TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

June 11, 2026

GLESEC 06/11/2026

TLP AMBER CISO
EXECUTIVE REPORT

This report corresponds to April 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

12%

The overall risk level remained stable at 12% compared to the previous month. Throughout the reporting period, security events continued to be detected across different monitored services, with activity primarily concentrated in web application and network-related threats. While no significant increase in the overall risk score was observed, the persistence of malicious activity highlights the importance of maintaining continuous monitoring and timely response efforts.

Accepted Risk

2%

This reduced risk has been classified as acceptable, which reflects a strong approach to the mitigation. Suggests that, given the under tolerance threshold, risks have been managed active form instead of being accepted.

Confidence

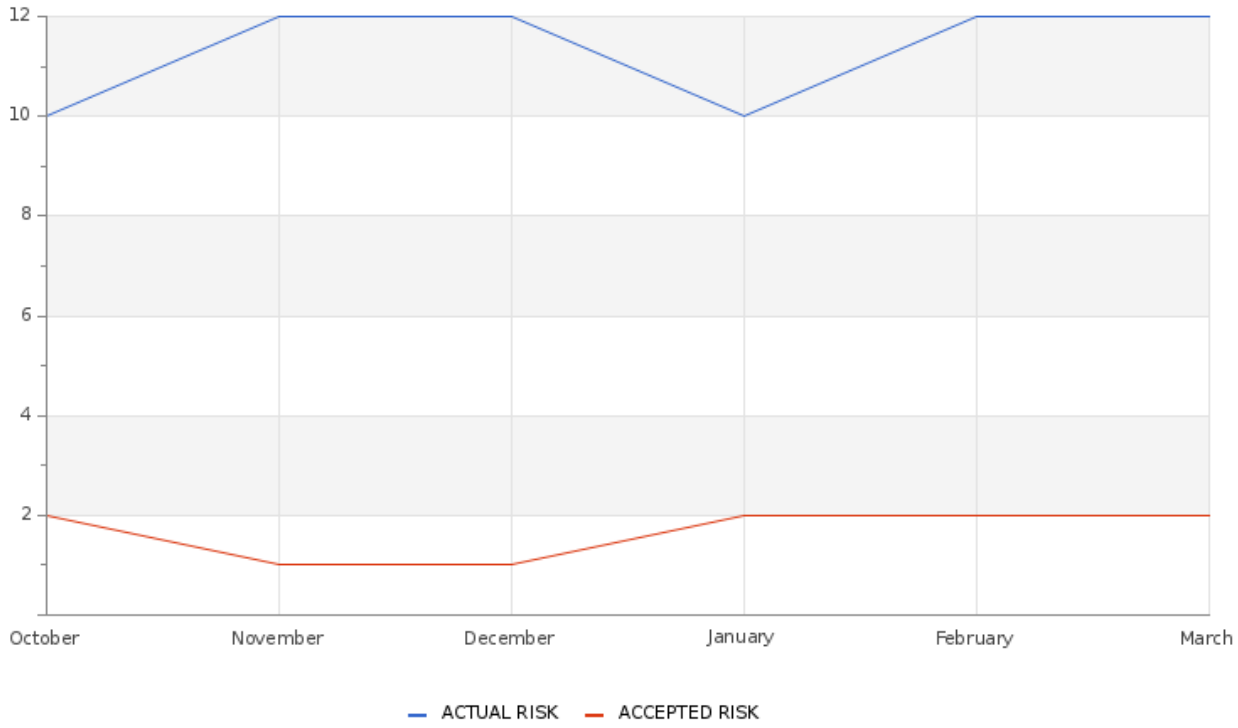
Medium

The confidence level remains Medium, indicating that sufficient information was available to assess the organization's current risk posture and identify the main threat trends observed during the month.

