TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

March 10, 2026

TLP AMBER CISO
EXECUTIVE REPORT

The report includes: RISK, Cybersecurity and Operational information.

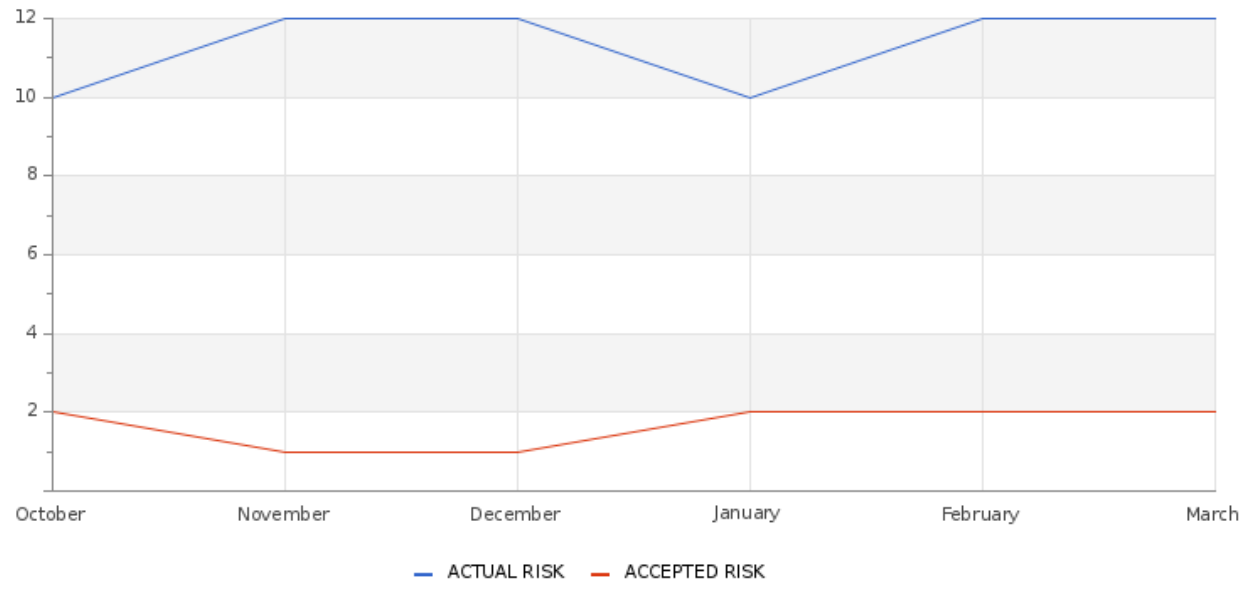
About this report

This on-demand report provides executive level information as of the state of Cybersecurity for your organization including top security indicators and performance.

