TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC

May 16, 2026

GLESEC 05/16/2026

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. Upon reviewing this data, we see that we have maintained this percentage since last month (February); however, there was a decrease in January, when we recorded a 10% figure. These figures suggest a reduction in the number of active threats targeting our most sensitive assets. We recommend maintaining constant vigilance in order to anticipate possible changes in this landscape.

Accepted Risk

2%

The accepted risk level has increased from 1% to 2%; this level reflects a strict threat mitigation strategy. This approach indicates that proactive risk management continues to take precedence over risk tolerance.

Confidence

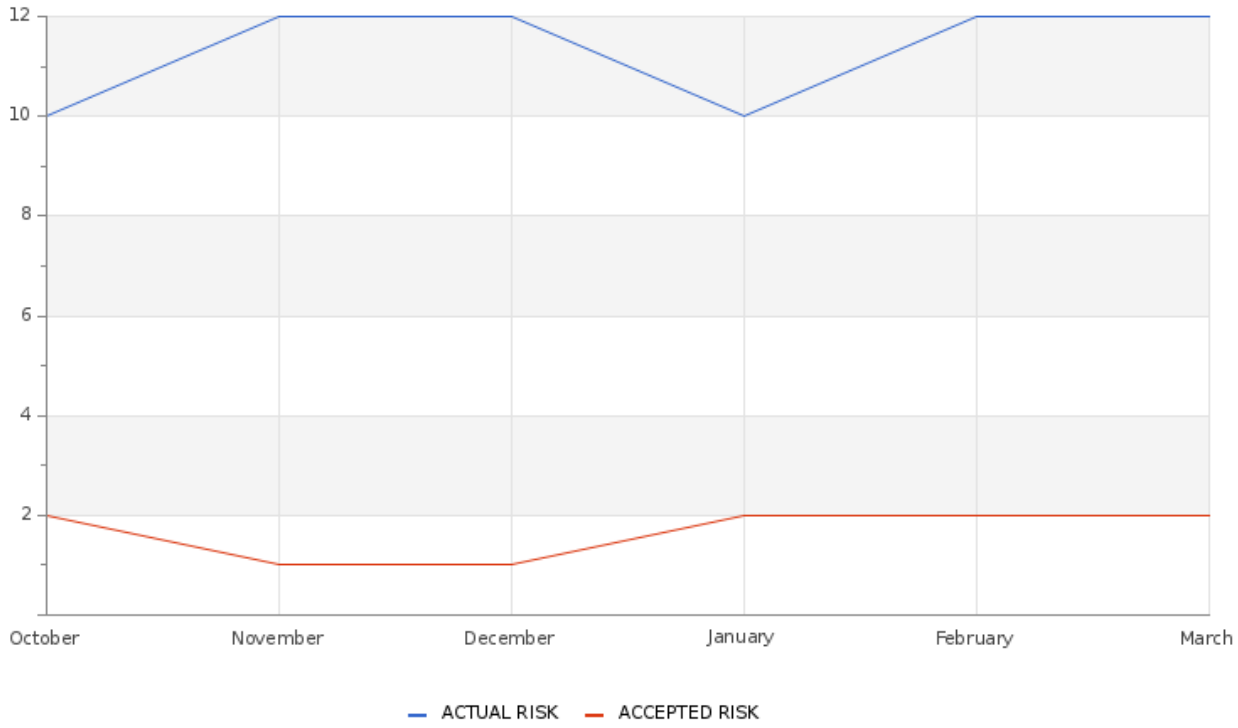
Medium

The assessment's confidence level is currently medium, as there is enough information to interpret the risks reasonably. Nevertheless, there is a 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 05/16/2026

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. However, there has been a shift in the risk composition, with accepted risk increasing from 1% last month to 2% this month. This increase reflects a higher proportion of risks that have been assessed and tolerated by the organization. While the overall level remains constant, this shift in risk distribution indicates a slightly higher potential exposure. This 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

