TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

March 31, 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	**Low**	**Medium**

Accepted & Actual Risk

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

CISO EXECUTIVE REPORT

Organo Judicial 03/31/2026

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

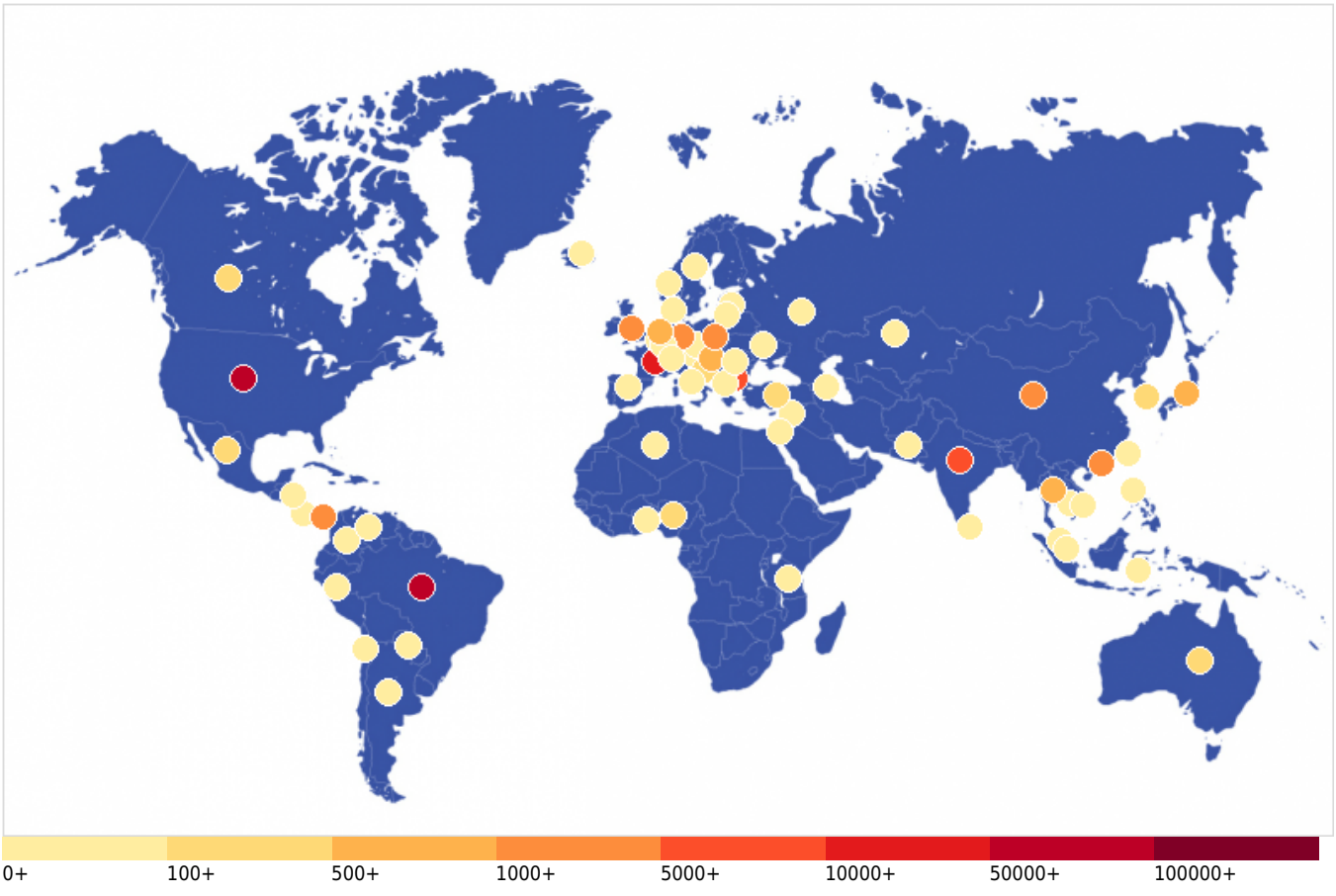
VULNERABILITY

Vulnerability Metric

12%

THREATS

Critical Attacks Per Country In Past Week

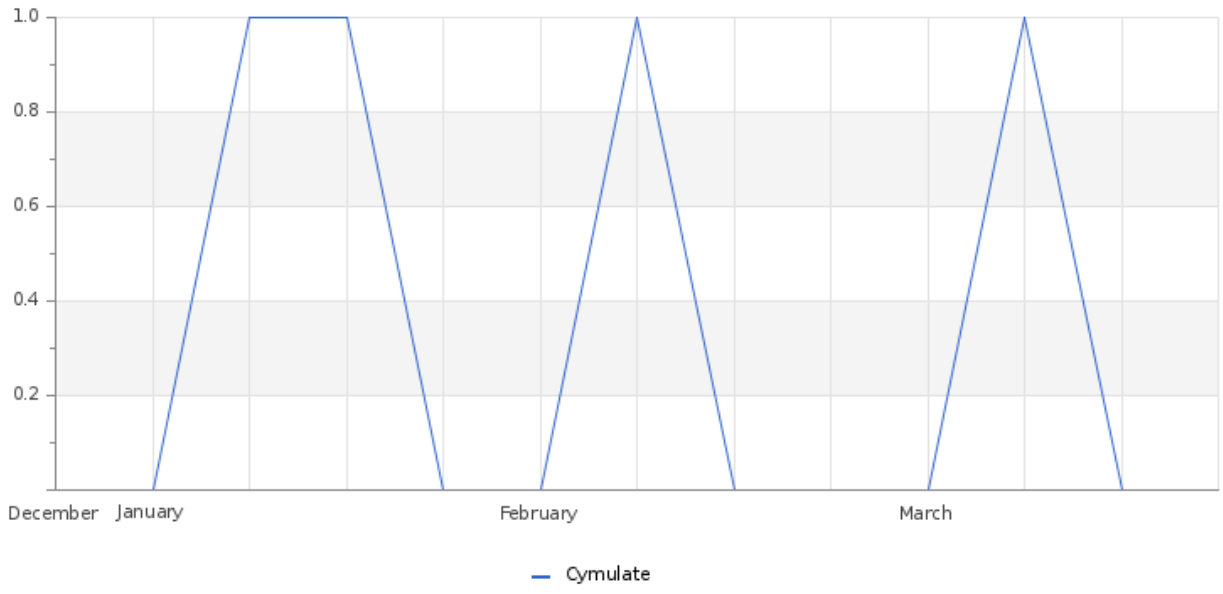


LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Algeria - 12
Argentina - 3
Australia - 351
Austria - 6
Azerbaijan - 3
Belgium - 6
Bosnia and Herzegovina - 295
Brazil - 63,339
Bulgaria - 5,604
Cambodia - 3
Canada - 348
Chile - 6
China - 2,407
Colombia - 72
Costa Rica - 6
Czechia - 3
Denmark - 3
France - 25,071
Georgia - 3
Germany - 1,110
Honduras - 3
Hong Kong - 2,173
Hungary - 859
Iceland - 3
India - 9,647
Indonesia - 46
Israel - 6
Italy - 6
Japan - 518
Kazakhstan - 3
Latvia - 6
Lithuania - 3
Luxembourg - 93
Malaysia - 24
Mexico - 227
Netherlands - 748
New Zealand - 9
Nigeria - 220
North Macedonia - 9
Norway - 59
Pakistan - 24
Panama - 1,472
Paraguay - 3
Peru - 9
Philippines - 3
Poland - 1,360
Romania - 3
Russia - 77
Seychelles - 50
Singapore - 74
South Korea - 174
Spain - 19
Sri Lanka - 35
Sweden - 49
Switzerland - 24
Taiwan - 39
Tanzania - 3
Thailand - 630
Togo - 3
Turkey - 413
Ukraine - 23
United Kingdom - 3,405
United States - 64,542
Venezuela - 3
Vietnam - 29

