IT & Sistem

KPI Insiden Keamanan per Bulan

Jumlah insiden cybersecurity yang dilaporkan tiap bulan.

RUMUS	SATUAN	FREKUENSI
`Hitung insiden per bulan (per severity tier)`	**Jumlah insiden**	**Bulanan**

TARGET	PENANGGUNG JAWAB	SUMBER DATA
0 critical; minimum total trend	**CISO / Security Engineer**	Monitoring tool (Datadog, Prometheus), ITSM ticket system, security log

Definisi & Konteks

Insiden Keamanan adalah event yang melibatkan pelanggaran kebijakan keamanan, kompromi sistem, atau potensi kebocoran data. Trending angka ini bersama severity menjadi indikator postur keamanan.

Mengapa KPI Ini Penting

- Mengukur reliabilitas & kualitas layanan IT yang langsung dirasakan user / customer.
- Trigger SLA breach detection — krusial untuk komitmen kontrak hosting, SaaS, dan MSP.
- Indikator kesehatan postur cybersecurity dan kapabilitas incident response tim.
- Bahan utama capacity planning, budget IT, dan justifikasi investasi tools / lisensi.

Cara Menghitung

1. Kumpulkan data sumber untuk periode pengukuran (Bulanan). Pastikan dari sistem otoritatif, bukan rekap manual.

2. Validasi kelengkapan dan akurasi data — buang outlier akibat kesalahan input atau periode tidak penuh.
3. Hitung dengan rumus: Hitung insiden per bulan (per severity tier).
4. Bandingkan hasil dengan target 0 critical; minimum total trend dan periode sebelumnya untuk lihat trend.
5. Dokumentasikan di dashboard KPI dan komunikasikan ke pemangku kepentingan dalam rapat rutin.

Contoh Kalkulasi

Substitusikan nilai aktual periode pengukuran ke rumus. Bandingkan hasil dengan target 0 critical; minimum total trend dan periode sebelumnya untuk melihat trend.

Interpretasi Hasil

Status	Apa yang Berarti	Tindakan Singkat
Off-target	Hasil di luar target (0 critical; minimum total trend). Trend memburuk atau jauh dari standar industri.	Aktifkan root cause analysis. Stop kampanye / proses jika dampak material. Eskalasi ke pemangku kepentingan.
Borderline	Hasil dekat target, tapi trend tidak konsisten — risk-off setiap saat.	Identifikasi 2–3 driver utama. Lakukan perbaikan iteratif sebelum jadi off-target permanen.
On-target	Hasil memenuhi target (0 critical; minimum total trend). Trend stabil atau membaik.	Pertahankan praktik baik. Dokumentasikan SOP dan transfer ke unit / shift lain.
Excellent	Hasil konsisten melampaui target. Trend positif berlanjut.	Bagikan praktik baik sebagai best practice internal. Pertimbangkan stretch target.

> **Hindari over-react ke 1 periode.** KPI bisa fluktuatif karena sebab di luar kendali tim. Trend 3 periode berturut-turut lebih meaningful.

Variasi Pengukuran & Best Practice

Dimensi	Mengapa Berguna
Per Tier Service	P1 (mission-critical) vs P4 (best-effort). SLA harus berbeda per tier.
Per Aplikasi / Sistem	Sistem core (ERP, CRM) vs supporting tools. Beda dampak ke bisnis.
Per Lokasi	Site HQ vs cabang vs remote. Pola insiden sering berbeda jauh.
Working vs Non-working Hours	SLA jam kerja vs di luar jam kerja perlu kebijakan staffing berbeda.

Kesalahan Umum & Solusinya

Kesalahan	Solusi
SLA seragam untuk semua sistem (one-size-fits-all)	Tier per kritikalitas — tidak semua sistem butuh 99.99%.
Monitoring hanya post-mortem, bukan proaktif	Tambah synthetic monitoring & alerting trend, bukan hanya threshold.
Tidak ada chaos drill / DR test rutin	Backup tanpa restore drill = tidak terbukti reliable. Test minimal 1× per kuartal.
Insiden tidak di-classify dengan benar (P1/P2/P3)	Definisi tertulis dan training tim sebelum on-call.
Vendor dependency tinggi tanpa runbook internal	Pastikan tim internal bisa eksekusi minimal recovery procedure.

Tindakan Berdasarkan Status

Off-target

Hasil di luar target / trend memburuk

Aktifkan war room / incident bridge. Komunikasi ke stakeholder per 30 menit. Setelah resolve, post-incident review dalam 5 hari kerja dengan action item bertanggal.

Borderline

Mendekati target, trend tidak konsisten

Tinjau capacity & infrastructure planning. Upgrade tier untuk sistem mission-critical. Tambah redundancy / failover. Update runbook dan training tim on-call.

On-target / Excellent

Memenuhi atau melampaui target

Konsolidasi praktik baik ke runbook. Eksplor self-healing automation. Adopsi engineering excellence: chaos engineering, SLO/SLI framework, observability tooling modern.

KPI Pendamping

KPI ini sebaiknya tidak berdiri sendiri. Padukan dengan KPI lain di kategori yang sama:

- **KPI IT Cost per User** — Rata-rata biaya IT per user / karyawan yang dilayani.
- **KPI Mean Time Between Failures (MTBF)** — Rata-rata waktu antara dua kegagalan sistem berturut-turut.
- **KPI Backup Success Rate** — Persentase backup data yang berhasil dijalankan sesuai jadwal.
- **KPI First Call Resolution (FCR) IT** — Persentase tiket IT yang selesai di kontak pertama tanpa eskalasi.

Checklist Implementasi

1. Tetapkan baseline. Ukur 1–2 periode sebelum set target — jangan langsung set target ambisius tanpa tahu starting point.
2. Definisikan formula tertulis. Tuliskan rumus, sumber data, exclusion rule di glossarium yang dapat diakses tim.
3. Otomatisasi pengumpulan data. Manual entry = rentan error & delay. Pakai sistem sumber otoritatif dengan ETL / sync rutin.

4. Set cadence review. Frekuensi pengukuran = Bulanan. Pastikan ada slot rapat rutin untuk membahas hasil dan action plan.
5. Action SLA. Setiap deviasi > threshold tertentu harus memicu action plan. Tanpa SLA = monitoring tanpa improvement.
6. Komunikasikan ke tim. Bagikan hasil + tindakan yang akan diambil. Karyawan yang tahu konteks lebih engaged dan kolaboratif.
7. Iterasi target tahunan. Target tahun lalu mungkin tidak relevan tahun ini. Adjust ke realitas bisnis saat strategic planning.

> **Tools:** Tools rekomendasi: Datadog, New Relic, atau Grafana Cloud untuk observability. ServiceNow / Jira Service Desk untuk ITSM. Untuk security: Sentry, Wazuh (open-source SIEM), atau Splunk. Setup alerting yang aksioner, bukan noise.