



GLE  
SEC

COMPLETELY  
PERCEPTIVE

**TLP:AMBER**

# CISO EXECUTIVE REPORT

GLESEC  
June 11, 2026



GLESEC 06/11/2026

# TLP AMBER CISO EXECUTIVE REPORT

This report corresponds to THIS MONTH and it is directed to Director or VP of IT, Cyber Security, Cyber Security Compliance or equivalent. The information is delivered following the GLESEC's Seven Elements Cyber Security Model (7eCSM TM), these elements are: Risk, Vulnerabilities, Threats, Assets, Compliance, Cyber Security Validation and Access

## ABOUT THIS REPORT

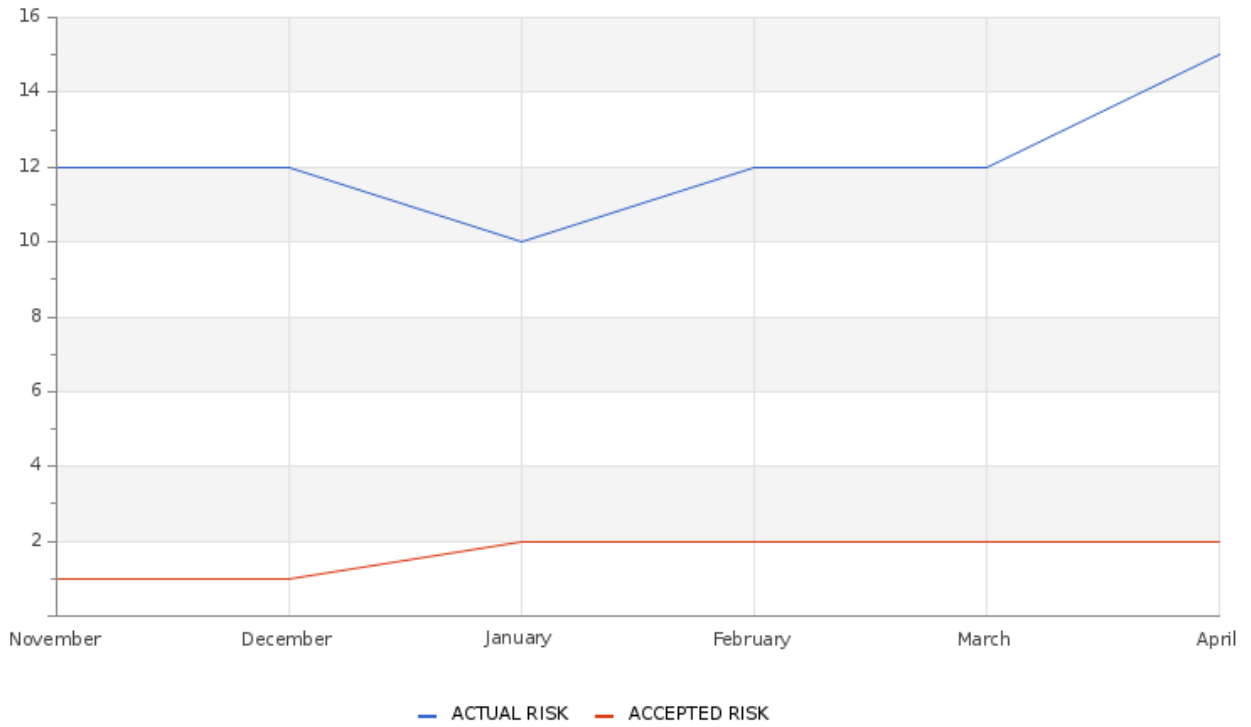
The purpose of this document is to report on the "state" of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed.

## RISK

**Actual Risk****15%****Accepted Risk****2%****Confidence****Medium**

GLESEC 06/11/2026

### Accepted & Actual Risk



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

	Current Month	Previous Month
Actual Risk	15	12
Accepted Risk	2	0

During the analyzed period, actual risk increased from 12 in the previous month to 15 in the current month, indicating a moderate rise in identified risk exposure across the environment. Accepted risk also increased from 0 to 2, reflecting a slight expansion in tolerated risk levels under the current operational context.