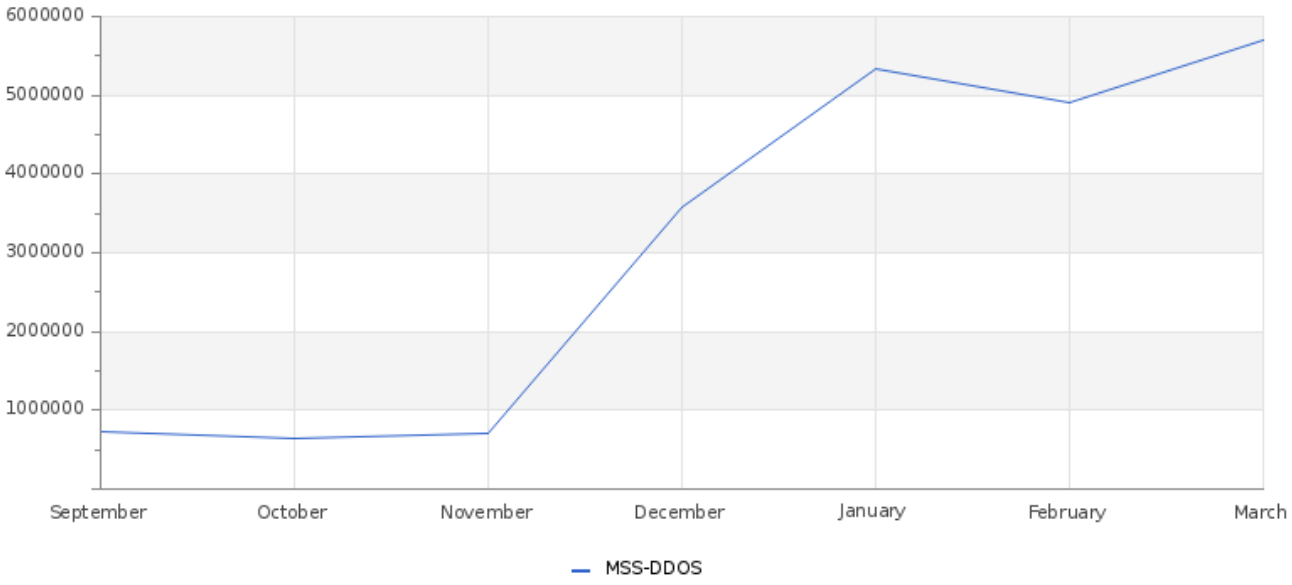
Total Number of Successful MFA authentications per application



