TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

June 11, 2026

GLESEC 06/11/2026

TLP AMBER CISO

EXECUTIVE REPORT

This report corresponds to "May" 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%

The overall risk level increased from 12% to 15% during the current reporting period. This variation indicates a moderate rise in the organization's exposure to security threats compared to the previous month. While the risk level remains within a manageable range, the increase suggests a higher volume of detected security events or the presence of more impactful threats requiring attention. Continuous monitoring and proactive mitigation efforts remain essential to prevent further escalation and maintain the organization's security posture.

Accepted Risk

2%

The accepted risk level remained stable at 2%, indicating that the organization's risk tolerance and mitigation strategy continue to be effectively applied. The consistency of this metric suggests that identified risks are being appropriately managed and that no significant changes were required in the current risk acceptance approach.

Confidence

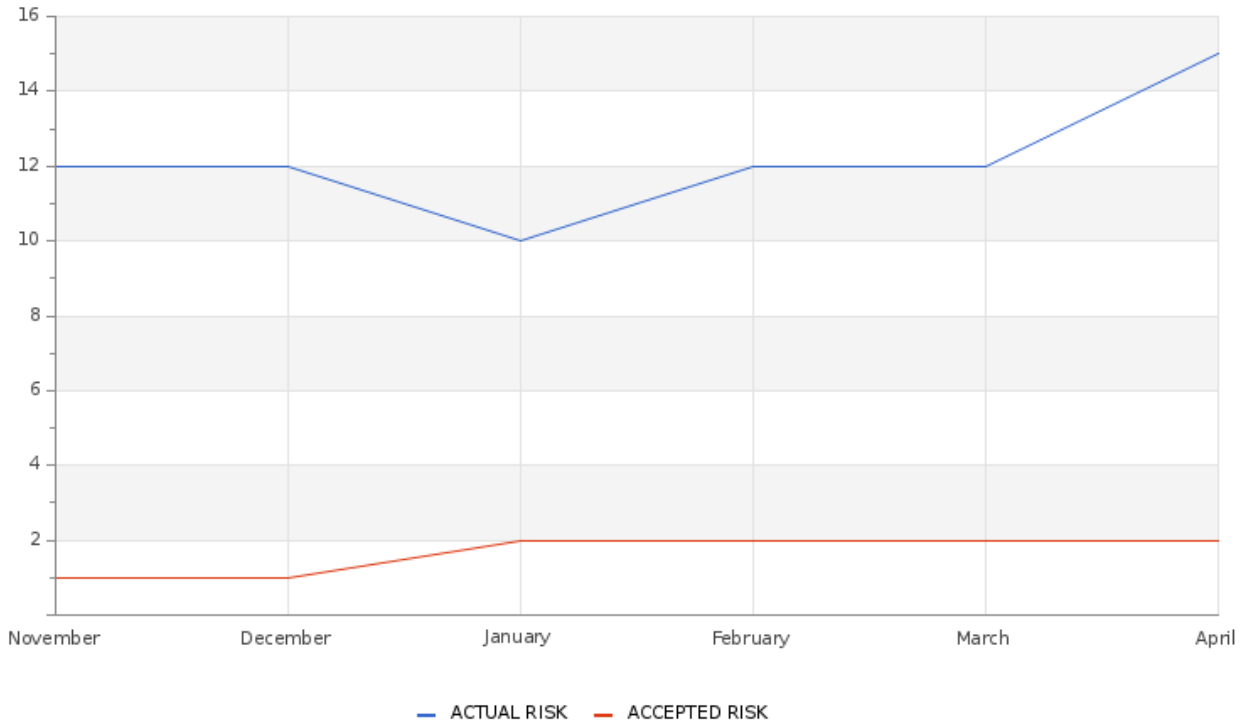
Medium

The confidence level remains Medium, reflecting the availability of sufficient information to assess the organization's overall risk posture and identify the primary threat trends observed during the reporting period. This level of confidence provides a reasonable basis for evaluating current security conditions and supporting decision-making processes.

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

GLESEC 06/11/2026

Accepted & Actual Risk



The organization's overall risk level remained relatively stable between 10% and 12% from November through March, reflecting a consistent security posture throughout most of the evaluation period. However, in April, the Actual Risk increased to 15%, representing the highest level observed during the analyzed timeframe and indicating a moderate rise in the organization's exposure to security threats. The Accepted Risk remained stable at 2% throughout the last four months of the period, demonstrating consistency in the organization's risk acceptance strategy and indicating that identified risks continue to be managed within established tolerance levels.