## VULNERABILITY

### Hosts & Vulnerable Hosts In Last 6 Months



GLESEC 06/11/2026

### Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	192.168.100.73	1
Current	0	

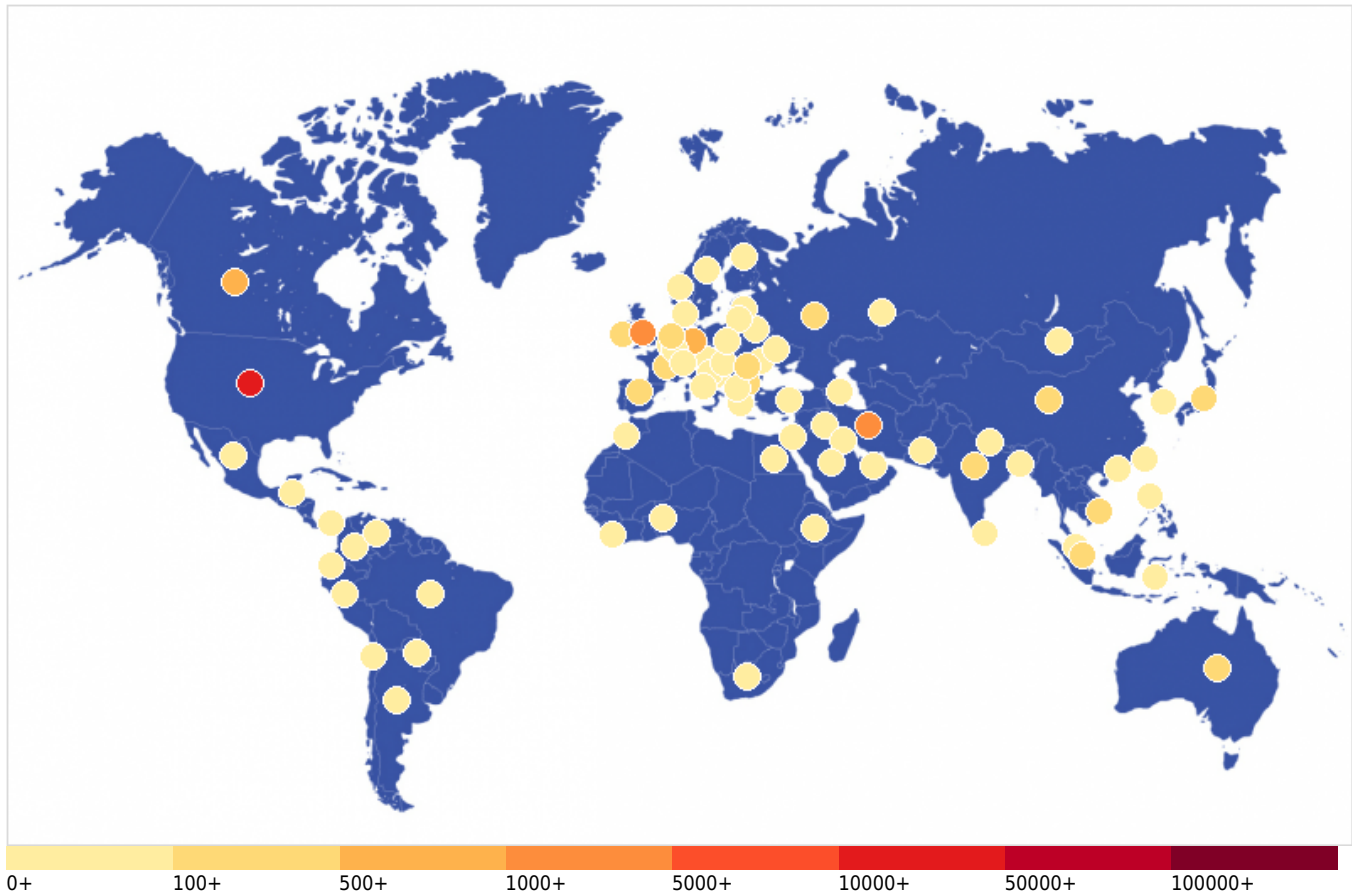
During the analyzed period, total vulnerability counts decreased from 1 in the previous month to 0 in the current month. This reflects a reduction in identified vulnerabilities across the monitored environment, with no active vulnerabilities recorded during the current reporting period.

