TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC

September 01, 2026

GLESEC 09/01/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

This report corresponds to April 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

15%

In our "Actual Risk" section, we identified an increase from 12% to 15% compared to the previous month (March), reaching the highest level recorded in the past six months. This increase contrasts with the stability observed between February and March, when the indicator held at 12% following a brief dip to 10% in January. This month's increase suggests a possible expansion in the number or scope of active threats targeting the organization's most sensitive assets. We recommend heightened vigilance and close monitoring of this indicator's evolution in the coming period.

Accepted Risk

2%

The accepted risk level remains stable at 2%, unchanged from last month (March). This level was reached following an increase from 1% recorded between December and January, and has held steady for the past three months. This stability reflects a consistent threat mitigation strategy, in which proactive risk management continues to take precedence over risk tolerance. We recommend continuing periodic evaluation of accepted risks to ensure this level does not evolve into scenarios that compromise the organization's critical assets.

Confidence

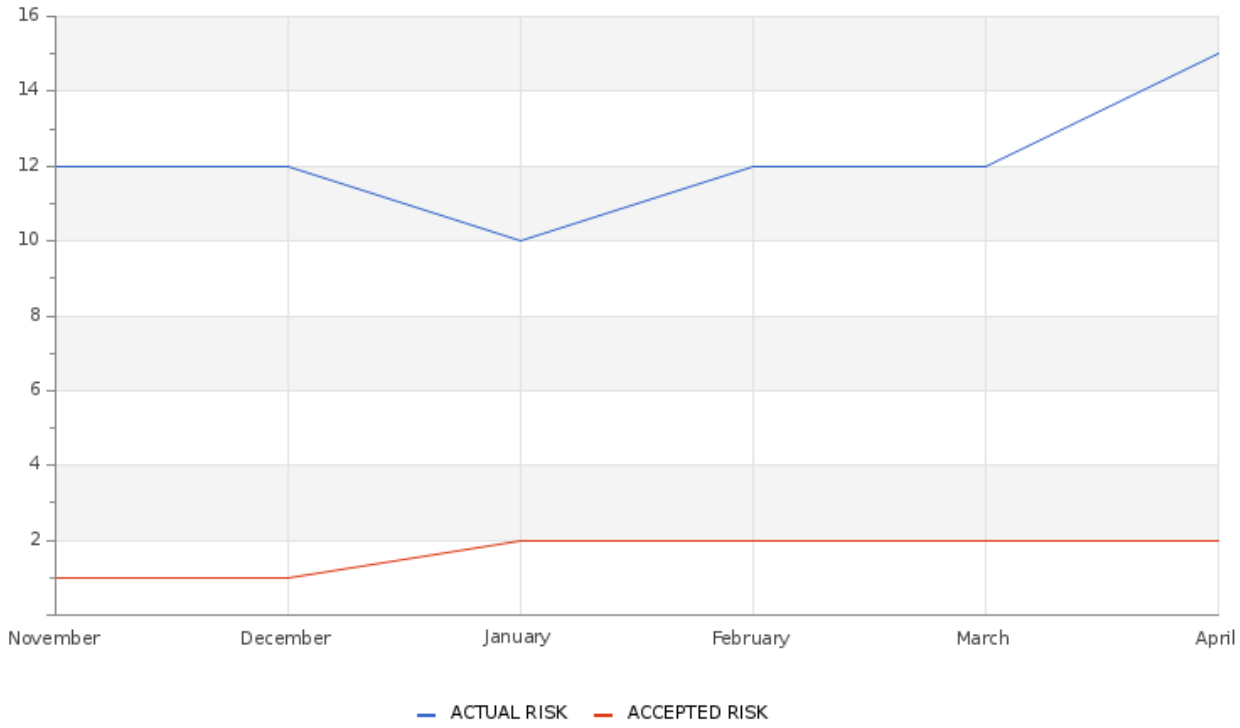
Medium

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 09/01/2026

Accepted & Actual Risk



The organization's overall risk level has increased to 15% compared to the previous period (March), reflecting a weakening of the security posture. However, accepted risk has remained stable at 2%, demonstrating that tolerable risk has remained under control. We suggest closely monitoring this indicator's evolution in the coming period, identifying the specific drivers behind the increase in actual risk in order to prioritize the corresponding mitigation actions.

