



PEMERINTAH KABUPATEN KUTAI TIMUR

KUTIM-CSIRT

COMPUTER SECURITY INCIDENT RESPONSE TEAM

TLP: CLEAR

BOLEH DISEBARLUASKAN

```
$ csirt report --monthly --period=2026-09 --tlp=clear
```

LAPORAN BULANAN PUBLIK

Hasil Monitoring Keamanan Siber

Rekapitulasi pemantauan keamanan, penanganan insiden, dan layanan publik di lingkungan Pemerintah Kabupaten Kutai Timur.

SEPTEMBER 2026

PERIODE 1 – 30 SEPTEMBER 2026

123

ASET MELAPOR

76

PERANGKAT DITANGANI

3.946.801

PERISTIWA BERMAKNA

19

ADVISORY TERBIT

TLP: CLEAR

KUTIM-CSIRT/LAPBUL/09/2026

csirt.kutaitimurkab.go.id

Daftar Isi

01	Ringkasan Eksekutif
02	Monitoring Keamanan Siber
03	Tingkat Keparahan & Klasifikasi Peristiwa
04	Jenis Peristiwa & Aset Terdampak
05	Sumber Serangan & Pola Sasaran
06	Teknik Serangan (MITRE ATT&CK)
07	Intelijen Ancaman
08	Keamanan Endpoint (EDR)
09	Tren Antarbulan
10	Insiden & Layanan Aduan
11	Kerentanan yang Dperingatkan
12	Indikator Ancaman, Berita & Edukasi
13	Kegiatan & Layanan Publik
14	Anjuran Tindak Lanjut
15	Metodologi, Batasan Data & Glosarium

Tentang laporan ini. Laporan bulanan publik KUTIM-CSIRT disusun dari tiga sumber: sistem pemantauan keamanan terpusat pada Security Operations Center Pemerintah Kabupaten Kutai Timur, sistem pemantauan perangkat kerja, dan basis data portal KUTIM-CSIRT. Seluruh angka dihasilkan otomatis dari data operasional — tidak ada nilai yang diisi manual. Metodologi dan batasannya dijelaskan pada bagian terakhir.

Ringkasan Eksekutif

periode: 1 – 30 September 2026

Laporan ini merangkum hasil pemantauan keamanan siber, penanganan insiden, serta layanan publik KUTIM-CSIRT sepanjang September 2026. Pemantauan dijalankan Security Operations Center Pemerintah Kabupaten Kutai Timur dalam **dua lapisan yang saling melengkapi**: pemantauan terpusat atas lalu lintas dan log seluruh layanan, serta pemantauan langsung pada perangkat kerja.

123

aset melapor ke pemantauan terpusat pada periode ini

76

perangkat kerja dengan temuan yang ditindaklanjuti

Kedua angka mengukur hal yang berbeda dan sengaja tidak dijumlahkan. Angka pertama adalah aset yang mengirim data pemantauan pada periode ini; angka kedua adalah perangkat kerja yang temuannya ditindaklanjuti, bukan seluruh perangkat yang diawasi.

TIKET BARU MASUK

0

tidak ada laporan baru periode ini

TIKET DITUNTASKAN

1

berasal dari periode sebelumnya

INSIDEN DITANGANI

0

tidak ada insiden pada periode ini

ADVISORY DITERBITKAN

19

peringatan kerentanan

BERITA KEAMANAN

6

artikel edukasi publik

INDIKATOR (IOC) BARU

0

dibagikan ke OPD

Cara membaca laporan ini. Angka pemantauan adalah jumlah peristiwa yang tercatat sistem, bukan jumlah serangan yang berhasil. Mayoritas peristiwa merupakan upaya yang berhasil ditahan atau aktivitas otomatis dari internet. Laporan berlabel TLP:CLEAR sehingga bebas disebarluaskan.