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

GLESEC 06/11/2026

Accepted & Actual Risk



The organization's overall risk level fluctuated between 10% and 12% during the evaluation period, remaining within a stable range without significant variations indicating relevant changes in overall exposure. Although a temporary decrease to 10% was observed in January, the indicator subsequently returned to 12%, maintaining the recurring pattern observed in previous months. Meanwhile, the accepted risk ranged between 1% and 2%, reflecting a small number of findings that have been formally accepted and continue to be monitored within the organization's risk management process.

Overall, the indicators show a stable security posture during the analyzed period. However, it is recommended to maintain continuous monitoring and review activities to promptly identify any changes in the threat landscape that could impact the organization's risk level.

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

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

The current risk remains at 12%, unchanged from the previous period. Although this value is within the levels observed on a recurring basis, it is recommended to maintain monitoring and control activities to promptly identify any changes that could impact the organization's exposure. The accepted risk currently stands at 2%, reflecting a limited number of findings that have been formally accepted and continue to be managed in accordance with the organization's established risk management process.

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

24

The vulnerability metric currently stands at 24, indicating the presence of identified vulnerabilities that continue to require attention and remediation. While the overall exposure remains at a manageable level, the findings highlight the importance of maintaining a structured vulnerability management process to reduce potential attack surfaces.

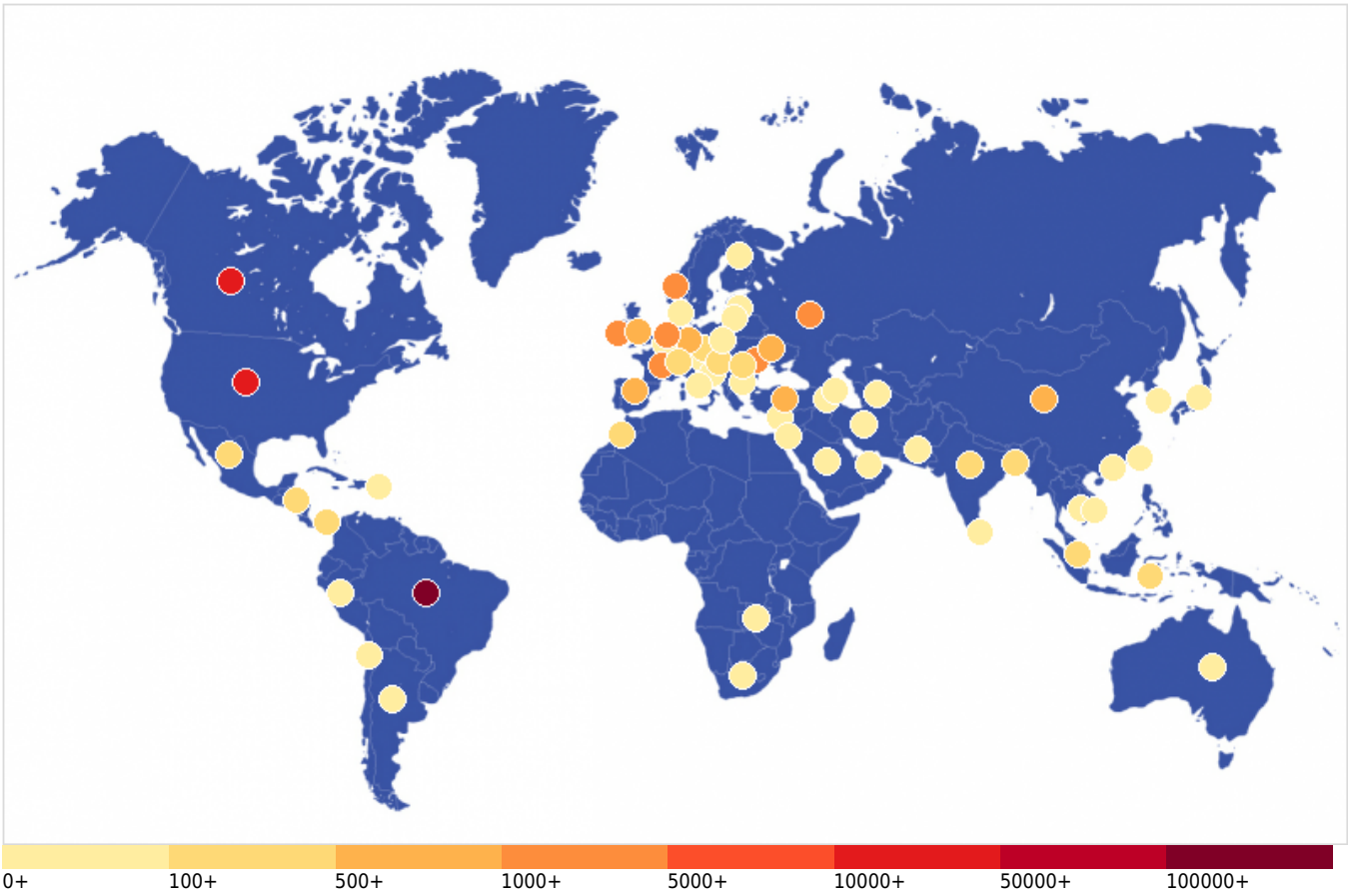
The observed vulnerabilities may include systems, applications, or services that require security updates, configuration improvements, or additional controls to mitigate potential risks. Prioritizing the remediation of high and critical vulnerabilities remains essential to minimize the likelihood of exploitation and to strengthen the organization's overall security posture.

