



GLE
SEC

COMPLETELY
PERCEPTIVE

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

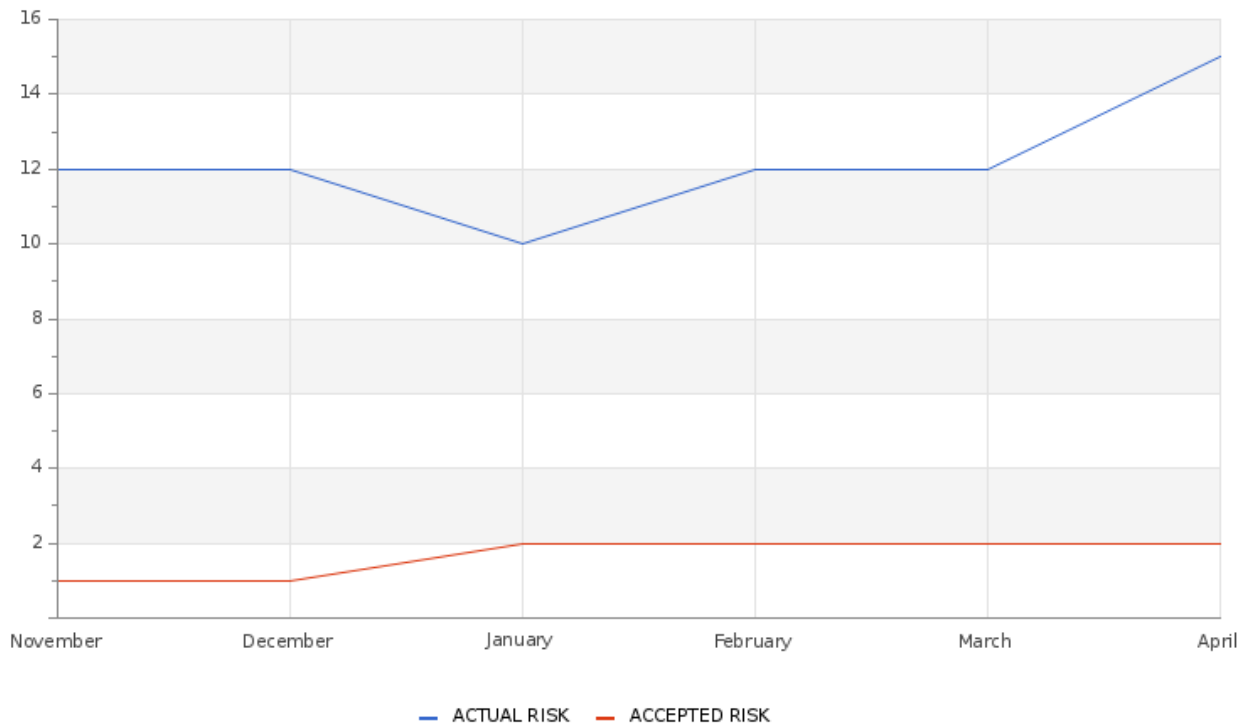
Medium

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.