Monitoring Keamanan Siber

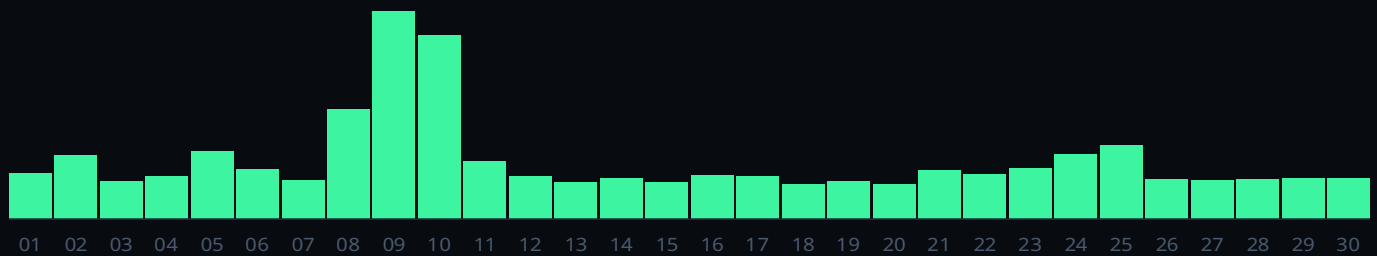
sumber: pemantauan keamanan terpusat – security operations center

13.103.454

PERISTIWA DIPROSES

Sepanjang September 2026, sensor SOC memproses peristiwa dari seluruh aset terpantau. Setelah penyaringan derau operasional (kegagalan layanan, rotasi log, status agen), tersisa **3.946.801 peristiwa bermakna** yang relevan bagi keamanan.

> Sebaran Peristiwa Harian



tanggal – september 2026

> Penyaringan Akses Internet

66.897.064

PERMINTAAN WEB DITOLAK

Gerbang akses internet menolak permintaan yang melanggar kebijakan keamanan dan kepatutan sebelum mencapai pengguna. Penyaringan ini mencakup **82 unit kerja** dengan puncak **115.430 pengguna serentak** pada periode ini.

> Penyaringan di Perimeter Jaringan

20.716

SERANGAN TERDETEKSI

Perangkat perimeter mencatat upaya serangan terhadap zona terlindungi sepanjang periode ini; mayoritas di antaranya ditahan sebelum mencapai sistem tujuan. Dengan kebijakan keamanan yang diterapkan, tingkat perlindungan zona terlindungi dinilai naik dari **Poor** menjadi **Excellent**.

114.737

Upaya serangan aplikasi web
(SQL injection, XSS, traversal)

18.872

Pemblokiran otomatis alamat IP
oleh sistem pemantauan

15.248

Kecocokan dengan indikator
ancaman yang telah dikenal

> Serangan Terpantau — Peta Serangan Live

723.129

SERANGAN TERPANTAU

Upaya serangan dari internet terhadap aset Pemerintah Kabupaten Kutai Timur, dihitung dengan definisi yang sama dengan halaman **Peta Serangan Live** (csirt.kutaitimurkab.go.id/peta-serangan). Sebanyak **96.989** diblokir langsung dan **100.719** bertingkat tinggi.

54.614

Alamat IP penyerang unik

175

Negara asal serangan

3.882

Alamat IP diblokir otomatis di tepi jaringan

Kategori serangan

Pemindaian celah (scanning)		562.195
Serangan web		103.120
Brute force		20.136
IP berbahaya terdaftar		18.093
Eksplorasi celah		13.414
Lainnya		4.671

Negara asal teratas

Amerika Serikat		245.134
Indonesia		121.355
Spanyol		62.946
Belanda		37.760
Singapura		31.257
Kanada		29.777

BAGIAN 03

Tingkat Keparahan & Klasifikasi

sebaran tingkat keparahan dan kategori peristiwa

> Sebaran Tingkat Keparahan

Kritis (13-15)		31.118
Tinggi (10-12)		335.109
Sedang (7-9)		3.580.574
Rendah / informasional (0-6)		9.156.653

Setiap peristiwa diberi tingkat keparahan pada skala 0–15. Tingkat 0–6 bersifat informasional dan mendominasi secara wajar; perhatian operasional difokuskan pada tingkat 7 ke atas.

