



PEMERINTAH KABUPATEN KUTAI TIMUR

KUTIM-CSIRT

COMPUTER SECURITY INCIDENT RESPONSE TEAM

```
$ csirt report --monthly --period=2026-07 --tlp=clear
```

LAPORAN BULANAN PUBLIK

Hasil Monitoring Keamanan Siber

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

JULI 2026

PERIODE 1 – 31 JULI 2026

118

ASET MELAPOR

85

PERANGKAT DITANGANI

574.653

PERISTIWA BERMAKNA

4

ADVISORY TERBIT

TLP: CLEAR

KUTIM-CSIRT/LAPBUL/07/2026

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 – 31 Juli 2026

Laporan ini merangkum hasil pemantauan keamanan siber, penanganan insiden, serta layanan publik KUTIM-CSIRT sepanjang Juli 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.

118

aset melapor ke pemantauan terpusat pada periode ini

85

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

2

laporan dari warga & Perangkat Daerah

TIKET DITUNTASKAN

0

termasuk sisa periode sebelumnya

INSIDEN DITANGANI

0

tidak ada insiden pada periode ini

ADVISORY DITERBITKAN

4

peringatan kerentanan

BERITA KEAMANAN

1

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

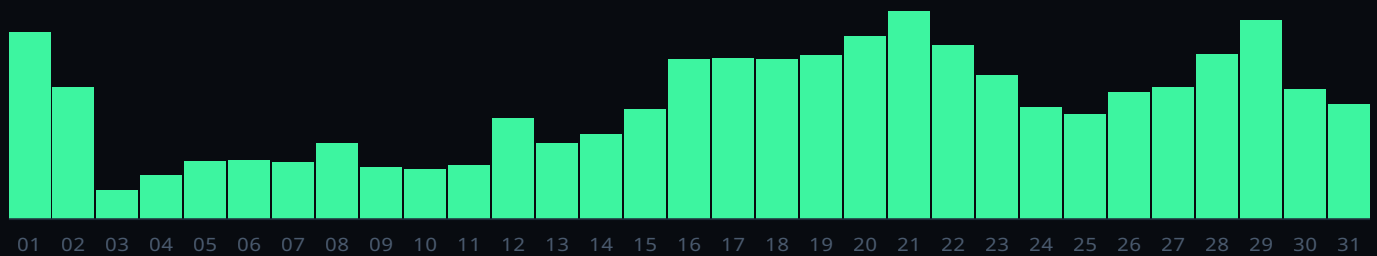
sumber: pemantauan keamanan terpusat – security operations center

6.053.217

PERISTIWA DIPROSES

Sepanjang Juli 2026, sensor SOC memproses peristiwa dari seluruh aset terpantau. Setelah penyaringan derau operasional (kegagalan layanan, rotasi log, status agen), tersisa **574.653 peristiwa bermakna** yang relevan bagi keamanan.

> Sebaran Peristiwa Harian



tanggal – juli 2026

> Penyaringan Akses Internet

59.365.749

PERMINTAAN WEB DITOLAK

Gerbang akses internet menolak permintaan yang melanggar kebijakan keamanan dan kepatutan sebelum mencapai pengguna. Penyaringan ini mencakup **80 unit kerja** dengan puncak **118.827 pengguna serentak** pada periode ini.

109.408

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

17.068

Pemblokiran otomatis alamat IP
oleh sistem pemantauan

18.252

Kecocokan dengan indikator
ancaman yang telah dikenal

Tingkat Keparahan & Klasifikasi

sebaran tingkat keparahan dan kategori peristiwa

> Sebaran Tingkat Keparahan

Kritis (13-15)		4.053
Tinggi (10-12)		260.463
Sedang (7-9)		310.137
Rendah / informasional (0-6)		5.478.564

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)		1.920.576
Kegagalan autentikasi		580.194
Deteksi kerentanan pada aset		268.926
Perubahan berkas sistem (FIM)		202.164
Web scanning (pemindaian layanan web)		109.220
Pemblokiran otomatis		66.606

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)		110.215
Kegagalan autentikasi SSH		45.118
Upaya akses directory index terlarang (Apache)		40.114
Kegagalan autentikasi SASL (Postfix)		37.834
Web scanning dari IP non-trusted		26.750
AAA RADIUS: BRUTE FORCE - 8+ login gagal dalam 120 detik untuk user [akun]		21.035
Brute force ke perangkat jaringan (8+ login gagal dalam 120 detik) dari [alamat internal]		20.836
IP diblokir otomatis oleh sistem		17.068

> Aset dengan Peristiwa Terbanyak

Portal dan aplikasi Perangkat Daerah		2.282.955
Layanan email dan kolaborasi		1.255.621
Sistem pengawasan CCTV		747.928
Server aplikasi internal		690.792
Layanan autentikasi jaringan		582.982

Sistem pemantauan dan audit		338.081
Portal CSIRT		62.577
Layanan otomasi dan pendukung		60.754

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.