### Vulnerability Metric

37

## THREATS

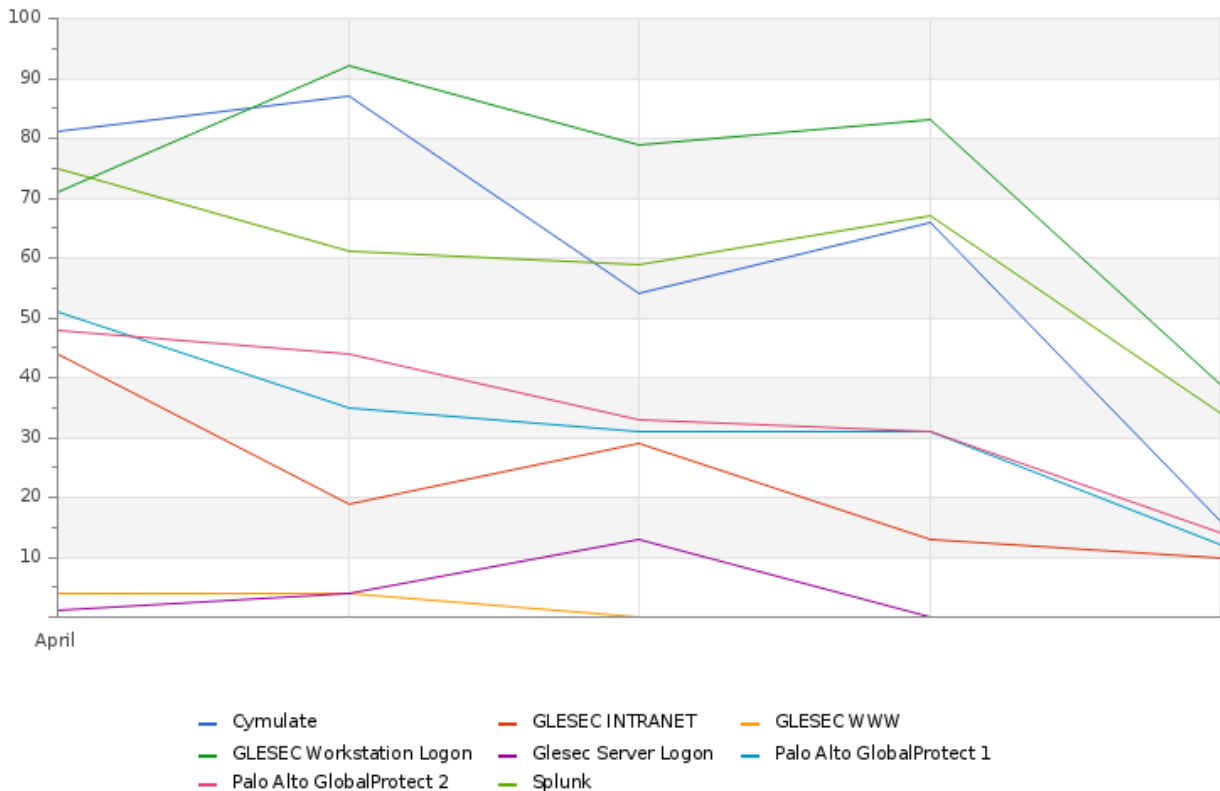
### Critical Attacks Per Country In Past Week