RISK

Actual Risk	Accepted Risk	Confidence
Low	**n/a**	**Medium**

Accepted & Actual Risk



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

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

	Current Month	Previous Month
Actual Risk	12	8
Accepted Risk	0	1

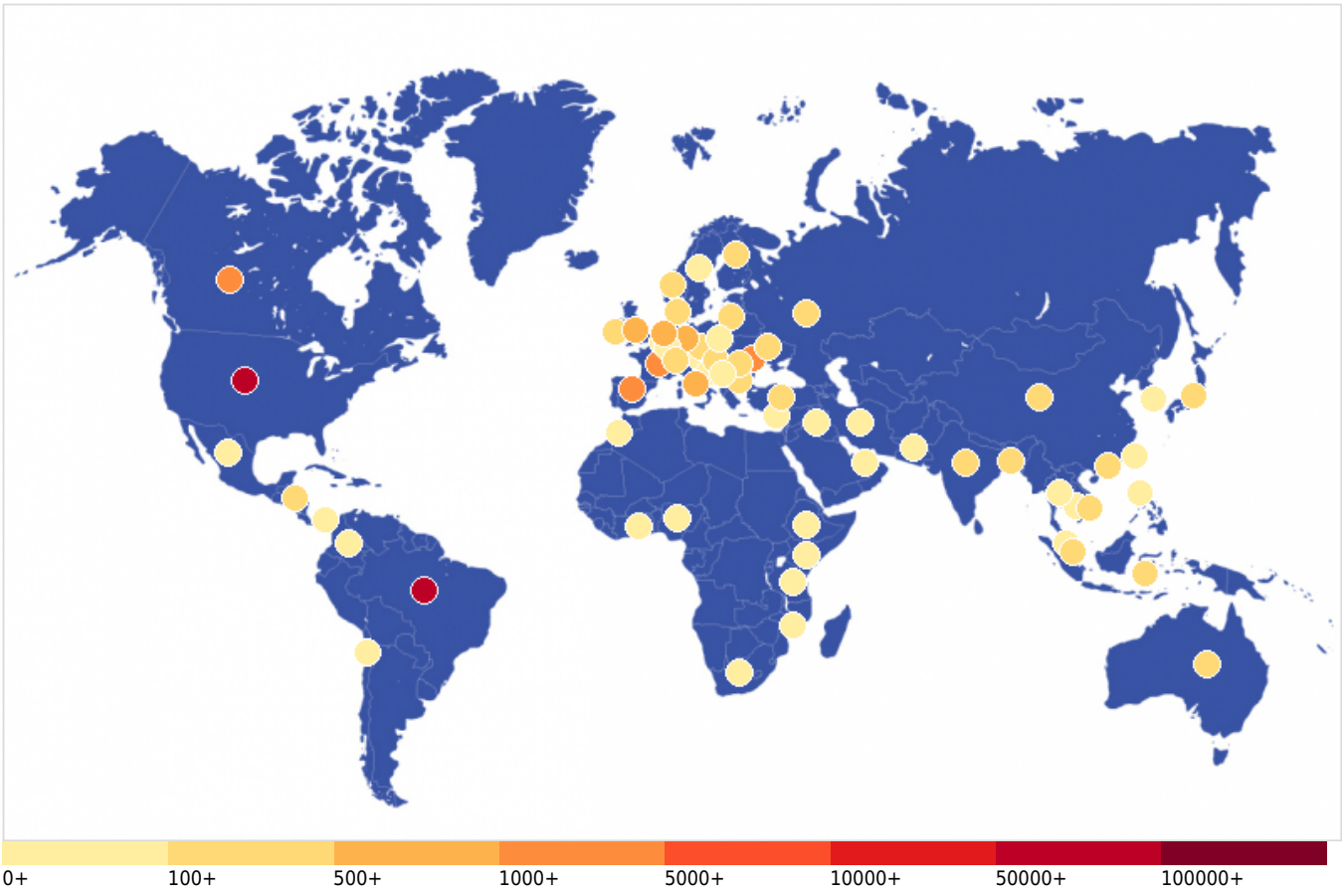
VULNERABILITY

Vulnerability Metric

11%

THREATS

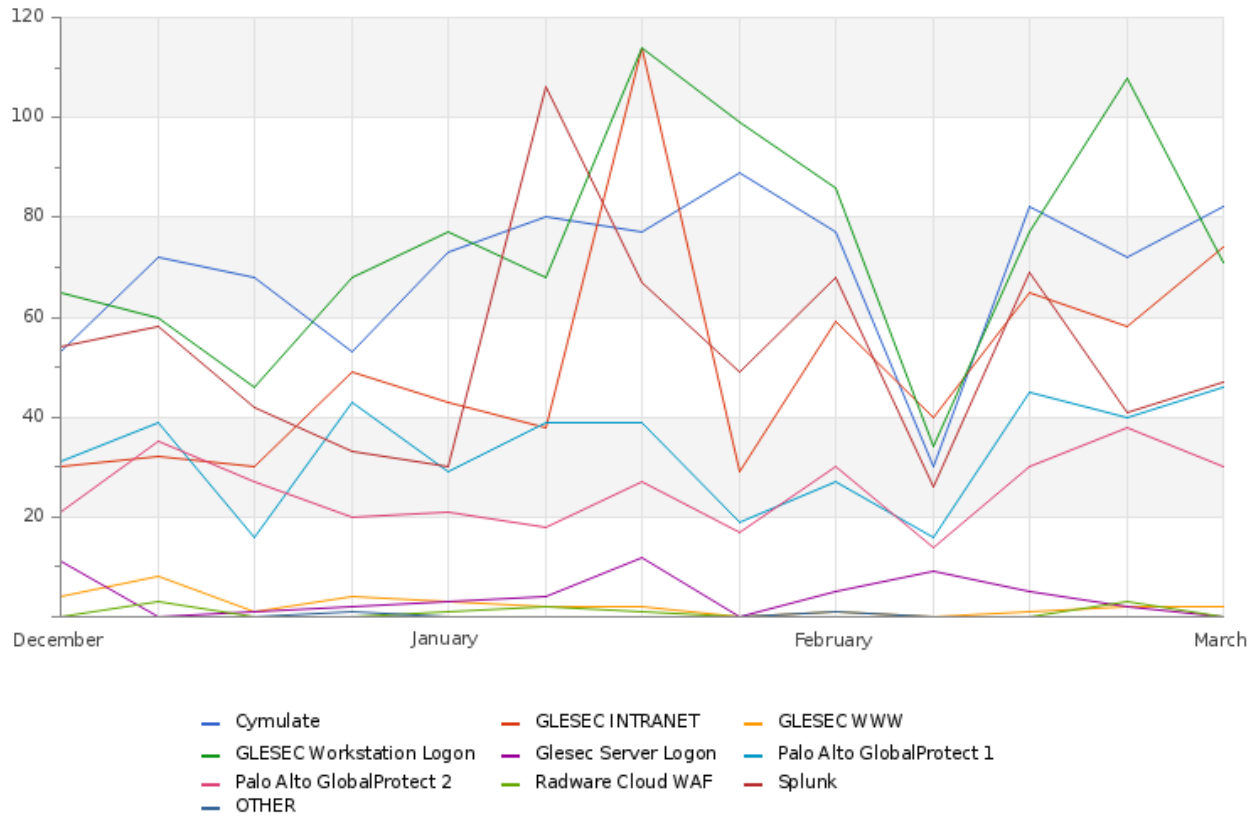
Critical Attacks Per Country In Past Week



