TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

December 17, 2025

GLESEC 12/17/2025

TLP AMBER CISO
EXECUTIVE REPORT

This report corresponds to November 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.

RISK

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

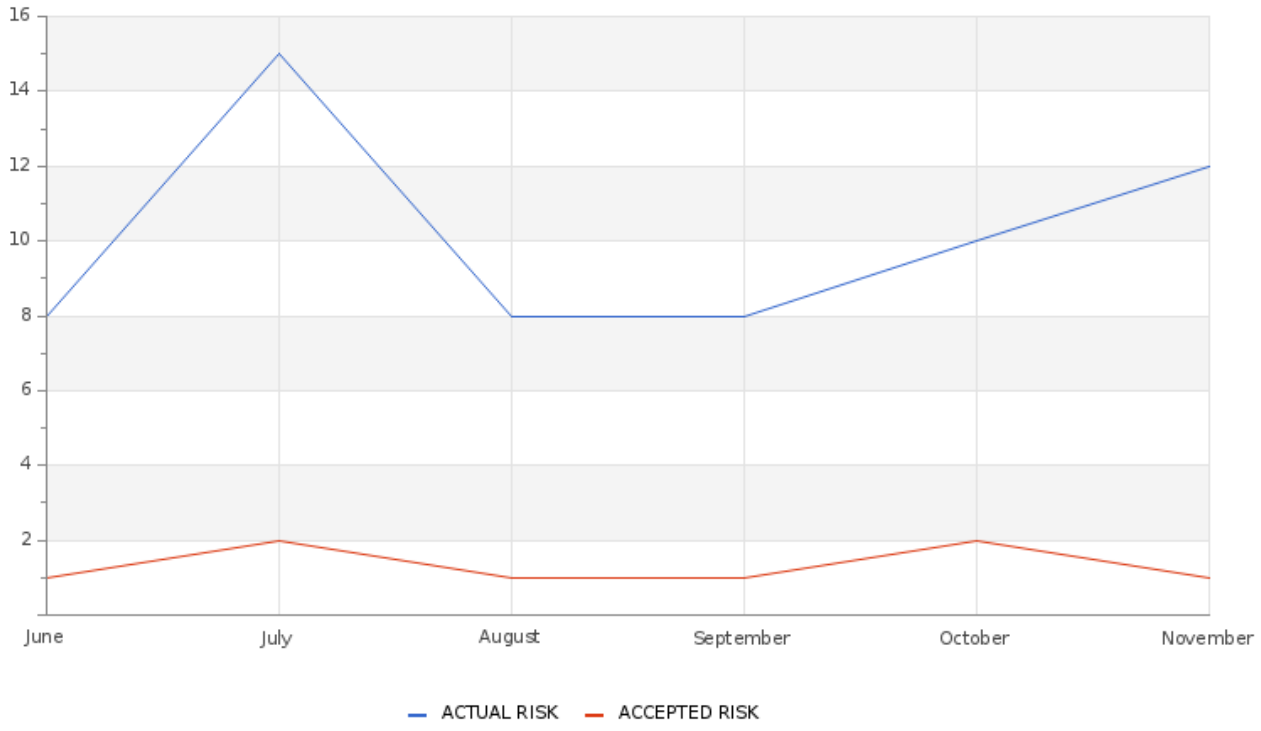
Medium

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 12/17/2025

Accepted & Actual Risk



The organization’s overall risk level rose by 12% from last month, reflecting heightened exposure, while the accepted risk decreased to 1%, underscoring a continued commitment to strict mitigation and proactive risk management. This indicates a considerable increase in the overall exposure that suggests a low probability of threats compromising critical assets. Continuous monitoring is recommended to remain aware of any potential changes

