



PEMERINTAH KABUPATEN KUTAI TIMUR

KUTIM-CSIRT

COMPUTER SECURITY INCIDENT RESPONSE TEAM

```
$ csirt report --monthly --period=2026-06 --tlp=clear
```

LAPORAN BULANAN PUBLIK

Hasil Monitoring Keamanan Siber

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

JUNI 2026

PERIODE 1 – 30 JUNI 2026

25

ASET MELAPOR

63

PERANGKAT DITANGANI

32.844

PERISTIWA BERMAKNA

11

ADVISORY TERBIT

TLP: CLEAR

KUTIM-CSIRT/LAPBUL/06/2026

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 Diperingatkan
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 Juni 2026

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

25

aset melapor ke pemantauan terpusat pada periode ini

63

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

1

kejadian periode sebelumnya,
dituntaskan bulan ini

ADVISORY DITERBITKAN

11

peringatan kerentanan

BERITA KEAMANAN

0

artikel edukasi publik

INDIKATOR (IOC) BARU

0

dibagikan ke OPD

Catatan: satu laporan yang naik menjadi insiden tetap dihitung pada kedua baris — tiket dan insiden. Pada periode ini tiket yang dituntaskan dan insiden yang ditangani merujuk pada **kasus yang sama**, bukan dua kejadian berbeda.

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

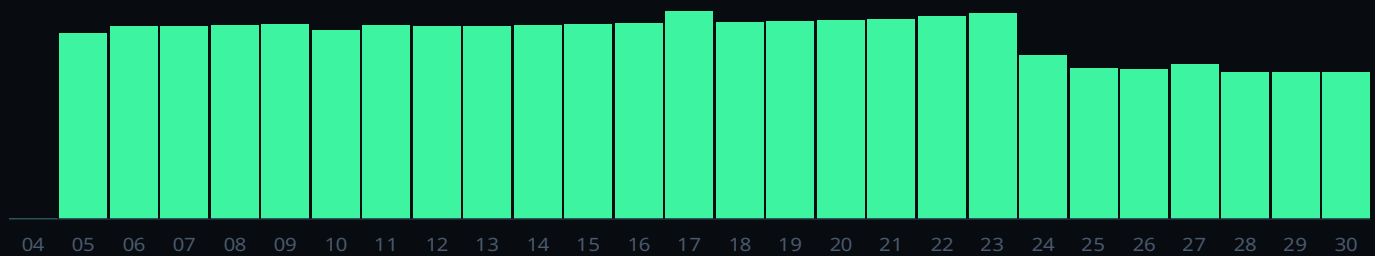
sumber: pemantauan keamanan terpusat – security operations center

9.993.522

PERISTIWA DIPROSES

Sepanjang Juni 2026, sensor SOC memproses peristiwa dari seluruh aset terpantau. Setelah penyaringan derau operasional (kegagalan layanan, rotasi log, status agen), tersisa **32.844 peristiwa bermakna** yang relevan bagi keamanan.

> Sebaran Peristiwa Harian



tanggal – juni 2026

Cakupan data pemantauan: tanggal 4–30 (27 dari 30 hari). Selisih disebabkan rentang arsip log yang tersedia, bukan terhentinya pemantauan.

> Penyaringan Akses Internet

51.972.895

PERMINTAAN WEB DITOLAK

Gerbang akses internet menolak permintaan yang melanggar kebijakan keamanan dan kepatutan sebelum mencapai pengguna. Penyaringan ini mencakup **77 unit kerja** dengan puncak **112.768 pengguna serentak** pada periode ini.

3.944

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

2.912

Pemblokiran otomatis alamat IP
oleh sistem pemantauan

1.511

Kecocokan dengan indikator
ancaman yang telah dikenal

Tingkat Keparahan & Klasifikasi

sebaran tingkat keparahan dan kategori peristiwa

> Sebaran Tingkat Keparahan

Kritis (13-15)		79
Tinggi (10-12)		12.380
Sedang (7-9)		20.385
Rendah / informasional (0-6)		9.960.678

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

Spam dan penyalahgunaan email		297.734
Serangan terhadap aplikasi (attack)		139.519
Kegagalan autentikasi		69.111
Perubahan berkas sistem (FIM)		8.766
Penilaian konfigurasi keamanan		6.104
Pemblokiran otomatis		4.579
Pemeriksaan rootkit		3.639
Web scanning (pemindaian layanan web)		2.292
Kecocokan indikator ancaman		1.699

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

Jenis Peristiwa & Aset Terdampak

> Jenis Peristiwa Keamanan Terbanyak

Kegagalan autentikasi sistem (syslog)		51.975
Kegagalan autentikasi SASL (Postfix)		17.125
IP diblokir otomatis oleh sistem		2.912
Blokir IP dicabut kembali		1.667
Upaya SQL injection		1.603
Serangan web dengan respons HTTP 200		844
Kecocokan indikator ancaman — Network activity		716
Upaya mail relay tidak sah (ditolak)		499

> Aset dengan Peristiwa Terbanyak

Layanan email dan kolaborasi		9.775.942
Portal dan aplikasi Perangkat Daerah		204.613
Portal CSIRT		9.328
Infrastruktur pusat operasi keamanan		1.395
Layanan tanda tangan elektronik		1.374
Perangkat infrastruktur jaringan		870

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
204.76.203.***	896
45.148.10.***	726
103.168.67.***	421
45.198.224.***	387
172.94.9.***	182
172.81.132.***	168
77.90.185.***	108
203.154.14.***	105

> Contoh Pola Sasaran

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

ALAMAT IP	TEKNIK	CONTOH JALUR DIMINTA
175.111.91.***	Scanning jalur umum	/csirt/feeds /kontak/rss /csirt/feed
34.143.149.***	Pencarian berkas backup	/env.bak
34.182.149.***	Enumerasi endpoint API · Pencarian berkas konfigurasi & kredensial	/credentials /actuator/sessions /api/aws.json
141.98.11.***	Scanning jalur umum	/123
50.114.43.***	Scanning jalur umum	/kontak/rss
202.155.19.***	HTTP response splitting · Pencarian berkas konfigurasi & kredensial	/configuration/.env /Set-Cookie:injected=true
103.121.97.***	Enumerasi halaman login · Path traversal	/webservice/get_usedspace.php?... /zentao/user-login.html /index.php?...
146.70.40.***	Enumerasi WordPress	//media/wp-includes/wlwmanifest.xml

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.

