TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

September 02, 2026

TLP AMBER CISO
EXECUTIVE REPORT

El informe incluye: RIESGO, Ciberseguridad e Información Operacional.

Sobre este reporte

Este informe a pedido proporciona información de nivel ejecutivo sobre el estado de la ciberseguridad para su organización, incluidos los principales indicadores de seguridad y rendimiento.

RISK

Actual Risk	Accepted Risk	Confidence
Low	n/a	Low

Accepted & Actual Risk

Table of Comparison of Actual and Acceptable Risk From Current to Previous Month

	Current Month	Previous Month
Actual Risk	5	5
Accepted Risk	0	0

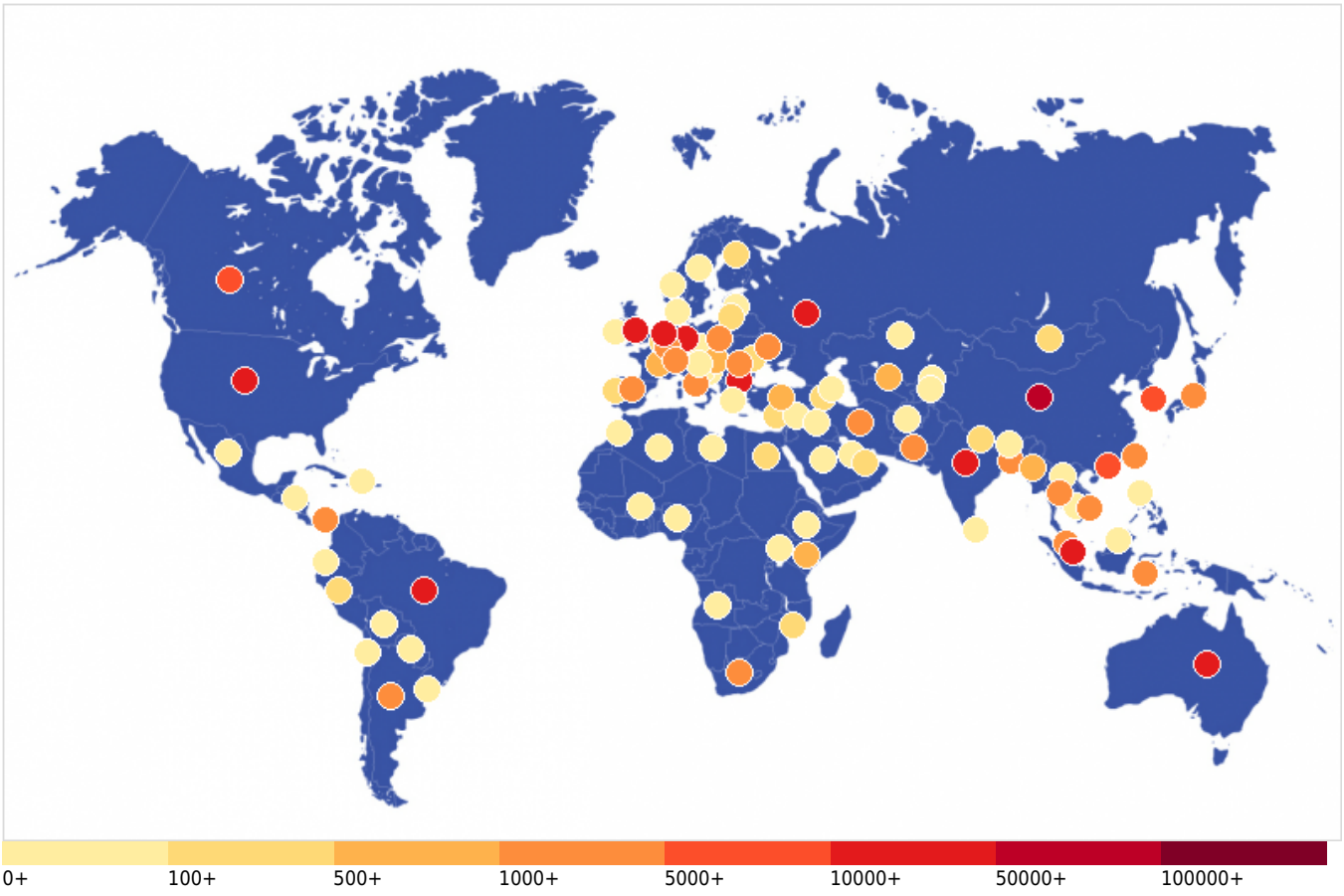
VULNERABILITY

Vulnerability Metric

12%

THREATS

Critical Attacks Per Country In Past Week



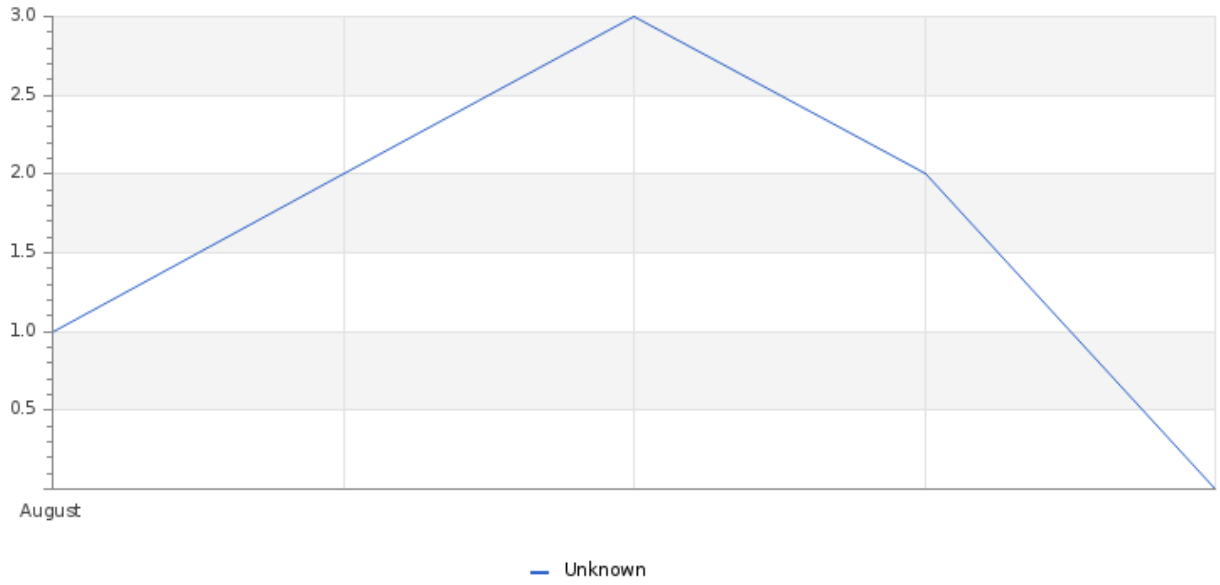
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