Table of Comparison of Actual and Acceptable Risk From Current to Previous Month

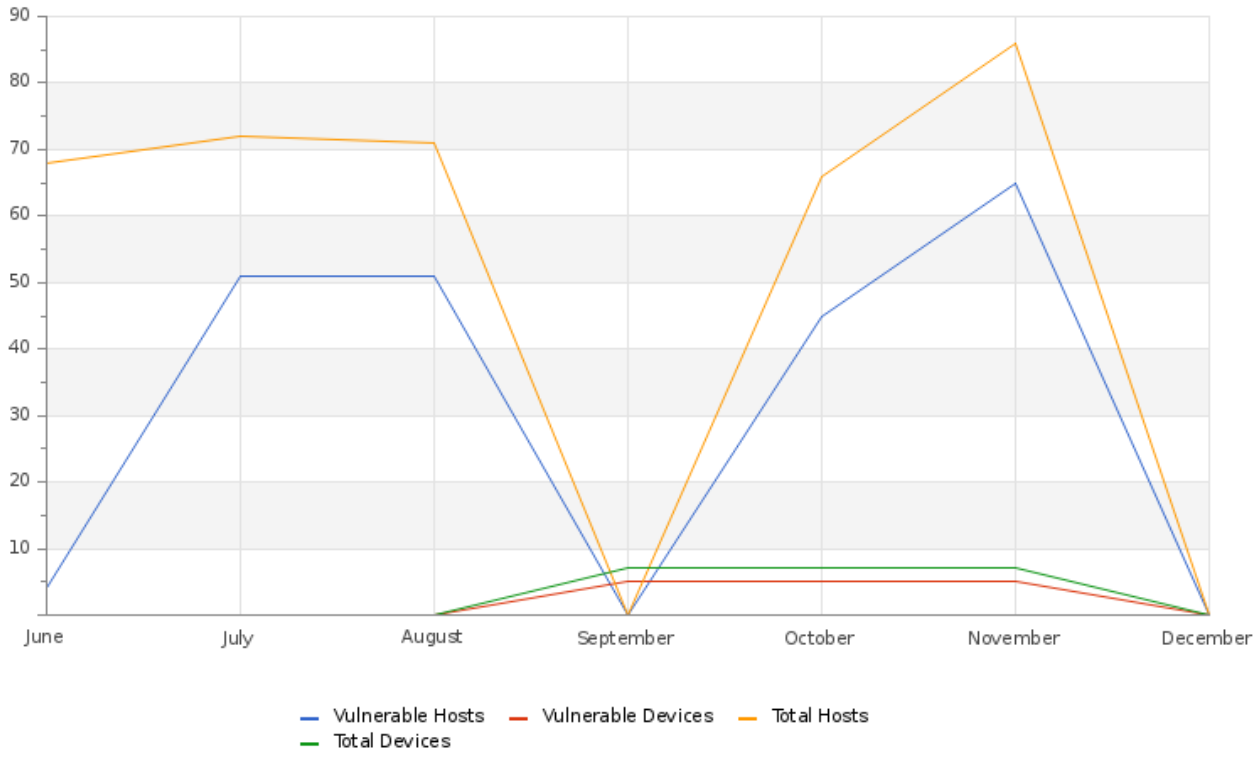
	Current Month	Previous Month
Actual Risk	12	10
Accepted Risk	1	2

The Actual risk has increase to 12% compared to 10% in the previous month. Accepted risk has shown a slight decrease, reaching 2%. This change reflects an adjustment in the risk tolerance policy, considering certain risk levels acceptable without the need to apply immediate mitigation measures.

VULNERABILITY

GLESEC 12/17/2025

Hosts & Vulnerable Hosts In Last 6 Months



In November, the number of hosts increased from 65 to 80, while vulnerable hosts rose from 45 to 65. The most frequently identified vulnerabilities included:
- SSL Certificate Cannot Be Trusted
- SSL Self-Signed Certificate
- Web Server Allows Password Auto-Completion
- SQLite < 3.50.2 Memory Corruption
- ICMP Timestamp Request Remote Date Disclosure
- SSL Certificate Expiry
- SQLite 3.44.0 < 3.49.1 Multiple Vulnerabilities
- libcurl 7.32.0 < 8.9.1 DoS (CVE-2024-7264)
- Security Update for Microsoft .NET Core (June 2025)
- Security Update for Microsoft .NET Core (May 2025)

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

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

GLESEC 12/17/2025

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	73	73
Hosts Discovered	72	63
Vulnerable Hosts	50	44
Baseline Devices	7	7
Vulnerable Devices	5	5
Critical Vulnerabilities Count	98	47
High Vulnerabilities Count	107	81
Medium Vulnerabilities Count	291	236
Low Vulnerabilities Count	65	56
Phishing Score	0	0
Email Gateway Score	7	6
Web Application Firewall Score	18	17
Web Gateway Score	60	59
Endpoint Score	14	13
Hopper Score	33	32
DLP Score	64	63

The number of baselined hosts remains stable at 73, while discovered hosts increased from 63 to 72, indicating improved asset visibility within the environment. At the same time, the number of vulnerable hosts rose from 44 to 50, accompanied by increases across all vulnerability severity levels, including critical, high, medium, and low vulnerabilities. These increases suggest a broader identification of vulnerabilities rather than a sudden deterioration of security posture. Baseline and vulnerable devices remain unchanged, reflecting stability at the device level. Security control scores, such as email gateway, web application firewall, web gateway, endpoint, hopper, and DLP, show slight improvements or remain consistent compared to the previous month, indicating a steady security posture. As previously recommended, blocking unused extensions and maintaining proactive remediation efforts would help reduce overall exposure and improve future evaluation results.

