TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC

March 20, 2026

GLESEC 03/20/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

This report corresponds to December 2025 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%

A considerable increase in overall exposure has been observed, with a rise from 10% to 12% in comparision with the previous month. This finding suggests a reduction in the number of active threats directed towards our most sensitive assets. Neverthless, it is recommended that continuous vigilance is exercised in order to anticipate potential shifts in the risk landscape.

Accepted Risk

1%

The level of risk accepted, reflecting a strict threat mitigation strategy. This approach indicates that proactive risk management continues to be prioritized over risk tolerance.

Confidence

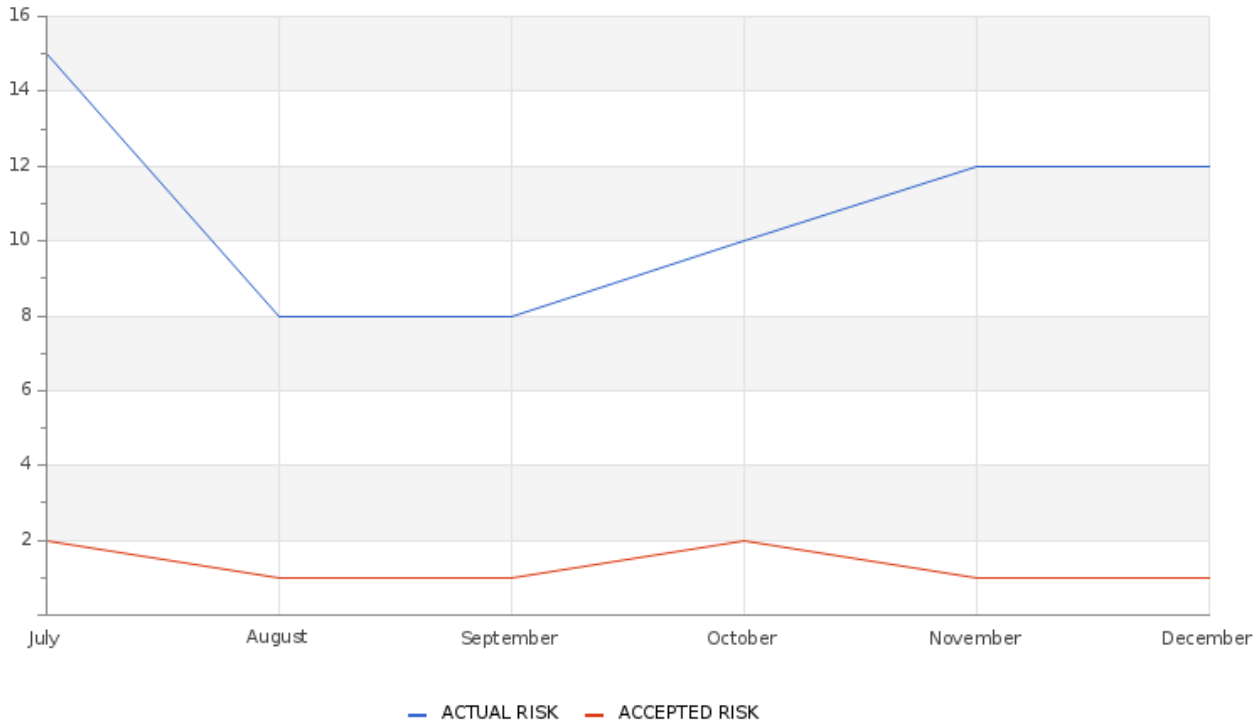
Medium

The assessment's confidence level is currently medium, as there is enough information to interpret therisks 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 03/20/2026