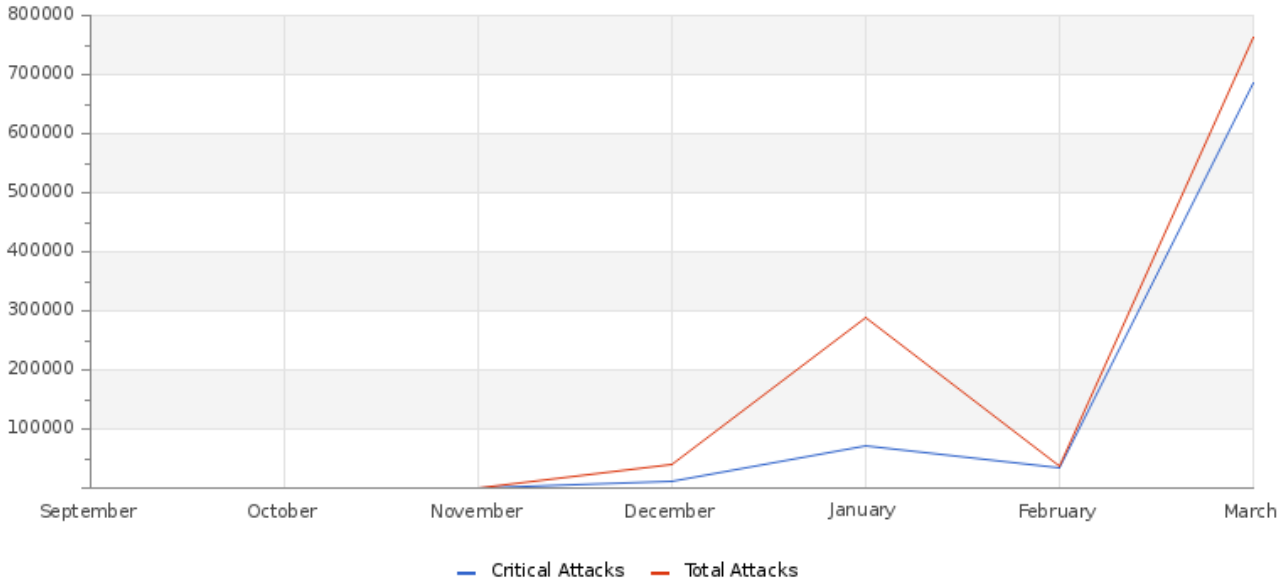
CISO EXECUTIVE REPORT

Organo Judicial 03/31/2026

Total Attacks Successfully Blocked Per Service



Attacks Successfully Blocked by Severity



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

CISO EXECUTIVE REPORT

Organo Judicial 03/31/2026

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		441	2026-03-01 01:57:00	2026-03-23 22:12:25
Consejo de Administración de la Carrera de la Defensa Pública	HTTP Advanced	Web Servers	Down		288	2026-03-01 00:02:25	2026-03-02 00:00:09
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		32	2026-03-10 18:29:21	2026-03-23 22:12:25
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		7	2026-03-01 03:02:36	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

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	1,152,263	0	1,056	0

OPERATIONAL

Total Number of Cases

Open	0
Answered	100
Closed	3276

Notable Events

Notable Event Type	How Many #
Change in High or Critical Vulnerabilities	3
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	1
Change in External High or Critical Vulnerabilities	2
Change in Systems Performance	1

Total Remediation Cases by Stage

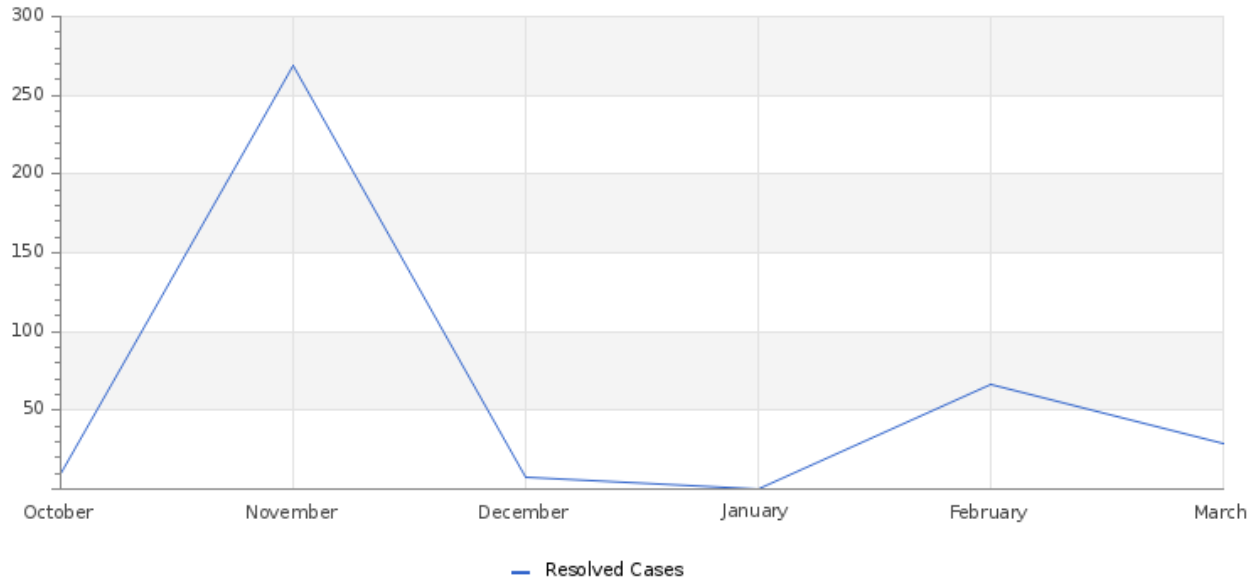
	Testing & Detection	Verification	Prioritization and Business Relevance	GLESEC Remediation Plan	Client Security Team	Client Remediation Team	Closed
SECURITY REMEDIATION AND INVESTIGATIONS	123	6	0	0	9	246	351
GOC: Security Incidents to investigate	172	1	0	0	2	156	358
Total	295	7	0	0	11	402	709

