



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC
April 07, 2026



GLESEC 04/07/2026

TLP AMBER BOARDROOM EXECUTIVE REPORT

This report corresponds to THIS MONTH 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

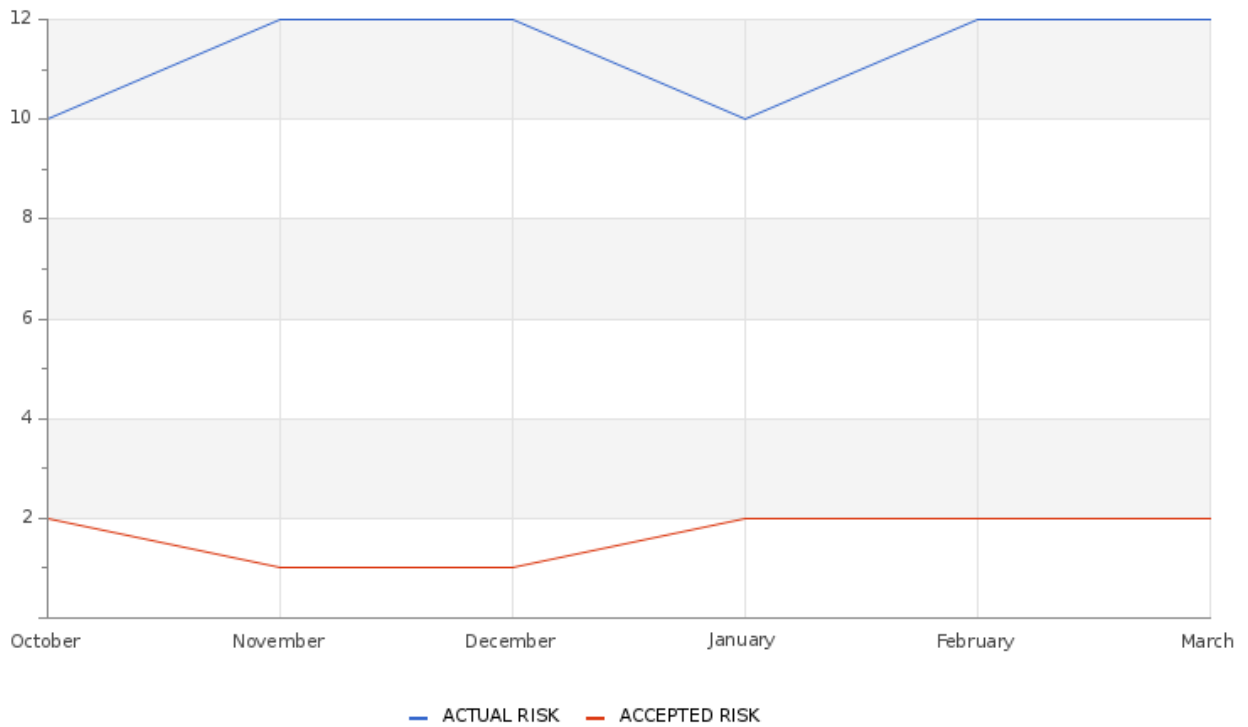
Medium

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.