CISO EXECUTIVE REPORT

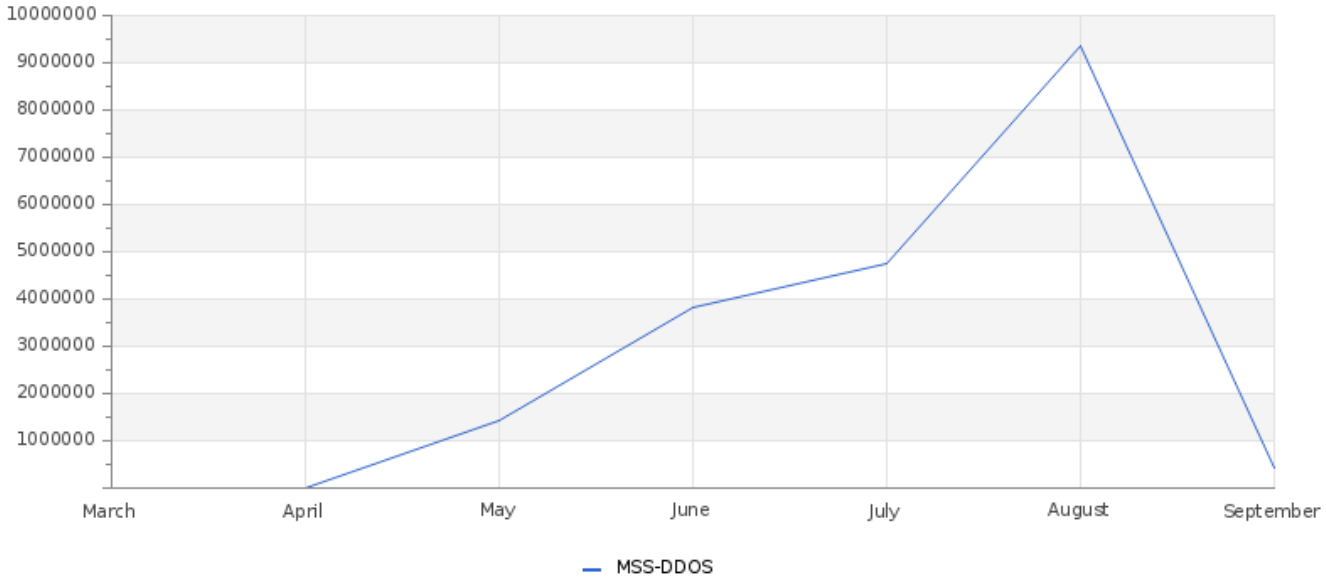
Organo Judicial 09/02/2026

Afghanistan - 84
Algeria - 97
Andorra - 591
Angola - 40
Argentina - 1,323
Armenia - 371
Australia - 34,516
Austria - 2
Azerbaijan - 34
Bahrain - 20
Bangladesh - 1,520
Belgium - 476
Bhutan - 7
Bolivia - 1
Bosnia and Herzegovina - 43
Brazil - 10,683
Brunei - 59
Bulgaria - 38,971
Burkina Faso - 41
Cambodia - 41
Canada - 8,121
Chile - 36
China - 88,501
Croatia - 2
Cyprus - 100
Czechia - 17
Denmark - 4
Dominican Republic - 8
Ecuador - 46
Egypt - 318
Ethiopia - 29
Finland - 303
France - 503
Georgia - 50
Germany - 20,384
Greece - 5
Honduras - 22
Hong Kong - 6,770
Hungary - 637
India - 12,344
Indonesia - 4,234
Iran - 4,924
Iraq - 43
Ireland - 20
Italy - 1,218
Japan - 2,544
Kazakhstan - 18
Kenya - 509
Kyrgyzstan - 65
Laos - 2
Latvia - 2
Libya - 1
Liechtenstein - 2
Lithuania - 152
Luxembourg - 2,900
Malaysia - 1,537
Mauritius - 202
Mexico - 14
Moldova - 173
Mongolia - 419
Morocco - 2
Mozambique - 157
Myanmar - 533
Nepal - 128
Netherlands - 13,093
New Zealand - 10
Nigeria - 18
Norway - 3
Pakistan - 1,747
Panama - 1,294
Paraguay - 4
Peru - 408
Philippines - 8
Poland - 1,495
Portugal - 444
Qatar - 2
Romania - 2,320
Russia - 10,256
Saint Kitts and Nevis - 1,176
Saudi Arabia - 4
Seychelles - 978
Singapore - 17,397
Slovenia - 47
South Africa - 3,566
South Korea - 6,325
Spain - 1,348
Sri Lanka - 26
Sweden - 38
Switzerland - 3,386
Taiwan - 3,428
Tajikistan - 4
Thailand - 1,127
Turkey - 915
Uganda - 97
Ukraine - 2,914
United Arab Emirates - 476
United Kingdom - 23,631
United States - 47,190
Uruguay - 1
Uzbekistan - 962
Vietnam - 1,849

