

TLP:AMBER

CISO EXECUTIVE REPORT

WINSOUTHCU

November 05, 2026



©2023. GLESEC. All Rights Reserved.

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
n/a	Low	Low

Accepted & Actual Risk



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

	Current Month	Previous Month
Actual Risk		
Accepted Risk	0	0

VULNERABILITY

Vulnerability Metric

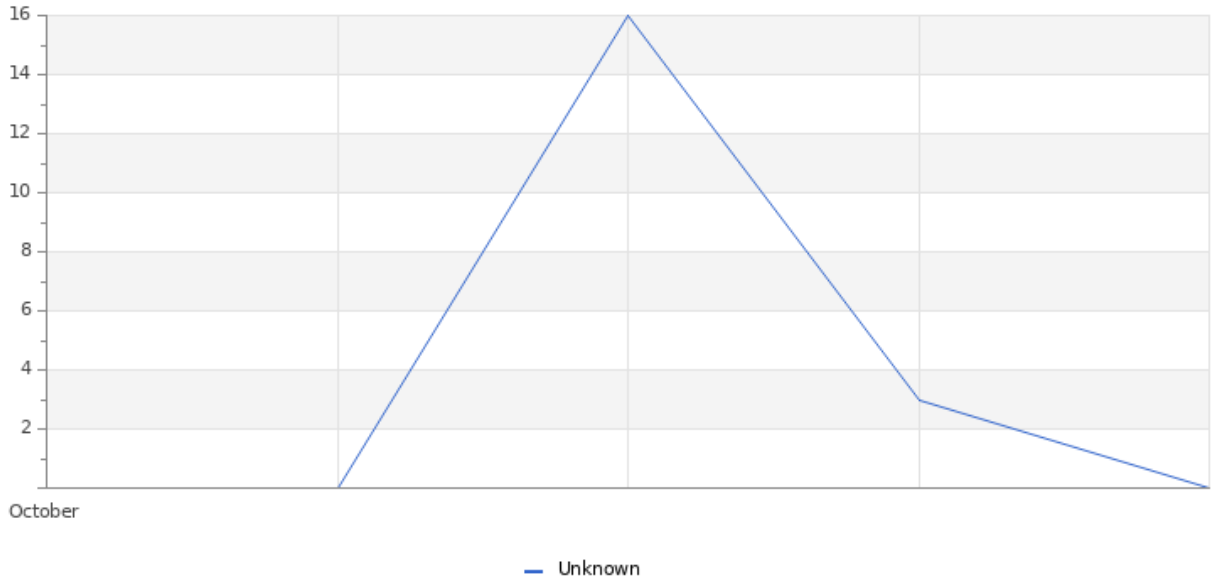
0%

©2023. GLESEC. All Rights Reserved.

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

THREATS

Total Number of Successful MFA authentications per application



Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
Probe Device	Disk Free	MSS-CSME-WINSOUTHCU	Warning		1,263	2026-10-19 05:12:41	2026-10-24 08:13:04
12.0.63.42	Ping	Gadsden	Down		122	2026-10-27 19:51:28	2026-11-04 02:14:54
Probe Device	System Health	MSS-CSME-WINSOUTHCU	Warning		30	2026-10-09 12:29:50	2026-11-05 05:59:21
162.159.130.6	SSL Certificate Sensor (Port 443)	Web Sites	Warning		1	2026-11-03 10:35:49	2026-11-03 10:35:49
12.7.71.10	Ping	Albertville	Down		1	2026-10-27 20:32:05	2026-10-27 20:32:05
162.159.130.6	Ping	Web Sites	Down		1	2026-10-27 19:51:50	2026-10-27 19:51:50
Probe Device	Probe Health	MSS-CSME-WINSOUTHCU	Down		1	2026-10-19 06:13:02	2026-10-19 06:13:02

