TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

June 11, 2026

Organo Judicial 06/11/2026

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde "Marzo 2026" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, Amenazas, Activos, Cumplimiento, Validación de Ciberseguridad y Acceso.

SOBRE ESTE INFORME

El propósito de este documento es informar sobre el estado" de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

RISK

Actual Risk

5%

El nivel de riesgo actual se sigue manteniendo en el mismo rango ya establecido. Esta tendencia refleja una menor actividad de amenazas sobre los activos supervisados, lo que evidencia la efectividad de las medidas de control aplicadas. Sin embargo, es fundamental continuar con un monitoreo constante para garantizar la permanencia de este nivel y anticipar posibles incrementos futuros.

Accepted Risk

1%

El riesgo aceptado permanece en valores bajos que demuestran una gestión adecuada del riesgo residual. Este resultado confirma que la organización mantiene un enfoque prudente en la aceptación del riesgo, dando prioridad a las acciones de mitigación y control frente a eventuales escenarios de exposición.

Confidence

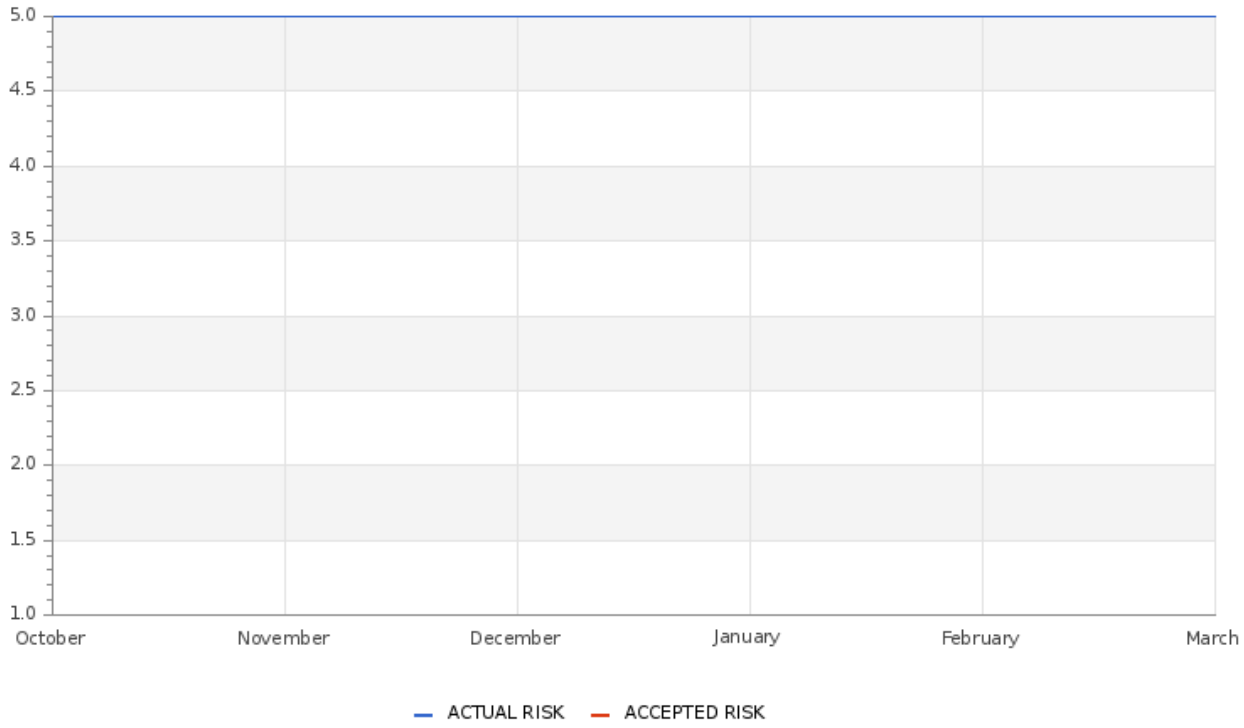
Low

La confiabilidad de la evaluación sigue siendo limitada debido a la insuficiencia y falta de consistencia de los datos disponibles. Se sugiere reforzar los procesos de recopilación y correlación de información para incrementar la precisión del análisis y proporcionar un soporte más sólido a la toma de decisiones en materia de seguridad.