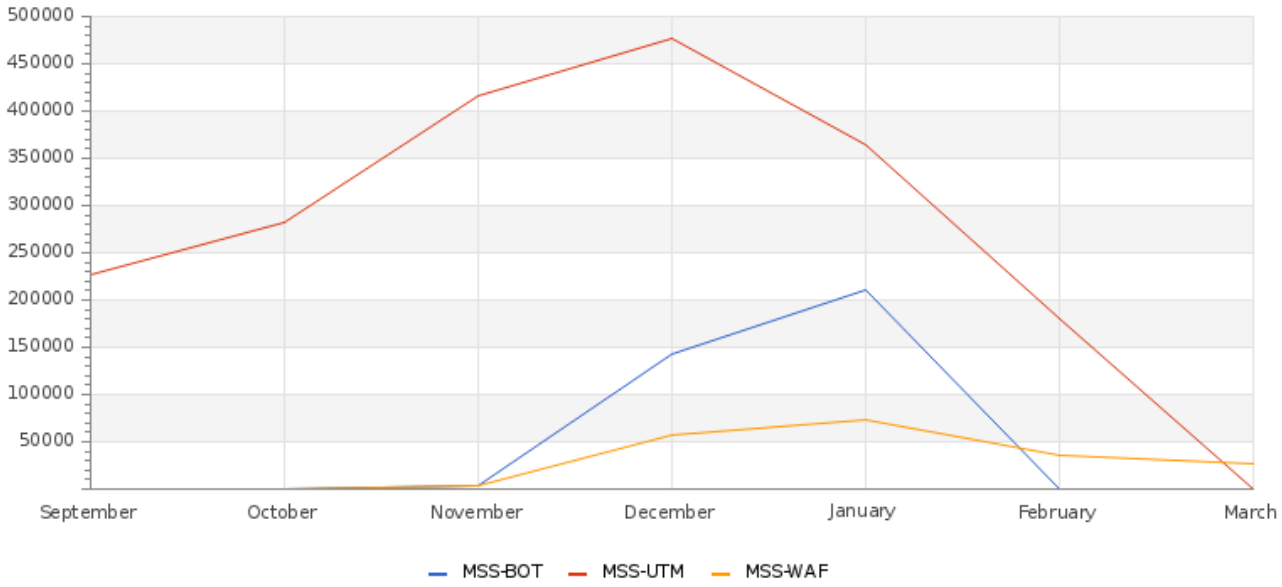
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