Accepted & Actual Risk

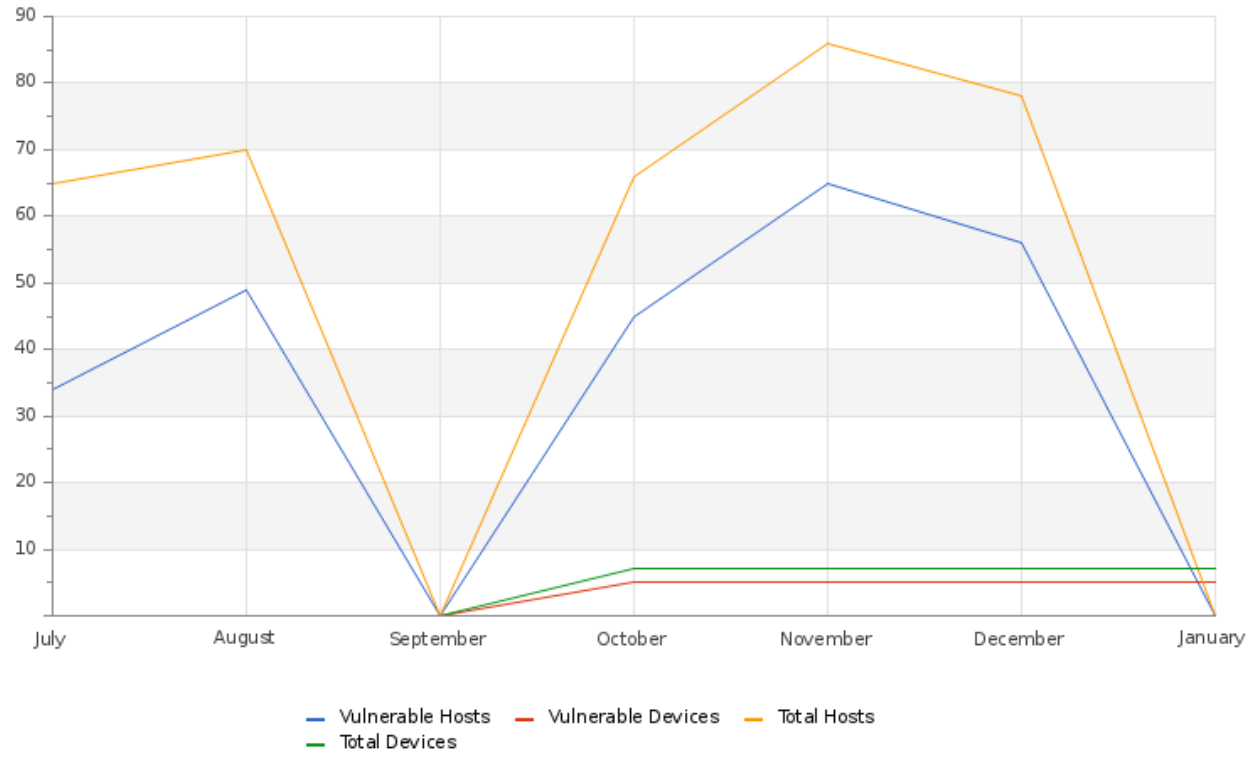


The organization's overall risk level has remained at 12% compared to last month, reflecting increased exposure, as has accepted risk, which remained at 1%, underscoring the ongoing commitment to strict mitigation and proactive risk management. This indicates a significant increase in overall exposure, suggesting a low probability of threats compromising critical assets. Continuous monitoring is recommended to stay abreast of any potential changes.

Hosts & Vulnerable Hosts In Last 6 Months

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

GLESEC 03/20/2026



In December, the number of hosts decrease from 85 to 75, while vulnerable hosts rose from 65 to 55. The most frequently identified vulnerabilities included:
- SSL Certificate Cannot Be Trusted
- SSL Self-Signed Certificate
- ICMP Timestamp Request Remote Date Disclosure
- SQLite < 3.50.2 Memory Corruption
- SQLite 3.44.0 < 3.49.1 Multiple Vulnerabilities
- SSL Certificate Expiry
- Veeam Agent for Microsoft Windows 6.x < 6.3.2.1205 Privilege Escalation (CVE-2025-24287)
- libcurl 7.17.0 < 8.18.0 Security Bypass.
- libcurl 7.32.0 < 8.9.1 DoS (CVE-2024-7264)
- Microsoft Windows Unquoted Service Path Enumeration

These findings highlight the critical need for continuous monitoring and timely patching to maintain infrastructure security and reduce exposure to potential threats

---

Total Attacks Successfully Blocked

7638

During the current reporting period, our security infrastructure successfully detected and mitigated 7,638 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.