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

Organo Judicial 06/11/2026

Accepted & Actual Risk



Riesgo Actual (5%) Durante el periodo analizado, el nivel de riesgo actual se mantuvo estable en comparación con el mes anterior. El valor del 5% se encuentra dentro de un rango bajo, indicando que la exposición a incidentes potenciales sigue controlada y que las medidas de seguridad implementadas continúan siendo efectivas. No obstante, es esencial mantener una vigilancia constante y una capacidad de respuesta adecuada para prevenir posibles incrementos futuros.

Riesgo Tolerado (1%) El riesgo tolerado se mantuvo en 1%, reflejando una gestión conservadora y consistente del riesgo residual. Este comportamiento demuestra la correcta aplicación de controles preventivos y la priorización de acciones de mitigación frente a posibles exposiciones, manteniendo el nivel de riesgo dentro de parámetros aceptables.

Organo Judicial 06/11/2026

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

	Current Month	Previous Month
Actual Risk	5	5
Accepted Risk	1	1

Nivel Actual de Riesgo (5%):
Durante este mes, el porcentaje de riesgo detectado en tiempo real se mantuvo en 5%, igual que el mes anterior. Esto indica que la exposición frente a amenazas activas se ha estabilizado, manteniendo la postura de seguridad sin incrementos en el nivel de riesgo. Aun así, es fundamental continuar con el monitoreo constante y la aplicación de controles adecuados para evitar posibles variaciones que puedan afectar la seguridad de la organización.

Riesgo Permitido (1%): La organización mantiene un umbral de riesgo aceptable de 1%, sin cambios respecto al periodo anterior. Este valor refleja un enfoque altamente conservador en la gestión del riesgo, priorizando la mitigación y el control continuo para mantener el nivel de riesgo dentro de los parámetros definidos.

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	5.13.46.200.dialup.psinetpa.net	0
Current	20	