Andorra - 4
Belgium - 27
Cambodia - 9
Colombia - 2
Ethiopia - 2
Ghana - 7
India - 368
Ireland - 427
Lithuania - 228
Moldova - 1,484
New Zealand - 28
Panama - 32
Russia - 160
South Africa - 12
Switzerland - 210
Turkey - 200
United States - 59,330
Australia - 157
Bosnia and Herzegovina - 61
Canada - 2,308
Cyprus - 2
Finland - 289
Honduras - 180
Indonesia - 129
Italy - 935
Luxembourg - 2
Morocco - 1
Nigeria - 2
Philippines - 13
Saint Kitts and Nevis - 36
South Korea - 94
Taiwan - 42
Ukraine - 373
Vietnam - 420
Austria - 6
Brazil - 72,297
Chile - 73
Czechia - 161
France - 1,261
Hong Kong - 105
Iran - 13
Japan - 158
Malaysia - 14
Mozambique - 1
Norway - 191
Poland - 51
Serbia - 1
Spain - 3,349
Tanzania - 1
United Arab Emirates - 46
Bangladesh - 133
Bulgaria - 176
China - 432
Denmark - 108
Germany - 996
Hungary - 138
Iraq - 1
Kenya - 1
Mexico - 3
Netherlands - 763
Pakistan - 5
Romania - 431
Singapore - 466
Sweden - 24
Thailand - 8
United Kingdom - 835

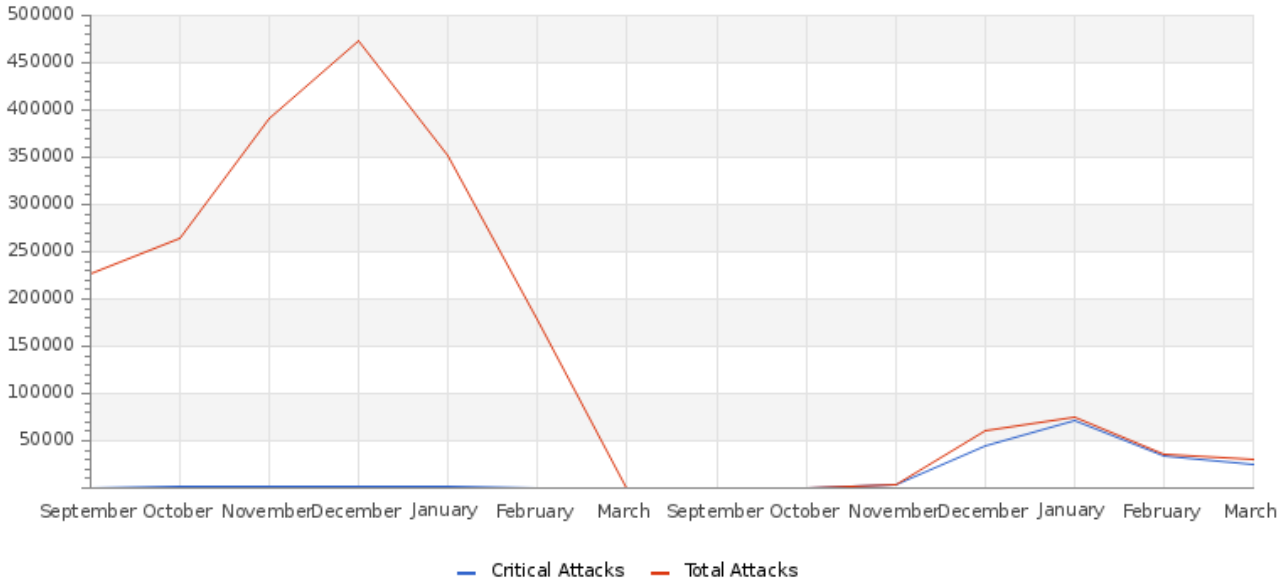
Total Number of Successful MFA authentications per application



