



PEMERINTAH KABUPATEN KUTAI TIMUR

KUTIM-CSIRT

COMPUTER SECURITY INCIDENT RESPONSE TEAM

```
$ csirt report --monthly --period=2026-08 --tlp=clear
```

LAPORAN BULANAN PUBLIK

Hasil Monitoring Keamanan Siber

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

AGUSTUS 2026

PERIODE 1 – 31 AGUSTUS 2026

118

ASET MELAPOR

78

PERANGKAT DITANGANI

767.430

PERISTIWA BERMAKNA

11

ADVISORY TERBIT

TLP: CLEAR

KUTIM-CSIRT/LAPBUL/08/2026

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 – 31 Agustus 2026

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

78

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

3

termasuk sisa periode sebelumnya

INSIDEN DITANGANI

3

kejadian baru pada periode ini

ADVISORY DITERBITKAN

11

peringatan kerentanan

BERITA KEAMANAN

4

artikel edukasi publik

INDIKATOR (IOC) BARU

45

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

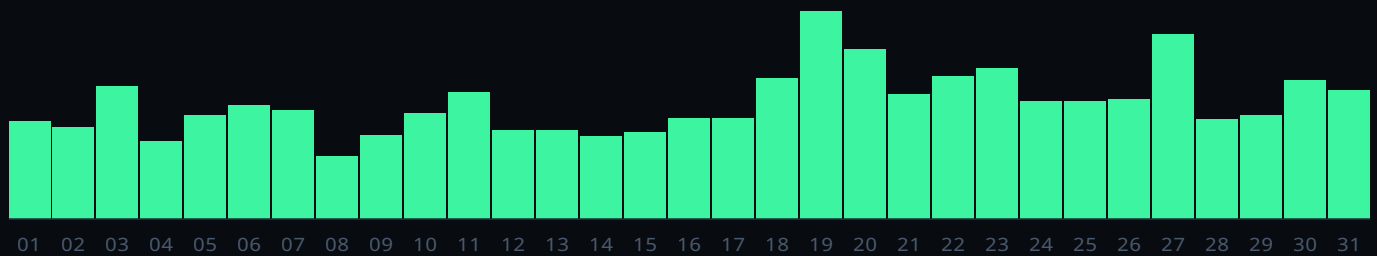
sumber: pemantauan keamanan terpusat – security operations center

8.540.271

PERISTIWA DIPROSES

Sepanjang Agustus 2026, sensor SOC memproses peristiwa dari seluruh aset terpantau. Setelah penyaringan derau operasional (kegagalan layanan, rotasi log, status agen), tersisa **767.430 peristiwa bermakna** yang relevan bagi keamanan.

> Sebaran Peristiwa Harian



tanggal – agustus 2026

> Penyaringan Akses Internet

54.420.617

PERMINTAAN WEB DITOLAK

Gerbang akses internet menolak permintaan yang melanggar kebijakan keamanan dan kepatutan sebelum mencapai pengguna. Penyaringan ini mencakup **85 unit kerja** dengan puncak **116.624 pengguna serentak** pada periode ini.

> Penyaringan di Perimeter Jaringan

52.754

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**.

133.720

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

40.866

Pemblokiran otomatis alamat IP
oleh sistem pemantauan

35.553

Kecocokan dengan indikator
ancaman yang telah dikenal

Tingkat Keparahan & Klasifikasi

sebaran tingkat keparahan dan kategori peristiwa

> Sebaran Tingkat Keparahan

Kritis (13-15)		16.550
Tinggi (10-12)		320.790
Sedang (7-9)		430.090
Rendah / informasional (0-6)		7.772.841

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)		1.909.809
Kegagalan autentikasi		1.544.688
Deteksi kerentanan pada aset		630.310
Perubahan berkas sistem (FIM)		282.923
Web scanning (pemindaian layanan web)		129.388
Pemblokiran otomatis		83.846

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)		626.795
Kegagalan autentikasi SASL (Postfix)		237.105
Permintaan berbahaya ditolak WAF		73.709
Kegagalan autentikasi SSH		53.352
IP diblokir otomatis oleh sistem		40.866
Web scanning dari IP non-trusted		26.652
Kecocokan indikator ancaman — Network activity		24.426
Common web attack (serangan web umum)		16.039