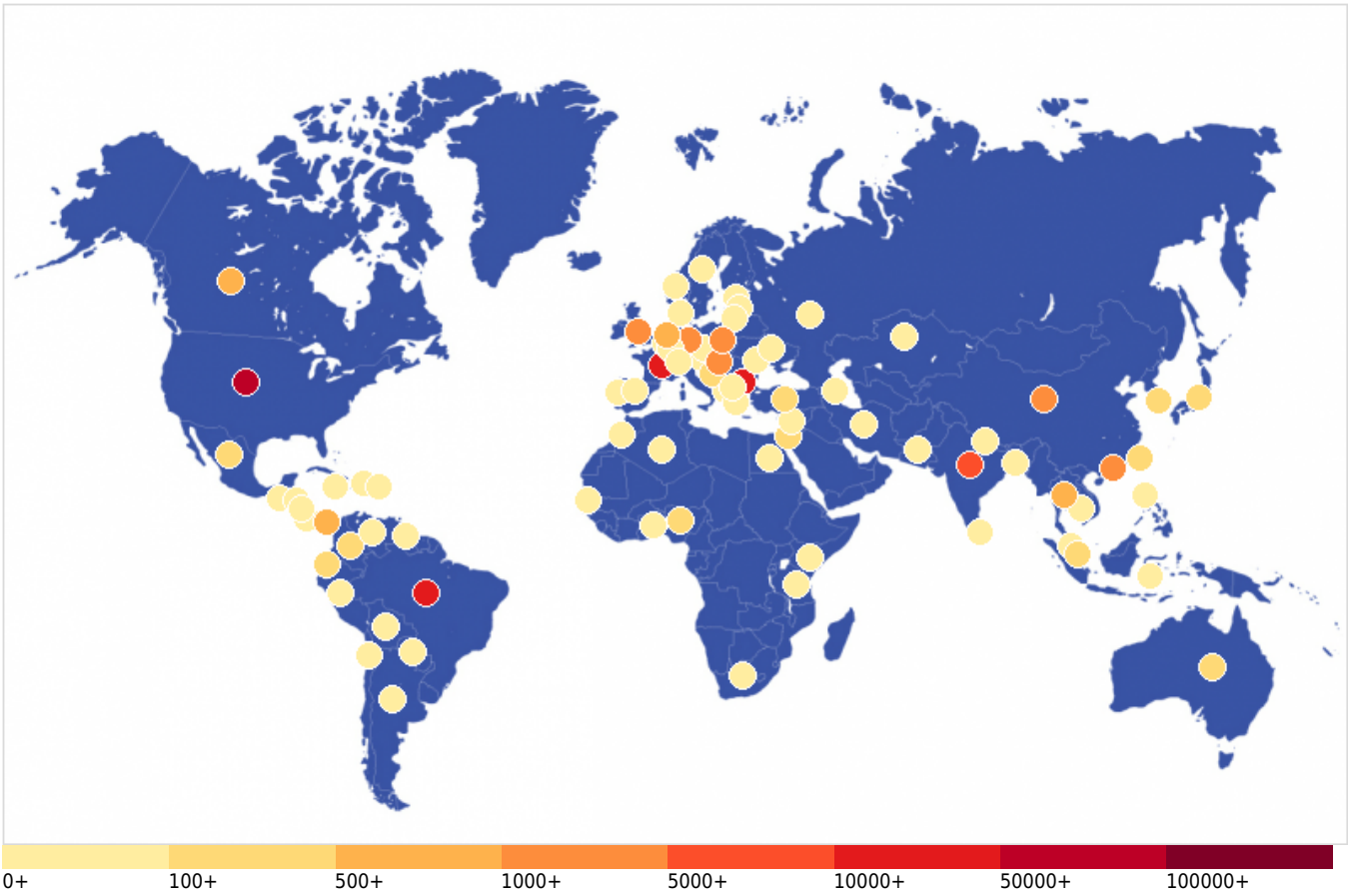
Vulnerability Metric

12

THREATS

Critical Attacks Per Country In Past Week

Organo Judicial 06/11/2026

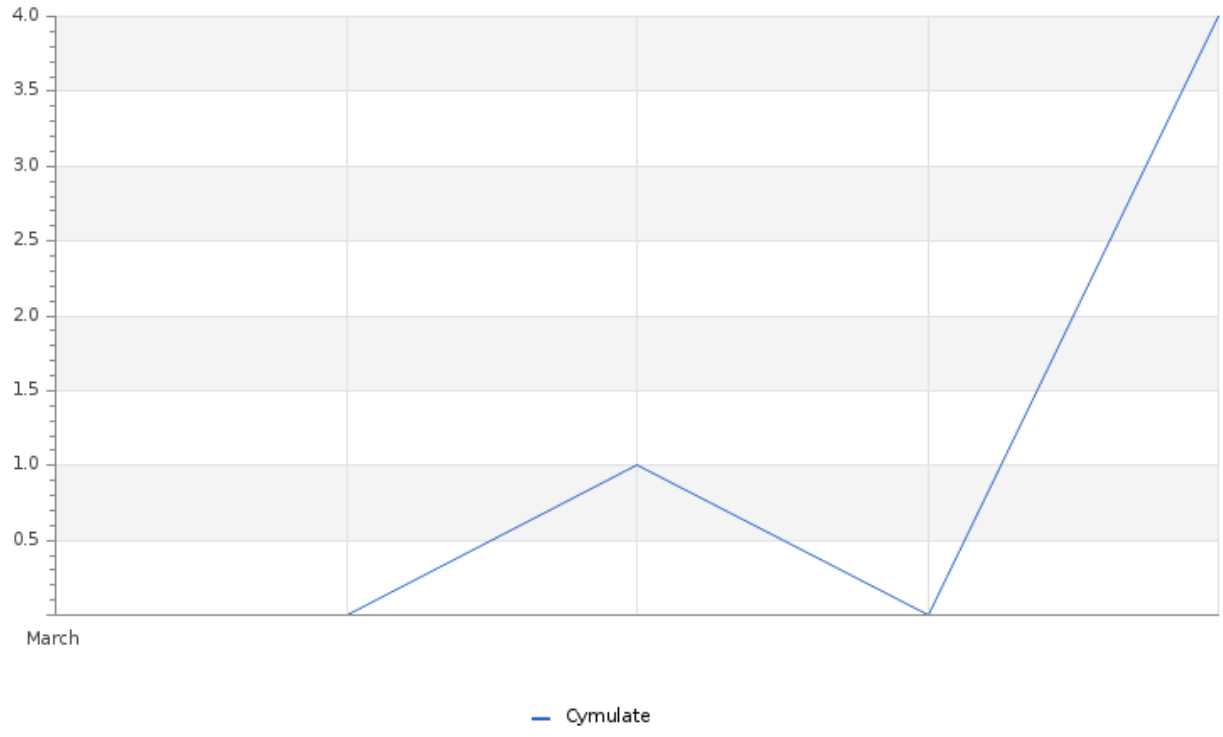


Albania - 59
Algeria - 21
Argentina - 99
Australia - 306
Austria - 3
Azerbaijan - 3
Bangladesh - 42
Belgium - 3
Bolivia - 53
Bosnia and Herzegovina - 305
Botswana - 9
Brazil - 23882
Bulgaria - 10441
Cambodia - 6
Canada - 520
Chile - 45
China - 2283
Colombia - 209
Costa Rica - 12
Czechia - 3
Denmark - 3
Dominican Republic - 6
Ecuador - 111
Egypt - 6
Estonia - 3
France - 26089
Germany - 1080
Greece - 3
Guatemala - 12
Guyana - 3
Honduras - 15
Hong Kong - 2100
Hungary - 1113
India - 9769
Indonesia - 69
Israel - 210
Jamaica - 12
Japan - 437
Jordan - 3
Kazakhstan - 34
Kenya - 9
Latvia - 12
Lebanon - 15
Lithuania - 6
Luxembourg - 87
Malaysia - 6
Mauritius - 9
Mexico - 462
Moldova - 3
Morocco - 6
Nepal - 3
Netherlands - 808
New Zealand - 3
Nicaragua - 9
Nigeria - 258
North Macedonia - 3
Norway - 66
Pakistan - 81
Panama - 720
Paraguay - 15
Peru - 12
Philippines - 12
Poland - 1374
Portugal - 3
Puerto Rico - 6
Russia - 61
Saint Kitts and Nevis - 3
Senegal - 9
Seychelles - 3
Singapore - 101
South Africa - 12
South Korea - 196
Spain - 16
Sri Lanka - 25
Sweden - 32
Switzerland - 21
Taiwan - 116
Tanzania - 15
Thailand - 606
Togo - 3
Turkey - 411
Ukraine - 24
United Kingdom - 3383
United States - 66821
Venezuela - 66

