



GLE
SEC

COMPLETELY
PERCEPTIVE

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

Low

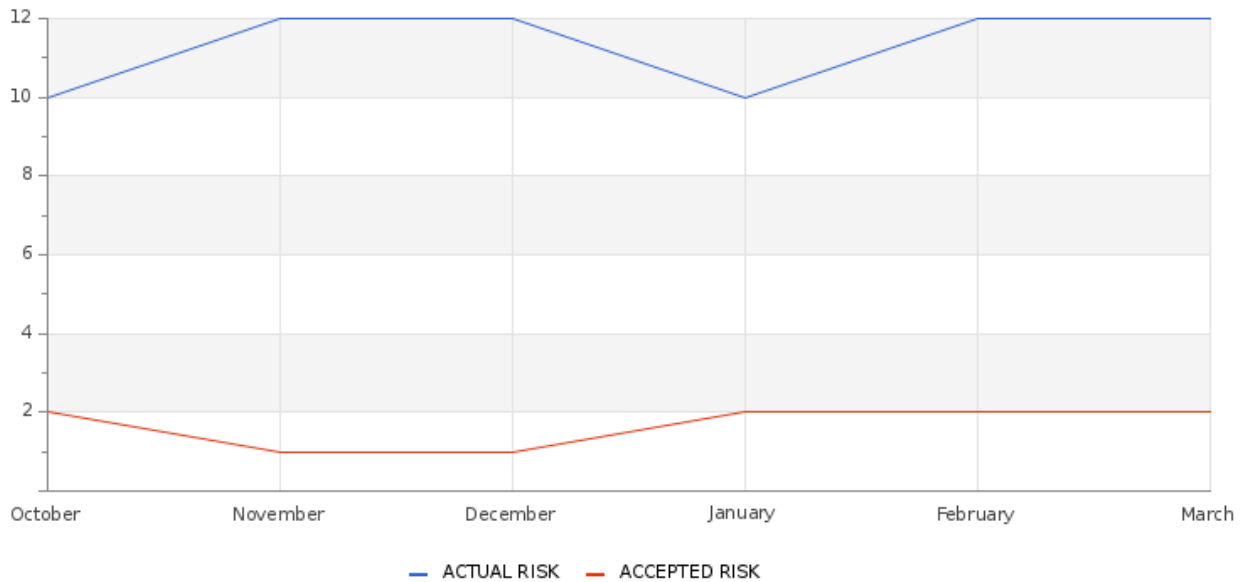
Accepted Risk

n/a

Confidence

Medium

Accepted & Actual Risk



CISO EXECUTIVE REPORT