> Klasifikasi Peristiwa Keamanan

Serangan terhadap aplikasi (attack)		1.621.568
Kegagalan autentikasi		1.220.005

Deteksi kerentanan pada aset		745.467
Perubahan berkas sistem (FIM)		525.384
Web scanning (pemindaian layanan web)		113.710

Catatan penghitungan. Satu peristiwa dapat membawa lebih dari satu klasifikasi sekaligus, sehingga angka pada tabel di atas tidak dimaksudkan untuk dijumlahkan menjadi total.

BAGIAN 04

Jenis Peristiwa & Aset Terdampak

> Jenis Peristiwa Keamanan Terbanyak

Kegagalan autentikasi sistem (syslog)		310.189
Permintaan berbahaya ditolak WAF		98.833
Kegagalan autentikasi SASL (Postfix)		74.898
Kegagalan autentikasi SSH		51.751
IP diblokir otomatis oleh sistem		18.872
Kecocokan indikator ancaman — Network activity		12.388
Web scanning dari IP non-trusted		7.977
Upaya login CMS (WordPress/Joomla)		7.455

> Aset dengan Peristiwa Terbanyak

Portal dan aplikasi Perangkat Daerah		7.786.213
Layanan email dan kolaborasi		2.204.941
Server aplikasi internal		816.781
Layanan autentikasi jaringan		740.207
Sistem pengawasan CCTV		411.700
Infrastruktur pusat operasi keamanan		404.556
Sistem pemantauan dan audit		311.811
Layanan otomasi dan pendukung		281.306

Catatan. Aset disajikan menurut jenis layanan, bukan per mesin — identitas sistem tidak dipublikasikan. Jumlah peristiwa yang tinggi pada suatu jenis aset juga tidak berarti aset itu paling rentan: layanan yang menghadap publik secara langsung, terutama email dan portal, secara alami menerima lebih banyak upaya otomatis dari internet dibanding sistem internal.

Sumber Serangan & Pola Sasaran

alamat ip sumber dan jalur yang diminta penyerang

> Alamat IP Sumber Serangan Terbanyak

ALAMAT IP	PERISTIWA
45.148.10.***	27.687
185.177.72.***	13.858
103.59.161.***	7.078
172.81.132.***	3.046
182.14.46.***	2.106
91.92.47.***	1.673

> Contoh Pola Sasaran

Jalur berikut benar-benar diminta oleh penyerang pada periode ini. Muatan eksploit sengaja dipangkas — yang ditampilkan hanya polanya, agar dapat dikenali tanpa dapat disalin ulang.

ALAMAT IP	TEKNIK	CONTOH JALUR DIMINTA
172.81.132.***	Path traversal · Scanning jalur umum	/cgi-bin/../../../../bin/sh /.vscode/sftp.json /upload/kcfinder/files/tdn.php
62.60.130.***	Pencarian berkas konfigurasi & kredensial	/.env.bak /.env.backup /.env.production
89.126.211.***	Scanning jalur umum	/index.php?... /phpunit/phpunit/Util/PHP/eval-stdin.php /V2/vendor/phpunit/phpunit/src/Util/PHP/eval-...
34.97.92.***	Pencarian berkas konfigurasi & kredensial	/.env.bak /.env.backup /.env.swp
169.150.227.***	Enumerasi endpoint API	/api/settings /api/debug
13.212.226.***	Enumerasi halaman login · Pencarian berkas konfigurasi & kredensial	/login /.env.local /.env.bak
159.89.194.***	Scanning jalur umum	/wp-content/plugins/pods/readme.txt
103.89.2.***	Scanning jalur umum	/beranda /website /home

Yang bisa dilakukan Perangkat Daerah. Pola di atas menunjukkan penyerang secara rutin menebak keberadaan berkas konfigurasi dan cadangan. Pastikan berkas seperti .env, wp-config.bak, dan backup.sql tidak berada di dalam direktori yang dilayani web server.