Hosts & Vulnerable Hosts In Last 6 Months

Total Attacks Successfully Blocked

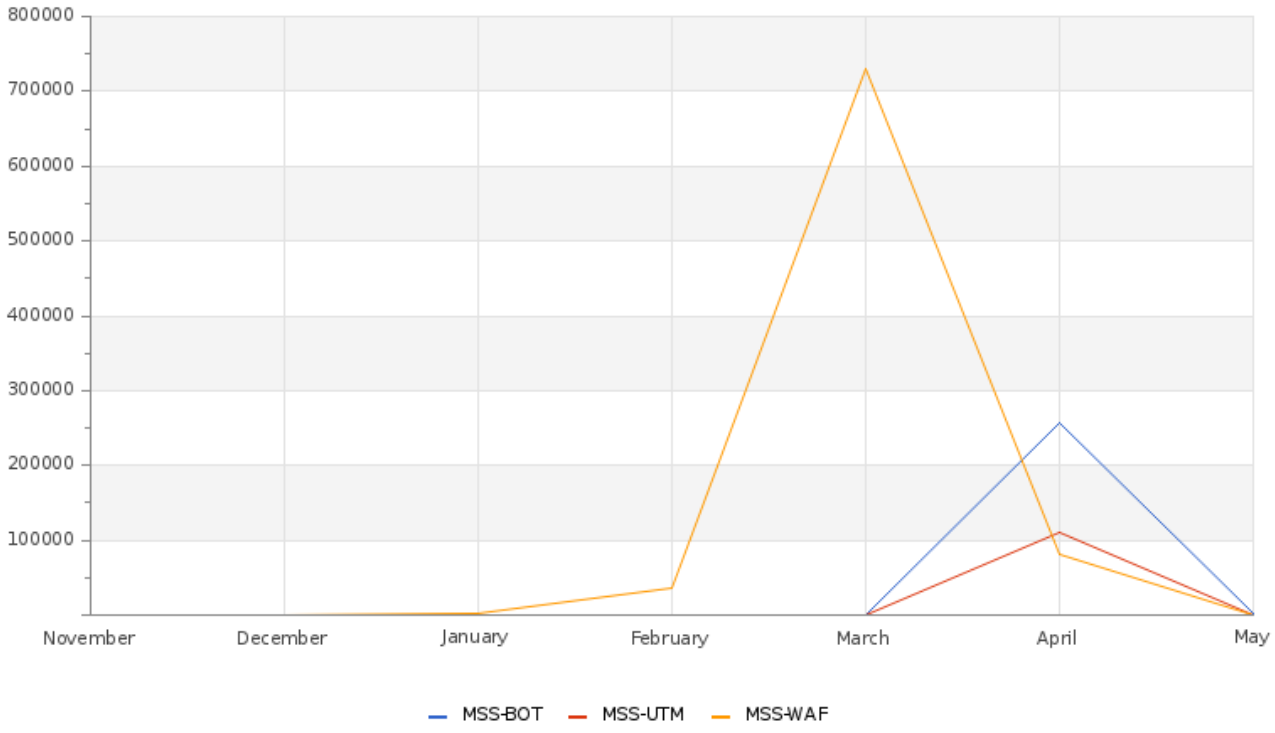
339250

Critical Attacks Successfully Blocked

795410

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

Attacks Successfully Blocked



Vulnerability Metric

37

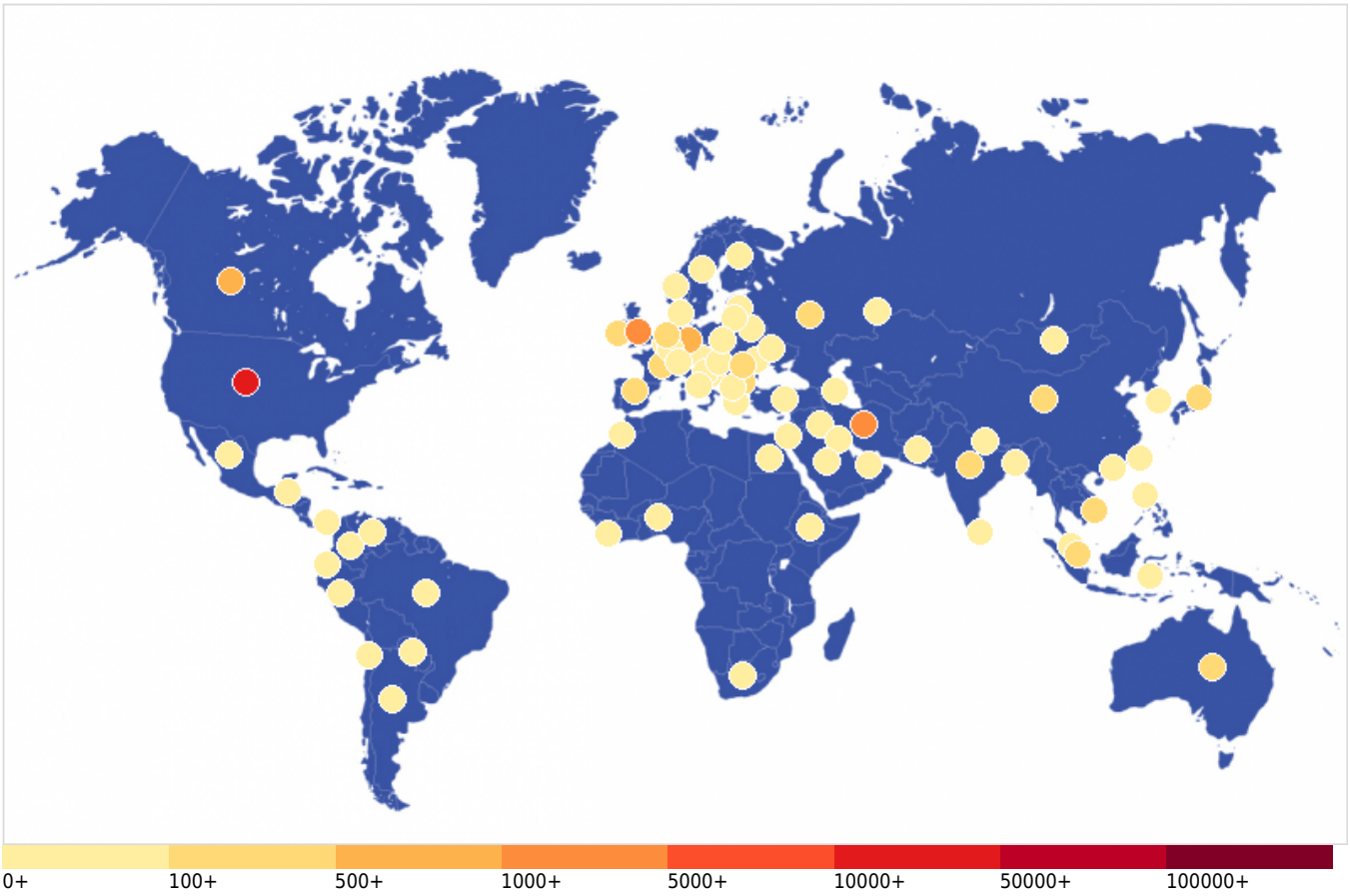
The vulnerability indicator increased from 24 to 37 points compared to the previous month (March). This increase is supported by changes observed in the vulnerability management detail panels during April: the Vulnerable Hosts History panel recorded an increase from 42 to 45 vulnerable hosts compared to March. Consistently, the Vulnerability Severity History panel showed an increase across all severity levels during the same period; for example, high-severity vulnerabilities rose from 455 in March to 522 in April.

This behavior reinforces the need to prioritize remediation of critical and high-severity vulnerabilities. Continuous monitoring and reinforced vulnerability management processes are recommended to reverse this trend in the coming periods.

Critical Attacks Per Country In Past Week

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

GLESEC 09/01/2026



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 shows a strong concentration across the Americas, Europe, and Asia. The United States remains the leading source of malicious activity with 20,436 incidents, significantly exceeding all other countries and representing the primary contributor to the observed activity. Iran follows with 3,852 incidents, making it the second-largest source and