GLESEC 04/07/2026

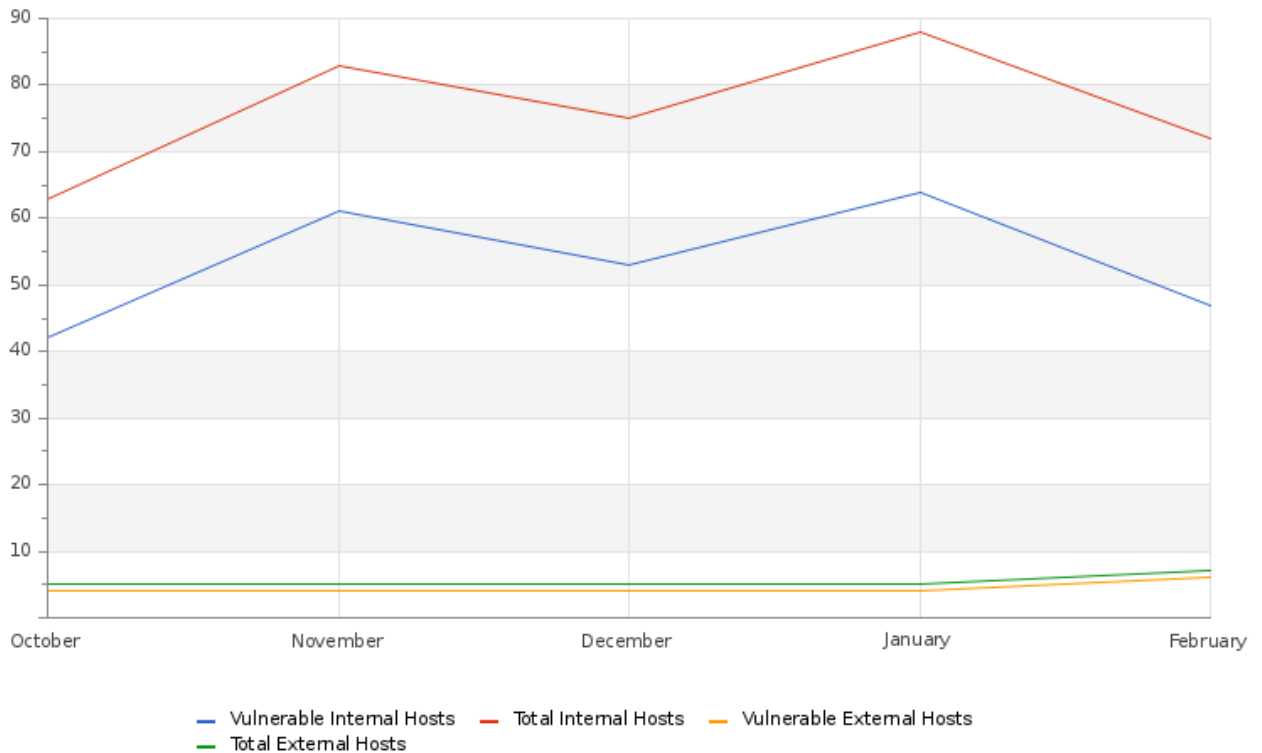
Accepted & Actual Risk



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

GLESEC 04/07/2026



During the period analyzed, the number of vulnerable hosts showed an upward trend from October through January, peaking at 51 vulnerable assets. From that point on, there was a gradual decline through April, when the number dropped to 11, suggesting the effective implementation of remediation measures and the strengthening of security controls. Regarding the overall infrastructure, the behavior of internal hosts follows a similar trend, with increases through the beginning of the year followed by a subsequent reduction. Meanwhile, external hosts have remained at low levels, though with a slight increase toward the end of the period, which could be associated with the addition of new assets or greater visibility of the external environment.

The most frequently identified vulnerabilities included: TLS Version 1.1 Deprecated Protocol, SSL Certificate Cannot Be Trusted, Microsoft Windows LAN Manager SNMP LanMan Shares Disclosure, OpenSSH < 10.1 / 10.1p1 Multiple Vulnerabilities, Ubuntu 20.04 LTS / 22.04 LTS: Linux kernel vulnerabilities (USN-7683-1)

Total Attacks Successfully Blocked

629317

During the current reporting period, our security infrastructure successfully detected and mitigated 629,317 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.