Total Attacks Successfully Blocked Per Service

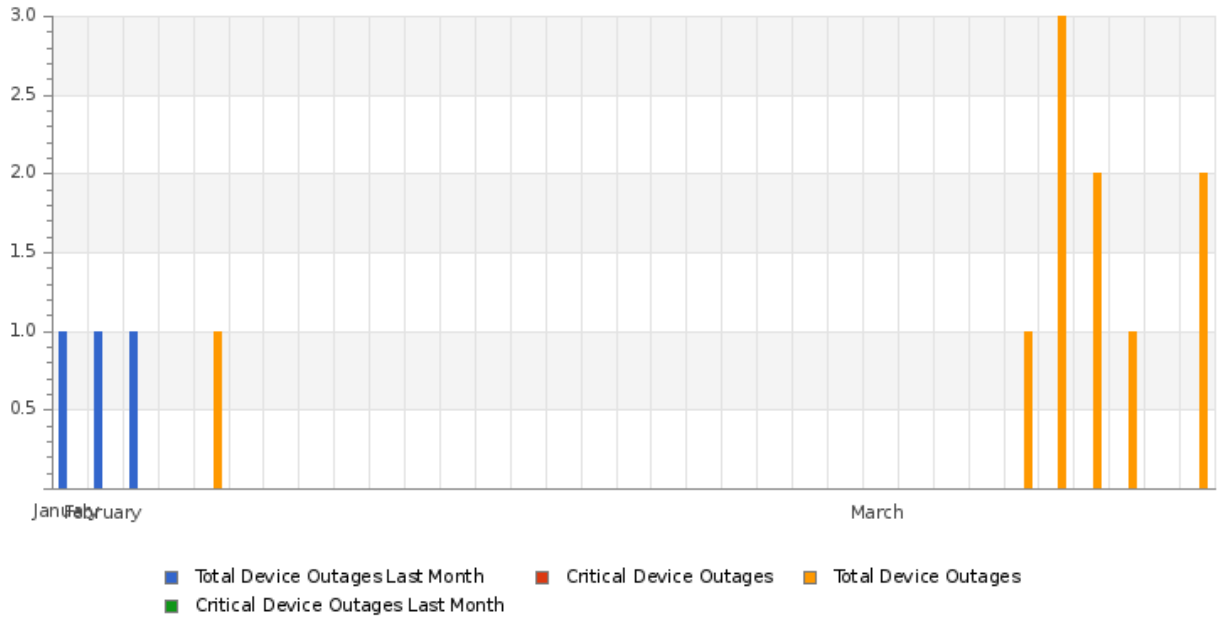


Attacks Successfully Blocked by Severity



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

Histogram of Total and Critical Device Outages



Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
20,903	306,956	0	50	431,909	23,626