THREATS

Critical Attacks Per Country In Past Week

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

GLESEC 06/11/2026



Andorra - 29
Austria - 2
Bosnia and Herzegovina - 8
Canada - 20885
Czechia - 153
Germany - 807
India - 318
Israel - 8
Lithuania - 6
Morocco - 109
Pakistan - 10
Puerto Rico - 3
Saudi Arabia - 2
South Korea - 55
Taiwan - 6
United Arab Emirates - 52
Zambia - 2

Argentina - 12
Azerbaijan - 4
Brazil - 117567
Chile - 12
Denmark - 3
Honduras - 172
Indonesia - 445
Italy - 79
Mauritius - 2
Netherlands - 1082
Panama - 153
Romania - 236
Seychelles - 22
Spain - 780
Turkey - 506
United Kingdom - 648

Armenia - 2
Bangladesh - 150
Bulgaria - 40
China - 696
Finland - 16
Hong Kong - 99
Iran - 17
Japan - 68
Mexico - 459
New Zealand - 35
Peru - 3
Russia - 1289
Singapore - 197
Sri Lanka - 3
Turkmenistan - 69
United States - 44847

Australia - 44
Belgium - 8
Cambodia - 3
Cyprus - 2
France - 1011
Hungary - 195
Ireland - 1006
Latvia - 4
Moldova - 1391
Norway - 1464
Poland - 93
Saint Kitts and Nevis - 70
South Africa - 4
Switzerland - 184
Ukraine - 745
Vietnam - 21

Critical attack activity was observed across multiple regions, with the highest concentration originating from the Americas, Europe, and parts of Asia. During the reporting period, Brazil recorded the highest volume of critical attacks with 117,915 events, followed by the United States with 44,847 and Canada with 20,885, highlighting a significant concentration of activity across North and South America.