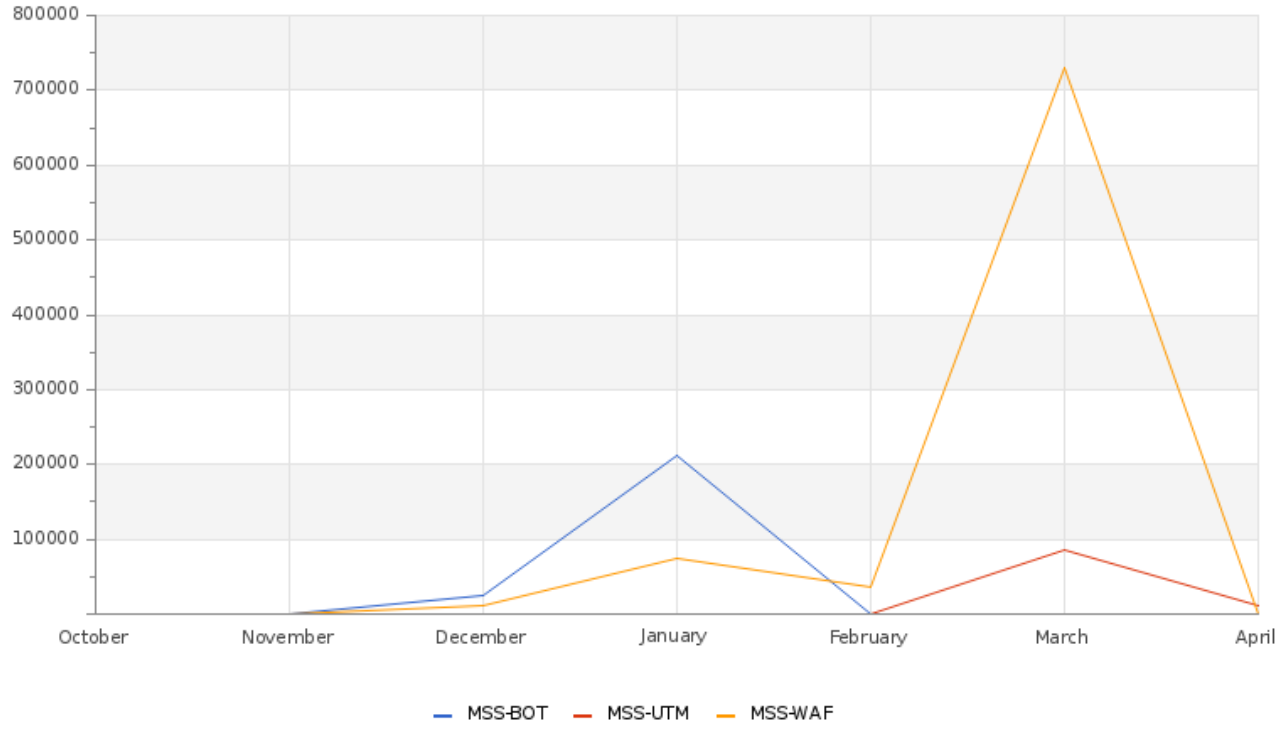
GLESEC 05/16/2026

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.

Attacks Successfully Blocked



Over the last few months, we saw a clear shift in attack patterns. Initially, most activity was concentrated at the network level through UTM, peaking in December. Starting in February, the focus moved to web application attacks, with a major spike in March driven by WAF detections. In April, we also began seeing bot-related activity for the first time. By May, all attack volumes dropped significantly, which may indicate successful mitigation or reduced threat activity. Overall, the key highlight is the transition from network-based to application-layer threats, with March being the highest risk period.