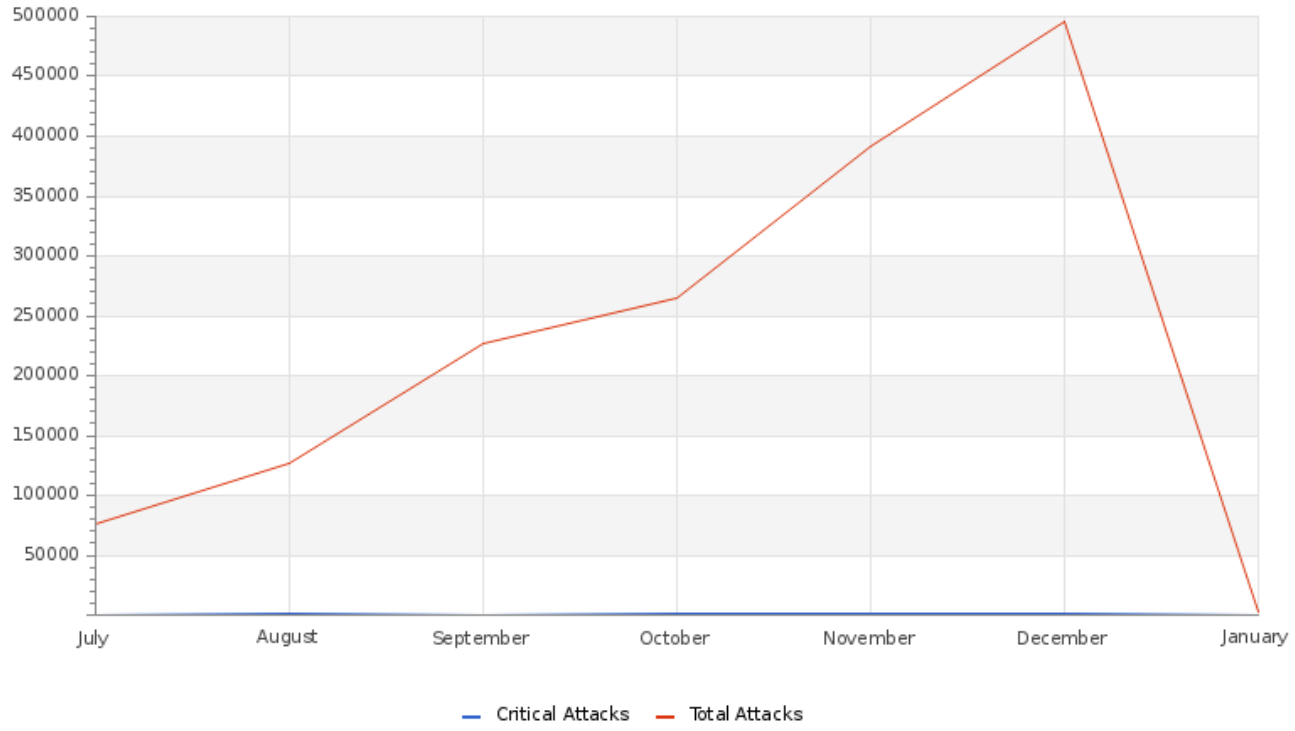
GLESEC 03/20/2026

Critical Attacks Successfully Blocked

226

In December, our monitoring systems recorded a total of 7,638 security incidents, of which 226 were classified as critical attacks and were successfully blocked. The proportion of critical incidents relative to total activity suggests either a temporary reduction in hostile operations or the effectiveness of the preventive measures currently in place, such as improved integration of threat intelligence and adaptive defense protocols. Preliminary analysis indicates that the observed activity patterns may reflect a shift in attacker behavior, with fewer high-severity attempts successfully penetrating initial defenses. Continuous monitoring and correlation with external threat intelligence sources will be essential to confirm whether this trend represents a sustained decline in malicious activity or a short-term fluctuation.

Attacks Successfully Blocked



During this month, the number of blocked attacks increased significantly compared to the previous month, reaching nearly 500,000. This surge may be attributed to either a large-scale coordinated malicious campaign or to enhanced detection and response capabilities resulting from recent system optimizations. Importantly, no critical incidents were recorded, confirming that all threats were effectively contained within the defensive perimeter. This outcome underscores the resilience of current security controls and highlights the effectiveness of proactive monitoring and automated mitigation strategies in neutralizing high-volume attack traffic.