BAGIAN 06

Teknik Serangan (MITRE ATT&CK)

pemetaan peristiwa ke kerangka mitre att&ck

MITRE ATT&CK adalah kerangka rujukan internasional yang memetakan teknik yang digunakan penyerang. Pemetaan ini membantu Perangkat Daerah memahami cara penyerang bekerja, bukan sekadar berapa banyak peristiwa yang tercatat.

TEKNIK	PERISTIWA
Valid Accounts	2.076.053
Remote Services	978.522
Stored Data Manipulation	237.660
Password Guessing	153.255
Sudo and Sudo Caching	149.010
File Deletion	132.749
Data Destruction	132.749
File and Directory Discovery	105.287

Membaca tabel ini. Nama teknik sengaja dipertahankan dalam istilah aslinya agar dapat ditelusuri langsung pada dokumentasi MITRE ATT&CK di attack.mitre.org.

BAGIAN 07

Intelijen Ancaman

kecocokan dengan indikator ancaman yang telah dikenal

SOC Pemerintah Kabupaten Kutai Timur berlangganan basis indikator ancaman yang dikelola bersama komunitas keamanan. Lalu lintas yang cocok dengan indikator yang telah dikenal berbahaya otomatis memunculkan peringatan.

15.248

KECOCOKAN INDIKATOR

Setiap kecocokan berarti ada komunikasi dengan alamat atau sumber daya yang sudah ditandai berbahaya oleh komunitas keamanan. Kategori kecocokan pada periode ini disajikan di bawah.

> Kategori Kecocokan Indikator

Network activity	15.189
Payload delivery	59



Keamanan Endpoint (EDR)

sumber: pemantauan keamanan perangkat kerja

76

ENDPOINT DIPANTAU

Lapisan ini melengkapi pemantauan terpusat: komputer kerja dan server diawasi langsung pada perangkatnya. Pada periode ini terdeteksi **93 temuan** dari **16 jenis ancaman** yang berbeda — seluruhnya terdeteksi dan tertahan pada tahap awal.

> Status Risiko Endpoint

COMPROMISED

75

endpoint

HIGH RISK

1

endpoint

> Keluarga Ancaman Terdeteksi

Cryptojacking / mining virus		5
Lainnya		2
Tunneling / evasion		2
Threat indicator match		1
Worm		1
Trojan		1
Hacktool		1
Malicious domain access		1
Exploitation (eksploitasi kerentanan)		1
Phishing		1

Angka menunjukkan banyaknya jenis ancaman pada tiap keluarga, bukan jumlah perangkat terdampak.

> Tahapan Ancaman

C&C (komunikasi command & control)		70
Propagation (penyebaran lateral)		8
Impact (dampak pada sistem)		4
Weakness (kelemahan terdeteksi)		1

> Kelemahan Konfigurasi

Improper configuration (konfigurasi tidak aman)		9
Weak password (kata sandi lemah)		1

Tindak lanjut. Setiap temuan ditindaklanjuti bersama Perangkat Daerah pemilik perangkat — pembersihan malware, penggantian kata sandi, dan penutupan celah konfigurasi. KUTIM-CSIRT mendampingi proses tersebut dan memantau perkembangannya hingga tuntas.

BAGIAN 09

Tren Antarbulan

perbandingan volume peristiwa antarperiode

BULAN	PERISTIWA DIPROSES		BERMAKNA
Juni		9.993.522	32.844
Juli		6.053.217	574.653
Agustus		8.540.271	767.430
September		13.103.454	3.946.801

BAGIAN 10

Insiden & Layanan Aduan

> Insiden yang Ditangani

Tidak ada insiden yang ditangani pada periode ini.

> Tiket Pelaporan

Tidak ada tiket baru yang masuk pada periode ini.

