TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC

August 31, 2026

GLESEC 08/31/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

This report corresponds to March 2026 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.

Actual Risk

12%

For our "Actual Risk" section, we maintain a 12% figure, unchanged from last month (February). This follows a temporary dip to 10% in January, after which the indicator returned to and has held at 12% for two consecutive months. This pattern reflects a return to the prior risk level after a brief improvement, rather than a sustained reduction in active threats. We recommend maintaining constant vigilance to anticipate possible changes in this landscape.

Accepted Risk

2%

The accepted risk level remains stable at 2%, unchanged from last month. This follows an increase from 1% to 2% recorded between December and January, which has since held steady. This level reflects a strict threat mitigation strategy, indicating that proactive risk management continues to take precedence over risk tolerance.

Confidence

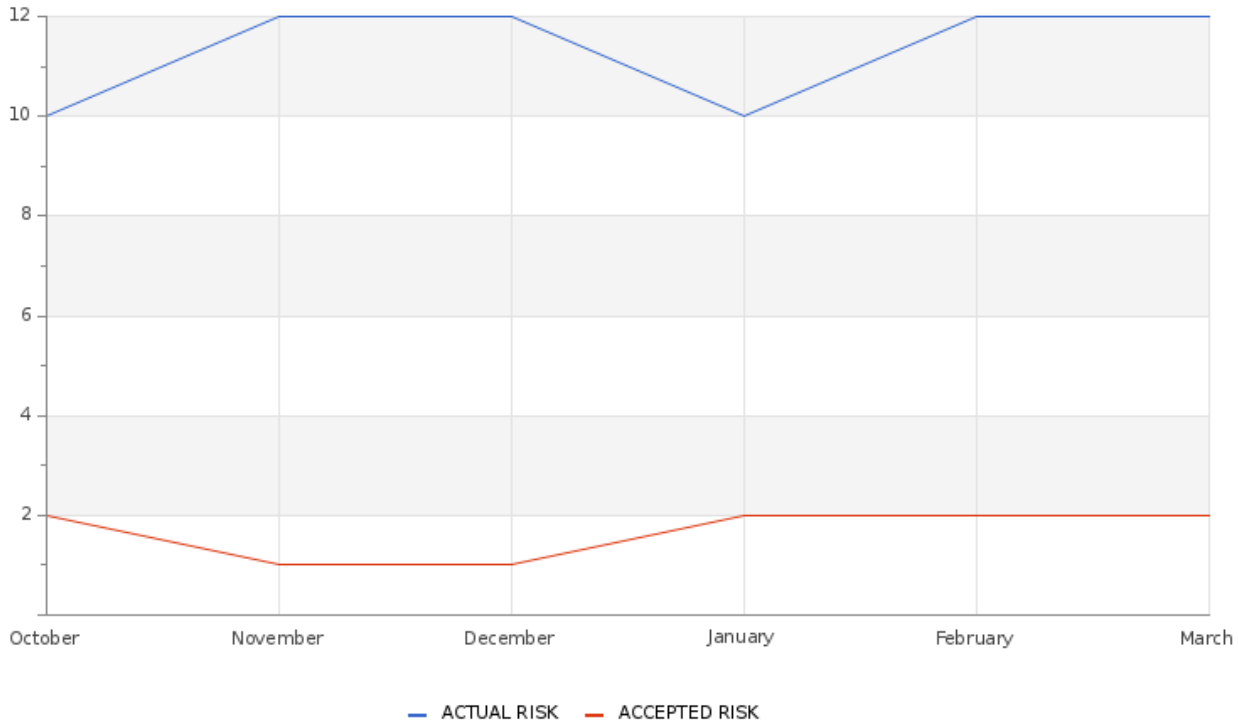
Medium

The assessment's confidence level is currently medium, as there is enough information to interpret the risks reasonably. Nevertheless, there is room to enhance the quality and clarity of the existing data, which could lead to more robust future analyses and strategic choices.

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

GLESEC 08/31/2026

Accepted & Actual Risk



The organization's overall risk level has remained at 12% compared to the previous month, reflecting general stability in the security posture. Accepted risk also remained stable at 2%, unchanged from last month; this level was reached following an increase from 1% recorded between December and January. While both indicators show short-term stability, the level of accepted risk remains elevated relative to the October–December baseline (1%–2%), which suggests the need for continuous monitoring and periodic evaluation of accepted risks to ensure they do not evolve into scenarios that compromise the organization's critical assets.