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

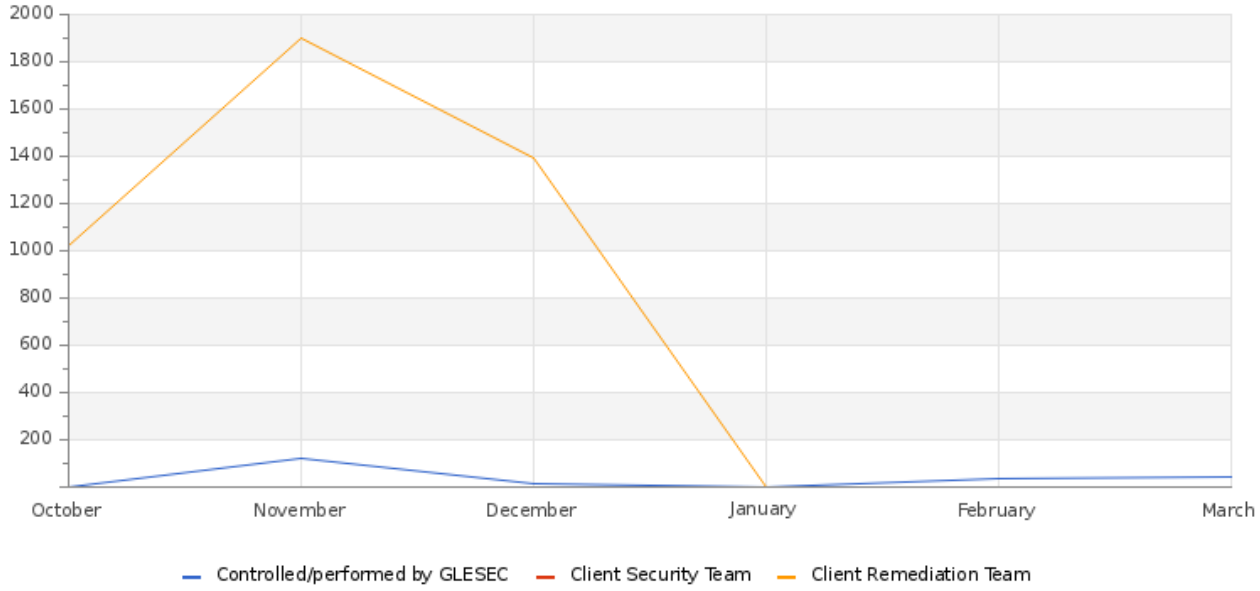
CISO EXECUTIVE REPORT

Organo Judicial 03/31/2026

Vulnerabilities Resolved Over Time



Vulnerabilities: Average Time to Resolve



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

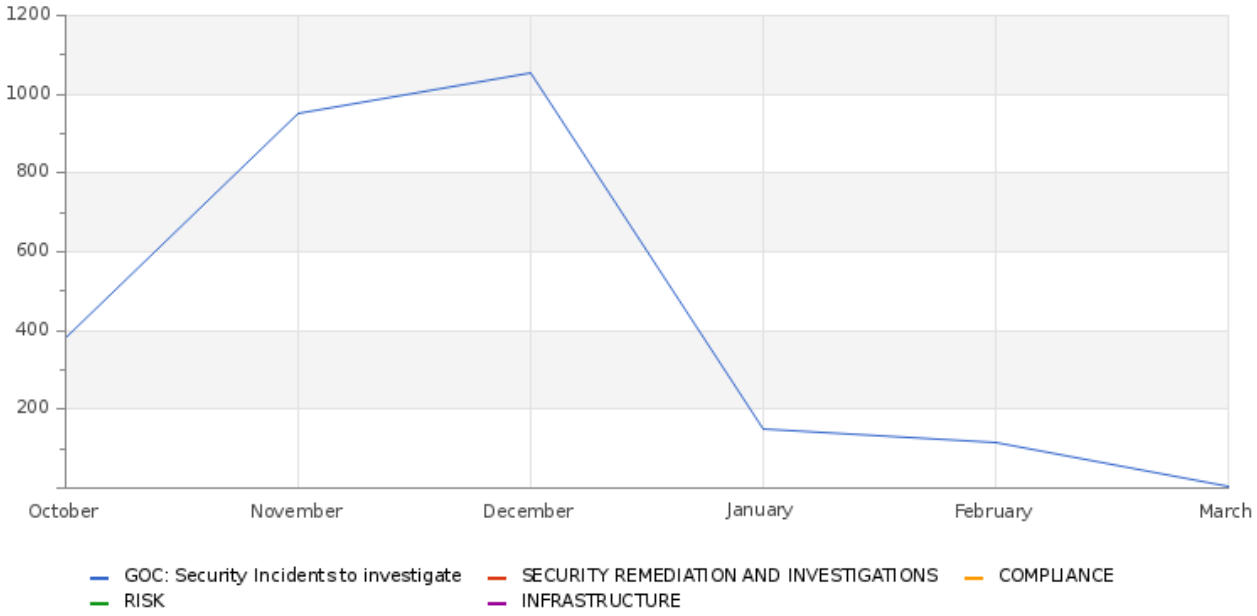
CISO EXECUTIVE REPORT

Organo Judicial 03/31/2026

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 3h 22m 18s
Verification	11d 5h 57m 51s
Prioritization and Business Relevance	0d 0h 0m 0s
GLESEC Incidents Plan	0d 11h 28m 53s
Client Security Team	0d 0h 0m 0s
Client Incidents Team	1d 1h 44m 55s

Workload

Stages	How Many #
Testing & Detection	1
Verification	0
Prioritization and Business Relevance	0
GLESEC Incidents Plan	1
Client Security Team	1
Client Incidents Team	25
Closed	1114

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	1d 22h 56m 38s
Verification	0d 1h 18m 15s
Prioritization and Business Relevance	0d 0h 0m 0s
GLESEC Remediation Plan	16d 4h 35m 24s
Client Security Team	0d 0h 0m 0s
Client Remediation Team	0d 0h 0m 0s

Workload

Stages	How Many #
Testing & Detection	0
Verification	7
Prioritization and Business Relevance	0
GLESEC Remediation Plan	0
Client Security Team	0
Client Remediation Team	33
Closed	685

DAILYBRIEF

Active High-Severity Items

0

0

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

CISO EXECUTIVE REPORT

Organo Judicial 03/31/2026