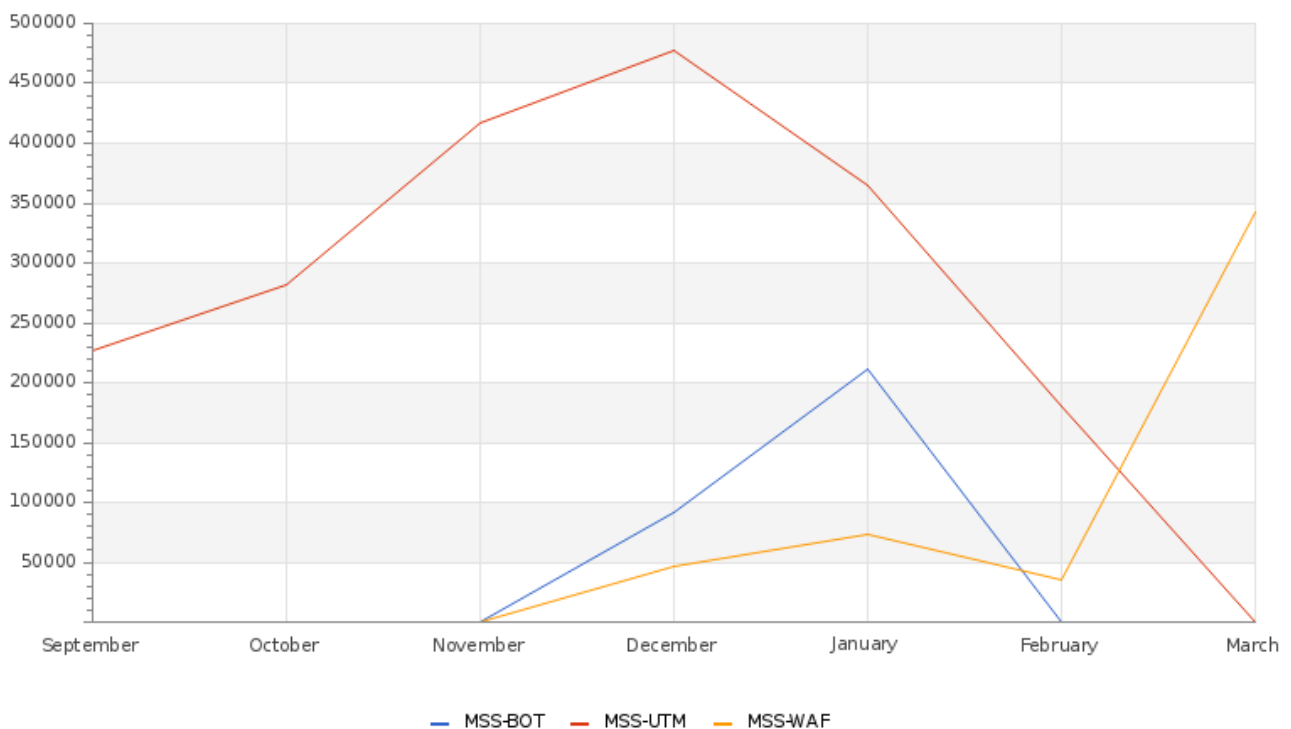
GLESEC 04/07/2026

Critical Attacks Successfully Blocked

458711

Our monitoring systems recorded a total of 629,317 security incidents, of which 458,711 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.