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

Organo Judicial 06/11/2026

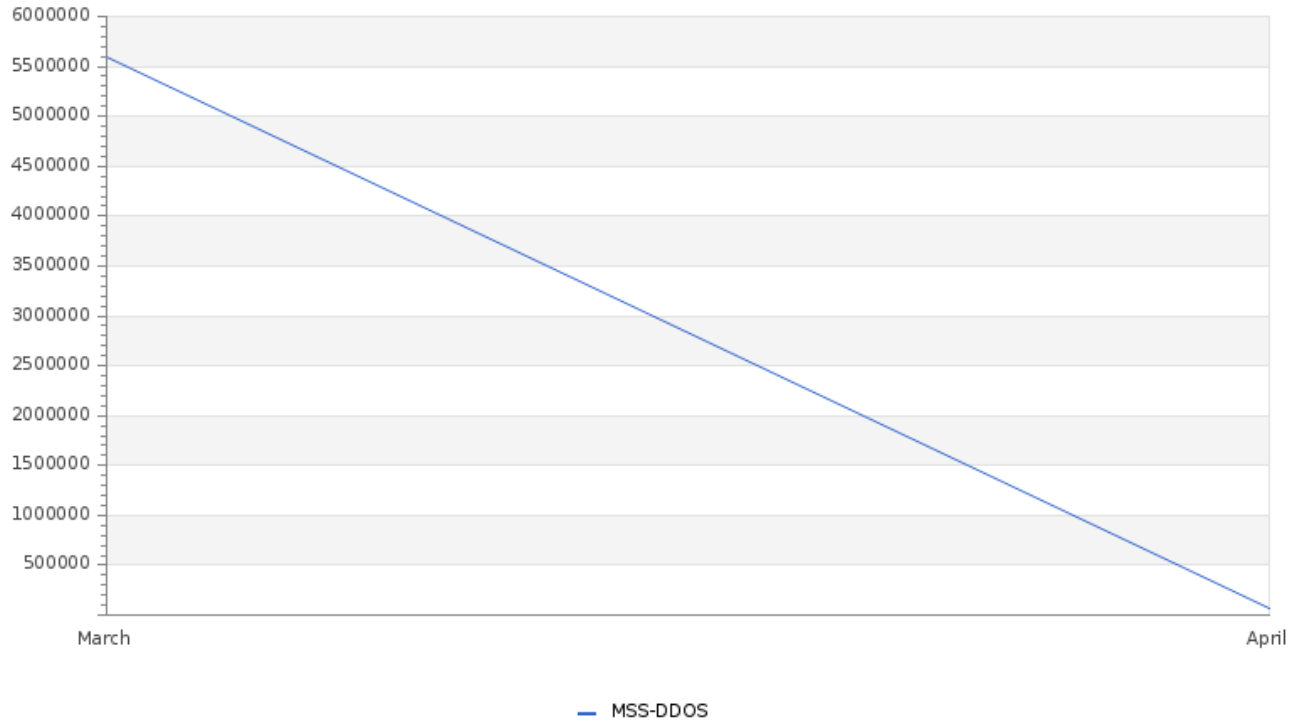
Total Number of Successful MFA authentications per application



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

Organo Judicial 06/11/2026

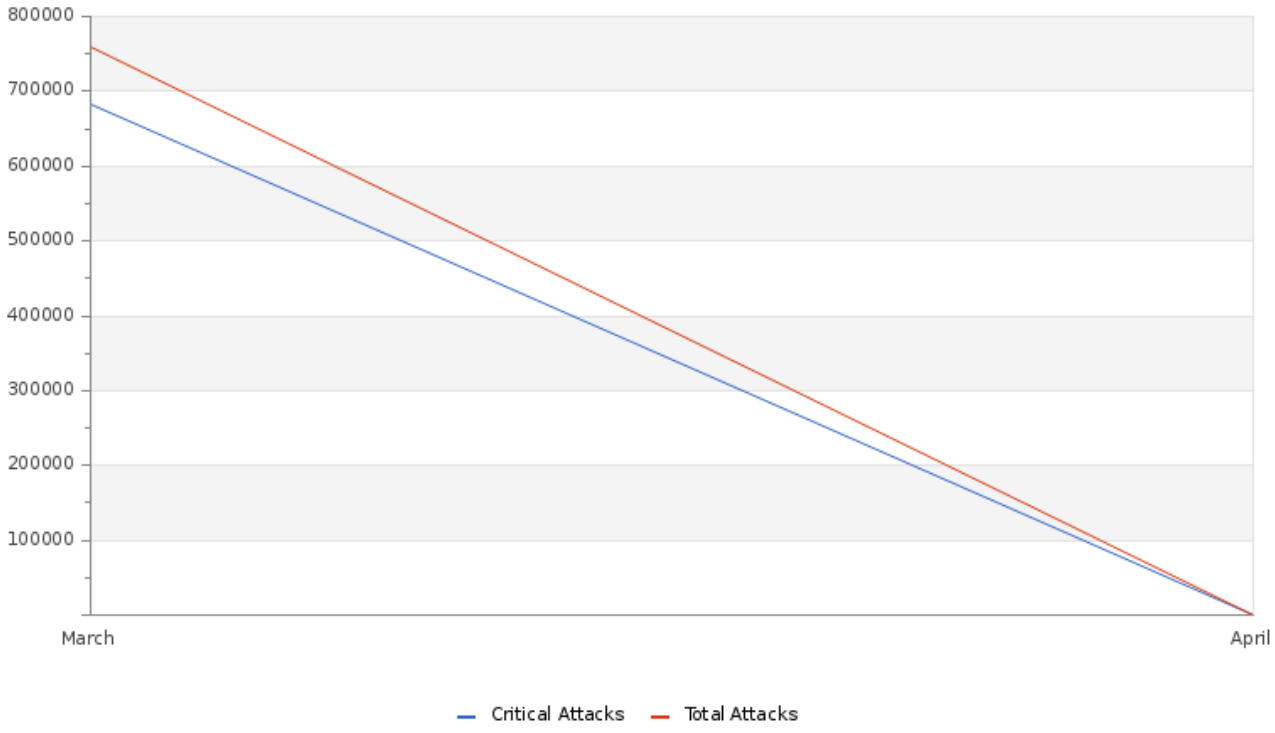
Total Attacks Successfully Blocked Per Service