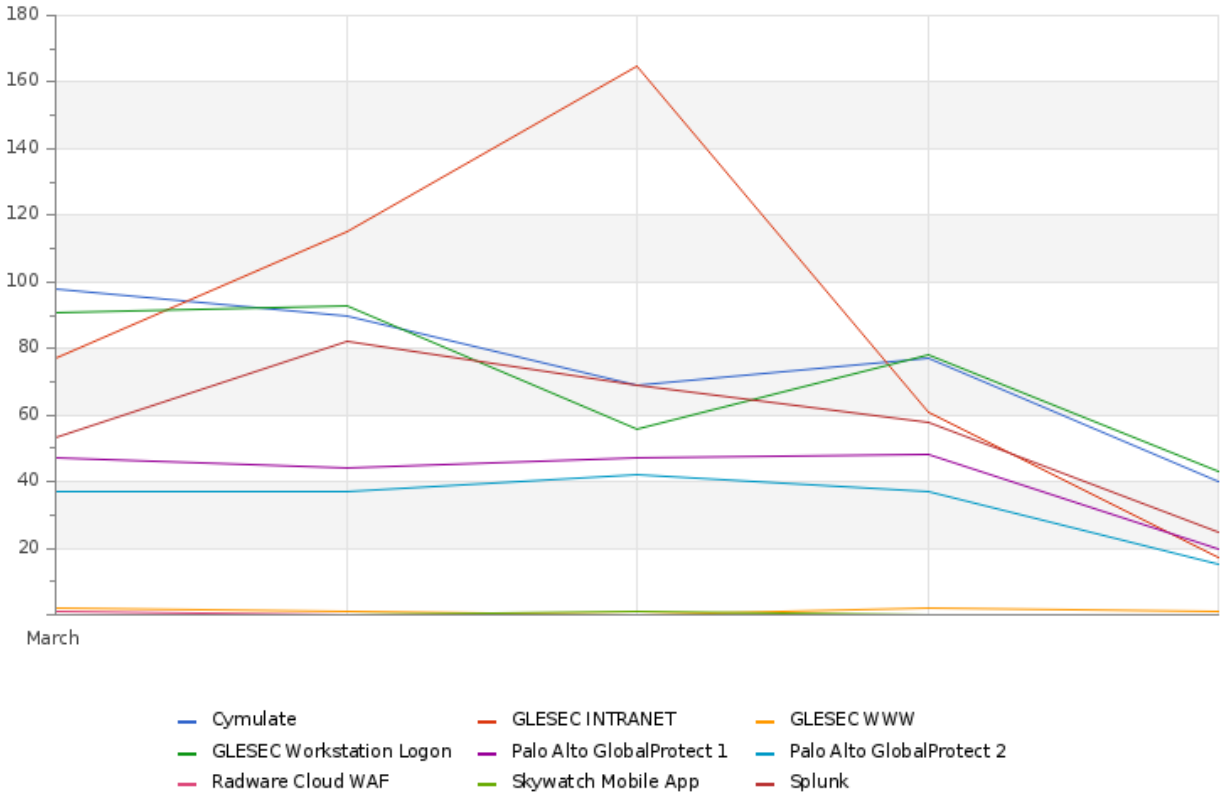
A secondary group of countries, including Moldova (1,391), Russia (1,289), Ireland (1,006), Germany (807), Ukraine (745),

and the United Kingdom (648), also contributed a notable volume of events, reflecting a broad distribution of attack sources across Europe.

Additional activity was identified in Asia and other regions, with contributions from countries such as India (318), Turkey (506), Mexico (459), Hungary (195), and Indonesia (notable regional presence). While these countries generated lower volumes than the primary sources, they demonstrate the continued geographic diversification of malicious activity.

The distribution observed during this period indicates that threat activity remains globally dispersed, although a significant proportion continues to originate from a limited number of countries with substantially higher event volumes. Maintaining geographic visibility and continuous monitoring remains essential to identify shifts in attacker behavior and support timely detection and response efforts.