©2023. GLESEC. All Rights Reserved. PROPRIETARY & CONFIDENTIAL

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	0	0	332,417	0

OPERATIONAL

Total Number of Cases

Open	0
Answered	19
Closed	229

Notable Events

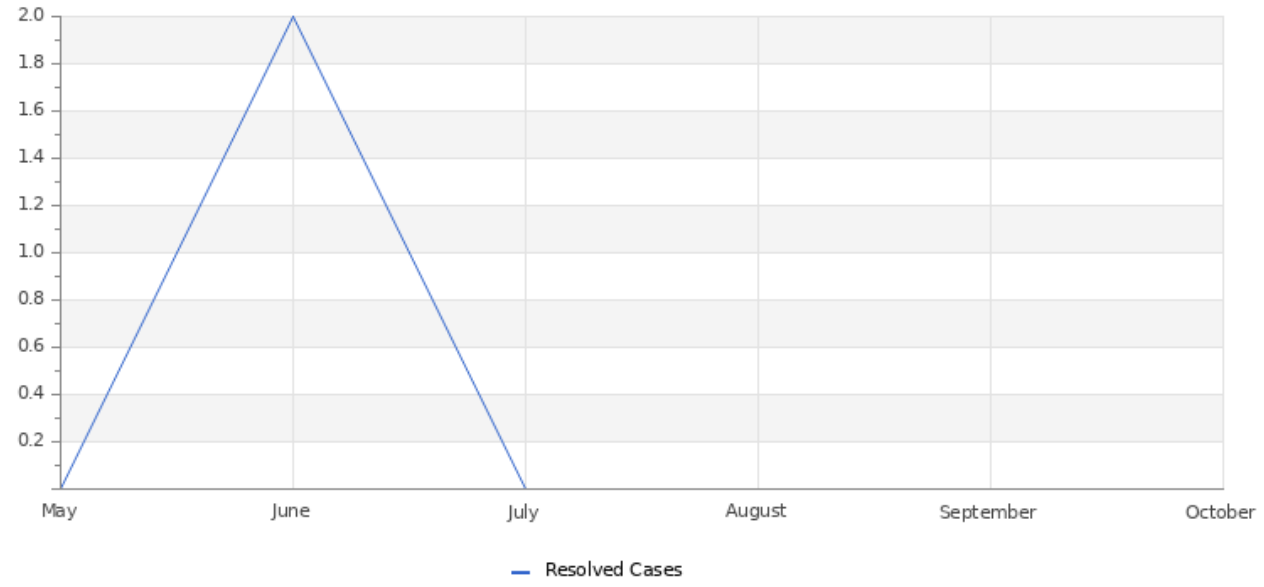
Notable Event Type	How Many #
	N/A

Total Remediation Cases by Stage

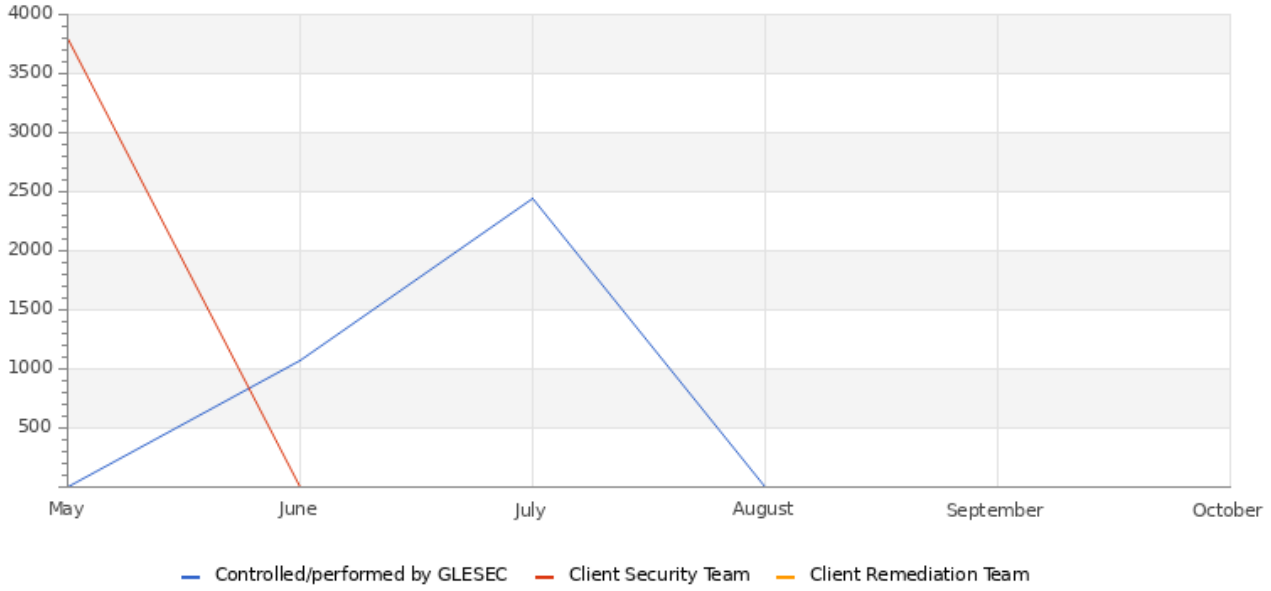
	Testing & Detection	Verification	Prioritization and Business Relevance	GLESEC Remediation Plan	Client Security Team	Client Remediation Team	Closed
GOC: Security Incidents to investigate	9	0	0	0	0	3	9
SECURITY REMEDIATION AND INVESTIGATIONS	3	0	0	0	2	23	65
Total	12	0	0	0	2	26	74

©2023. GLESEC. All Rights Reserved. PROPRIETARY & CONFIDENTIAL
LATAM HQ +507 836-5355
US HQ +1 (321) 430-0500

