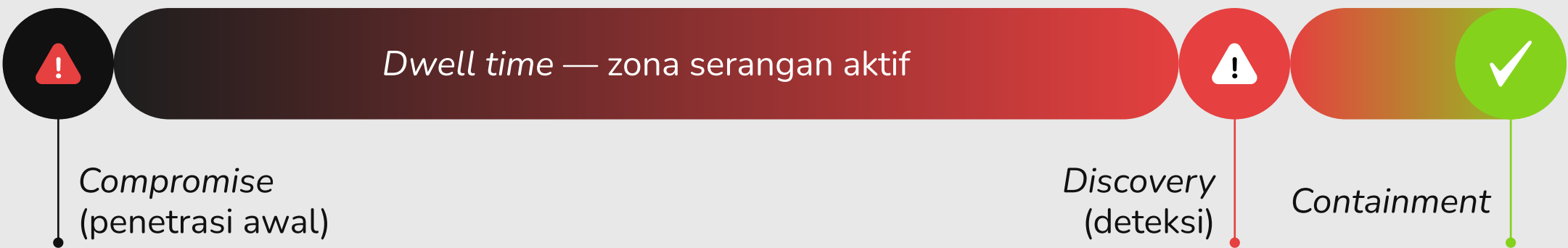
Dwell Time Sebagai Kerentanan Utama

Faktor kerentanan fundamental yang menghubungkan seluruh tolak ukur di atas adalah *dwell time*, yakni jeda antara penetrasi awal *attacker* hingga respons efektif *defender*. *Credential stuffing* yang dicegat dalam beberapa menit tidak mampu mengakumulasi *attempt throughput* yang dibutuhkan untuk mencapai ambang batas statistik peretasan, sementara serangan yang tidak terdeteksi selama sehari-hari membuat *operational runway* 2–3 hari sukses terjadi secara maksimal.⁷ Secara finansial, selisih USD 4,18 juta vs. USD 5,08 juta pun pada esensinya adalah kerugian akibat *dwell time* yang panjang.⁵

Di Indonesia, risiko ini terus memburuk karena rantai pasokan kredensial dikelola oleh ekosistem *cybercrime-as-a-service* terotomatisasi. BSSN mengonfirmasi *malware infostealer* seperti Lumma dan StealC digunakan secara terorganisir untuk memanen kredensial dari *endpoints* di seluruh Indonesia, yang kemudian menyebabkan keberhasilan pembajakan dan suplai berkelanjutan ke pasar *darknet* global.³

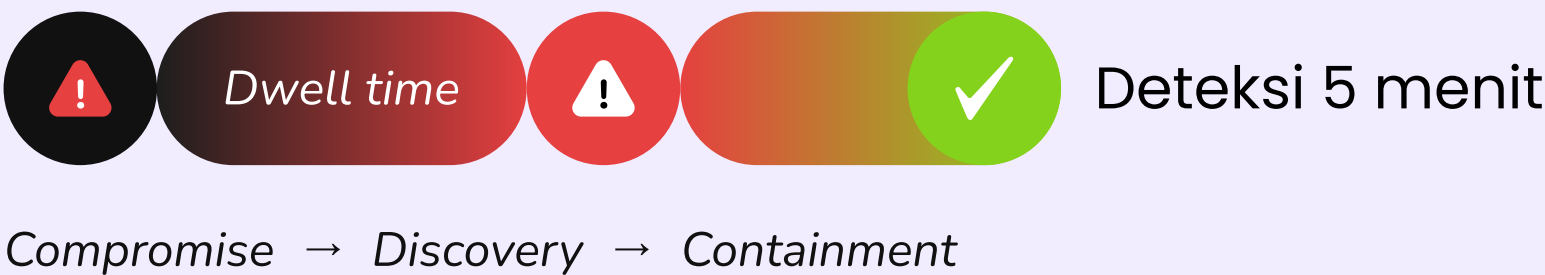
Dwell time panjang

Runway attacker 2–3 hari



Dwell time pendek

Serangan dimatikan sebelum berkembang



Dampak *Dwell Time* Panjang

pada Keberlangsungan Bisnis



Technical Risk

Extended dwell time memungkinkan *credential-testing* tereskalasi menjadi *session-level access*. Ketika kredensial valid teridentifikasi, *API calls*, *data queries*, dan *configuration changes* dapat berjalan secara otomatis, mengeskalasi tahap serangan dari deteksi menjadi *containment* dan forensik.



Business Process Risk

Serangan berkepanjangan menghabiskan waktu *threat hunter* secara tidak proporsional dan meningkatkan probabilitas *force-reset massal*, mengganggu operasi bisnis normal khususnya pada jasa keuangan, di mana akses akun menjadi kunci dari pemrosesan transaksi.



Financial Risk

Keterlambatan deteksi insiden (*dwell time*) memicu *cost premium* sebesar 21,5%, di mana biaya kerugian melonjak dari USD 4,18 juta (deteksi dini) menjadi USD 5,08 juta (*post-impact*)⁵. Sebaliknya, penerapan AI dan otomasi keamanan mampu mempercepat siklus deteksi (MTTD/MTTC) hingga 80 hari sekaligus menghemat biaya rata-rata USD 1,9 juta per insiden^{5,8}.



Legal and Regulatory Risk

Kebijakan notifikasi pelanggaran di sebagian besar yurisdiksi dihitung berdasarkan waktu sejak titik *discovery* (penemuan) dan bukan sejak titik *compromise* (peretasan). Oleh karena itu, *dwell time* yang panjang sebelum deteksi terjadi akan semakin mempersempit rentang durasi investigasi teknikal bagi tim terkait sebelum tenggat waktu regulasi diaktifkan.