Total Number of Successful MFA authentications per application

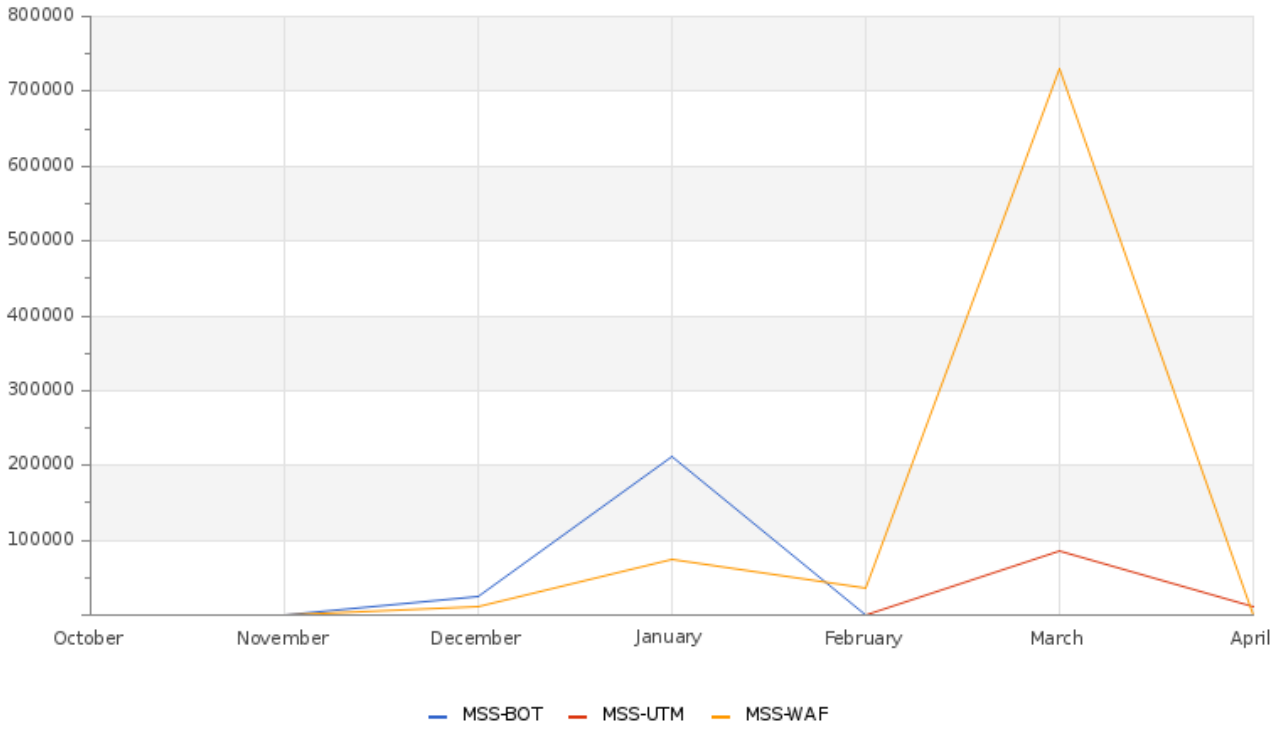


The chart illustrates login activity during March, reflecting user interaction across different platforms and the relative usage of each application within the environment. During the analyzed period, the intranet platform (Orbit) recorded a significant peak in activity, reaching approximately 165 successful authentications before experiencing a subsequent decline.

Most other applications maintained relatively stable authentication levels throughout the month. Overall, the data reflects consistent MFA adoption across the monitored environment.