Vulnerabilities Resolved Over Time



Vulnerabilities: Average Time to Resolve



©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL

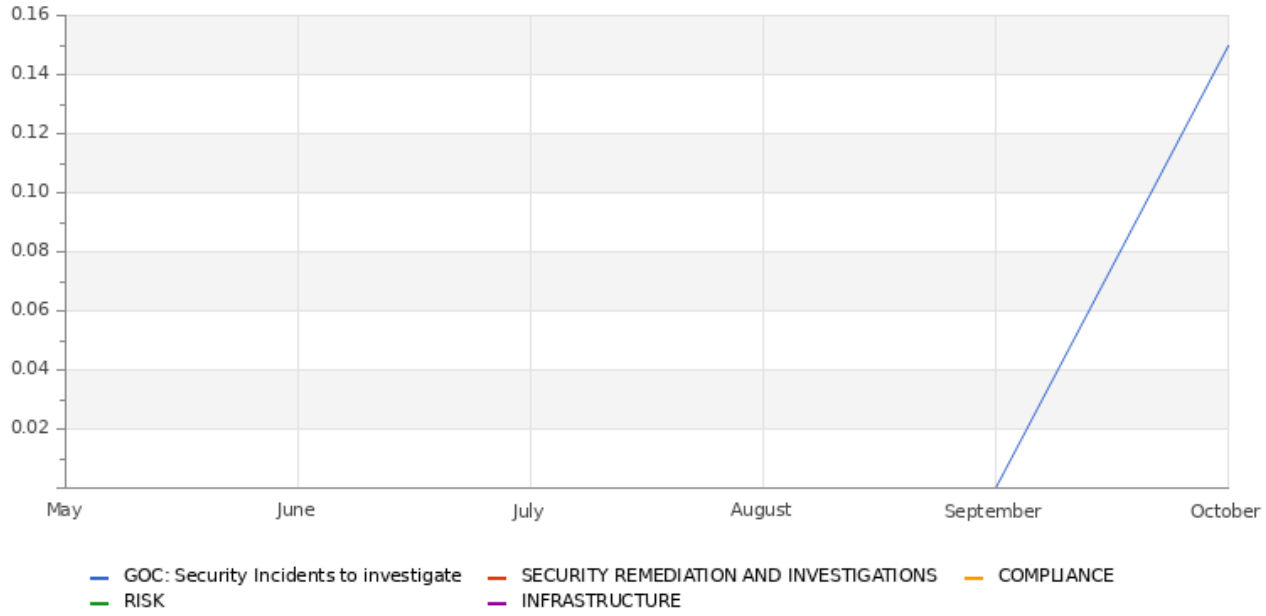
CISO EXECUTIVE REPORT

WINSOUTHCU 11/05/2026

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



©2023. GLESEC. All Rights Reserved.

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 4h 31m 8s
Verification	3d 10h 24m 54s
Prioritization and Business Relevance	0d 0h 0m 0s
GLESEC Remediation Plan	102d 1h 59m 44s
Client Security Team	158d 11h 31m 56s
Client Remediation Team	0d 0h 0m 0s

Workload

Stages	How Many #
Testing & Detection	0
Verification	0
Prioritization and Business Relevance	0
GLESEC Remediation Plan	0
Client Security Team	1
Client Remediation Team	15
Closed	74

©2023. GLESEC. All Rights Reserved. PROPRIETARY & CONFIDENTIAL
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 1m 8s
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	124

DAILYBRIEF

Active High-Severity Items

2

0

©2023. GLESEC. All Rights Reserved. PROPRIETARY & CONFIDENTIAL

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

CISO EXECUTIVE REPORT

WINSOUTHCU 11/05/2026

Executive Action Required

▲

2 items pending executive awareness or decision

Threat Relevance Score (TRS)

52

▼ -5

Risk Score (RS)

50

▼ -4

External Threat Context

Threat Headline	Relevance
OTX [APT29]: Poisoned Source: APT29 Watering Holes Targets Mobile Devices	Threat actor activity detected
OTX [DarkBlinders]: DarkBlinders: Active Espionage Campaign	Sector-relevant threat intelligence

Ongoing cases

Case #	Service	Priority	Hours	Status