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.

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

GLESEC 06/11/2026

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months

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

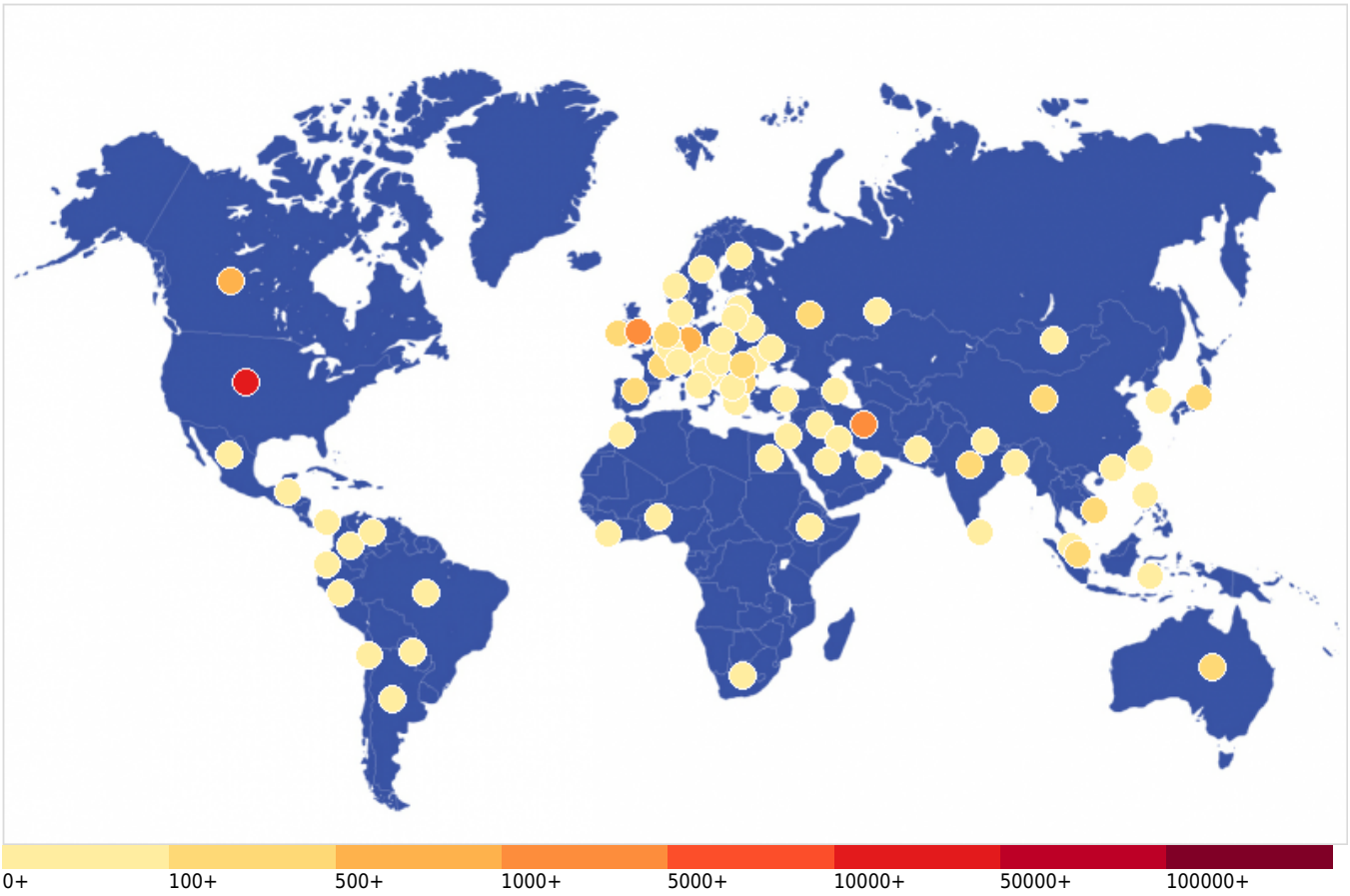
37

The Vulnerability Metric increased from 24 to 37 during the reporting period, reflecting ongoing vulnerability management and assessment activities across the environment. The identified findings continue to be tracked and managed through established remediation processes, providing visibility into areas requiring attention. This increase highlights the organization's continued focus on identifying and addressing security weaknesses. Ongoing remediation efforts and risk-based prioritization remain key to reducing exposure and maintaining a strong security posture.