Brand and Reputational Risk

Asimetri biaya antara *breach* yang dideteksi dini vs. *post-impact* dari IBM belum menghitung eksposur reputasi, yang skalanya mengikuti tingkat visibilitas dan durasi insiden. Pelanggaran yang terbongkar dari luar (oleh pelanggan atau *threat actor* sendiri) jauh lebih merusak kepercayaan dan mengundang liputan media dibandingkan jika diselesaikan secara internal.

Strategi Mitigasi dan Batas Waktu Deteksi

BSSN sudah merekomendasikan langkah mitigasi berupa *account lockout* ketat, MFA/2FA wajib, dan *password* minimal 8 karakter alfanumerik+simbol.³ Namun, dibutuhkan langkah preventif yang proaktif agar *reconnaissance* dan indikator serangan awal dapat diidentifikasi dalam waktu sesingkat-singkatnya.

Untuk merealisasikannya, dibutuhkan arsitektur SOC modern dengan korelasi multi-perspektif lintas *Application Log*, *Cloud Audit Log*, dan *Kubernetes Cluster Log*.



Metode inilah yang mendasari *correlation rules* yang diuji tim Cisometric SOC untuk mengidentifikasi *brute force attack* dalam <5 menit dan berhasil menekan risiko *account takeover* hingga 95%.

Pukul 02:10 Dini Hari

Dalam waktu singkat, sebuah **aplikasi public-facing** dengan puluhan ribu pengguna harian mengalami **lonjakan login attempt dari berbagai negara** dalam waktu singkat. Polanya mengarah pada *brute force attack* terdistribusi, upaya menyisir akun-akun dengan kredensial lemah untuk kemudian digunakan masuk ke dalam sistem.

Dari sisi bisnis, **risiko utamanya** adalah **account takeover**, potensi akses tidak sah ke data pengguna, serta **gangguan terhadap kepercayaan pelanggan**. Risiko semakin besar karena sebagian akun masih hanya mengandalkan *username* dan *password*, sementara OTP (*One-Time Password*) belum diwajibkan untuk seluruh pengguna.

02:10

Login attempt • Multi origin

Account takeover

Akses data tak sah

Kepercayaan pelanggan



Apa artinya untuk bisnis Anda?

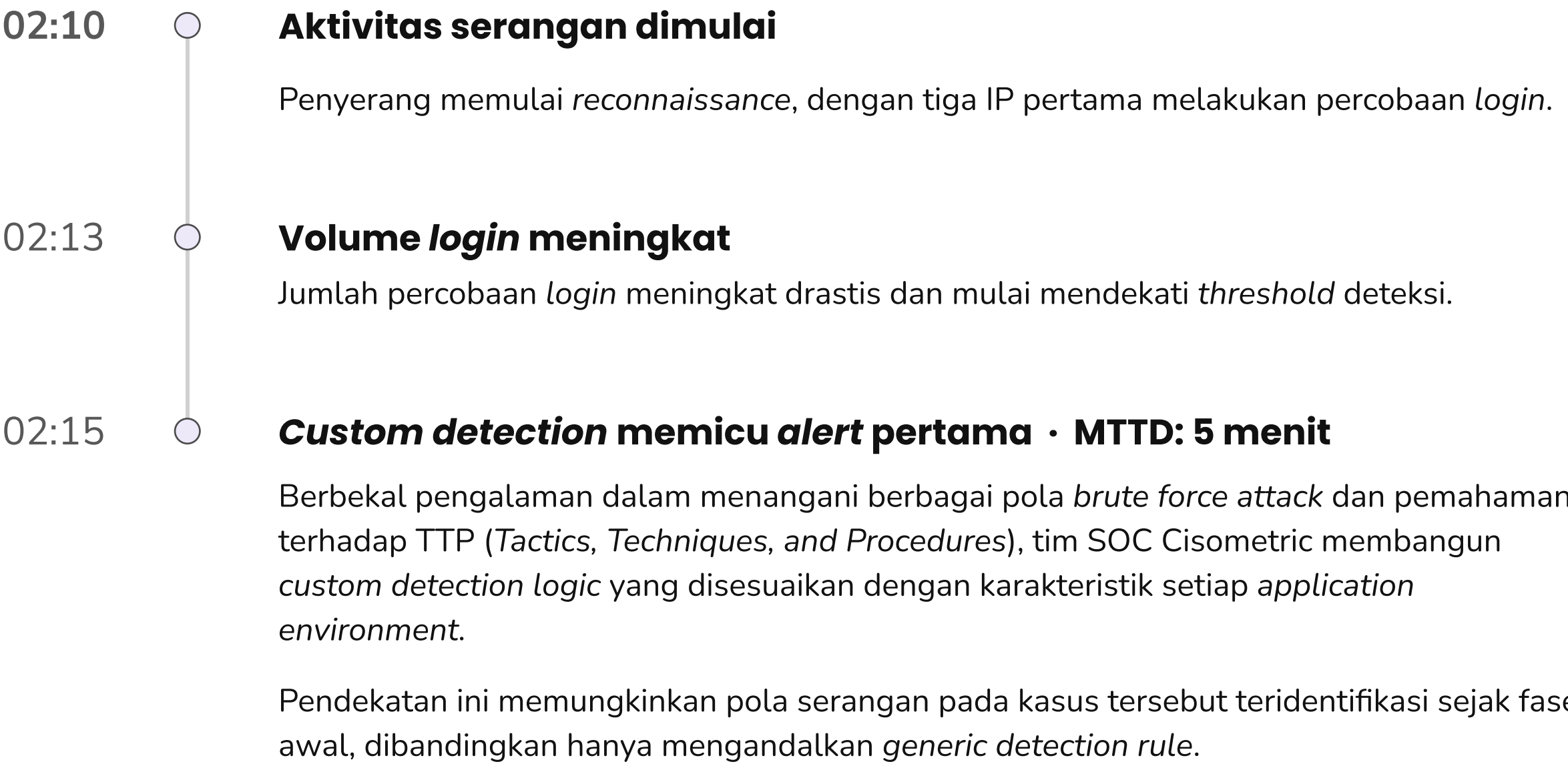
Skenario ini merupakan realita yang dihadapi sebagian besar aplikasi dengan basis pengguna besar. Tantangan utamanya bukan lagi apakah serangan akan terjadi, melainkan seberapa cepat organisasi dapat mendeteksinya saat serangan itu berlangsung.