Total Number of Successful MFA authentications per application

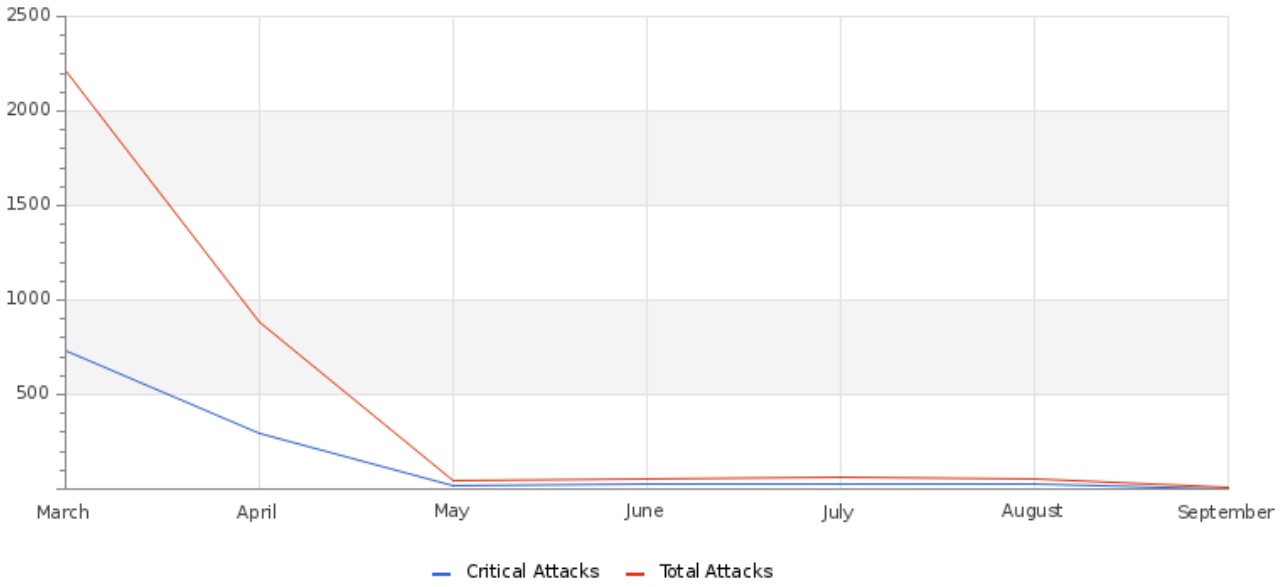


Total Attacks Successfully Blocked Per Service



LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Attacks Successfully Blocked by Severity