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

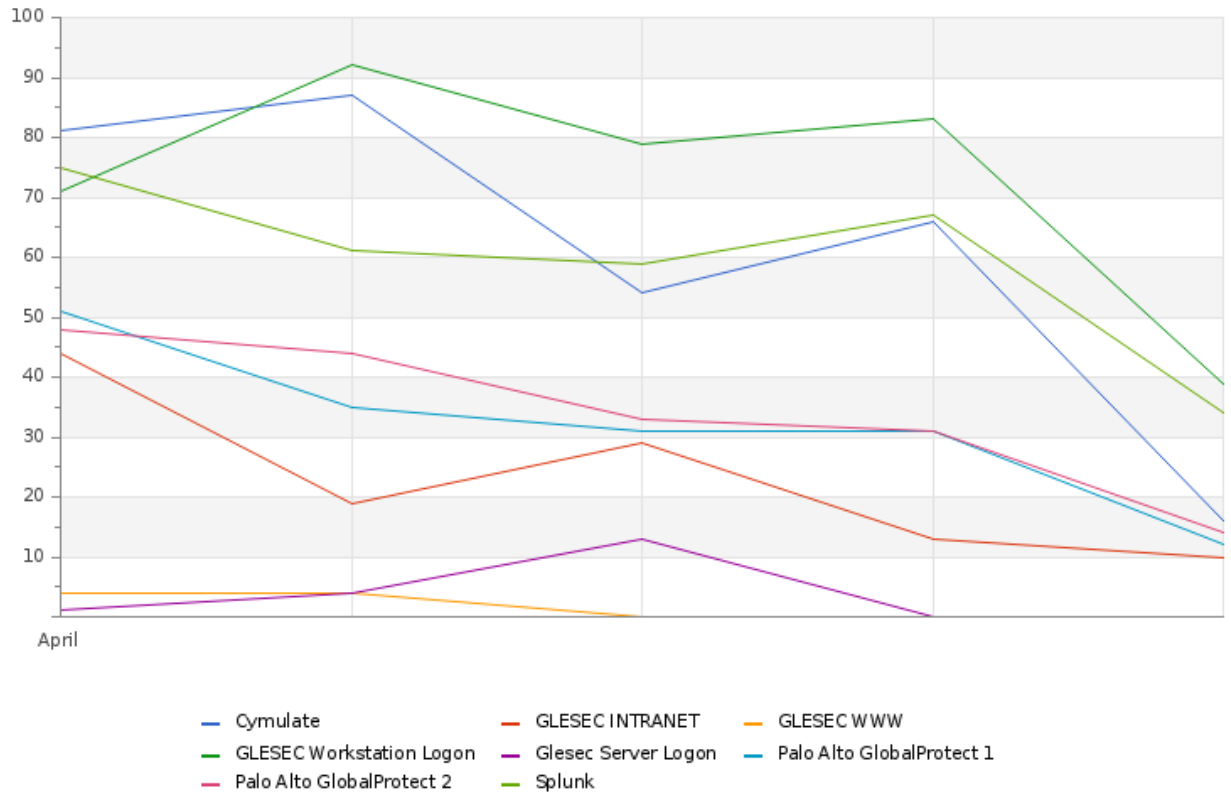
Critical attack activity continued to originate from multiple regions worldwide, demonstrating the persistent global nature of the threat landscape. During the current reporting period, the United States recorded the highest volume of critical attacks with 20,436 events, significantly exceeding all other observed sources and representing the primary contributor to

overall attack activity.

A secondary group of countries generated notable volumes of events, including the United Kingdom (1,024), Canada (661), Germany (549), Russia (441), Spain (406), and Iran (3,852). These figures indicate that attack activity remains distributed across North America, Europe, and parts of Asia, although with a stronger concentration among a limited number of countries. Compared to the previous reporting period, the geographic distribution shifted considerably. While Brazil previously represented one of the most significant sources of critical attacks, current activity is more heavily concentrated in the United States, with several European and Asian countries contributing a larger share of observed events.

Overall, the data shows that critical attack activity remains globally dispersed, but with a higher concentration among a smaller number of key source countries.