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

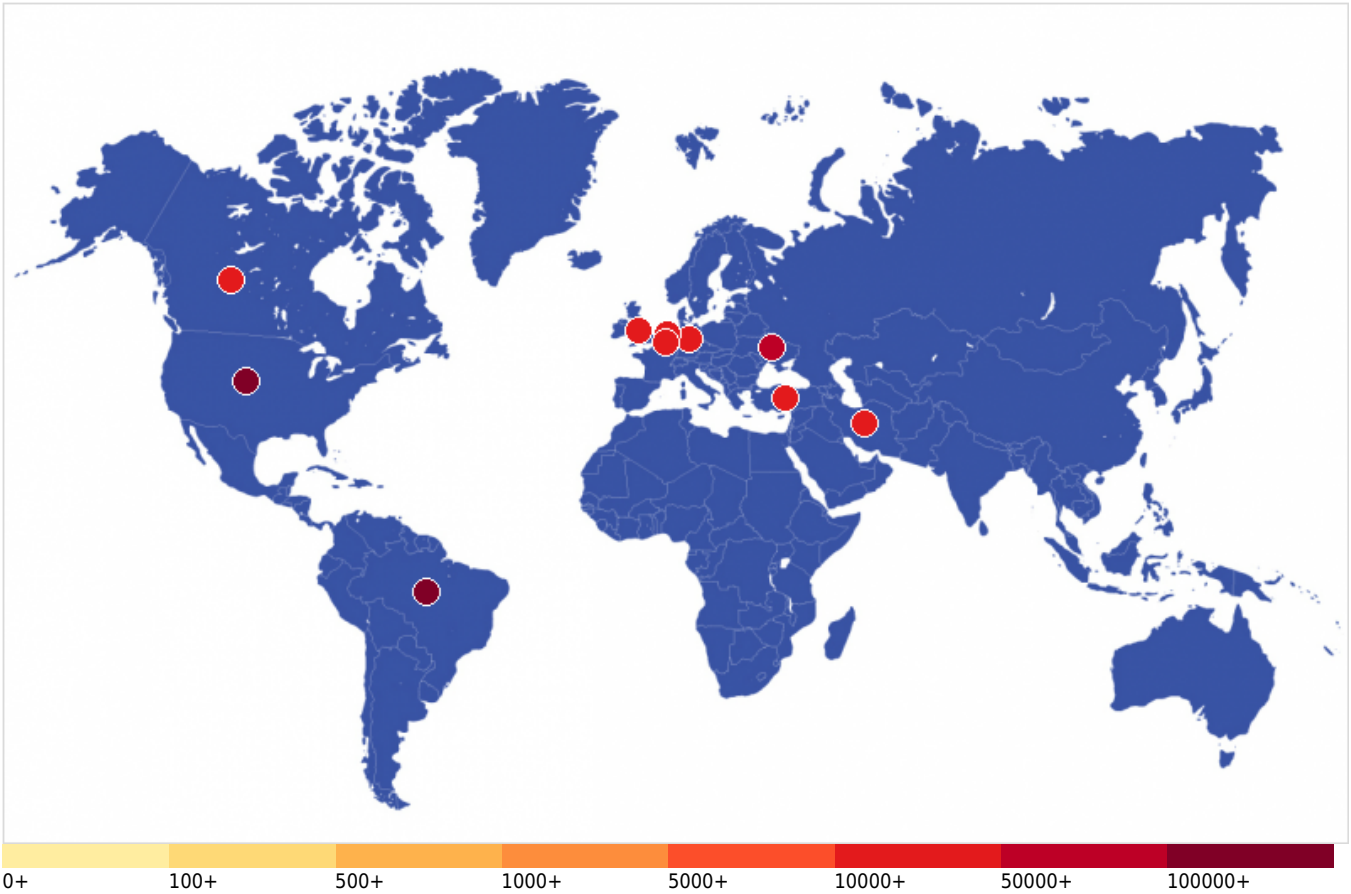
GLESEC 03/20/2026

Vulnerability Metric

68

The vulnerability metric registered a substantial escalation, decrease from 78 to 68. This surge reflects a heightened exposure profile, attributable either to the identification of newly emerging high-risk vulnerabilities or enhanced visibility achieved through recent scanning initiatives. The upward trajectory underscores the urgency of prioritized remediation, with a focus on addressing critical vulnerabilities that pose the greatest potential impact. Continuous monitoring and validation remain essential to ensure that detection improvements translate into effective risk reduction and to prevent adversaries from exploiting these weaknesses.

Critical Attacks Per Country In Past Week



Brazil - 178803
Turkey - 45915
Canada - 15272
United States - 156138
Iran - 30520
Belgium - 15156
Ukraine - 60442
United Kingdom - 16970
Germany - 46021
Netherlands - 16115

The graph for the analyzed period shows a significant concentration of cyberattacks originating mainly from North America and Europe, with additional presence in the Middle East and South America.

In this period, Ukraine ranks as the primary source of malicious attempts with 60,442 records, followed by Germany with 45,021 and Iran with 30,520. These are followed by the United Kingdom (16,970) and the United States (15,138), which continue to represent a significant share of the total detected events.

GLESEC 03/20/2026

At a secondary level, Brazil (17,808), Turkey (4,591), the Netherlands (1,615), Canada (1,572), and Belgium (1,516) are also identified, reflecting a geographically diversified origin of attacks.

This distribution highlights a notable shift in trends, with a considerable increase in activity from Eastern and Central Europe—particularly Ukraine and Germany—as well as significant participation from the Middle East through Iran. Additionally, traditional sources such as the United States and the United Kingdom remain active, while new focal points in Latin America, such as Brazil, are also emerging.

This scenario reinforces the need to adjust monitoring strategies and strengthen controls in regions with higher activity levels, while maintaining a global perspective on the threat landscape. Geographic visualization continues to be a key tool for prioritizing defensive actions in a dynamic and constantly evolving threat 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 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