> Aset dengan Peristiwa Terbanyak

Portal dan aplikasi Perangkat Daerah		4.012.533
Layanan email dan kolaborasi		1.905.390
Server aplikasi internal		823.204
Layanan autentikasi jaringan		706.404
Sistem pengawasan CCTV		376.846
Sistem pemantauan dan audit		324.054
Layanan otomasi dan pendukung		264.778
Infrastruktur pusat operasi keamanan		70.557

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.***	46.842
213.176.26.***	14.189
185.177.72.***	12.860
129.212.209.***	8.931
109.123.239.***	7.656
129.212.216.***	6.589
103.59.161.***	6.577
172.81.132.***	5.863

> 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
45.148.10.***	Pencarian berkas backup · Pencarian berkas konfigurasi & kredensial	/config.php.bak /form/.env /private/.env
109.123.239.***	Enumerasi halaman login · Path traversal	/fuel/pages/select/?... /session/language?... /plugins/editors/jckeditor/plugins/jtreelink...?...
194.233.72.***	Scanning jalur umum	/members/?... /member-directory/?... /users/?...
20.100.186.***	Scanning jalur umum	/abc.php /css.php /hplfuncs.php
80.76.53.***	Scanning jalur umum	/?... /cgi-bin/account_mgr.cgi?... /cgi-bin/account_mgr.cgi?...
93.123.109.***	Enumerasi halaman login · Scanning jalur umum	/cms/ /blog/ /cms/wp-login.php
20.104.18.***	Enumerasi WordPress · Scanning jalur umum	/wp-content/plugins/wp-sec/xleet.php /wp-admin/about.php /pki-validationk.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	1.122.428
Remote Services	422.171
Password Guessing	164.109
Stored Data Manipulation	116.816
File and Directory Discovery	91.009
Sudo and Sudo Caching	67.691
SSH	52.915
Email Collection	48.785

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.

35.553

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

35.553

BAGIAN 08

Keamanan Endpoint (EDR)

sumber: pemantauan keamanan perangkat kerja

78

ENDPOINT DIPANTAU

Lapisan ini melengkapi pemantauan terpusat: komputer kerja dan server diawasi langsung pada perangkatnya. Pada periode ini terdeteksi **82 temuan** dari **16 jenis ancaman** yang berbeda — seluruhnya terdeteksi dan tertahan pada tahap awal.

> Status Risiko Endpoint

COMPROMISED

78

endpoint

> Keluarga Ancaman Terdeteksi

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

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

> Tahapan Ancaman

C&C (komunikasi command & control)		69
Impact (dampak pada sistem)		10

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

BAGIAN 10

Insiden & Layanan Aduan

> Insiden yang Ditangani

TANGGAL	JENIS	TINGKAT	STATUS	KETERANGAN
07 Agu	Penyisipan Konten Judi (Judol)	TINGGI	Dalam Penanganan	Penyalahgunaan Subdomain Resmi untuk Situs Perjudian Online
07 Agu	Penyisipan Konten Judi (Judol)	TINGGI	Dalam Penanganan	Pengambilalihan Akun Pengelola dan Penyisipan Situs Perjudian pada...
18 Agu	Web Defacement	TINGGI	Dalam Penanganan	Perusakan Tampilan Situs dan Penanaman Akses Ilegal pada Situs RSUD...

> Pembelajaran dari Insiden

Penyalahgunaan Subdomain Resmi untuk Situs Perjudian Online

Perangkat Daerah diimbau mendata ulang seluruh subdomain yang pernah diminta dan memastikan setiap subdomain aktif benar-benar masih digunakan serta diawasi. Subdomain resmi tidak boleh diarahkan ke layanan pihak ketiga tanpa pengawasan, dan yang sudah tidak terpakai sebaiknya dinonaktifkan. Ajukan permohonan penonaktifan atau laporkan kejanggalan ke KUTIM-CSIRT melalui kanal pelaporan resmi.

Pengambilalihan Akun Pengelola dan Penyisipan Situs Perjudian pada Layanan SIKAMU

Insiden ini menegaskan bahwa rekomendasi pascainsiden wajib dituntaskan — terutama penggantian menyeluruh seluruh kredensial, karena sandi yang pernah bocor akan terus dipakai kembali oleh penyerang. Perangkat Daerah diimbau: mengganti kredensial secara berkala dan segera setelah insiden, mengaktifkan verifikasi dua langkah pada seluruh akun pengelola, tidak berbagi satu akun untuk banyak orang, memastikan tidak ada berkas arsip atau cadangan aplikasi yang dapat diunduh bebas dari halaman situs, serta menonaktifkan permanen layanan yang sudah tidak digunakan. Laporkan kejanggalan sedini mungkin ke KUTIM-CSIRT.