Hosts & Vulnerable Hosts In Last 6 Months

Total Attacks Successfully Blocked

964340

During the current reporting period, our security infrastructure successfully detected and mitigated 964,340 intrusion attempts targeting organizational assets. These events were neutralized through continuous real-time monitoring and the rapid deployment of countermeasures specifically engineered to address advanced persistent threats (APTs). Analysis indicates that the majority of these attempts originated from compromised IP addresses and were executed by malicious actors leveraging malware and automated attack tools. This reinforces the critical importance of proactive threat intelligence integration and adaptive defense strategies in maintaining system resilience.

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

GLESEC 08/31/2026

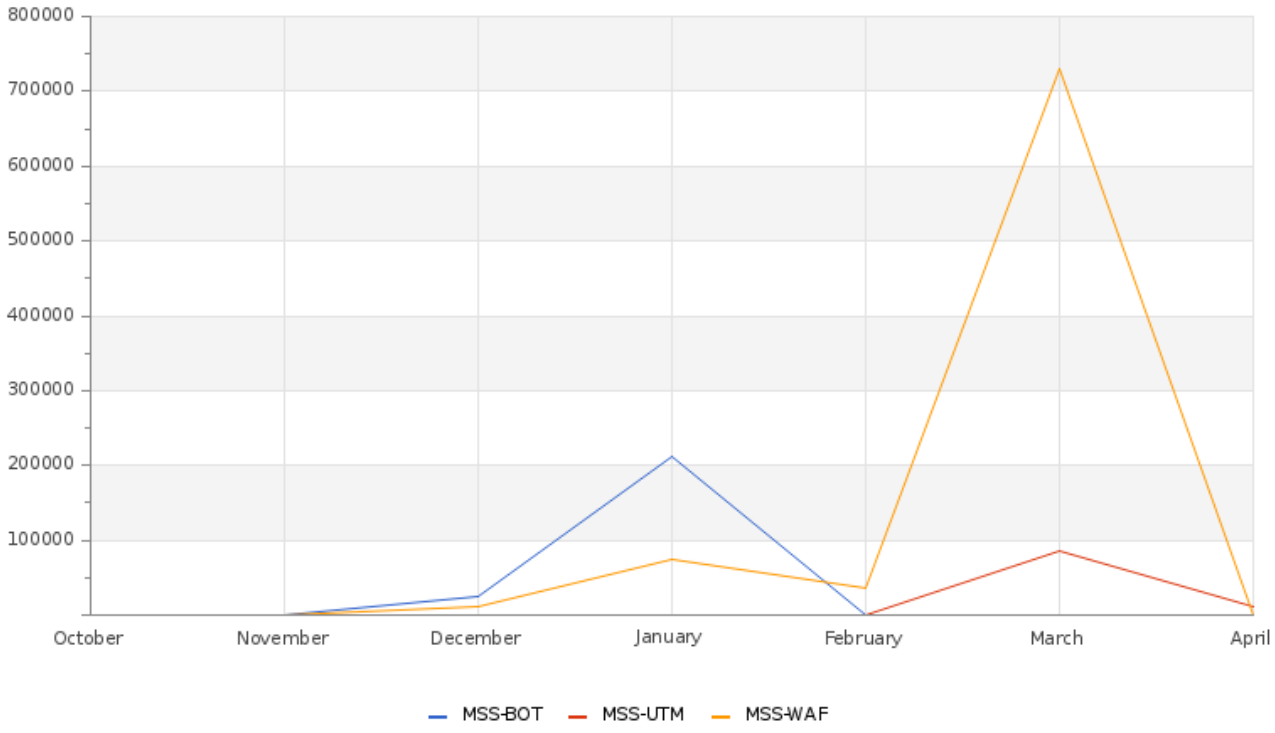
Critical Attacks Successfully Blocked

790216

Our monitoring systems recorded a total of 964,340 security incidents, of which 790,216 were classified as critical attacks and successfully blocked. These results demonstrate the high effectiveness of the security controls implemented, particularly in the detection and mitigation of high-impact threats. The proportion of critical attacks relative to the total is significant, indicating an active threat environment; however, the successful blocking of these events demonstrates the responsiveness and robustness of the preventive and containment measures adopted. It is recommended to maintain continuous monitoring and reinforce defense strategies to sustain this level of protection.