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
Email Collection	297.734
Valid Accounts	279.020
Remote Services	105.155
Sudo and Sudo Caching	29.151
Stored Data Manipulation	6.721
Exploit Public-Facing Application	1.891
File Deletion	1.178
Data Destruction	1.178

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.

1.511

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	1.200
Payload delivery	292
Other	19

Keamanan Endpoint (EDR)

sumber: pemantauan keamanan perangkat kerja

63

ENDPOINT DIPANTAU

Lapisan ini melengkapi pemantauan terpusat: komputer kerja dan server diawasi langsung pada perangkatnya. Pada periode ini terdeteksi **70 temuan** dari **24 jenis ancaman** yang berbeda — seluruhnya terdeteksi dan tertahan pada tahap awal.

> Status Risiko Endpoint

COMPROMISED

58

endpoint

HIGH RISK

5

endpoint

> Keluarga Ancaman Terdeteksi

Trojan		7
Cryptojacking / mining virus		4
Tunneling / evasion		2
Phishing		2
Hacktool		2
Backdoor		2
Threat indicator match		1
Worm		1
Malware lainnya		1
Exploitation (eksploitasi kerentanan)		1
Malicious domain access		1

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

> Tahapan Ancaman

C&C (komunikasi command & control)		46
Impact (dampak pada sistem)		9
Weakness (kelemahan terdeteksi)		6
Propagation (penyebaran lateral)		3

> Kelemahan Konfigurasi

Improper configuration (konfigurasi tidak aman)

6

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

Perbandingan antarbulan belum tersedia — arsip pemantauan untuk bulan-bulan sebelumnya belum terkumpul. Bagian ini akan terisi pada laporan periode berikutnya.

BAGIAN 10

Insiden & Layanan Aduan

> Insiden yang Ditangani

TANGGAL	JENIS	TINGKAT	STATUS	KETERANGAN
31 Mei → 24 Jun	Lainnya	KRITIS	Selesai	Kerentanan Eksekusi Kode Jarak Jauh pada Portal SIGAP Dinas Koperasi

> Pembelajaran dari Insiden

Kerentanan Eksekusi Kode Jarak Jauh pada Portal SIGAP Dinas Koperasi

Insiden ini menegaskan dua hal penting: pertama, pembaruan berkala pada seluruh komponen aplikasi (termasuk pustaka dan kerangka kerja pihak ketiga) adalah keharusan, karena celah kritis sering muncul dari komponen yang tertinggal versi. Kedua, kolaborasi dengan peneliti keamanan yang beriktikad baik sangat berharga — Perangkat Daerah diimbau mendukung mekanisme pengungkapan kerentanan yang aman dan berkoordinasi dengan KUTIM-CSIRT untuk penguatan sistem.

> Tiket Pelaporan

Tidak ada tiket baru yang masuk pada periode ini.

Total 3 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-2026-10520	Ivanti Sentry	10,0	CRITICAL	YA
CVE-2026-48908	SP Page Builder	10,0	CRITICAL	YA
CVE-2026-34910	Ubiquiti UniFi OS	10,0	CRITICAL	YA
CVE-2026-48558	SimpleHelp	10,0	CRITICAL	YA
CVE-2026-48907	Ekstensi Joomla Content Editor	9,8	CRITICAL	YA
CVE-2026-20253	Splunk Enterprise	9,8	CRITICAL	YA
CVE-2026-13028	Google Chrome	9,6	CRITICAL	—
CVE-2026-50751	Check Point Security Gateway	9,3	CRITICAL	YA
CVE-2026-11645	Google Chrome	8,8	HIGH	YA
CVE-2026-20230	Cisco Unified CM	8,6	HIGH	YA
CVE-2026-55957	Apache Tomcat	7,3	HIGH	—

Kolom **KEV** menandai kerentanan

yang tercatat pada katalog Known Exploited Vulnerabilities CISA — sudah terkonfirmasi dieksploitasi di dunia nyata: **9 dari 11** advisory periode ini. Naskah lengkap setiap advisory tersedia di csirt.kutaitimurkab.go.id/posts.

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

Tidak ada artikel berita keamanan yang terbit pada periode ini.

Kegiatan & Layanan Publik

Tidak ada kegiatan yang tercatat pada periode ini.

> Layanan Publik

KUNJUNGAN PORTAL 2.886 csirt.kutaitimurkab.go.id	DOKUMEN PANDUAN 9 tersedia untuk publik	PELAPOR DIAPRESIASI 0 Hall of Fame VDP
--	---	--

Anjuran Tindak Lanjut

disusun dari temuan periode ini, bukan anjuran umum

Setiap anjuran di bawah diturunkan langsung dari temuan Juni 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: 69.100 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: 17.624 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: 3.944 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: 1.511 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: 9 dari 11 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 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. Perbedaan 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/06/2026