OPERATIONAL

Total Number of Cases

Open	15
Answered	43
Closed	7090

Notable Events

Notable Event Type	How Many #
Monitoring Event for SPLUNK CLOUD	3

TLP:AMBER

CISO EXECUTIVE REPORT

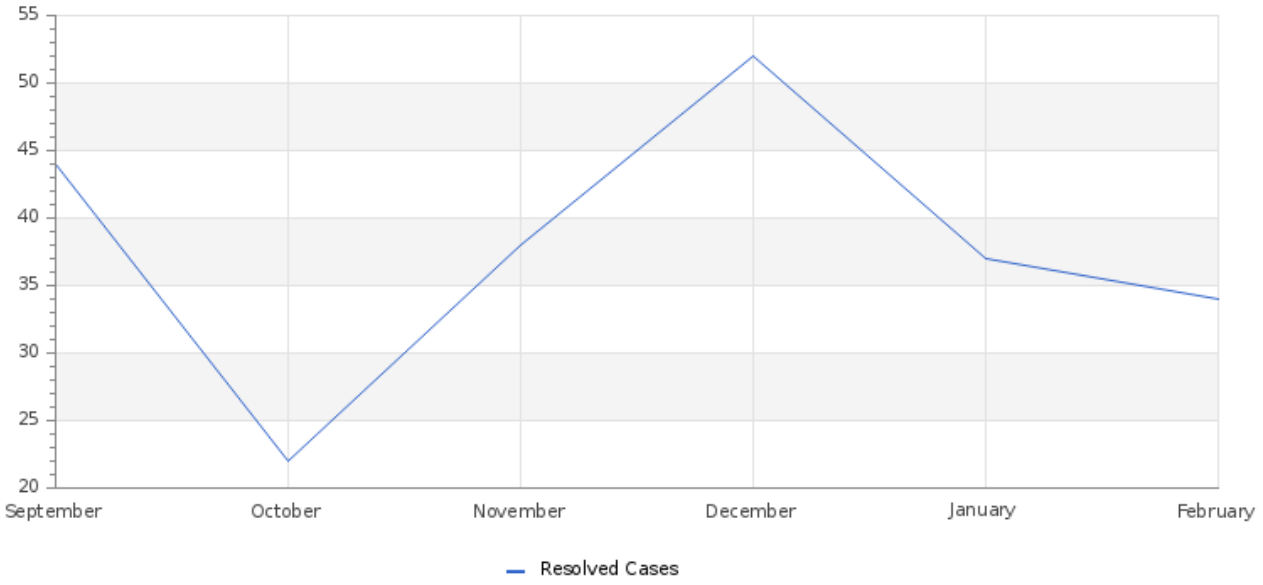
GLESEC 03/10/2026

Notable Event Type	How Many #
BAS Web Security	10

Total Remediation Cases by Stage

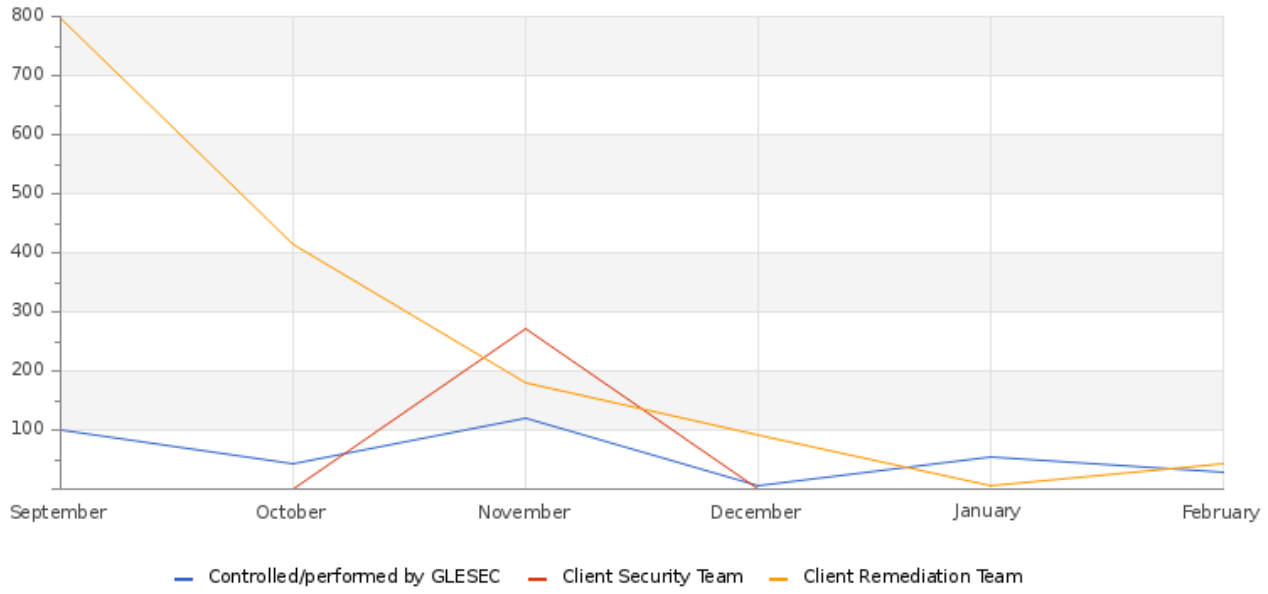
	Testing & Detection	Verification	Prioritization and Business Relevance	GLESEC Remediation Plan	Client Security Team	Client Remediation Team	Closed
INFRASTRUCTURE	0	0	0	0	2	12	104
SECURITY REMEDIATION AND INVESTIGATIONS	3	7	0	3	1	93	577
GOC: Security Incidents to investigate	200	0	0	0	0	49	184
Total	203	7	0	3	3	154	865