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

Attacks Successfully Blocked



Over the reporting period (October to April), attack activity remained low across all three vectors—MSS-BOT, MSS-UTM, and MSS-WAF—through October and November. A moderate increase began in December, led primarily by WAF detections.

January marked the first significant spike, driven by bot-related activity (MSS-BOT), which reached its highest volume of the entire period at approximately 210,000 blocked attempts, alongside a smaller, secondary rise in WAF and UTM detections. In February, all three vectors dropped sharply to near-baseline levels.

March saw the most significant event of the period: a major spike in web application attacks, with WAF detections reaching approximately 725,000 blocked attempts—by far the highest volume recorded across any vector or month—accompanied by a secondary increase in UTM activity. By April, all attack volumes had dropped back to near-baseline levels.

The key highlight of this period is the shift from bot-driven activity in January to a dominant, application-layer threat surge in March, with WAF as the primary vector of concern. We recommend prioritizing continued monitoring of web application traffic given the scale and recency of the March spike.

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

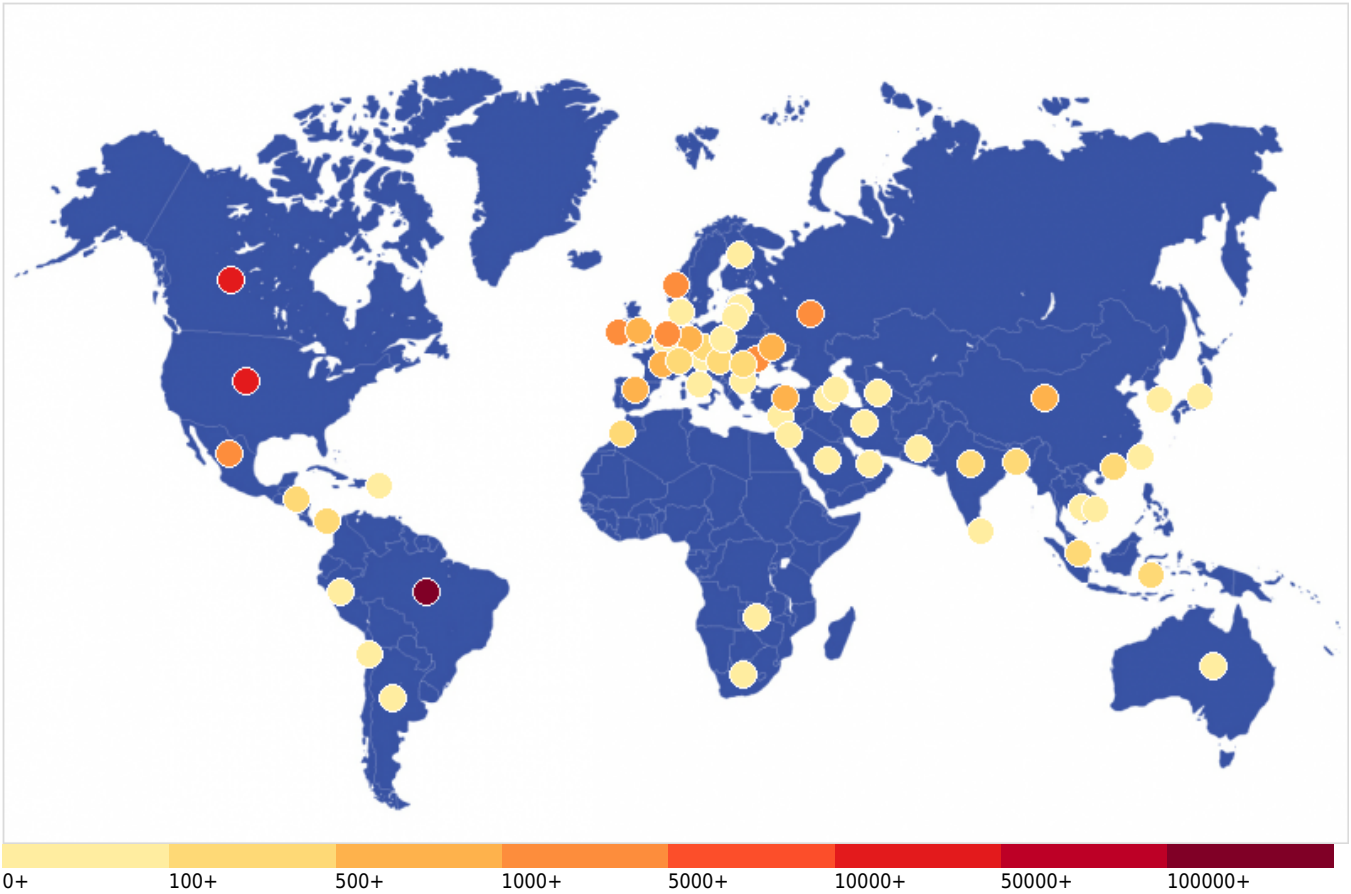
GLESEC 08/31/2026

Vulnerability Metric

24

The vulnerability indicator registered a notable decrease, dropping from 68 to 24, reflecting a reduction in the level of exposure. This improvement may be associated with the effective remediation of previously identified vulnerabilities or with a strengthening of implemented security controls. Despite this positive trend, it is crucial to maintain a focus on continuous vulnerability management, prioritizing high-criticality vulnerabilities that could pose a greater risk to the organization. Likewise, constant monitoring and validation remain essential to ensure that this reduction is sustained over time and to prevent the reappearance or exploitation of new weaknesses.

Critical Attacks Per Country In Past Week



Andorra - 29
Argentina - 19
Armenia - 2
Australia - 44
Austria - 2
Azerbaijan - 9
Bangladesh - 150
Belgium - 16
Brazil - 117915
Bulgaria - 40
Cambodia - 2