Dari *Alert Pertama* hingga *Containment*

Kronologi penanganan insiden ini menunjukkan bagaimana proses deteksi, investigasi, eskalasi, *containment*, hingga tindak lanjut dilakukan secara bertahap.

Proses tersebut dibagi ke dalam tiga metrik: *Mean Time to Detect (MTTD)*, *Mean Time to Respond (MTTResponse)*, dan *Mean Time to Resolution (MTTResolution)*.

01 • MTTD 5 menit hingga serangan terdeteksi



Key takeaway: MTTD 5 menit tidak hanya ditentukan oleh kecepatan SIEM, tetapi juga oleh kesiapan *detection logic* sebelum serangan terjadi.

02 • MTTResponse

Begitu *alert* muncul, tugas SOC belum selesai. Tim perlu memastikan bahwa sinyal tersebut benar-benar menunjukkan insiden, menentukan tingkat risikonya, lalu mengaktifkan jalur eskalasi dan respons yang tepat.

02:21



L1 melakukan investigasi dan *validasi alert*

L1 tidak mengambil keputusan berdasarkan satu sinyal. Tim melakukan korelasi dengan berbagai sumber untuk memastikan *alert* memiliki tingkat akurasi yang tinggi, termasuk:

- *Threat Intelligence*
- *Platform* sumber *log* lain yang relevan
- *User behavior*
- Riwayat kejadian atau *past events*

Tujuannya adalah memperoleh konteks yang lebih lengkap sebelum insiden diekskalasi.

SOC mengkorelasikan *threat intelligence*, sumber *log* lain, *user behavior*, dan riwayat kejadian untuk memastikan indikasi serangan memiliki *high fidelity*.

02:28



L1 mengeskalsi insiden ke L2

Hasil observasi awal menunjukkan lonjakan permintaan *login* anomali dalam skala besar melalui portal klien. Kondisi tersebut membutuhkan investigasi yang lebih dalam dan respons yang cepat.

L1 kemudian mengaktifkan prosedur eskalasi internal melalui *incident management tools* (seperti PagerDuty atau OneUptime), sehingga L2 dapat segera bergabung untuk melanjutkan investigasi.

Indikasi aktivitas dalam skala besar membutuhkan investigasi lebih dalam, sehingga prosedur eskalasi internal segera diaktifkan.

02:50



L2 mengonfirmasi indikasi *account compromise*

Investigasi lebih lanjut menemukan pola *successful login after multiple failures*, yang mengindikasikan bahwa salah satu atau beberapa akun telah berhasil dikompromikan.

Temuan tersebut membuat insiden perlu ditangani segera pada level berikutnya.

03:00



Incident response bersama klien dimulai

Setelah insiden terkonfirmasi, tim SOC mengaktifkan *call tree procedure* bersama klien. L3 dan SOC Manager bergabung dalam *incident call*, dengan SOC Manager bertindak sebagai *Incident Commander*.

Incident Commander mengoordinasikan respons, menentukan prioritas tindakan, dan mendelegasikan eksekusi kepada pihak klien yang memiliki otorisasi, termasuk penonaktifan sementara akun yang terdampak.

Client call tree diaktifkan untuk memastikan pihak yang memiliki otorisasi dapat segera menjalankan tindakan *containment*.

03:15

Mass blocking dimulai

Tim memulai pemblokiran terhadap sekitar **200 IP pertama** yang teridentifikasi terkait dengan aktivitas serangan.

03:30

Rate limiting dan account disable dijalankan

Rate limiting diaktifkan dan akun yang terindikasi *compromise* dinonaktifkan untuk menghentikan akses lebih lanjut.

03:45

Password reset selesai

Password akun anomali di-reset sebagai bagian dari *immediate containment*.

Fase Peredaan

04:30

Volume serangan menurun drastis

Setelah tindakan *containment* diterapkan, intensitas serangan mulai turun secara signifikan.

06:00

Serangan mereda

Aktivitas serangan aktif tidak lagi menunjukkan volume seperti pada fase sebelumnya.

03 • MTTResolution

Day+1

Incident Analysis & Mitigation Plan

Setelah insiden terkendali, tim menyusun dokumentasi dan tindak lanjut untuk memahami signifikansi serangan serta menentukan langkah perbaikan berikutnya.