GLESEC 03/10/2026

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

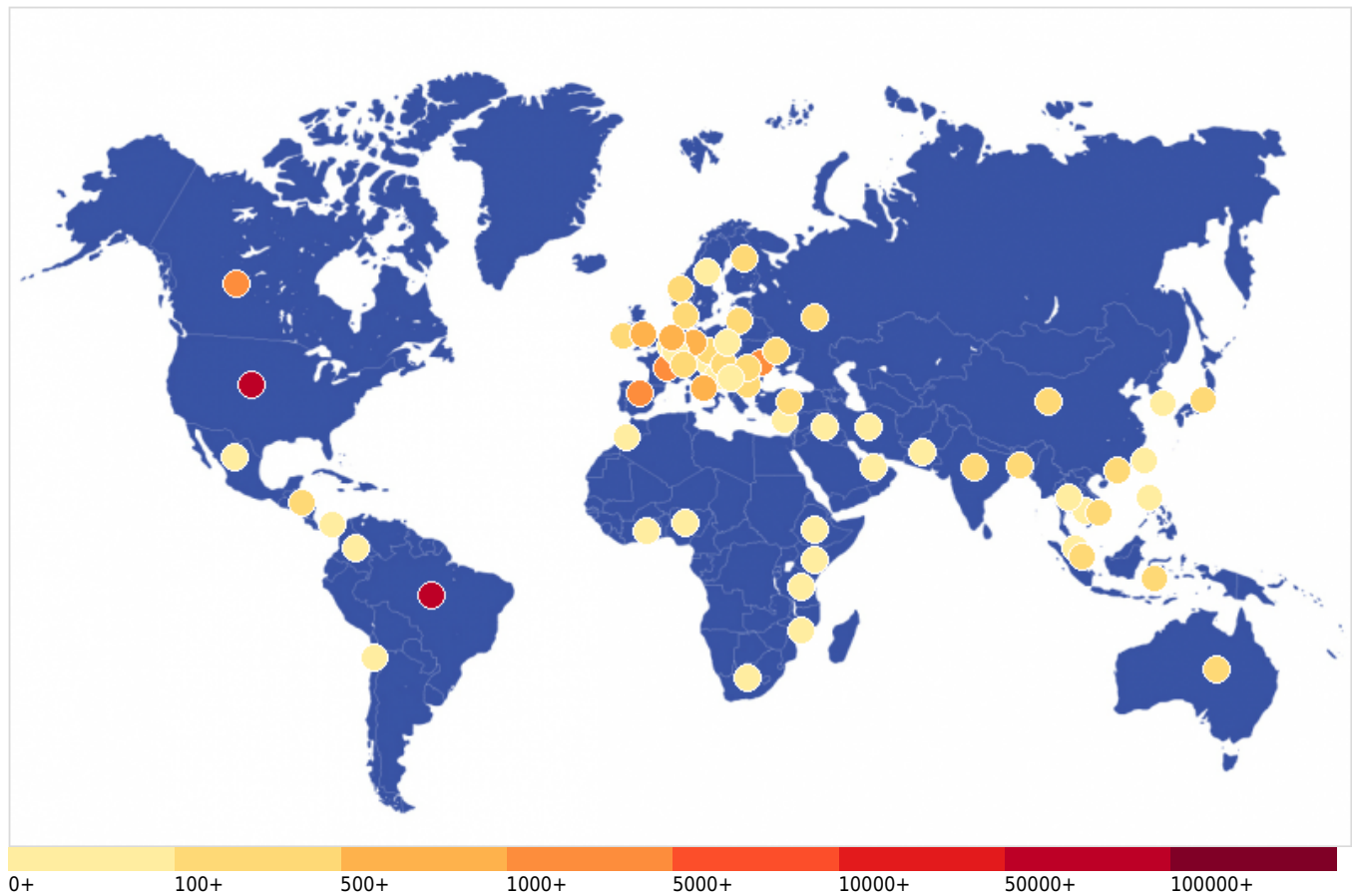
VULNERABILITY

Vulnerability Metric

11%

THREATS

Critical Attacks Per Country In Past Week