Canada - 25431
Chile - 12
China - 913
Cyprus - 2
Czechia - 155
Denmark - 3
Finland - 16
France - 579
Germany - 839
Honduras - 172
Hong Kong - 130
Hungary - 449
India - 352
Indonesia - 482
Iran - 17
Ireland - 1485
Israel - 7
Italy - 79
Japan - 89
Latvia - 4
Lithuania - 6
Mauritius - 2
Mexico - 1301
Moldova - 1391
Morocco - 188
Netherlands - 1102
New Zealand - 35
Norway - 1029
Pakistan - 11

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

GLESEC 08/31/2026

Panama - 155	Peru - 3	Poland - 93	Puerto Rico - 4
Romania - 238	Russia - 1295	Saint Kitts and Nevis - 70	Saudi Arabia - 2
Seychelles - 44	Singapore - 244	South Africa - 4	South Korea - 66
Spain - 783	Sri Lanka - 8	Switzerland - 183	Taiwan - 6
Turkey - 509	Turkmenistan - 69	Ukraine - 751	United Arab Emirates - 52
United Kingdom - 783	United States - 38515	Vietnam - 23	Zambia - 4

Critical attack activity shows a high concentration across the Americas, Europe, and, to a lesser extent, Asia. Brazil remains the leading source of malicious activity with 117,915 incidents, followed by the United States (38,515) and Canada (25,431), both maintaining a consistent and elevated presence alongside Brazil as primary contributors from the Americas.

At a secondary level, Ireland (1,485), Moldova (1,391), Mexico (1,301), Russia (1,295), the Netherlands (1,102), Norway (1,029), China (913), Germany (839), Spain (783), and the United Kingdom (783) account for a smaller but consistent share of detected attacks, reflecting broad distribution across Europe and parts of Asia.

Additional activity was observed in Ukraine (751), France (579), Turkey (509), Indonesia (482), Hungary (449), and India (352), indicating continued diversification of attack origins beyond the primary regions.

Overall, the data confirms the Americas as the dominant source region, with Brazil, the United States, and Canada consistently accounting for the highest volumes, while Europe—including a notable concentration in Eastern Europe led by Moldova—and Asia contribute a broader, more distributed pattern of activity. Maintaining geographically aware monitoring remains essential to detect shifts in attacker behavior and adapt mitigation strategies accordingly.

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

BOARDROOM 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