Executive Action Required

No executive action required today

Threat Relevance Score (TRS)

68

▲ +43

Risk Score (RS)

70

▲ +34

External Threat Context

Threat Headline	Relevance
ThreatFox IOCs for 2026-03-28	Sector-relevant threat intelligence
OTX [North Korean APT group]: EtherRAT & SYS_INFO Module: C2 on Ethereum...	Threat actor activity detected

Ongoing cases

Case #	Service	Priority	Hours	Status

Cybersecurity News

Title	Categories	Industries
Silver Fox Expands Asia Cyber Campaign with AtlasCross RAT and Fake Domains	Cyber Attacks, Malware	Banking and Financial, Blockchain
Microsoft fixes Outlook Classic crashes caused by Teams Meeting add-in	Cyber Attacks	Government
Hacker charged with stealing $53 million from Uranium crypto exchange	Cyber Attacks, Malware	Banking and Financial, Legal Services, Blockchain

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

CISO EXECUTIVE REPORT

Organo Judicial 03/31/2026

Title	Categories	Industries
Dutch Finance Ministry takes treasury banking portal offline after breach	Cyber Attacks	Government, Banking and Financial, Education
Dutch Finance Ministry takes treasury banking portal offline after breach	Cyber Attacks	Government, Banking and Financial, Education
CISA orders feds to patch actively exploited Citrix flaw by Thursday	Cyber Attacks, Vulnerabilities, Malware	Government, Education, Legal Services

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