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

Organo Judicial 06/11/2026

Attacks Successfully Blocked by Severity



System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	17	3
Critical Device Outages	0	0

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

Organo Judicial 06/11/2026

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
www.organojudicial.gob.pa	HTTP	200.46.13.0/26	Down, Warning		435	2026-03-09 11:30:46	2026-03-23 22:12:25
Plataforma Moodle Escuela Judicial	HTTP Advanced	Web Servers	Down, Warning		50	2026-03-10 18:09:19	2026-03-29 00:18:59
Sistema automatizado de gestion judicial	HTTP Advanced	Web Servers	Down, Warning		33	2026-03-10 18:29:21	2026-03-31 21:39:27
Repositorio digital	HTTP Advanced	Web Servers	Down, Warning		29	2026-03-10 18:09:19	2026-03-18 06:45:11
Plataforma de correo	HTTP Advanced	Web Servers	Down		27	2026-03-05 00:24:52	2026-03-23 22:12:25
Reporte biometrico	HTTP Advanced	Web Servers	Down, Warning		25	2026-03-10 18:24:21	2026-03-20 00:35:00
Probe Device	System Health	Organo Judicial	Warning		23	2026-03-14 03:03:39	2026-03-31 03:03:40
Consulta de fallos	HTTP Advanced	Web Servers	Down, Warning		20	2026-03-10 18:14:20	2026-03-18 06:45:11
GMSA-OJ-VM.in.glesec.com	Ping	GMSA-OJ	Down, Warning		15	2026-03-22 03:35:53	2026-03-30 13:16:20
Plataforma de Gestion de Pleno	HTTP Advanced	Web Servers	Down, Warning		15	2026-03-10 18:24:21	2026-03-18 06:45:11
Gestor Documental	HTTP Advanced	Web Servers	Down, Warning		14	2026-03-10 18:19:20	2026-03-13 13:32:03
Probe Device	System Health	Organo Judicial C-GMSA	Warning		5	2026-03-10 03:02:35	2026-03-12 03:03:05
GMSA-OJ HyperV	HTTP	GMSA-OJ	Down, Warning		4	2026-03-30 13:16:36	2026-03-30 13:16:36
DevConsejo de Administración de la Carrera Judicial ice	HTTP Advanced	Web Servers	Down, Warning		4	2026-03-30 13:16:31	2026-03-30 13:16:31
Sistema Integral de Gestión de Recursos Humanos	HTTP Advanced	Web Servers	Down, Warning		4	2026-03-17 13:38:13	2026-03-30 13:16:08

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	1,166,463	0	977	0

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

Organo Judicial 06/11/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Systems Performance	220
Change in Systems Availability	97
Change in High or Critical Vulnerabilities	3
Non Baselined Discovered System	1076
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	24
Change in External High or Critical Vulnerabilities	97
Notable Event Alert: Endpoint Configuration Management High Priority Event	6
Monitoring for open ports	26
Change in Critical Perimeter Attacks	364
High Persistency Detection	70
Threat Intelligence Validation	5
TEVR BAS Immediate Threats	1
Targeted Campaign Alignment	8

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.**

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

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