indicating a notable concentration of activity originating from the Middle East. Other significant contributors include the United Kingdom (1,024), Canada (661), Germany (549), Romania (498), Russia (441), and Spain (406).

At a secondary level, Bulgaria (293), Vietnam (258), Ireland (249), China (185), India (184), Australia (177), Japan (132), Singapore (127), and the Netherlands (116) account for additional activity. These figures demonstrate that, although the majority of incidents are concentrated in a limited number of countries, malicious activity remains geographically distributed across Europe, Asia, and the Pacific region.

Additional activity was observed from Brazil (86), Ukraine (61), Italy (59), Saudi Arabia (53), Hungary (48), Sweden (42), Saint Kitts and Nevis (38), Mexico (36), Lithuania (29), Poland (27), Turkey (27), Indonesia (23), Israel (20), and South Africa (14). Lower-volume activity was also detected across several other countries, including France, Austria, Belgium, China, South Korea, Hong Kong, and New Zealand.

Overall, the current data confirms the Americas as the dominant source region, primarily driven by the United States and supported by Canada and Brazil. Asia and the Middle East also represent a significant portion of the observed activity, particularly due to Iran's 3,852 incidents, while Europe shows a broad and distributed pattern led by the United Kingdom, Germany, Romania, Russia, and Spain. The geographic diversity of the sources highlights the importance of maintaining geographically aware monitoring and continuously evaluating changes in attack-origin patterns to identify emerging concentrations and potential shifts in attacker infrastructure.

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