Incident Analysis

Bertujuan untuk memahami signifikansi dan risiko serangan, mencakup:

- Nama insiden
- Kronologi
- Attacker
- Severity
- Jenis attack
- Impacted assets

Mitigation Plan

Menerjemahkan hasil analisis menjadi tindak lanjut yang dapat dijalankan, mencakup:

- Rekomendasi resolusi / *action items*
- Mitigasi jangka pendek
- Mitigasi jangka menengah
- Mitigasi jangka panjang

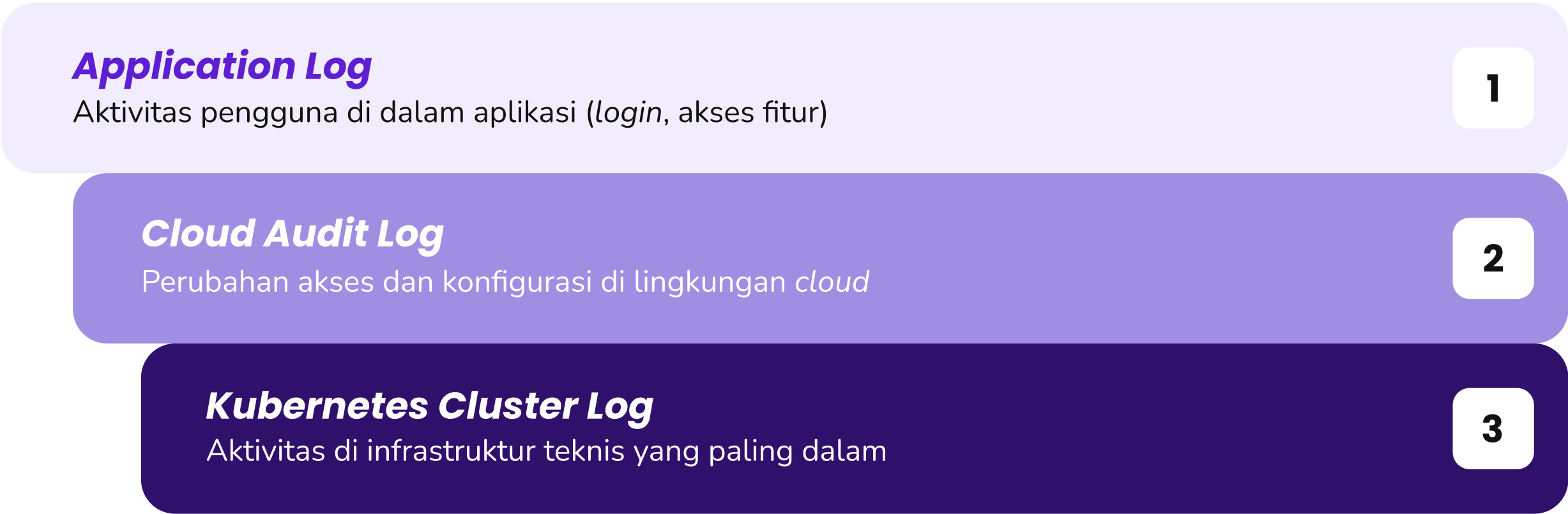


Karakteristik IP source

Tim Cisometric menemukan bahwa serangan ini menggunakan pendekatan *distributed*: rata-rata hanya 15–40 percobaan per IP agar lolos dari per-IP *rate limiting* sederhana. Tanpa *correlation rule* yang menyilang antar-IP, pola semacam ini akan tetap tidak terlihat di sebagian besar SIEM dengan konfigurasi standar.

Bagaimana SOC Mendeteksi Serangan

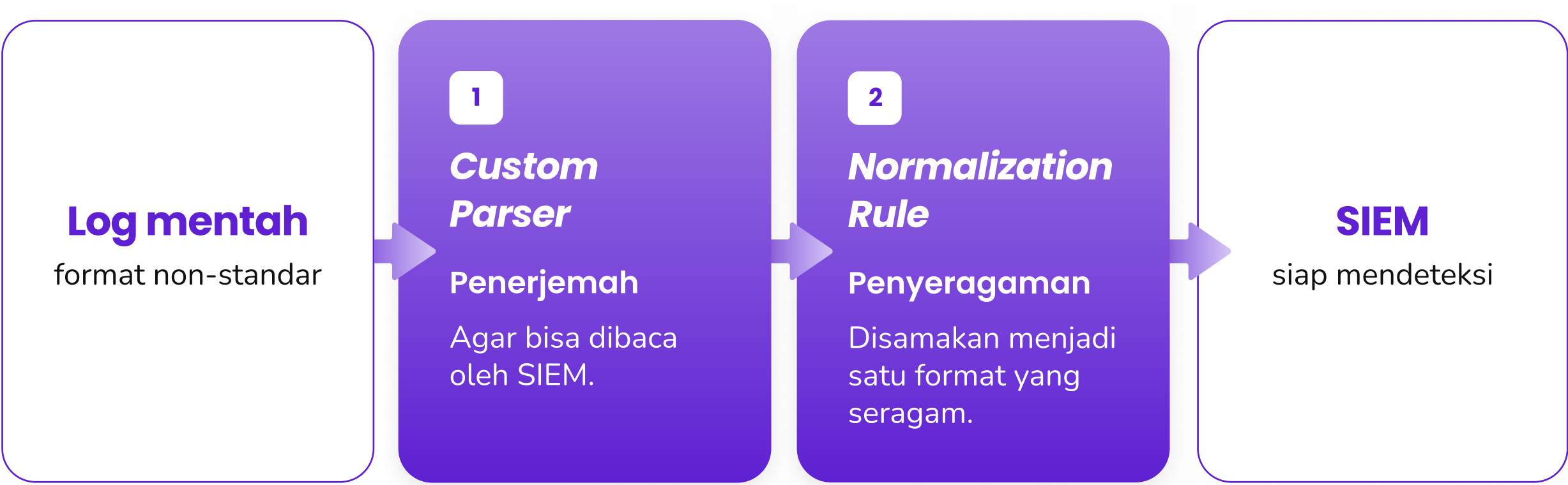
Sebelum bisa mendeteksi apa pun, SOC (*Security Operations Center*) harus terlebih dahulu mampu mengakses tiga sumber log, yang masing-masing membuka satu lapisan berbeda:



Ketiga lapisan ini bersama-sama memberikan SOC pandangan yang menyeluruh, dari apa yang dilakukan pengguna di permukaan, hingga apa yang berubah di sistem paling dalam.