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

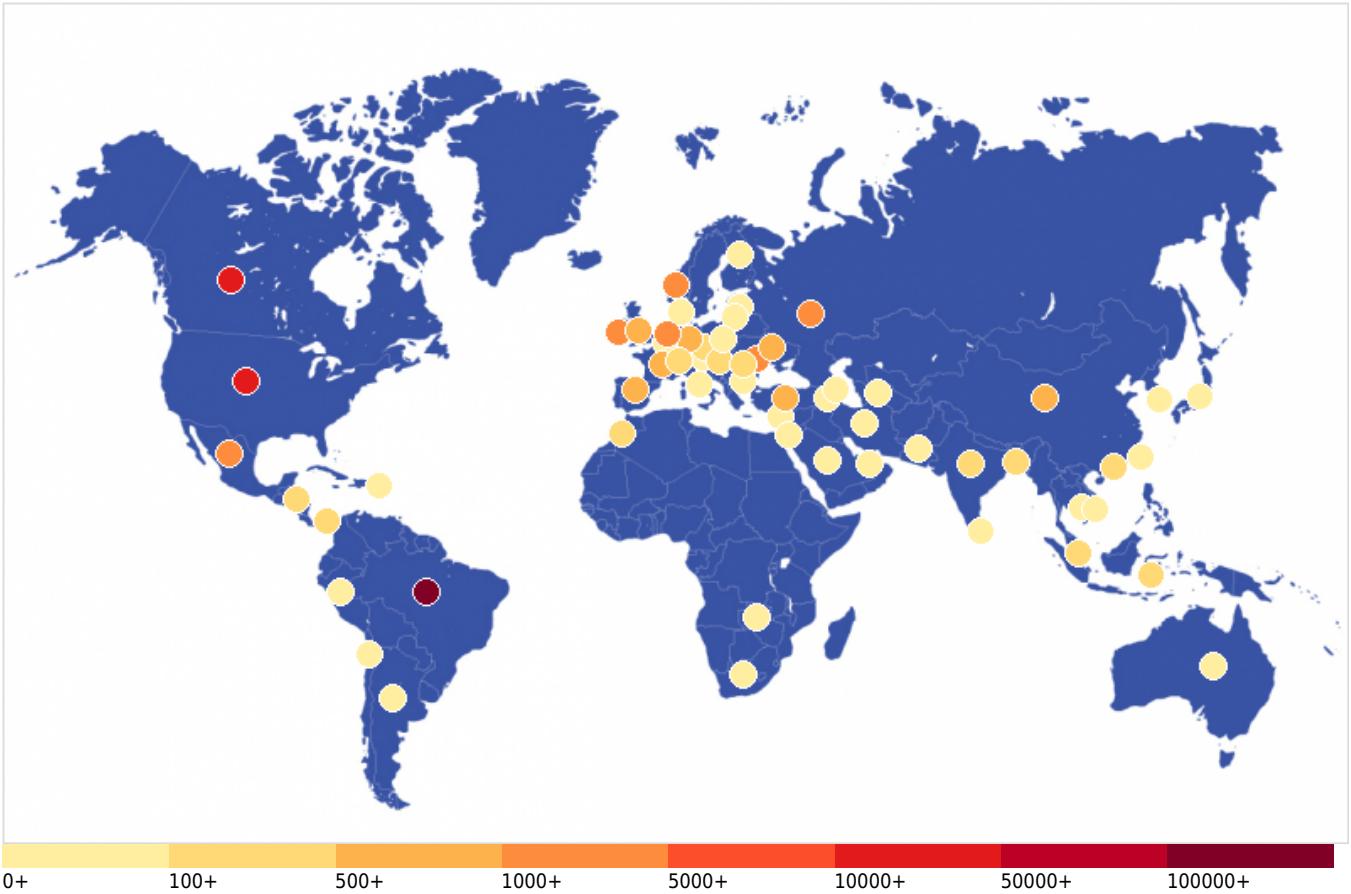
GLESEC 05/16/2026

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

GLESEC 05/16/2026

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

There is a high concentration of critical attacks originating from multiple regions, primarily Latin America, North America, and Europe, with additional activity observed across Asia.

During this period, Brazil remains the primary source of malicious activity with 117,915 incidents, followed by the United States with 38,515 and Canada with 25,431, all showing significantly higher volumes compared to other countries. This reinforces a strong concentration of activity across the Americas.

At a secondary level, countries such as Ireland (1,485), Mexico (1,301), Russia (1,295), the Netherlands (1,102), Norway (1,029), China (913), Germany (839), Spain (783), and the United Kingdom (783) maintain a relevant share of detected attacks, reflecting a broad and sustained distribution across Europe and parts of Asia.

Additional activity is observed in regions such as Eastern Europe and Asia, with contributions from Ukraine (751), Turkey (509), Indonesia (482), Hungary (449), and India (352), indicating continued diversification in attack origins.

This trend confirms a sustained dominance of the Americas—particularly Brazil, the United States, and now Canada as a key emerging source—while Europe and Asia continue to contribute with a distributed but consistent volume of activity. Compared to previous periods, the geographic distribution remains broad, though with a stronger consolidation in high-volume countries rather than isolated spikes.

This scenario underscores the importance of maintaining a comprehensive and geographically aware monitoring strategy, prioritizing regions with the highest activity while ensuring visibility across emerging sources. Continuous geographic analysis remains essential to anticipate shifts in attacker behavior and adapt detection and 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