Perusakan Tampilan Situs dan Penanaman Akses Ilegal pada Situs RSUD Kudungga

Pemulihan situs setelah insiden hanya boleh dilakukan dari salinan yang sudah dipastikan bersih, atau dari pemasangan ulang yang bersih dengan memindahkan isi terpilih. Memulihkan dari cadangan yang dibuat setelah penyusupan hanya akan menghidupkan kembali masalahnya. Perangkat Daerah juga diimbau memastikan tidak ada berkas arsip atau cadangan aplikasi yang dapat diunduh bebas dari halaman situs, memperbarui aplikasi beserta seluruh komponen tambahannya secara berkala, memasang komponen hanya melalui prosedur dan pihak yang berwenang, mengaktifkan pemantauan perubahan berkas pada folder situs, serta menyimpan...

> Tiket Pelaporan

NOMOR TIKET	KATEGORI	TINGKAT	STATUS	RINGKASAN
CSIRT-2026-00004	Kerentanan Keamanan	KRITIS	Selesai	Laporan Kerentanan Keamanan diterima 01 Agu 2026, selesai 02 Agu
CSIRT-2026-00005	Kerentanan Keamanan	SEDANG	Selesai	Laporan Kerentanan Keamanan diterima 02 Agu 2026, selesai 03 Agu

Total 17 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-2026-69836	Microsoft Entra ID	10,0	CRITICAL	—
CVE-2026-72898	Metabase	10,0	CRITICAL	YA
CVE-2026-59310	VMware vCenter	9,8	CRITICAL	YA
CVE-2026-33824	Layanan IKE Windows Berujung Ekse...	9,8	CRITICAL	YA
CVE-2026-8452	Citrix NetScaler ADC dan Gateway	9,8	CRITICAL	YA
CVE-2026-55040	Microsoft SharePoint	9,1	CRITICAL	YA
CVE-2026-73570	Zimbra Collaboration	8,9	HIGH	YA
CVE-2026-75149	Notebook Marimo	8,7	HIGH	—
CVE-2026-20349	Cisco Secure Firewall ASA dan FTD	8,6	HIGH	YA
CVE-2026-34486	Apache Tomcat	7,5	HIGH	YA
CVE-2026-68820	Windows AFD WinSock	7,0	HIGH	YA

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

Judol		15
Eksplotasi		9
Pemindaian		9
Malware		7
Defacement		4
C2		1

> Berita & Edukasi Keamanan

11 Agu Waspada Ransomware Gunra: Sektor Pemerintahan Termasuk Sasaran Utama

15 Agu Menambal Berdasarkan Risiko, Bukan Sekadar Skor: Pelajaran dari Arah Baru Manajemen Kerentanan

26 Agu Ratusan Mail Server Zimbra Dikompromikan Lewat Celah SNMP yang Belum Ditambal

28 Agu Edge Device Kian Jadi Sasaran: Catatan dari Gelombang Kerentanan Agustus 2026

BAGIAN 13

Kegiatan & Layanan Publik

\$ 27 Agu 2026

Forum Analisis dan Berbagi Informasi Gov-CSIRT Tahun 2026

Aula Mayjen TNI (Purn) dr. Roebiono Kertopati, BSSN, Sawangan, Depok, Jawa Barat

\$ 27–28 Agu 2026

Kunjungan Kerja dan Permohonan Asistensi IKASANDI kepada BSSN

Badan Siber dan Sandi Negara (BSSN), Depok, Jawa Barat

> Layanan Publik

KUNJUNGAN PORTAL

900

csirt.kutaitimurkab.go.id

DOKUMEN PANDUAN

9

tersedia untuk publik

PELAPOR DIAPRESIASI

3

Hall of Fame VDP

BAGIAN 14

Anjuran Tindak Lanjut

disusun dari temuan periode ini, bukan anjuran umum

Setiap anjuran di bawah diturunkan langsung dari temuan Agustus 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: 917.252 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: 237.105 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: 133.720 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: 35.553 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 Tuntaskan penanganan insiden yang masih berjalan

Pemulihan layanan belum berarti akar masalah tertutup. Pastikan berkas asing, akun tidak dikenal, dan mekanisme akses tersembunyi sudah dibersihkan, lalu lakukan verifikasi ulang sebelum insiden dinyatakan selesai.

Dasar: 3 insiden berstatus Dalam Penanganan

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/08/2026