Tantangan: Log yang Tidak Bisa Langsung Dibaca

Pada kasus ini, format log aplikasi klien tidak mengikuti standar umum, sehingga *Security Information and Event Management* (SIEM) tidak bisa langsung membacanya. Tim Cisometric menyiasatinya melalui dua langkah:



Seluruh proses integrasi ini memakan waktu **3–5 minggu** hingga benar-benar siap agar *production deployment* dan *detection rule* tervalidasi.

Empat *Detection Rule* Memicu *Alert*

Tim SOC Cisometric menggunakan 4 *rule*, yang terbagi ke dalam 2 kategori:

Threshold-based simple rule

(Rule 1 & 2) bekerja secara sederhana, dengan menghitung kuantitas **satu hal**; misalnya, alarm berbunyi ketika jumlah login gagal melewati batas tertentu.

Correlation rule

(Rule 3 & 4) lebih kompleks karena menghubungkan **beberapa kejadian sekaligus**; pada *Rule 3*, misalnya, alarm berbunyi ketika empat syarat terpenuhi secara bersamaan.

Kategori 1 • *Threshold-Based*

Rule 1 • Brute Force by Source IP

Alarm berbunyi jika ada **20+ login gagal** (HTTP 401) dari **satu alamat IP** dalam **5 menit**.

Rule 2 • Brute Force Against Single Account

Alarm berbunyi jika ada **10+ login gagal** terhadap **satu akun** dalam **10 menit**.

Kategori 2 • *Correlation Rule*

Rule 3 • Successful Login After Multiple Failures Critical

Alarm berbunyi jika ada **10+ login gagal** yang **diikuti login berhasil** (HTTP 200), dari **alamat IP yang sama** atau **terhadap username yang sama**, dalam **15 menit**.

Rule 4 • Distributed Brute Force

Alarm berbunyi jika **50+ IP** mencoba **login** dalam **10 menit** dengan tingkat kegagalan **>70%**.

Mengapa 5 Menit MTTD Krusial

01

Success probability ditentukan sejak menit-menit pertama

Rasio sukses *credential stuffing* (0,1%–4%) bersifat **akumulatif**, terus bertambah seiring setiap percobaan yang dibiarkan berjalan. Pada menit kelima, penyerang baru mengakumulasi volume percobaan dari tiga IP awal, masih jauh di bawah ambang yang diperlukan untuk *statistical compromise*.

02

Attacker memiliki runway 2–3 hari jika tidak terdeteksi

Begitu lolos dari fase deteksi awal, serangan *distributed* semacam ini bisa terus mempertahankan *high-velocity probing* selama 2–3 hari dengan sekitar 90% kasus baru berakhir dalam satu minggu.

Mendeteksinya di menit kelima berarti memotong *runway* itu bahkan sebelum sempat terbentuk.

03

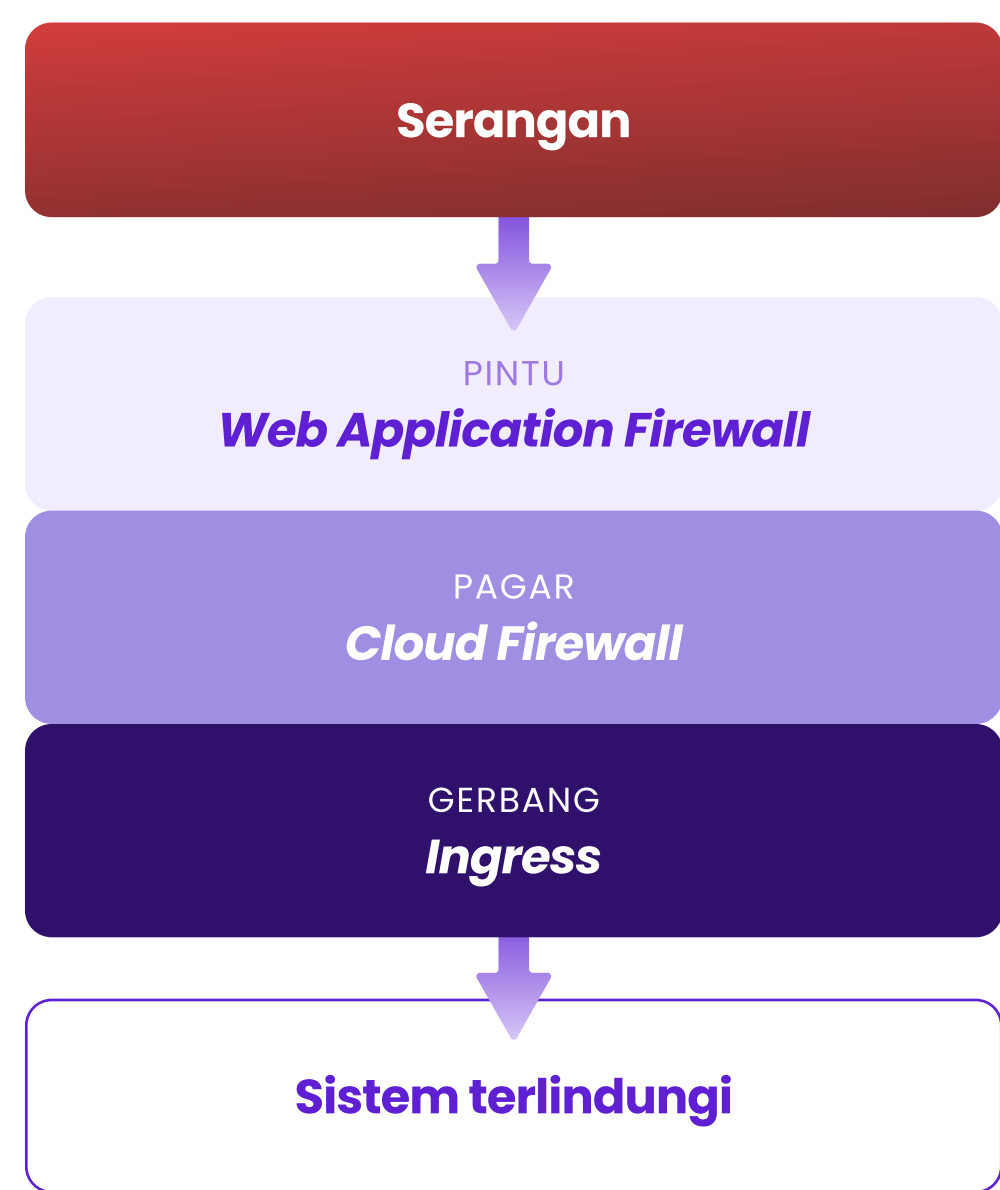
Setiap menit penundaan menambah eksposur finansial