CISO EXECUTIVE REPORT

Organo Judicial 09/02/2026

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
Oficina del Sistema Penal Acusatorio de La Chorrera - Plaza Milenio	Ping v2	MSS-CSM-OJ	Down		3,209	2026-08-17 16:12:44	2026-09-02 09:00:29
Juzgado Municipal de Embera	Ping v2	MSS-CSM-OJ	Down		3,208	2026-08-17 16:12:44	2026-09-02 09:00:29
Juzgado Municipal de Ninez y Adolescencia - UTINA	Ping v2	MSS-CSM-OJ	Down		3,208	2026-08-17 16:12:44	2026-09-02 09:00:29
Juzgado Municipal de San Lorenzo	Ping v2	MSS-CSM-OJ	Down		3,208	2026-08-17 16:12:44	2026-09-02 09:00:29
Juzgado Municipal de Taboga	Ping v2	MSS-CSM-OJ	Down		3,208	2026-08-17 16:12:44	2026-09-02 09:00:29
Juzgado Municipal de Besiko	Ping v2	MSS-CSM-OJ	Down		3,208	2026-08-17 16:12:44	2026-09-02 09:00:28
Juzgado Municipal de Kankintu	Ping v2	MSS-CSM-OJ	Down		3,208	2026-08-17 16:12:44	2026-09-02 09:00:28
Juzgado Municipal de Muna	Ping v2	MSS-CSM-OJ	Down		3,208	2026-08-17 16:12:44	2026-09-02 09:00:28
Edificio 210 - Ancon	Ping v2	MSS-CSM-OJ	Down		3,207	2026-08-17 16:12:44	2026-09-02 09:00:29
Juzgado Municipal Civil de Santiago	Ping v2	MSS-CSM-OJ	Down		3,207	2026-08-17 16:12:44	2026-09-02 09:00:29
Juzgado Municipal de Chagres	Ping v2	MSS-CSM-OJ	Down		3,207	2026-08-17 16:12:44	2026-09-02 09:00:29
Juzgado Municipal de Tole	Ping v2	MSS-CSM-OJ	Down		3,207	2026-08-17 16:12:44	2026-09-02 09:00:29
Oficina del Sistema Penal Acusatorio de Guna Yala	Ping v2	MSS-CSM-OJ	Down		3,207	2026-08-17 16:12:44	2026-09-02 09:00:28
Unidad Judicial Regional de Changuinola/SPA	Ping v2	MSS-CSM-OJ	Down		3,207	2026-08-17 16:12:44	2026-09-02 09:00:28
Juzgado Municipal de Alanje	Ping v2	MSS-CSM-OJ	Down		3,206	2026-08-17 16:12:44	2026-09-02 09:00:29

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	0	93,956	0	237,229	0

OPERATIONAL

Total Number of Cases

Open	0
Answered	245
Closed	6260

Notable Events

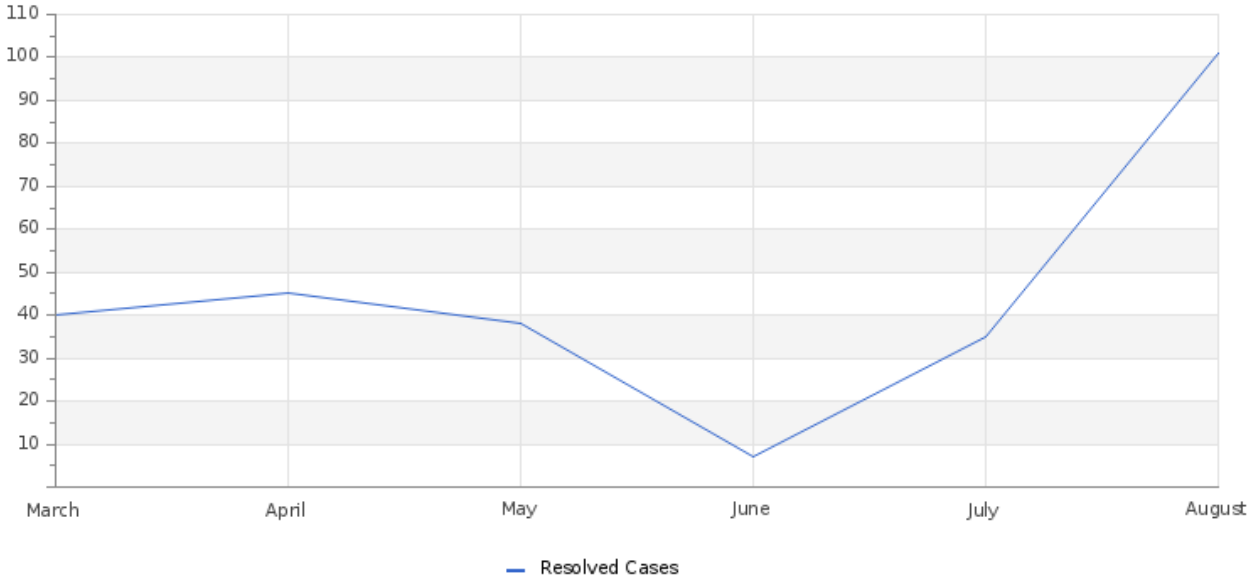
Notable Event Type	How Many #
High Persistency Detection	1
Change in Critical Perimeter Attacks	3
Monitoring for open ports	1