Total 1 pembaruan tiket dicatat pada periode ini. Kanal pelaporan: csirt.kutaitimurkab.go.id/lapor

Kerentanan yang Diperingatkan

advisory yang diterbitkan pada periode ini

CVE	PRODUK	CVSS	TINGKAT	KEV
CVE-2026-21962	Oracle HTTP Server	10,0	CRITICAL	YA
CVE-2026-69240	Sequelize ORM	9,8	CRITICAL	—
CVE-2026-18431	Tema WordPress Avada	9,8	CRITICAL	—
CVE-2026-32566	Plugin WordPress ACPT	9,8	CRITICAL	—
CVE-2026-20212	—	9,8	CRITICAL	—
CVE-2026-76461	Secure Email Gateway	9,8	CRITICAL	—
CVE-2026-93616	—	9,8	CRITICAL	—
CVE-2026-32479	Plugin WordPress Visitor Traffic...	9,3	CRITICAL	—
CVE-2023-54391	—	9,3	CRITICAL	—
CVE-2026-94127	—	9,3	CRITICAL	—
CVE-2026-81094	mcp-router CLI	9,1	CRITICAL	—
CVE-2026-7273	—	8,8	HIGH	—
CVE-2026-65660	Microsoft SharePoint Server	8,8	HIGH	—
CVE-2026-91813	—	8,8	HIGH	—
CVE-2026-5423	Neo4j GraphQL	8,2	HIGH	—
CVE-2025-25249	—	8,1	HIGH	—
CVE-2026-87902	—	8,1	HIGH	—
CVE-2026-81934	Redis dengan TLS	7,5	HIGH	—
CVE-2026-85706	—	—	—	—

Kolom **KEV** menandai kerentanan

yang tercatat pada katalog Known Exploited Vulnerabilities CISA — sudah terkonfirmasi dieksploitasi di dunia nyata: **1 dari 19** advisory periode ini. Naskah lengkap setiap advisory tersedia di csirt.kutaitimurkab.go.id/posts.

Indikator, Berita & Edukasi

> Indikator Ancaman (IoC) yang Dibagikan

42

INDIKATOR DI THREAT FEED LOKAL

Posisi per akhir September 2026: indikator ancaman yang terbit dan masih berlaku di csirt.kutaitimurkab.go.id/ioc, dalam format terbuka yang dapat ditarik otomatis oleh perangkat jaringan Perangkat Daerah. Sepanjang periode ini terbit **0** indikator baru.

Tidak ada indikator ancaman baru yang dibagikan pada periode ini. Indikator yang telah terbit sebelumnya tetap tersedia di csirt.kutaitimurkab.go.id/ioc.

> Berita & Edukasi Keamanan

- 02 Sep Zero Trust: Mengapa Jaringan Internal Tidak Lagi Otomatis Tepercaya
- 03 Sep Serangan Rantai Pasok: Ketika Instansi Diserang Lewat Pihak yang Sudah Dipercaya
- 09 Sep Serangan Siber pada Sistem Pengelolaan Air di Minnesota dan Pelajarannya bagi Sistem OT Daerah
- 09 Sep Dari Infostealer ke Pengambilalihan Akun: Menghapus Malware Saja Belum Menutup Insiden
- 30 Sep Waspada Email Pemberitahuan Audit Pajak: Kampanye SilverFox Menyasar Organisasi di Indonesia
- 30 Sep Ransomware Mengincar Layanan SaaS Perkantoran: Pelajaran dari Insiden SmartHRMS

Kegiatan & Layanan Publik

Tidak ada kegiatan yang tercatat pada periode ini.

> Layanan Publik

KUNJUNGAN PORTAL

545

csirt.kutaitimurkab.go.id

DOKUMEN PANDUAN

35

tersedia untuk publik

PELAPOR DIAPRESIASI

3

Hall of Fame VDP

Anjuran Tindak Lanjut

disusun dari temuan periode ini, bukan anjuran umum

Setiap anjuran di bawah diturunkan langsung dari temuan September 2026 dan mencantumkan dasar angkanya.