Selisih biaya antara *breach* yang terdeteksi dini vs. *post-impact* pada esensinya adalah beban finansial dari *dwell time*. **MTTD 5 menit berada jauh di bawah ambang 200 hari** yang menjadi titik infleksi *cost premium* IBM, menempatkan insiden ini pada kategori biaya rendah (**USD 3,61 juta**) bukan kategori biaya tinggi (USD 5,49 juta).^{5,8}

Menekan Risiko Account Takeover hingga 95%

Respons yang dilakukan

- Begitu serangan terkonfirmasi, tim memasang blokir di **tiga lapis sekaligus** (WAF, *cloud firewall*, dan *ingress*) seperti menutup pintu, pagar, dan gerbang depan secara bersamaan
- **Total ~450 alamat IP diblokir**, termasuk sejumlah jaringan yang seluruhnya diblokir
- Akun yang tersusupi langsung dinonaktifkan, *password* di-*reset*, dan *user* dikabari melalui *email*



Hasil akhir

2–5 akun terdampak

Hanya 2–5 akun yang benar-benar terdampak, dari potensi ratusan hingga ribuan.

0 data tercuri

Tidak ada data yang berhasil dicuri, *attacker* masih di tahap verifikasi kredensial dan belum sempat berbuat lebih jauh.

38.000+ percobaan diblokir

38.000+ percobaan login berhasil diblokir setelah mitigasi aktif.

24 jam percobaan ulang, 0 berhasil.

Attacker sempat mencoba lagi selama 24 jam setelahnya, tetapi tidak satu pun berhasil masuk.

Mitigation Plan: Jangka Pendek hingga Panjang

Sebagai *security partner*, Cisometric membantu klien menyusun *mitigation plan* berdasarkan temuan insiden dan kondisi sistem yang ada. Rekomendasi ini menjadi *baseline knowledge* bagi tim klien, yang kemudian dipantau dan diingatkan secara berkala untuk mendukung peningkatan *cybersecurity posture* secara berkelanjutan.

Short-term

- *IP blocking*
- *Force password reset* untuk akun yang terindikasi *compromise*
- *Mandatory MFA enrollment* untuk semua *user*. *Notify affected users via email* tentang potensi *compromise* dan rekomendasi *password reset*

Mid-term

- *CAPTCHA implementation* pada *login page* setelah *n failed attempts*
- *Anomaly-based account lockout policy* setelah *n consecutive failures*
- *Rate limiting tuning, enable permanent* di *ingress layer*
- Analisis lanjutan pada *application log* untuk memeriksa *impact* lanjutan (apakah ada aktivitas pengambilan/perubahan data pasca-*compromise*)

Long-term

- *Bot protection solution*
- *Continuous credential monitoring*
- *Dark web monitoring* untuk kredensial klien yang bocor



Apa artinya untuk bisnis Anda?

Penurunan risiko ini datang dari **rangkaian respons yang berlapis dan bertahap**: deteksi dini membuka peluangnya, lalu respons terkoordinasi menutup serangan sebelum sempat berkembang.

Apa yang Harus Disiapkan Sebelum Serangan Terjadi

Untuk *Business Owner*

01 Integrasi log harus selesai sebelum serangan terjadi

SOC hanya dapat mendeteksi aktivitas yang tercakup dalam sumber data yang sudah terintegrasi. Pada kasus ini, proses integrasi membutuhkan 3–5 minggu karena format log aplikasi tidak mengikuti standar umum dan memerlukan pembuatan *custom parser* serta *normalization rule*. Selama periode tersebut, aplikasi beroperasi tanpa visibilitas *real-time* ke dalam SIEM.

Implikasinya: Jika integrasi baru dimulai setelah serangan berlangsung, *window* deteksi pertama sudah terlewat. Seluruh sumber log (*application log*, *cloud audit log*, dan *Kubernetes cluster log*) harus sudah terhubung, sudah melalui proses parsing, dan tervalidasi ke dalam SIEM sebelum insiden terjadi.

Bare minimum: Log dari seluruh lapisan aplikasi sudah terintegrasi secara aktif ke SOC, bukan hanya tersimpan di sistem masing-masing.

02 MFA harus diwajibkan, bukan bersifat opsional

Pada kasus ini, sebagian akun masih hanya mengandalkan kombinasi *username* dan *password* karena OTP belum diwajibkan untuk seluruh pengguna. Celah ini yang memungkinkan *credential stuffing* menghasilkan *successful login* sebelum blokir sempat dieksekusi.