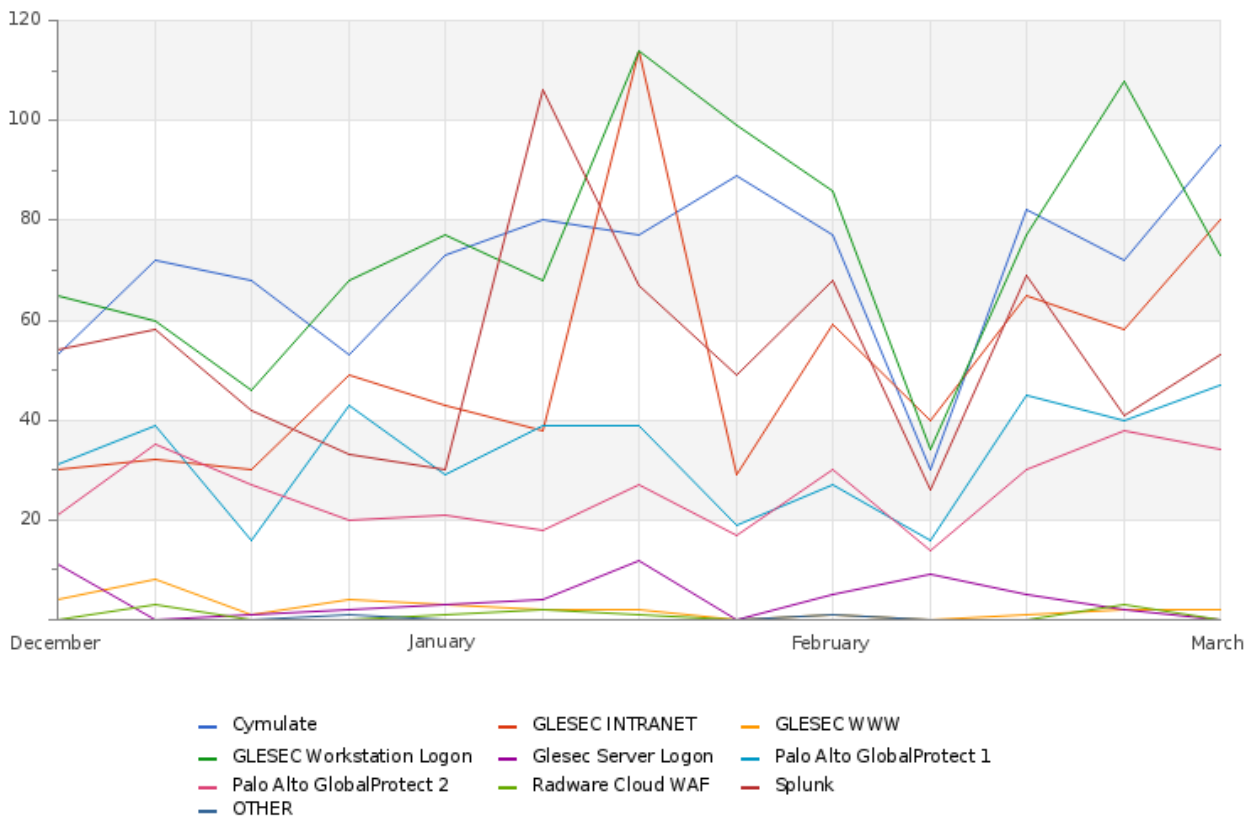


CISO EXECUTIVE REPORT

GLESEC 03/10/2026

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

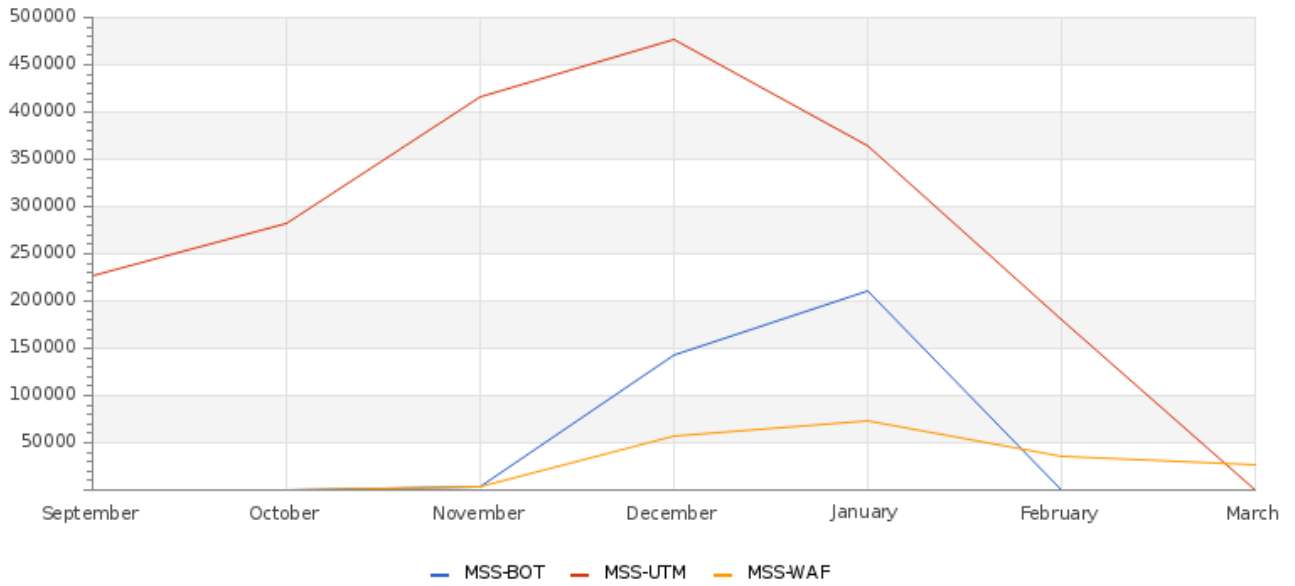
Total Number of Successful MFA authentications per application