42626 CASE – Linux Privilege Escalation Exposure Review – CVE-2026-46300 / Fragnesia- WINSOUTHCU	MSS-INT	High	0	Answered
48144 WinSouth Credit Union TEAR 070326	MSS-INT	High	0	Answered

Cybersecurity News

Title	Categories	Industries
mSecure password manager hack prompts password reset warnings	Cyber Attacks	Banking and Financial, Blockchain
Russian Police Arrest 3 Suspected VasyGrek Hackers, Dismantle Criminal Infrastructure	Cyber Attacks, Malware	Government, Banking and Financial, Utilities, Legal Services

©2023. GLESEC. All Rights Reserved. PROPRIETARY & CONFIDENTIAL

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

TLP:AMBER

CISO EXECUTIVE REPORT

WINSOUTHCU 11/05/2026

Title	Categories	Industries
Binance Reveals How Fake Job Interviews and AI Tool Abuse Led to $6.43 Billion Theft	Cyber Attacks, Malware	Banking and Financial, Legal Services, Blockchain
Google Warns LLMjacking Attacks Are Costing Some Enterprises Up to $1 Million in Cloud Charges	Cyber Attacks, Data Breaches, Vulnerabilities, Malware	Banking and Financial, Utilities, Pharmaceutical, Transportation, Blockchain
Hackers Exploit BTCPay Server Flaw to Steal Bitcoin and Litecoin From Hot Wallets	Cyber Attacks, Data Breaches, Vulnerabilities, Malware	Banking and Financial, Blockchain
New Wave of Refrigeration Cyberattacks Hits Supermarkets Across Europe, Forcing Stores to Pull Food	Cyber Attacks	Banking and Financial, Insurance

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.**

©2023. GLESEC. All Rights Reserved.

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.

© 2023. GLESEC. All Rights Reserved.

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