Deteksi dalam 5 menit tidak mencegah *compromise* jika satu percobaan login yang berhasil sudah cukup untuk memberikan akses. MFA memutus rantai tersebut di titik autentikasi, jauh sebelum SOC perlu turun tangan.

Bare minimum: MFA diwajibkan untuk 100% akun pengguna. Tanpa pengecualian, tidak terbatas hanya untuk akun dengan privilese tinggi.

03

Prosedur respons harus sudah terdefinisi sebelumnya

Pada kasus ini, terdapat jeda sekitar 60 menit antara deteksi pertama (02:15) dan eksekusi pemblokiran massal (03:15), sebagian karena proses eskalasi dan notifikasi klien yang harus dilalui terlebih dahulu. Kecepatan respons SOC tidak hanya ditentukan oleh kapabilitas teknis, tetapi juga oleh kejelasan otorisasi: siapa yang berwenang mengeksekusi pemblokiran, siapa yang harus dihubungi, dan dalam urutan seperti apa.

Bare minimum: *Incident response playbook* harus sudah disepakati antara klien dan SOC sebelum insiden terjadi, termasuk delegasi wewenang yang memungkinkan tindakan *containment* dieksekusi tanpa menunggu persetujuan berlapis saat serangan sedang aktif berjalan.

Untuk IT Personnel

KONDISI

MENGAPA KRUSIAL UNTUK DETEKSI 5 MENIT

Format log terdokumentasi

Custom parser tidak dapat dibangun tanpa spesifikasi *format log* yang jelas dan konsisten pada setiap aplikasi atau perangkat. Detail pada *log data* juga harus komprehensif dan bermanfaat untuk pemantauan, seperti: *HTTP code*, *URL Path*, *username*, *email*, *timestamp*, dan *body message*.

Log retention minimal 90 hari

Correlation rule membutuhkan data historis sebagai *baseline* untuk membedakan anomali dari perilaku normal.

Sinkronisasi timestamp antar sumber (UTC)

Inkonsistensi waktu antar sumber *log* merusak urutan kejadian dalam *correlation rule* dan berpotensi menghasilkan *false negative*.

HTTP status code tercatat dalam log

Rule 1 hingga 3 bergantung pada *HTTP 401* dan *HTTP 200*. Jika tidak tersedia dalam *log*, *rule* tidak dapat berfungsi.

Log dikirimkan secara real-time (streaming)

Pengiriman *log* berdasarkan *batch*, misalnya per jam, menjadikan *MTTD* minimum setara dengan interval *batch* tersebut.

Volume log stabil dan terprediksi

Lonjakan volume *log* yang tidak terduga dapat menutupi sinyal serangan atau memicu *false positive* yang menenggelamkan *alert* sesungguhnya.

Tingkat Efisiensi Deteksi dan Reduksi Risiko Menggunakan SOC

Sebuah *uncontrolled environment* yang menghadapi volume serangan berupa **38.000+ login attempts** berpotensi kehilangan **ratusan hingga ribuan account takeovers**. Mengacu pada *success rate* 0,1%–4% per *tested credential*, aplikasi *public-facing* dalam analisis ini diperkirakan akan mengalami **setidaknya 38 akun mengalami compromise**. Dengan SOC, angka tersebut berhenti di **2–5 akun**.

METRIK EVALUASI	BENCHMARK INDUSTRI	AKTUAL SOC	HASIL AKHIR
Kecepatan deteksi (vs. MTTD IBM)	181 hari ⁵	5 menit	~52.000× lebih cepat
Kecepatan deteksi (vs. MTTD Verizon)	5 hari ⁶	5 menit	~1.440× lebih cepat
Tingkat peretasan akun (vs. batas bawah 0,1%)	38 akun (estimasi) ⁴	2 - 5 akun aktual	Reduksi >87%
Tingkat keberhasilan serangan	Baseline 0,1% - 4%* ⁴	~0%**	~100% pencegahan pasca-containment
Window persistensi serangan	2 - 3 hari ⁷	~1 jam 45 menit hingga <i>containment</i>	>25× lebih cepat
Reduksi risiko account takeover keseluruhan	Tidak terkontrol: ratusan hingga ribuan akun berisiko	2 - 5 terkonfirmasi (seluruh fase)	Reduksi risiko ~95%

* tanpa *defense control*
** dengan *defense control*, termasuk SOC

Realita yang Dihadapi Banyak Organisasi

Kondisi klien sebelum memakai SOC **bukanlah pengecualian**, ini realita yang dialami sebagian besar organisasi. Secara global, rata-rata organisasi membutuhkan **181 hari** untuk mengidentifikasi sebuah *breach*, dan *breach* yang baru diketahui setelah ada dampaknya rata-rata menghabiskan biaya **USD 5,08 juta**, dibandingkan dengan **USD 4,18 juta** untuk yang terdeteksi lebih awal oleh tim internal.⁵

“ Skala serangan menentukan seberapa besar ancamannya, sedangkan kesiapan merespons dan kecepatan mendeteksi menentukan seberapa besar kerugiannya.

Faktor Penentu Keberhasilan Penanganan Insiden

Hasil pada kasus di atas bukan kebetulan. Ada empat hal yang memungkinkannya:

Integrasi yang *vendor-neutral*

Mampu menyatukan log dari aplikasi, *cloud*, dan format apa pun, sehingga korelasi tiga lapis log bisa dijalankan sejak awal.

Custom detection

Rule dirancang khusus per aplikasi, bukan *generic template*, termasuk *correlation rule* yang sanggup menangkap pola seperti *Rule 3*.

Eskalasi yang terstruktur

Penanganan insiden melibatkan L1, L2, L3, hingga *SOC Manager*, dengan peran dan tingkat eskalasi yang jelas untuk mendukung investigasi dan respons yang terkoordinasi.