GLESEC 06/11/2026

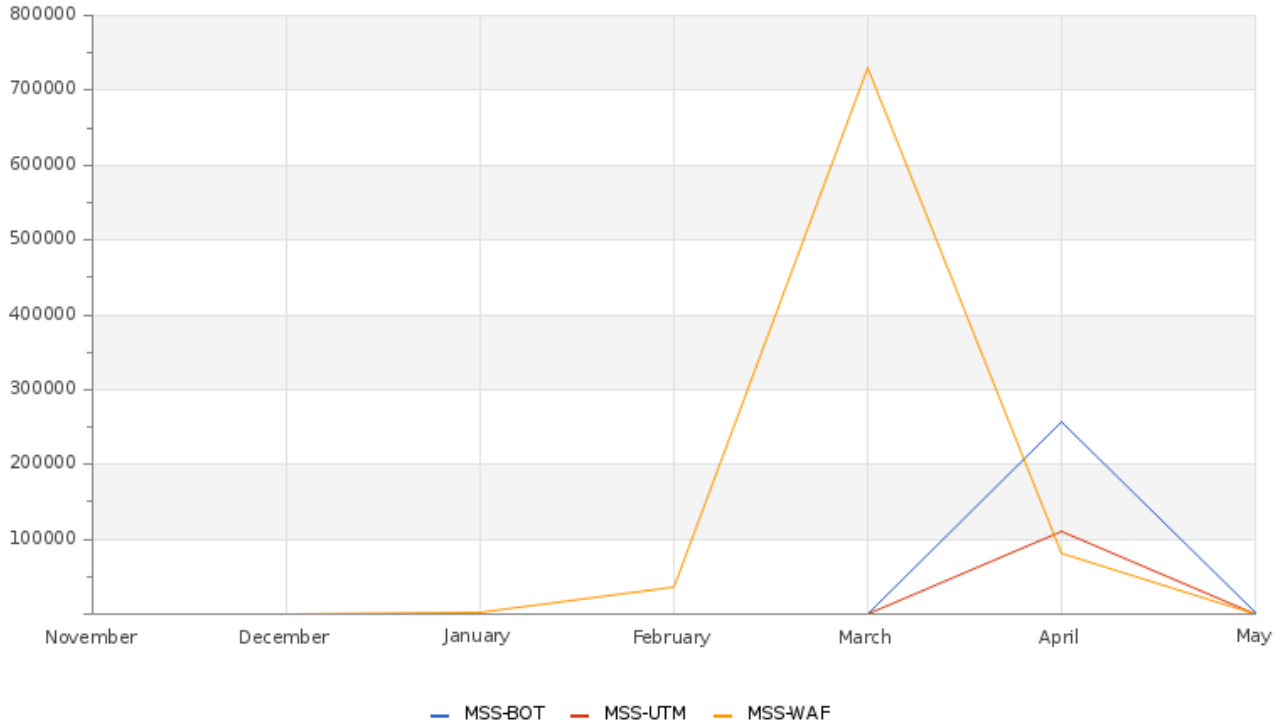
Andorra - 190	Argentina - 2	Australia - 177	Austria - 5
Azerbaijan - 2	Bangladesh - 5	Belarus - 8	Belgium - 4
Belize - 1	Benin - 2	Bosnia and Herzegovina - 9	Brazil - 86
Bulgaria - 293	Canada - 661	Chile - 5	China - 185
Colombia - 1	Croatia - 4	Denmark - 4	Ecuador - 1
Egypt - 12	Ethiopia - 3	Finland - 47	France - 137
Germany - 549	Greece - 2	Hong Kong - 67	Hungary - 48
India - 184	Indonesia - 23	Iran - 3852	Iraq - 4
Ireland - 249	Israel - 20	Italy - 59	Japan - 132
Jordan - 2	Kuwait - 8	Latvia - 2	Liberia - 55
Lithuania - 29	Luxembourg - 6	Malaysia - 12	Mexico - 36
Moldova - 1	Mongolia - 3	Morocco - 2	Nepal - 1
Netherlands - 116	New Zealand - 6	North Macedonia - 1	Norway - 1
Oman - 1	Pakistan - 7	Panama - 13	Paraguay - 1
Peru - 1	Philippines - 1	Poland - 27	Romania - 498
Russia - 441	Saint Kitts and Nevis - 38	Saudi Arabia - 53	Seychelles - 2
Singapore - 127	South Africa - 14	South Korea - 14	Spain - 406
Sri Lanka - 1	Sweden - 42	Switzerland - 21	Taiwan - 2
Turkey - 27	Ukraine - 61	United Arab Emirates - 9	United Kingdom - 1024
United States - 20436	Venezuela - 1	Vietnam - 258	