Total Remediation Cases by Stage

	Testing & Detection	Verification	Prioritization and Business Relevance	GLESEC Remediation Plan	Client Security Team	Client Remediation Team	Closed
SECURITY REMEDIATION AND INVESTIGATIONS	123	0	0	1	10	346	588
GOC: Security Incidents to investigate	172	0	0	0	2	155	359
Total	295	0	0	1	12	501	947

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Vulnerabilities Resolved Over Time



Vulnerabilities: Average Time to Resolve

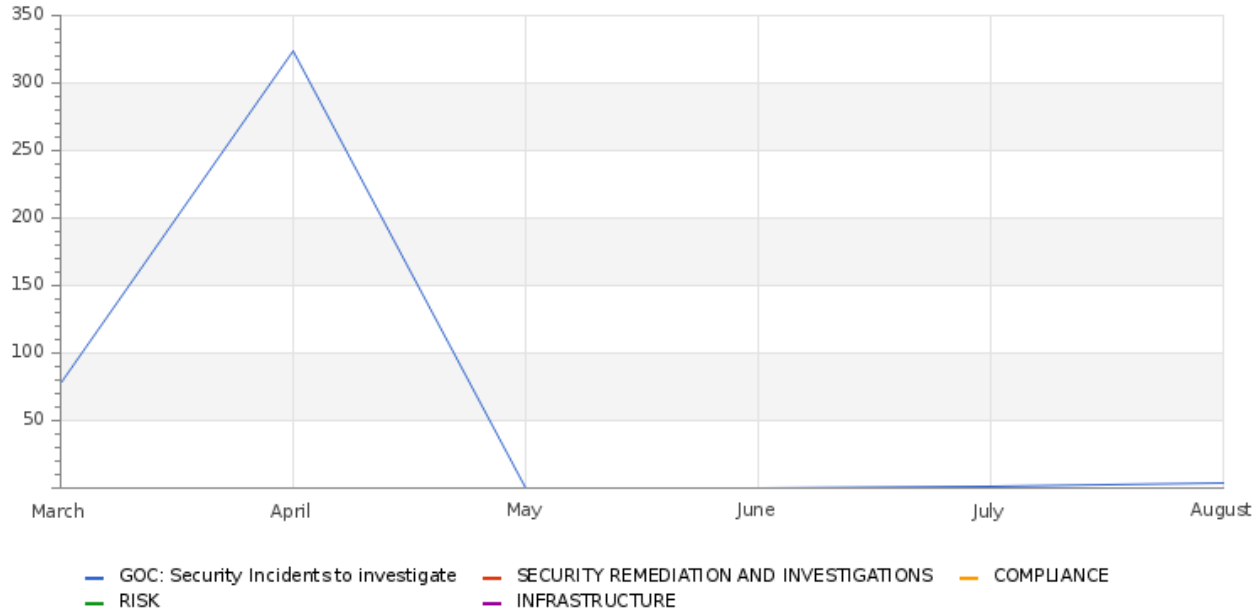
CISO EXECUTIVE REPORT

Organo Judicial 09/02/2026

Operational Metrics per Queue Over Time

Divisions	AVG. Time To Resolve, H	AVG. Time To Respond, H
GOC: Security Incidents to investigate	0	0
SECURITY REMEDIATION AND INVESTIGATIONS	0	0
COMPLIANCE	0	0
RISK	0	0
INFRASTRUCTURE	0	0

Monthly Average Time per Department



LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Threat Mitigation Procedure (ASM-TMP)

Average Time to Remediate

Stages	How Many #
Testing & Detection	0d 18h 24m 8s
Verification	1d 16h 33m 14s
Prioritization and Business Relevance	0d 0h 0m 0s
GLESEC Incidents Plan	8d 11h 55m 6s
Client Security Team	7d 13h 33m 49s
Client Incidents Team	0d 0h 0m 22s