Vulnerabilities Resolved Over Time



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

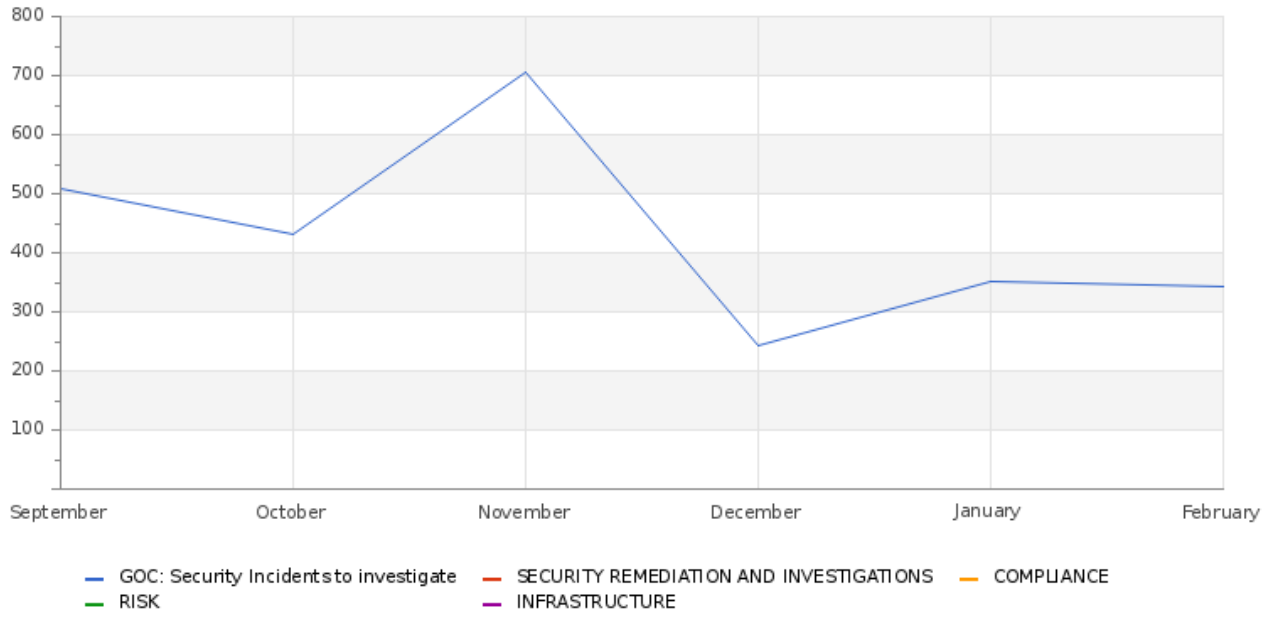
Vulnerabilities: Average Time to Resolve



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 0h 23m 11s
Verification	0d 0h 0m 0s
Prioritization and Business Relevance	0d 0h 0m 0s
GLESEC Incidents Plan	0d 0h 0m 0s
Client Security Team	0d 0h 0m 0s
Client Incidents Team	0d 0h 0m 0s

Workload

Stages	How Many #
Testing & Detection	0
Verification	0
Prioritization and Business Relevance	0
GLESEC Incidents Plan	0
Client Security Team	0
Client Incidents Team	3
Closed	847

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 10h 37m 36s
Verification	16d 16h 52m 53s
Prioritization and Business Relevance	0d 0h 0m 0s
GLESEC Remediation Plan	0d 0h 0m 0s
Client Security Team	0d 0h 0m 0s
Client Remediation Team	0d 0h 0m 0s

Workload

Stages	How Many #
Testing & Detection	2
Verification	4
Prioritization and Business Relevance	0
GLESEC Remediation Plan	0
Client Security Team	0
Client Remediation Team	17
Closed	815

DAILYBRIEF

Active High-Severity Items

0

0

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC 03/10/2026

Executive Action Required

No executive action required today

Threat Relevance Score (TRS)

57
→ 0

Risk Score (RS)

53
→ 0

External Threat Context

Threat Headline	Relevance
ThreatFox IOCs for 2026-03-08	Sector-relevant threat intelligence
URLhaus IOCs for 2026-03-08	Sector-relevant threat intelligence

Ongoing cases

Case #	Service	Priority	Hours	Status

Cybersecurity News

Title	Categories	Industries
Microsoft Teams phishing targets employees with A0Backdoor malware	Cyber Attacks, Malware	Banking and Financial
Dutch govt warns of Signal, WhatsApp account hijacking attacks	Cyber Attacks, Data Breaches	Government, Telecommunication, Military
President Trump's Cyber Strategy for America: What It Means for the U.S. and Why It Matters Globally	Cyber Attacks, Vulnerabilities, Malware	Government, Banking and Financial, Education, Transportation, Telecommunication, Blockchain

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

TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC 03/10/2026

Title	Categories	Industries
President Trump's Cyber Strategy for America: What It Means for the U.S. and Why It Matters Globally	Cyber Attacks, Vulnerabilities, Malware	Government, Banking and Financial, Education, Transportation, Telecommunication, Blockchain
Google: Cloud attacks exploit flaws more than weak credentials	Cyber Attacks, Data Breaches, Vulnerabilities, Malware	Government, Banking and Financial, Legal Services, Military, Blockchain
Google: Cloud attacks exploit flaws more than weak credentials	Cyber Attacks, Data Breaches, Vulnerabilities, Malware	Government, Banking and Financial, Legal Services, Military, Blockchain

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