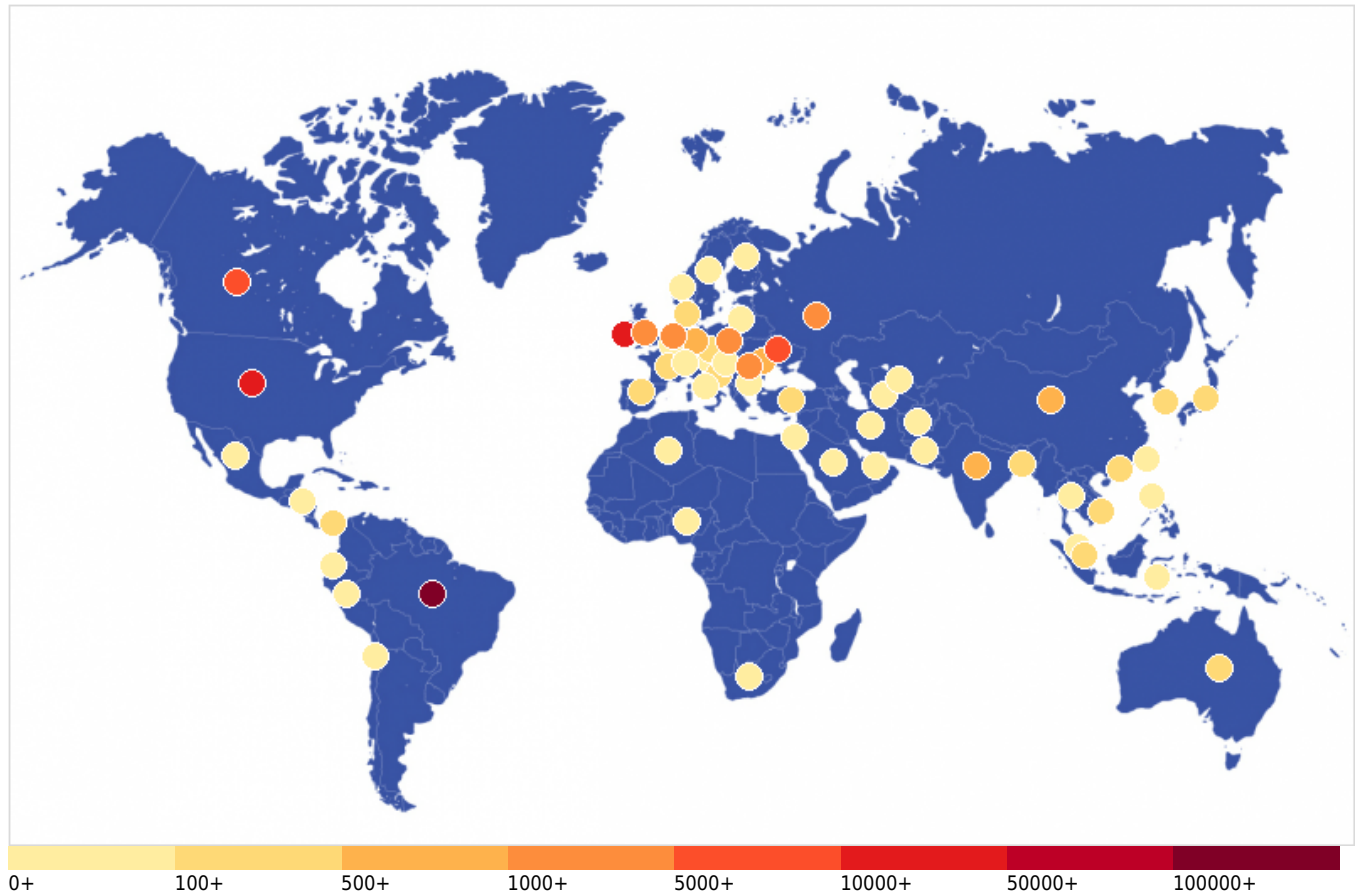
Attacks Successfully Blocked



During the period analyzed, there was a significant variation in the number of attacks blocked across the different security layers. The MSS-UTM solution accounted for the highest volume of events, showing steady growth from September through December, peaking in December, followed by a gradual decline through March. On the other hand, MSS-BOT shows activity primarily between December and January, with a significant peak in January, which can be interpreted as a temporary increase in malicious automation attempts, followed by a considerable reduction in the subsequent months. As for MSS-WAF, an upward trend is observed toward the final months, with a notable increase in March. This behavior could be associated with greater exposure of web applications or an increase in exploitation attempts targeting these assets. These variations reflect changes in attack vectors over time, highlighting the importance of maintaining a multi-layered defense strategy and continuous monitoring to adapt to evolving threats.

GLESEC 04/07/2026

Critical Attacks Per Country In Past Week



Afghanistan - 2	Algeria - 7	Andorra - 6	Australia - 123
Austria - 2	Bangladesh - 170	Belgium - 8	Bosnia and Herzegovina - 150
Brazil - 110579	Bulgaria - 79	Canada - 6107	Chile - 4
China - 838	Czechia - 145	Denmark - 125	Ecuador - 8
Finland - 25	France - 170	Germany - 705	Honduras - 88
Hong Kong - 144	Hungary - 86	India - 545	Indonesia - 42
Iran - 3	Ireland - 28557	Israel - 4	Italy - 15
Japan - 352	Lithuania - 4	Malaysia - 4	Mexico - 8
Moldova - 762	Netherlands - 1356	New Zealand - 32	Nigeria - 39
Norway - 25	Pakistan - 14	Panama - 155	Peru - 2
Philippines - 10	Poland - 1139	Romania - 1246	Russia - 1015
Saint Kitts and Nevis - 93	Saudi Arabia - 3	Seychelles - 2	Singapore - 248
South Africa - 10	South Korea - 160	Spain - 356	Sweden - 6
Switzerland - 37	Taiwan - 10	Thailand - 79	Turkey - 111
Turkmenistan - 3	Ukraine - 6762	United Arab Emirates - 43	United Kingdom - 1560
United States - 38248	Uzbekistan - 2	Vietnam - 109	

TLP:AMBER

GLESEC 04/07/2026

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.**



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.