GLESEC 09/01/2026

Accepted & Actual Risk



Hosts & Vulnerable Hosts In Last 6 Months



Total Attacks Successfully Blocked

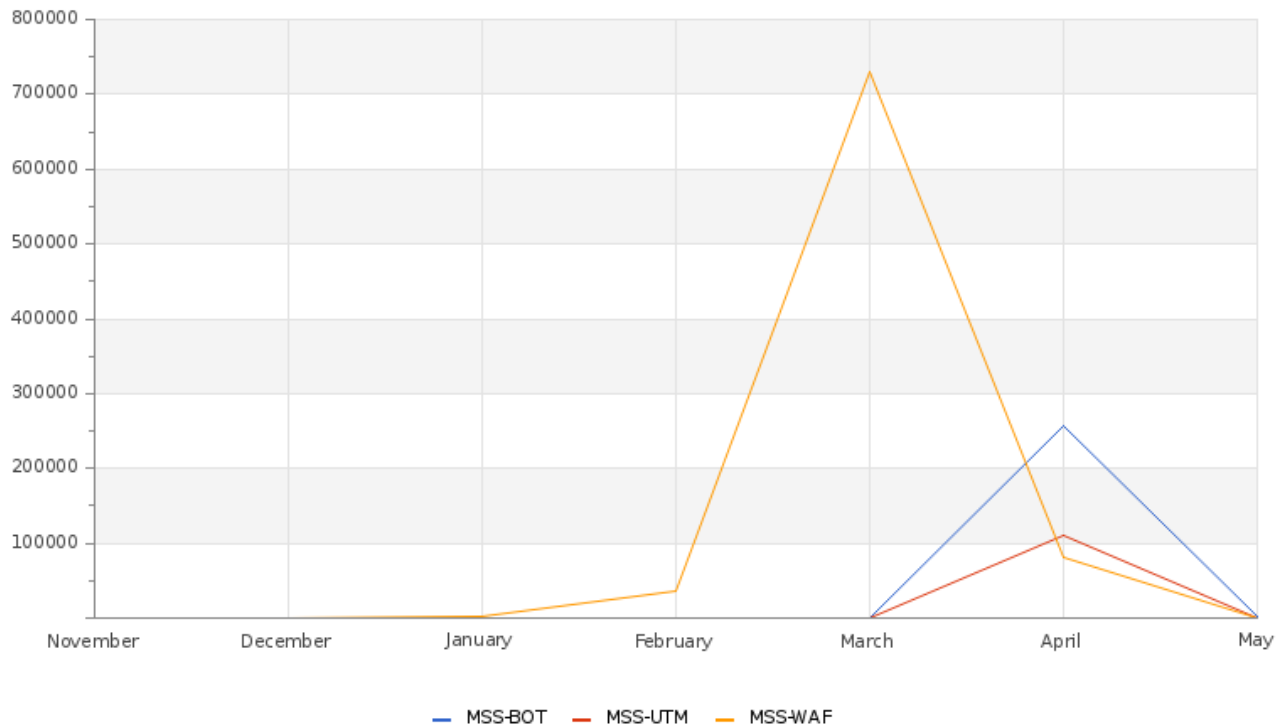
339250

Critical Attacks Successfully Blocked

795410

GLESEC 09/01/2026

Attacks Successfully Blocked



Vulnerability Metric

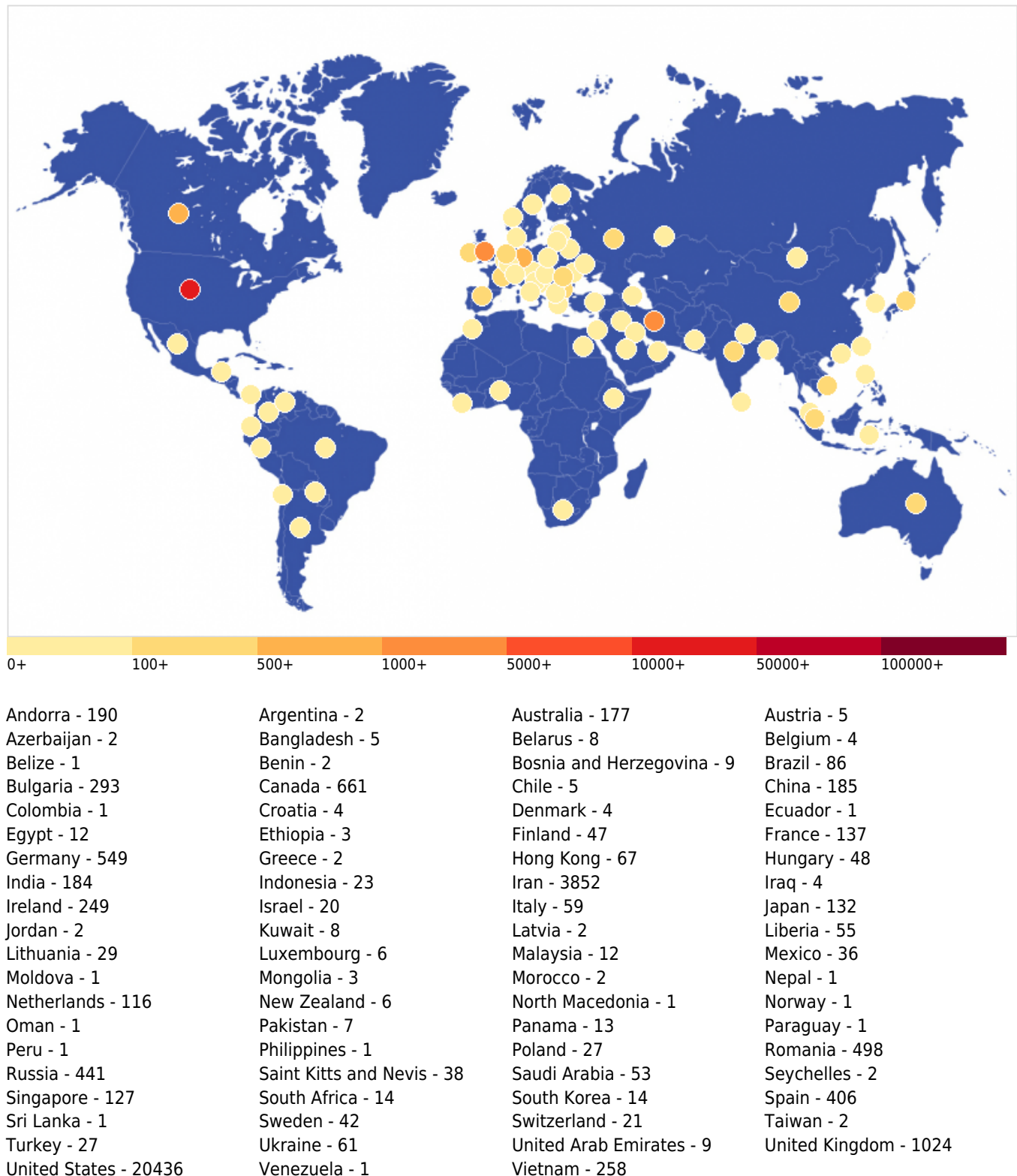
37

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

GLESEC 09/01/2026



GLESEC 09/01/2026

= 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.**



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