01 Perkuat autentikasi pada layanan yang terekspos internet

Kegagalan autentikasi mendominasi peristiwa bulan ini. Aktifkan multi-factor authentication (MFA) untuk seluruh akun administratif, terapkan penguncian akun setelah percobaan gagal beruntun, dan pastikan pemblokiran otomatis aktif pada layanan akses jarak jauh serta panel pengelola.

Dasar: 436.838 peristiwa kegagalan autentikasi

02 Kunci konfigurasi mail server

Pastikan tidak ada open relay, aktifkan rate limiting per pengirim, dan lengkapi domain dengan SPF, DKIM, serta DMARC. Tinjau akun email yang menjadi sasaran percobaan login beruntun dan paksa penggantian kata sandi.

Dasar: 74.898 peristiwa pada layanan email

03 Tempatkan penyaring aplikasi web di depan seluruh portal Perangkat Daerah

Penyaring permintaan di depan aplikasi web terbukti menahan sebagian besar upaya serangan bulan ini. Perangkat Daerah yang portalnya belum dilindungi dianjurkan segera berkoordinasi dengan KUTIM-CSIRT.

Dasar: 114.737 upaya serangan aplikasi web

04 Keluarkan berkas konfigurasi dan cadangan dari webroot

Penyerang secara rutin menebak jalur seperti `.env`, `wp-config.bak`, dan `backup.sql`. Simpan berkas tersebut di luar direktori yang dilayani web server, dan tambahkan aturan penolakan akses untuk berkas berawalan titik serta berekstensi `.bak`, `.sql`, dan `.old`.

Dasar: terpantau pada contoh jalur yang disasar bulan ini

05 Perketat pengelolaan WordPress

Perbarui core, tema, dan plugin secara berkala; hapus yang tidak dipakai. Larang eksekusi PHP di dalam direktori uploads — langkah ini memutus rantai serangan arbitrary file write bahkan ketika berkas berhasil ditulis.

Dasar: terdeteksi enumerasi dan upaya login CMS

06 Manfaatkan IoC Feed KUTIM-CSIRT di perangkat perimeter

Indikator yang cocok dengan basis ancaman dapat langsung diblokir di firewall atau gateway masing-masing Perangkat Daerah. Daftar indikator tersedia terbuka dalam format JSON dan CSV di csirt.kutaitimurkab.go.id/ioc.

Dasar: 15.248 kecocokan indikator ancaman

07 Dahulukan penambalan kerentanan berstatus KEV

Kerentanan yang tercatat pada katalog Known Exploited Vulnerabilities CISA sudah terkonfirmasi dieksploitasi di dunia nyata, sehingga menjadi prioritas tertinggi. Cocokkan daftar advisory pada laporan ini dengan inventaris aset masing-masing Perangkat Daerah.

Dasar: 1 dari 19 advisory bulan ini berstatus KEV

08 Laporkan dugaan insiden sedini mungkin

Kanal pelaporan KUTIM-CSIRT terbuka bagi seluruh Perangkat Daerah dan masyarakat melalui csirt.kutaitimurkab.go.id/lapor. Pelaporan dini memperbesar peluang penanganan sebelum dampak meluas.

Dasar: layanan tersedia sepanjang periode

BAGIAN 15

Metodologi & Batasan Data

> Sumber Data

Laporan ini menggabungkan data dari beberapa lapis perangkat keamanan yang dioperasikan Pemerintah Kabupaten Kutai Timur. Yang disebut di bawah adalah jenis perangkatnya; merek dan konfigurasi tidak dipublikasikan.

SIEM	Pemantauan dan korelasi log terpusat — sumber angka peristiwa, klasifikasi, tingkat keparahan, sumber serangan, dan pemetaan MITRE ATT&CK.
EDR	Endpoint Detection and Response — deteksi ancaman langsung pada komputer kerja dan server: malware, C&C, dan kelemahan konfigurasi.
NGFW	Next-Generation Firewall — penyaringan lalu lintas di perimeter jaringan beserta pemblokiran serangan yang masuk.
NDR	Network Detection and Response — korelasi anomali lalu lintas jaringan untuk mengenali pola serangan yang melintasi banyak aset.
IAG	Internet Access Gateway — gerbang akses internet yang menyaring permintaan keluar berdasarkan kebijakan keamanan dan keputusan.
WAF	Web Application Firewall — penyaring permintaan berbahaya di depan aplikasi web Perangkat Daerah.
Threat intelligence	Basis indikator ancaman yang dikelola bersama komunitas keamanan, dipadankan otomatis dengan lalu lintas yang terpantau.
Portal KUTIM-CSIRT	Basis data layanan publik — tiket pelaporan, insiden, advisory kerentanan, indikator ancaman, kegiatan, dan panduan.