GLESEC 06/11/2026

Total Attacks Successfully Blocked Per Service

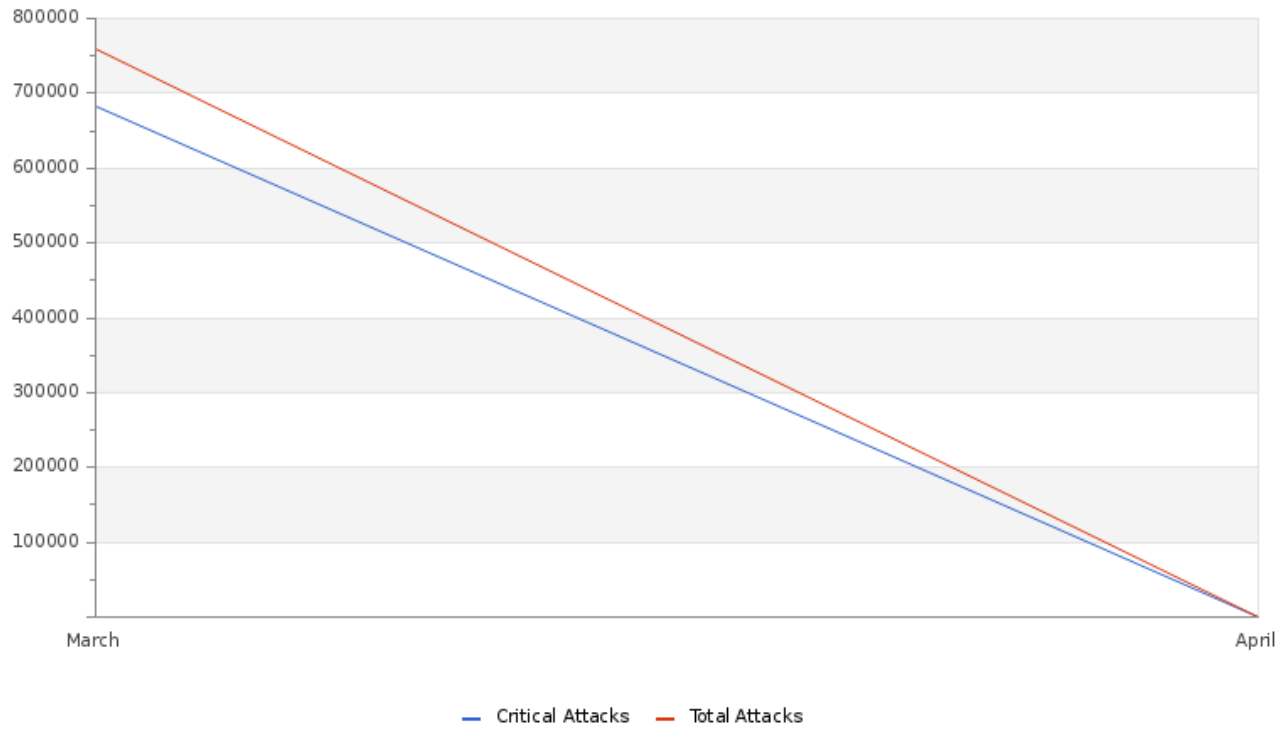


The chart illustrates login activity across the monitored period up to April, reflecting user interaction across different platforms and highlighting the relative usage and relevance of each application within the environment. Overall, the observed behavior shows consistent engagement across services, providing visibility into platform utilization trends over time.

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

GLESEC 06/11/2026

Attacks Successfully Blocked by Severity



In March, total attack activity reached a peak of 586,586 events, with 526,642 classified as critical, representing a significantly elevated level of malicious activity during the period. In contrast, April showed a notable decline, decreasing to 336,832 total attacks and 75,347 critical attacks.

This month-over-month reduction indicates a clear decrease in both overall and high-severity threat activity, suggesting an improvement in the threat landscape or the effectiveness of security controls during the later period.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	12	3
Critical Device Outages	0	0

During the current month, a total of 12 device outages were recorded, compared to 3 in the previous month. Despite this increase in total outages, no critical device outages were reported in either period. These interruptions were non-critical and did not have a significant impact on overall system performance. The absence of critical outages reflects effective monitoring and timely response actions, ensuring service continuity across the environment.