Penanganan *end-to-end*

Dari deteksi, investigasi, respons, dan laporan *post-incident*, hingga *monitoring* dan *reminder* berkala untuk memastikan rekomendasi serta tindak lanjut tetap berjalan.

Menjaga Masa Depan Digital Indonesia

Nama kami mencerminkan komitmen untuk melindungi organisasi di era digital. Kami membantu perusahaan-perusahaan di Indonesia menghadapi dan mempertahankan diri dari ancaman siber yang terus berkembang, sekaligus membangun masa depan digital yang lebih aman dan tangguh.

Dengan pengalaman nyata sebagai CISO (*Chief Information Security Officer*) di industri teknologi, kami menghadirkan pendekatan yang praktis dan relevan dalam menyediakan solusi teknis yang disesuaikan dengan kebutuhan unik setiap klien.

Keahlian ini memungkinkan kami menghadirkan layanan *cybersecurity* dengan standar tinggi. Dengan kerja sama yang erat dengan tim internal klien, Cisometric membantu menjembatani kesenjangan keamanan dan memastikan setiap inisiatif yang dijalankan selaras dengan tujuan bisnis serta kondisi operasional masing-masing organisasi.

SERTIFIKASI

Tim kami terdiri dari para ahli keamanan siber dengan sertifikasi profesional dan pengalaman selama puluhan tahun secara kolektif. Pengalaman tersebut mencakup sektor finansial dan teknologi, termasuk berbagai industri dengan tingkat regulasi yang tinggi di Indonesia.





Keamanan Aplikasi, Infrastruktur, dan Cloud

Manajemen Privasi



Risiko, Manajemen, dan Audit Keamanan Siber

Kepatuhan (Compliance)

VISI KAMI

Kami ingin meningkatkan kematangan keamanan siber setiap perusahaan di Indonesia yang telah memasuki ranah digital.

Kami ingin menanamkan pentingnya keamanan siber, serta memastikan bahwa setiap organisasi memahami risiko dan konsekuensi dari mengabaikannya.

Kami ingin menjadi mitra terpercaya bagi organisasi di Indonesia dalam menghadapi ancaman siber, dengan menjunjung tinggi nilai kepercayaan, keandalan, dan kompetensi.

MISI KAMI

1

Mengedukasi organisasi dan profesional tentang pentingnya peranan keamanan siber dalam era digital.

2

Mendukung organisasi di Indonesia untuk mencapai kematangan keamanan siber yang optimal melalui layanan konsultasi dan pelatihan dari para ahli.

3

Mendorong pertumbuhan generasi profesional keamanan siber baru di Indonesia.

Tim Editorial

Penulis & Riset

Yulis Vidya Dwentari, Ninabelle Nathania

Kontributor Teknis

Muhammad Luqman, Tim SOC Cisometric
(L1, L2, L3, SOC Manager)

Editor

Patricia Antoinette Pramono

Desain dan Tata Letak

Erina Adani Wibisono

Diterbitkan oleh

Cisometric · 2026

White paper ini disusun berdasarkan studi kasus penanganan insiden nyata oleh tim SOC Cisometric, dilengkapi data dan benchmark dari berbagai sumber industri terpercaya.

Daftar Pustaka

- [1] Verizon. (2025). *2025 Data Breach Investigations Report*. Verizon Business. <https://www.verizon.com/business/resources/articles/credential-stuffing-attacks-2025-dbir-research/>, diakses pada 16 Juni 2026
- [2] BSSN. (2024). *Lanskap Keamanan Siber Indonesia 2023*. Direktorat Operasi Keamanan Siber, Badan Siber dan Sandi Negara. <https://csirt.kemenpora.go.id/wp-content/uploads/2025/02/keamanan.pdf>, diakses pada 16 Juni 2026
- [3] BSSN. (2025). *Lanskap Keamanan Siber Indonesia 2024*. Direktorat Operasi Keamanan Siber, Badan Siber dan Sandi Negara. <https://alika.pesisirbaratkab.go.id/files/272/E-BOOK/262/Lanskap-Kemanan-Siber-Indonesia-2024--BSSN.pdf>, diakses pada 16 Juni 2026
- [4] Imperva. (2024). *What Is Credential Stuffing?* Imperva Research Labs. <https://www.imperva.com/learn/application-security/credential-stuffing/>, diakses pada 16 Juni 2026
- [5] IBM Security & Ponemon Institute. (2025). *Cost of a Data Breach Report 2025*. IBM Corporation. <https://www.ibm.com/reports/data-breach>, diakses pada 16 Juni 2026
- [6] Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon Business. <https://www.verizon.com/business/resources/reports/dbir/>, diakses pada 16 Juni 2026
- [7] Sodja, C., & Carroll, J. A. N. (2023). *Detection of brute force attacks* (U.S. Patent No. 11,757,931). United States Patent and Trademark Office. <https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/11757931>, diakses pada 16 Juni 2026
- [8] IBM Security. (2024). *Cost of a Data Breach Report 2024*. IBM Corporation. <https://www.ibm.com/reports/data-breach>, diakses pada 16 Juni 2026

Ingin serangan ke aplikasi Anda bisa terdeteksi dalam hitungan menit dan potensi *account takeover* ditekan hingga 95%?

Tim SOC Cisometric dapat membantu, mulai
dari integrasi log, *custom detection*, hingga
respons *end-to-end*.

CISOMETRIC

PT Perisai Digital Indonesia

MidPlaza 2, 25th Floor
Jl. Jend. Sudirman Kav. 10 – 11
+62 21 573 7777

www.cisometric.com

SECURING TOMORROW, TODAY

HUBUNGI KAMI