Tidak semua lapisan berkontribusi pada setiap bagian laporan; cakupan tiap angka dijelaskan pada bagian yang bersangkutan.

> Cara Angka Dihitung

- › **Peristiwa diproses** adalah seluruh baris peringatan yang masuk ke sistem pemantauan, termasuk derau operasional.
- › **Peristiwa bermakna** adalah peristiwa dengan tingkat keparahan 7 ke atas pada skala 0–15. Pembedaan ini dibuat agar angka besar tidak disalahartikan sebagai jumlah serangan.
- › **Peristiwa yang disaring** mencakup kegagalan layanan berulang, rotasi log, status agen, pemeriksaan integritas berkas rutin, serta lalu lintas otomasi monitoring internal.
- › **Serangan terpantau** (Peta Serangan Live) adalah upaya serangan dari alamat di luar jaringan Pemerintah Kabupaten Kutai Timur yang terdeteksi lapisan pemantauan, perimeter, WAF, dan pemblokiran otomatis. Crawler mesin pencari yang hanya mengenai halaman tidak ditemukan tidak dihitung. Definisinya sama dengan angka pada halaman Peta Serangan Live.
- › **Threat Feed Lokal** adalah posisi indikator ancaman yang terbit dan masih berlaku pada akhir periode; indikator kedaluwarsa tidak dihitung.
- › **Alamat IP milik Pemerintah Kabupaten Kutai Timur** dikeluarkan dari daftar sumber serangan, demikian pula alamat privat dan rentang dokumentasi.

> Batasan

- › Jumlah peristiwa **bukan** jumlah serangan berhasil. Sebagian besar merupakan upaya yang ditahan atau pemindaian otomatis dari internet.
- › Cakupan terbatas pada aset yang terpasang agen pemantauan; sistem di luar itu tidak terwakili.
- › Identitas sistem dan alamat internal tidak dipublikasikan, sehingga penyajian aset dilakukan pada tingkat jenis layanan.

> Glosarium

SOC	Security Operations Center — unit yang memantau keamanan siber secara terus-menerus.
EDR	Endpoint Detection and Response — perangkat lunak pemantau ancaman pada komputer kerja dan server.
IoC	Indicator of Compromise — indikator teknis yang menandakan aktivitas berbahaya, misalnya alamat IP atau nama domain.
KEV	Known Exploited Vulnerabilities — katalog CISA berisi kerentanan yang terbukti dieksploitasi.
CVSS	Skor baku tingkat keparahan kerentanan, rentang 0,0–10,0.
Pemblokiran otomatis	Tindakan yang dijalankan sistem tanpa campur tangan operator, misalnya menolak alamat IP yang terbukti menyerang.
Brute force	Percobaan menebak kata sandi secara beruntun.
C&C	Command and Control — saluran kendali penyerang terhadap perangkat yang terinfeksi.
TLP	Traffic Light Protocol — penanda tingkat kerahasiaan dokumen. CLEAR berarti bebas disebarluaskan.

Penutup. Laporan insiden dapat disampaikan melalui csirt.kutaitimurkab.go.id/lapor atau csirt@kutaitimurkab.go.id. Dokumen berlabel **TLP:CLEAR** dan bebas disebarluaskan. Diterbitkan oleh **KUTIM-CSIRT** — Diskominfo Staper Kabupaten Kutai Timur · KUTIM-CSIRT/LAPBUL/09/2026