Total Number of Successful MFA authentications per application

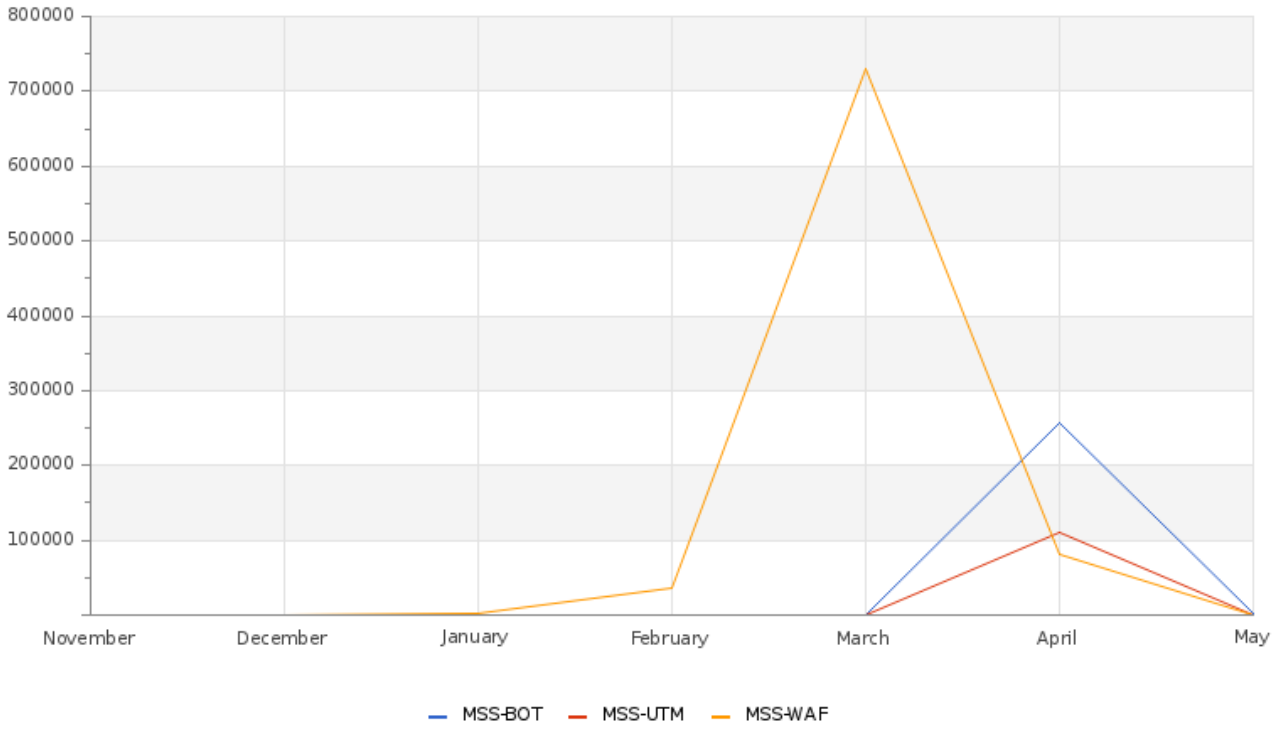


The chart shows continued MFA usage across multiple applications throughout the reporting period. While authentication levels fluctuated among platforms, overall activity remained relatively consistent during most of the observed timeframe. Several applications recorded higher authentication volumes during the first half of the period, followed by a gradual decline toward the final month. This reduction was observed across multiple platforms simultaneously, suggesting a change in overall user activity rather than an issue affecting a specific application.

Despite these variations, MFA adoption remained evident across the monitored environment, demonstrating the continued use of enhanced authentication controls to support secure access to organizational resources.