BAGIAN 05

Sumber Serangan & Pola Sasaran

alamat ip sumber dan jalur yang diminta penyerang

> Alamat IP Sumber Serangan Terbanyak

ALAMAT IP	PERISTIWA
185.177.72....	23.635
125.166.34....	7.339
180.241.29....	6.562
180.241.31....	4.996
82.197.69....	4.582
130.195.213....	4.100
110.137.82....	3.836
129.212.216....	3.613
129.212.209....	3.368

> 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
168.144.142....	Scanning jalur umum	/wp-content/themes/alera/alpha.php /lx.php /jindex.php
103.59.160....	SQL injection · Scanning jalur umum	/index.action?... /solr/Beranda/select?... /plugins/editors/jckeditor/plugins/jtreelink...?...
20.226.81....	Scanning jalur umum	/sppxcanzbu.php
103.87.68....	Scanning jalur umum	/musrenbang/index.php?... /kutiim/administrator/index.php

172.81.132.***	Enumerasi endpoint API · Scanning jalur umum	/api/vendor/phpunit/phpunit/src/Util/PHP/tdns... /public/plugins/jquery-file-upload//bower.json /api/vendor/phpunit/phpunit/src/Util/PHP/eval...
193.148.56.***	Enumerasi halaman login	/wp-login.php
175.111.91.***	Scanning jalur umum	/kontak/feed /advisory/rss /beranda/feed
74.248.17.***	Scanning jalur umum	/solo1.php //goods.php

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	701.087
Remote Services	226.482
Stored Data Manipulation	148.116
Password Guessing	132.201
Exploit Public-Facing Application	68.330
Sudo and Sudo Caching	53.242
SSH	45.490
Vulnerability Scanning	42.609

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

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.

18.252

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		17.463
Payload delivery		648
Other		141

Keamanan Endpoint (EDR)

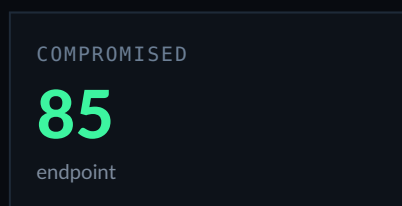
sumber: pemantauan keamanan perangkat kerja

85

ENDPOINT DIPANTAU

Lapisan ini melengkapi pemantauan terpusat: komputer kerja dan server diawasi langsung pada perangkatnya. Pada periode ini terdeteksi **99 temuan** dari **24 jenis ancaman** yang berbeda — seluruhnya terdeteksi dan tertahan pada tahap awal.

> Status Risiko Endpoint



> Keluarga Ancaman Terdeteksi

Trojan		6
Cryptojacking / mining virus		4
Hacktool		3
Malicious download		2

Tunneling / evasion		2
Phishing		2
Threat indicator match		1
Worm		1
Malicious domain access		1
Exploitation (eksploitasi kerentanan)		1
Exploitation		1

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

> Tahapan Ancaman

C&C (komunikasi command & control)		85
Impact (dampak pada sistem)		7
Propagation (penyebaran lateral)		5
Exploitation (upaya eksploitasi)		1

> Kelemahan Konfigurasi

Improper configuration (konfigurasi tidak aman)		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

BAGIAN 10

Insiden & Layanan Aduan

> Insiden yang Ditangani

Tidak ada insiden yang ditangani pada periode ini.

> Tiket Pelaporan

NOMOR TIKET	KATEGORI	TINGKAT	STATUS	RINGKASAN
CSIRT-2026-00002	Lainnya	RENDAH	Ditutup	Laporan Lain-lain diterima 16 Jul 2026
CSIRT-2026-00003	Kebocoran / Pencurian Data	TINGGI	Selesai	Laporan Kebocoran / Pencurian Data diterima 30 Jul 2026

Total 4 pembaruan tiket dicatat pada periode ini. Kanal pelaporan: csirt.kutaitimurkab.go.id/lapor

BAGIAN 11

Kerentanan yang Diperingatkan

advisory yang diterbitkan pada periode ini

CVE	PRODUK	CVSS	TINGKAT	KEV
CVE-2026-63030	WordPress Core Berujung Eksekusi...	9,8	CRITICAL	YA
CVE-2026-8451	Citrix NetScaler ADC dan Gateway	8,8	HIGH	—
CVE-2026-45659	Microsoft SharePoint Server	8,8	HIGH	YA
CVE-2026-60137	WordPress Core	5,9	MEDIUM	YA

Kolom **KEV** menandai kerentanan

yang tercatat pada katalog Known Exploited Vulnerabilities CISA — sudah terkonfirmasi dieksploitasi di dunia nyata: **3 dari 4** advisory periode ini. Naskah lengkap setiap advisory tersedia di csirt.kutaitimurkab.go.id/posts.

BAGIAN 12

Indikator, Berita & Edukasi

> Indikator Ancaman (IoC) yang Dibagikan

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

23 Jul Dua Celah WordPress Dirantai Jadi Eksekusi Kode: Ancaman Nyata bagi Situs Perangkat Daerah

Kegiatan & Layanan Publik

Tidak ada kegiatan yang tercatat pada periode ini.

> Layanan Publik

KUNJUNGAN PORTAL 2.314 csirt.kutaitimurkab.go.id	DOKUMEN PANDUAN 9 tersedia untuk publik	PELAPOR DIAPRESIASI 1 Hall of Fame VDP
---	--	---

Anjuran Tindak Lanjut

disusun dari temuan periode ini, bukan anjuran umum

Setiap anjuran di bawah diturunkan langsung dari temuan Juli 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: 193.167 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: 37.834 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: 109.408 upaya serangan aplikasi web

04 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: 18.252 kecocokan indikator ancaman

05 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.

06 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 kepatutan.
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.
- › **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/07/2026