**Total Number of Successful MFA authentications per application**



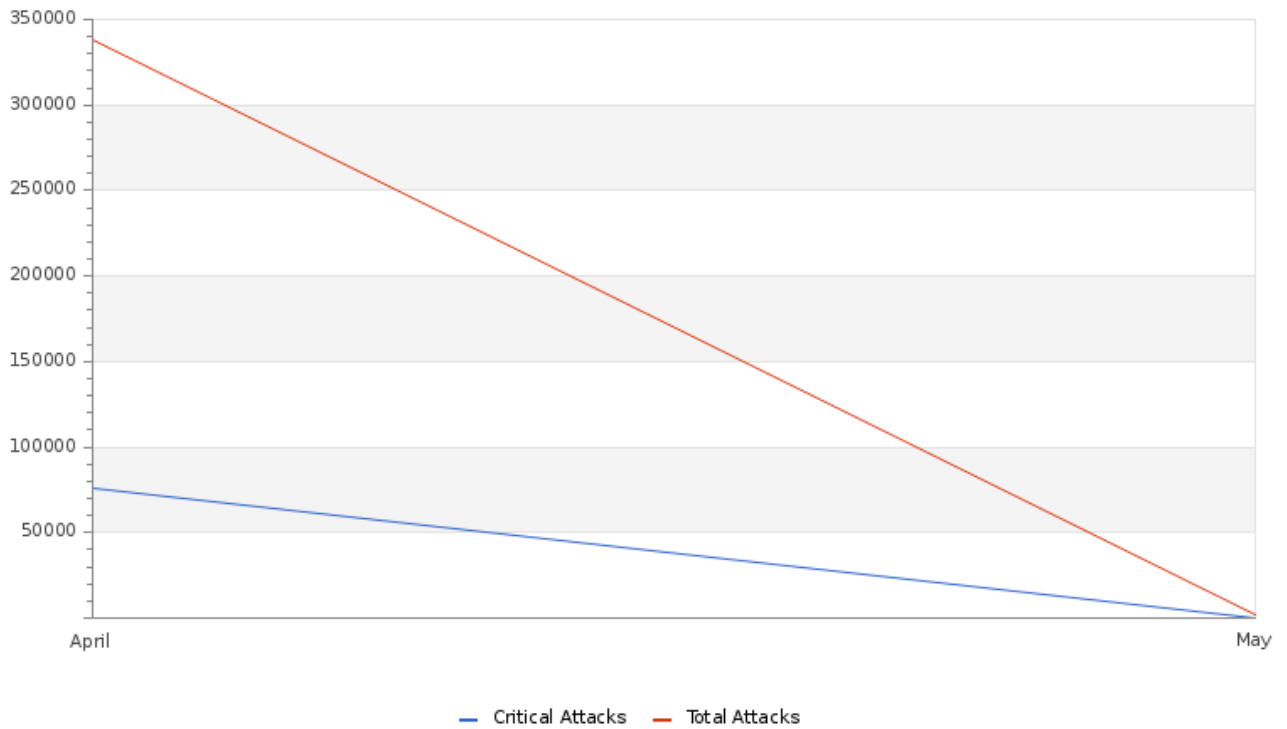
GLESEC 06/11/2026

### Total Attacks Successfully Blocked Per Service



GLESEC 06/11/2026

### Attacks Successfully Blocked by Severity



### System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	7	0
Critical Device Outages	0	0

GLESEC 06/11/2026

**Histogram of Total and Critical Device Outages**

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
DUO-PROXY-AWS-1	Pagefile Usage	GOC VPC	Warning		1955	2026-04-02 08:58:45	2026-05-01 08:54:12
Monitor-GOC1	Ping	GOC PAN	Down		558	2026-04-05 18:15:29	2026-04-28 13:20:00
goc-latam-fw.in.glesec.com	HTTPS	GOC PAN	Down		519	2026-04-18 17:37:41	2026-04-20 13:05:18
goc-latam-fw.in.glesec.com	Ping	GOC PAN	Down		519	2026-04-18 17:37:41	2026-04-20 13:05:18
Probe Device	System Health	GLESEC AWS	Down, Warning		105	2026-04-01 03:53:47	2026-05-01 03:54:14
Probe Device	System Health	Organo Judicial	Warning		30	2026-04-01 02:48:40	2026-04-30 11:19:39
SPLUNK	HTTP Advanced	Web-VPC	Down, Warning		9	2026-04-10 04:14:26	2026-04-17 23:22:25
www.glesec.com	HTTPS	Web-VPC	Warning		7	2026-04-07 18:12:43	2026-04-27 18:59:31
goc-usa-fw.glesec.com (172.28.2.65) [Linux/Unix]	Ping	GOC USA	Down		3	2026-04-01 05:04:57	2026-04-02 04:56:32
Probe Device	Probe Health	Organo Judicial	Down		2	2026-04-20 17:26:57	2026-04-21 08:26:00
goc-usa-sw.in.glesec.com	Ping	GOC USA	Down		2	2026-04-02 04:06:34	2026-04-02 04:56:34
Probe Device	Probe Health	GLESEC AWS	Down		1	2026-04-20 17:26:56	2026-04-20 17:26:56
intranet.glesec.com	HTTPS	Web-VPC	Down		1	2026-04-02 13:29:03	2026-04-02 13:29:03

**Total and Critical Attacks Successfully Blocked by Security Layer and Department**

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
296	257,404	0	0	168,730	16,898

GLESEC 06/11/2026

# OPERATIONAL

## Notable Events Active For The Last Month

Notable Event Type	How Many #
Notable Event Alert: Risk of Threats and Vulnerability Correlation Alert	394
FW Alerts	24
Change in External High or Critical Vulnerabilities	69
BAS Web Security	3
Monitoring for open ports	4
Notable Event Alert: Endpoint Configuration Management High Priority Event	32
Non Baselined Discovered System	10
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	84
Change in Systems Performance	53
Change in Systems Availability	12
High Number of Failed Authentications	5
High Persistency Detection	168
Threat Intelligence Validation	22
TEVR BAS Immediate Threats	1
Targeted Campaign Alignment	84

**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.