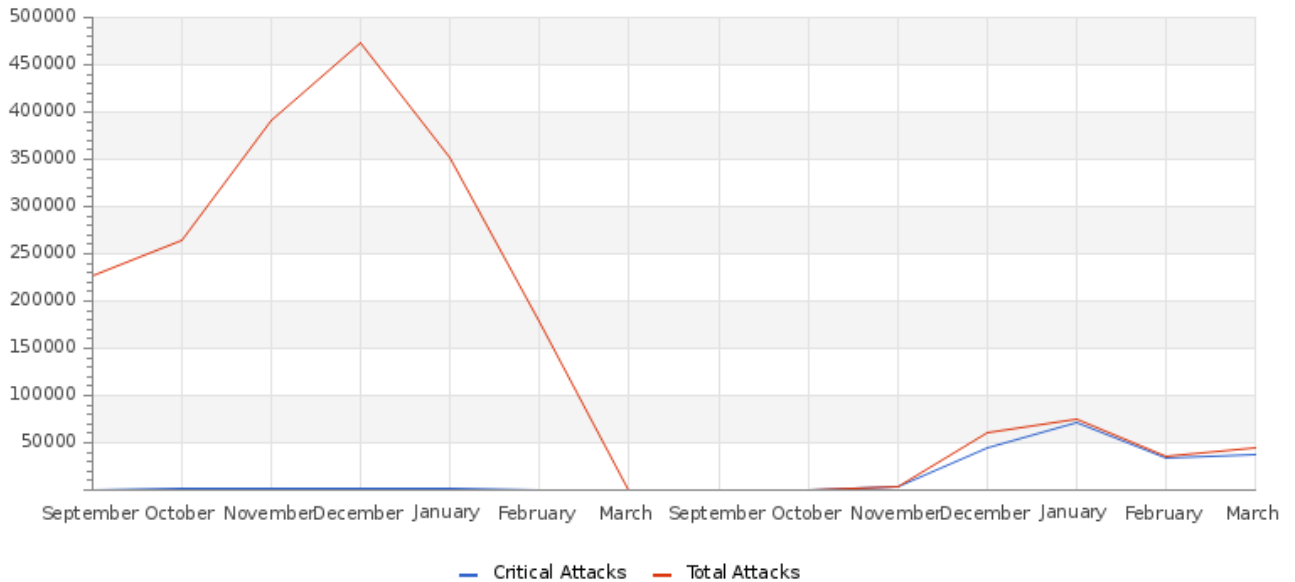
CISO EXECUTIVE REPORT

GLESEC 03/10/2026

Total Attacks Successfully Blocked Per Service



Attacks Successfully Blocked by Severity



CISO EXECUTIVE REPORT

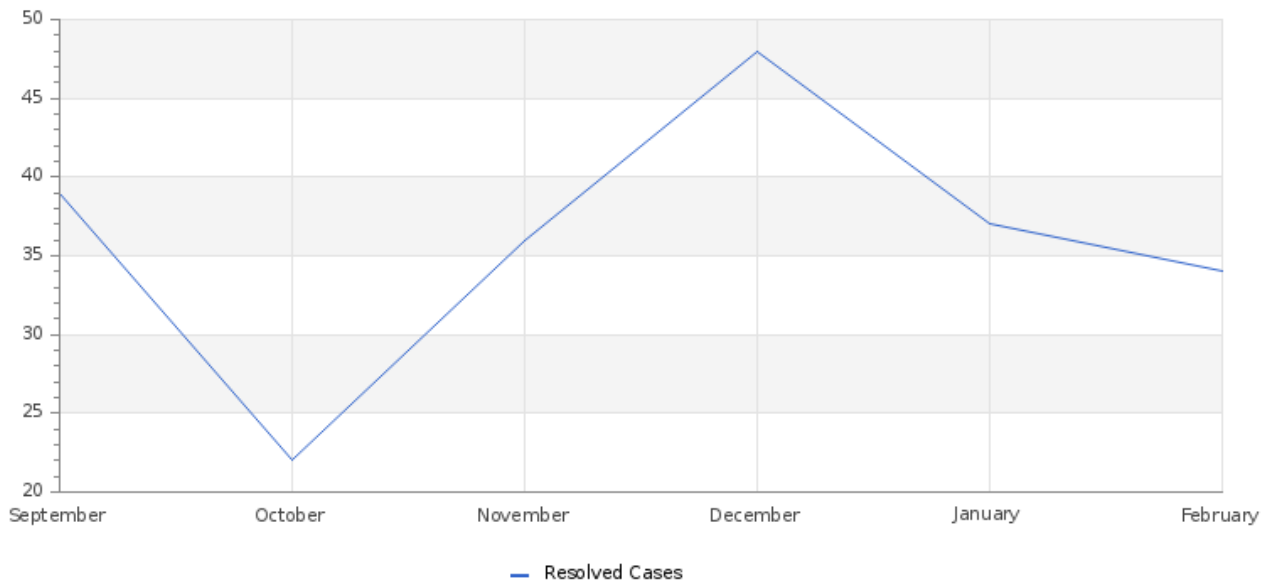
GLESEC 03/10/2026

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

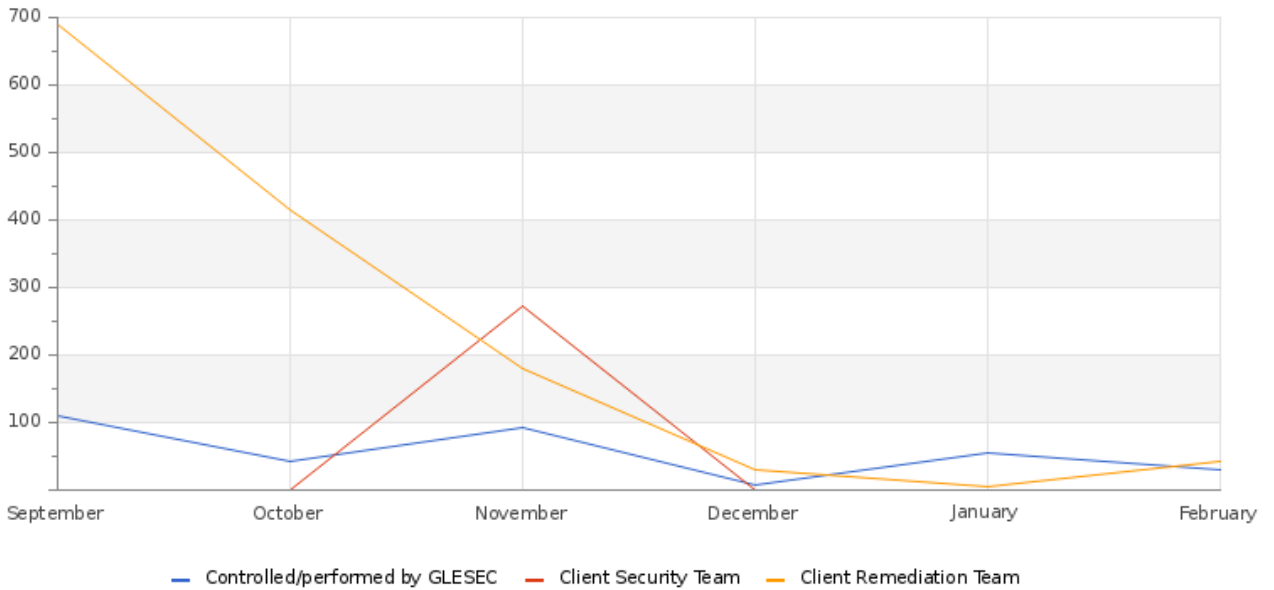
Vulnerabilities Resolved Over Time



CISO EXECUTIVE REPORT

GLESEC 03/10/2026

Vulnerabilities: Average Time to Resolve



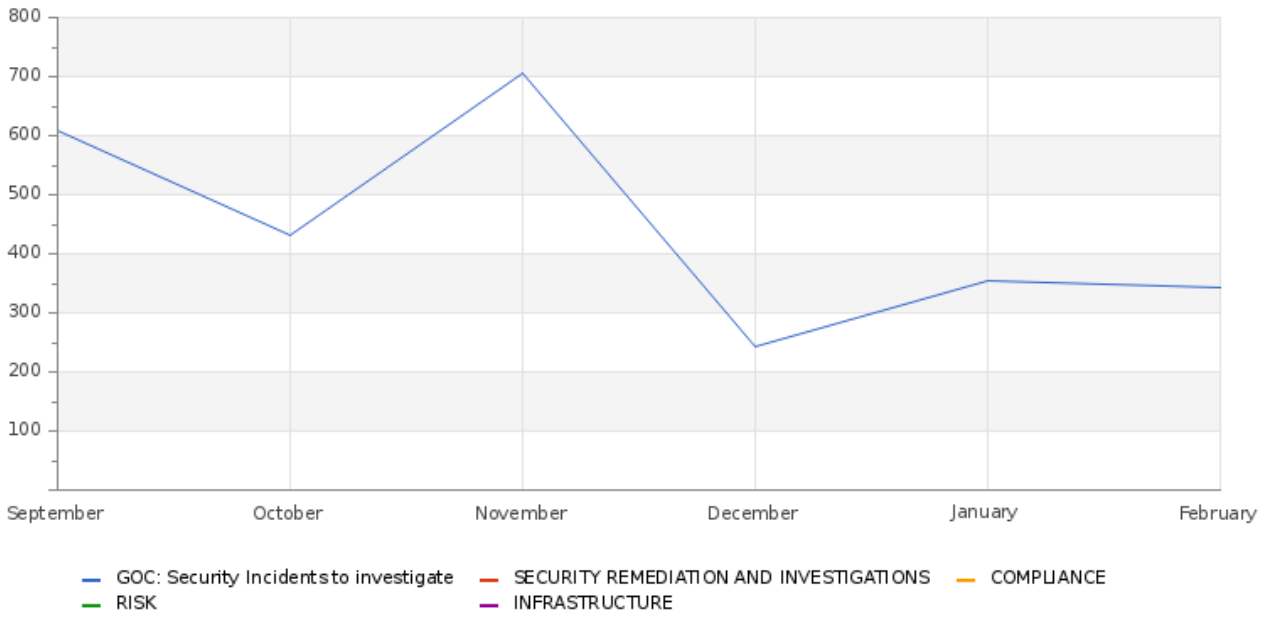
Operational Metrics per Queue Over Time

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

CISO EXECUTIVE REPORT

GLESEC 03/10/2026

Monthly Average Time per Department



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

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



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
How to Stop AI Data Leaks: A Webinar Guide to Auditing Modern Agentic Workflows	Cyber Attacks	Government
The Zero-Day Scramble is Avoidable: A Guide to Attack Surface Reduction	Cyber Attacks, Vulnerabilities, Malware	Government
APT28 Uses BEARDSHELL and COVENANT Malware to Spy on Ukrainian Military	Cyber Attacks, Data Breaches, Malware	Government, Military

CISO EXECUTIVE REPORT

GLESEC 03/10/2026

Title	Categories	Industries
Threat Actors Mass-Scan Salesforce Experience Cloud via Modified Auralnspector Tool	Cyber Attacks, Vulnerabilities, Malware	Government
Microsoft brings phishing-resistant Windows sign-ins via Entra passkeys	Cyber Attacks, Malware	Government, Military, Blockchain
New KadNap botnet hijacks ASUS routers to fuel cybercrime proxy network	Cyber Attacks, Malware	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.**



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

HOW CAN WE HELP?

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