GLESEC 06/11/2026

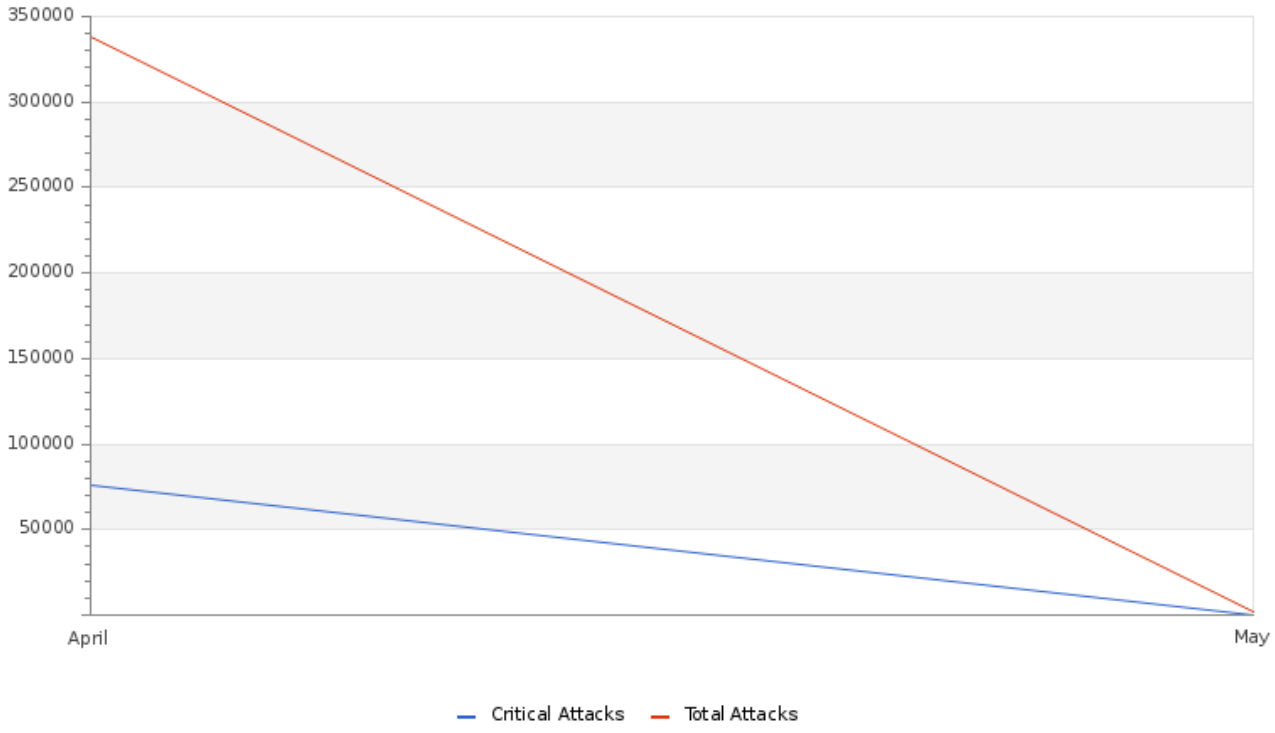
Total Attacks Successfully Blocked Per Service



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

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

During the reporting period, total device outages decreased from 12 to 7, reflecting improved system availability and operational stability. No critical outages were recorded, maintaining the positive trend observed in previous months and indicating that service continuity was preserved despite the occurrence of minor interruptions.

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

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

During the analyzed period, devices under the MSS-CSM service were continuously monitored to assess availability and connectivity status. Some fluctuations were observed, including intermittent transitions between Down and Warning states across certain devices. However, after validation and review, all affected devices were confirmed to have restored connectivity and remained operational. These events were transient in nature and did not result in sustained outages, indicating stable overall service performance

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

During the analyzed period, the organization's security services successfully blocked a total of 443,328 attacks across the monitored environment. The highest volume of prevented activity was recorded by the MSS-BOT service, followed by MSS-EDR and MSS-WAF, demonstrating the continued effectiveness of multiple security layers in detecting and mitigating malicious activity. The MSS-DDOS and MSS-DLP services did not report detected or mitigated incidents during the reporting period.

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	91
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

During the current reporting period, a total of 972 notable events were recorded across the monitored environment, representing a decrease from 1,587 events observed during the previous month. This reduction indicates a lower volume of notable security activity while maintaining visibility into key risk indicators and monitoring controls.

The most significant contributor continued to be the Notable Event Alert: Risk of Threats and Vulnerability Correlation Alert, with 394 events, followed by High Persistency Detection (168), Change in Internal High or Critical Vulnerabilities for IT, IoT and OT (91), and Targeted Campaign Alignment (84). These categories remained the primary drivers of notable event activity and continue to highlight areas requiring ongoing monitoring and risk management attention.

Overall, the distribution of notable events suggests that vulnerability-related alerts, persistent threat indicators, and targeted campaign monitoring remain the most relevant sources of security activity. The reduction in total events compared to the previous month reflects a lower overall alert volume while maintaining focus on the most significant risk indicators across the environment.

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**

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

GLESEC 06/11/2026

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