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		1538	2026-03-06 16:48:45	2026-03-30 09:38:45
Probe Device	System Health	GLESEC AWS	Down, Warning		85	2026-03-03 06:42:47	2026-04-01 03:59:47
SPLUNK	HTTP Advanced	Web-VPC	Down, Warning		74	2026-03-08 08:33:47	2026-03-27 23:42:27
Probe Device	System Health	Organo Judicial	Warning		27	2026-03-14 03:04:38	2026-04-01 03:13:40
goc-usa-fw.glesec.com (172.28.2.65) [Linux/Unix]	Ping	GOC USA	Down, Warning		20	2026-03-10 06:57:47	2026-04-01 05:04:57
goc-usa-sw.in.glesec.com	Ping	GOC USA	Down, Warning		19	2026-03-10 06:58:04	2026-03-28 13:36:34
Probe Device	System Health	Organo Judicial C-GMSA	Warning		18	2026-03-02 03:10:36	2026-03-13 04:02:38
GMSA-OJ-VM.in.glesec.com	Ping	GMSA-OJ	Down		14	2026-03-22 03:35:35	2026-03-30 13:26:35
intranet.glesec.com	HTTPS	Web-VPC	Down, Warning		11	2026-03-05 10:46:03	2026-03-26 17:43:24
Monitor-GOC1	Ping	GOC PAN	Down		9	2026-03-06 00:35:33	2026-03-31 20:16:54
Tropigas-GMSA- HyperV	Ping	Tropigas-GMSA	Down, Warning		7	2026-03-18 05:53:52	2026-03-19 20:54:27
Tropigas-GMSA- HyperV	HTTP	Tropigas-GMSA	Down		5	2026-03-19 19:24:19	2026-03-19 20:54:19
www.glesec.com	SSL Certificate Sensor	Web-VPC	Down, Warning		5	2026-03-06 06:16:38	2026-03-14 18:07:37
goc-latam-fw.in.glesec.com	HTTPS	GOC PAN	Down, Warning		4	2026-03-06 00:35:25	2026-03-31 20:16:47
goc-latam-fw.in.glesec.com	Ping	GOC PAN	Down, Warning		4	2026-03-06 00:35:33	2026-03-31 20:16:19

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.

GLESEC 06/11/2026

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
14,395	210,626	0	0	156,715	267,438

During the analyzed period, our MSS-UTM, MSS-WAF, MSS-EDR, and MSS-BOT services successfully blocked a total of 649,174 attacks. The DDoS and DLP layers reported no detected or mitigated incidents, highlighting the effectiveness of the deployed security controls and the current stability of these protection layers.

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

GLESEC 06/11/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Systems Performance	66
Threat Intelligence Detection	10
BAS Web Security	26
Monitoring Event for SPLUNK CLOUD	2
Change in Systems Availability	36
EDR Alerts	3
Internal user deleted or moved a SoftwareMine	106
BAS WAF	2
Notable Event Alert: Risk of Threats and Vulnerability Correlation Alert	718
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	85
Change in External High or Critical Vulnerabilities	249
Non Baselined Discovered System	43
Notable Event Alert: Endpoint Configuration Management High Priority Event	33
FW Alerts	24
Monitoring for open ports	4
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 last month, a total of 1,587 notable events were recorded across the monitored environment. The most significant contributor was the Notable Event Alert: Risk of Threats and Vulnerability Correlation Alert, with 718 cases, followed by Change in External High or Critical Vulnerabilities (249) and High Persistency Detection (168), indicating sustained exposure to risk and persistent suspicious activity patterns.

Other relevant categories included Internal user deleted or moved a SoftwareMine (106), Change in Internal High or Critical Vulnerabilities for IT, IoT and OT (85), and Targeted Campaign Alignment (84), reflecting both configuration changes and potential targeted threat activity across the environment.

Additional notable activity was observed in Change in Systems Performance (66) and Non Baselined Discovered System (43), while security monitoring and detection controls such as BAS Web Security (26), FW Alerts (24), and Threat Intelligence Validation (22) remained active throughout the period.

Overall, the distribution of notable events highlights a security landscape driven primarily by vulnerability correlation alerts and external exposure changes, reinforcing the importance of continuous monitoring.

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

GLESEC 06/11/2026

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