Workload

Stages	How Many #
Testing & Detection	0
Verification	0
Prioritization and Business Relevance	0
GLESEC Incidents Plan	0
Client Security Team	3
Client Incidents Team	107
Closed	3786

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Vulnerability Handling Procedure (ASM-VP)

Average Time to Remediate

Stages	How Many #
Testing & Detection	0d 17h 58m 50s
Verification	4d 18h 37m 42s
Prioritization and Business Relevance	0d 0h 0m 0s
GLESEC Remediation Plan	8d 14h 3m 3s
Client Security Team	31d 15h 51m 50s
Client Remediation Team	0d 0h 0m 59s

Workload

Stages	How Many #
Testing & Detection	0
Verification	0
Prioritization and Business Relevance	0
GLESEC Remediation Plan	1
Client Security Team	1
Client Remediation Team	129
Closed	923

DAILYBRIEF

Active High-Severity Items

49

0

TLP:AMBER

CISO EXECUTIVE REPORT

Organo Judicial 09/02/2026

Executive Action Required

▲

10 items pending executive awareness or decision

Threat Relevance Score (TRS)

71

→ 0

Risk Score (RS)

77

▼ -1

External Threat Context

Threat Headline	Relevance
OTX [Mirage Kitten]: Switches to Node.js and JavaScript malware	Sector-relevant threat intelligence
OTX [BREEZE COMET]: Financially Motivated Threat Actor Targets Brazil	Threat actor activity detected

Ongoing cases

Case #	Service	Priority	Hours	Status
42479 Notable Event Alert: InstallFix Campaign Uses Fake Claude AI Installer Pages	MSS-INT	Medium	0	Answered
42589 Organo Judicial TEVR 051426	MSS-INT	High	0	Answered
42597 CASE – Validación de Exposición Linux Relacionada a CVE-2026-46300 / Fragnesia-ORGANO JUDICIAL	MSS-INT	High	0	Answered
43813 Notable Event Alert: New TrickMo Variant Device Take Over malware targeting Banking Fintech Wallet Auth apps	MSS-INT	High	0	Answered
43814 Notable Event Alert: RVTools Leveraged In Multiple Attack Campaigns	MSS-INT	High	0	Answered
43817 Notable Event Alert: Vibe Hacking Two AI-Augmented Campaigns Target Government and Financial Sectors in Latin America	MSS-INT	High	0	Answered
43820 Notable Event Alert: New Maoloa Ransomware Variant	MSS-INT	High	0	Answered

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

CISO EXECUTIVE REPORT

Organo Judicial 09/02/2026

Case #	Service	Priority	Hours	Status
43899 Notable Event Alert: Kimsukys Advanced Attack Techniques JSONPing Webex Spoofing and a New HttpSpy Variant	MSS-INT	High	0	Answered
43900 Notable Event Alert: Trellix Telemetry - Remus Stealer Infection Via Malicious Driver Update	MSS-INT	High	0	Answered
43901 Notable Event Alert: Attack Campaign Compromises Red Hat Cloud Services Packages	MSS-INT	High	0	Answered

Cybersecurity News

Title	Categories	Industries
FBI Probes Service Selling 153M+ Drivers Licenses	Cyber Attacks, Malware	Government, Healthcare, Banking and Financial, Hospitality, Transportation, Telecommunication
Breeze Comet Executes Hundreds of Fraudulent Transactions via Brazilian Payment Systems	Cyber Attacks, Malware	Government, Banking and Financial, Utilities
Hackers abuse Faronics Deploy admin tool to install ScreenConnect	Cyber Attacks	Government
Aesto Health says data breach affects over 9.5 million patients	Cyber Attacks, Compliance	Government, Healthcare, Banking and Financial, Education, Insurance
Nearly 22,000 Microsoft Exchange servers vulnerable to hijack attacks	Cyber Attacks, Vulnerabilities, Malware	Government, Legal Services
Massive Microsoft 365 outage causes auth issues, service failures	Cyber Attacks	Government

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP:AMBER

CISO EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500