Vulnerability Metric

78

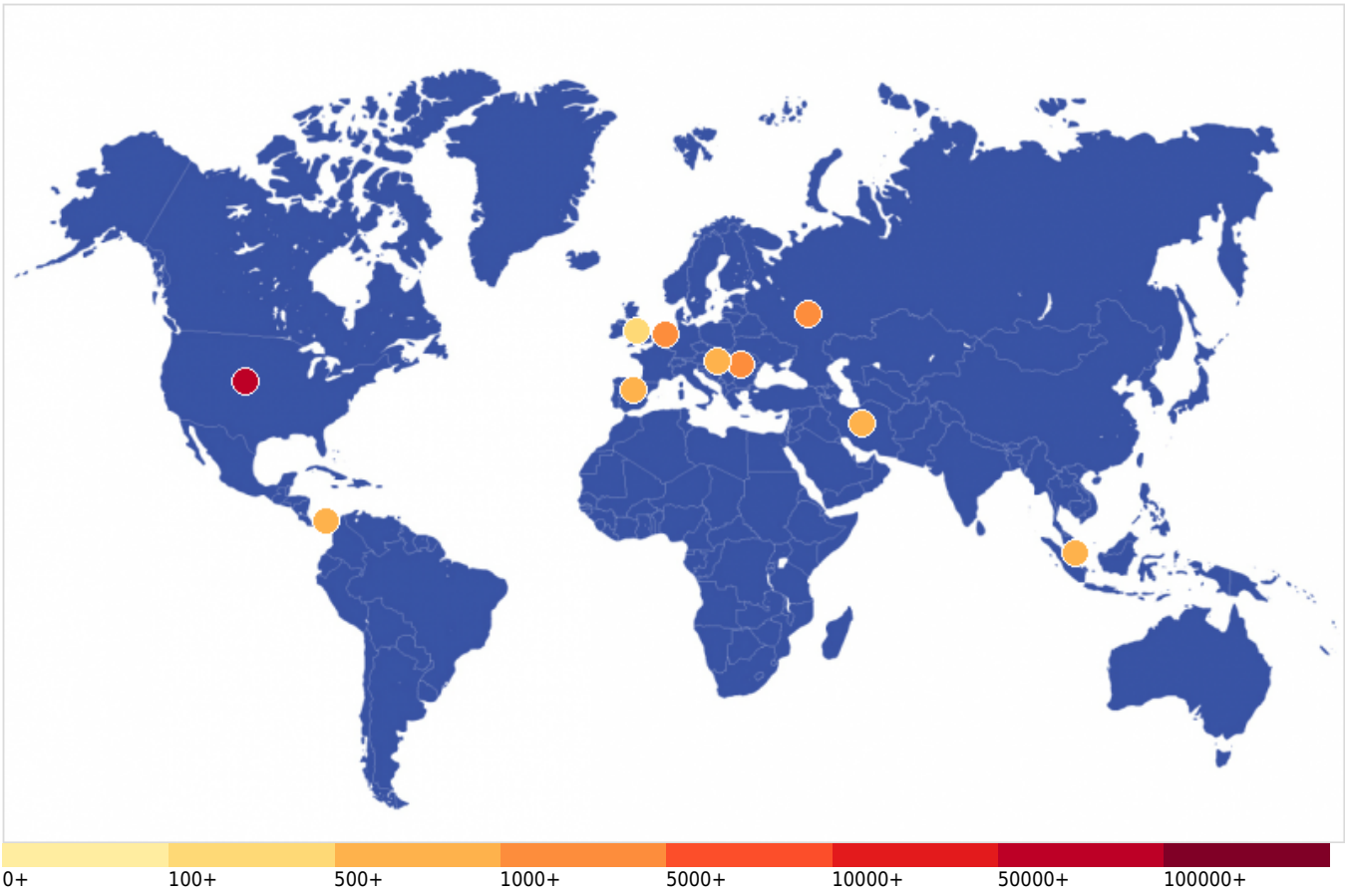
The vulnerability metric registered a substantial escalation, increasing from 15 to 78. This surge reflects a heightened exposure profile, attributable either to the identification of newly emerging high-risk vulnerabilities or enhanced visibility achieved through recent scanning initiatives. The upward 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.

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

GLESEC 12/17/2025

THREATS

Critical Attacks Per Country In Past Week



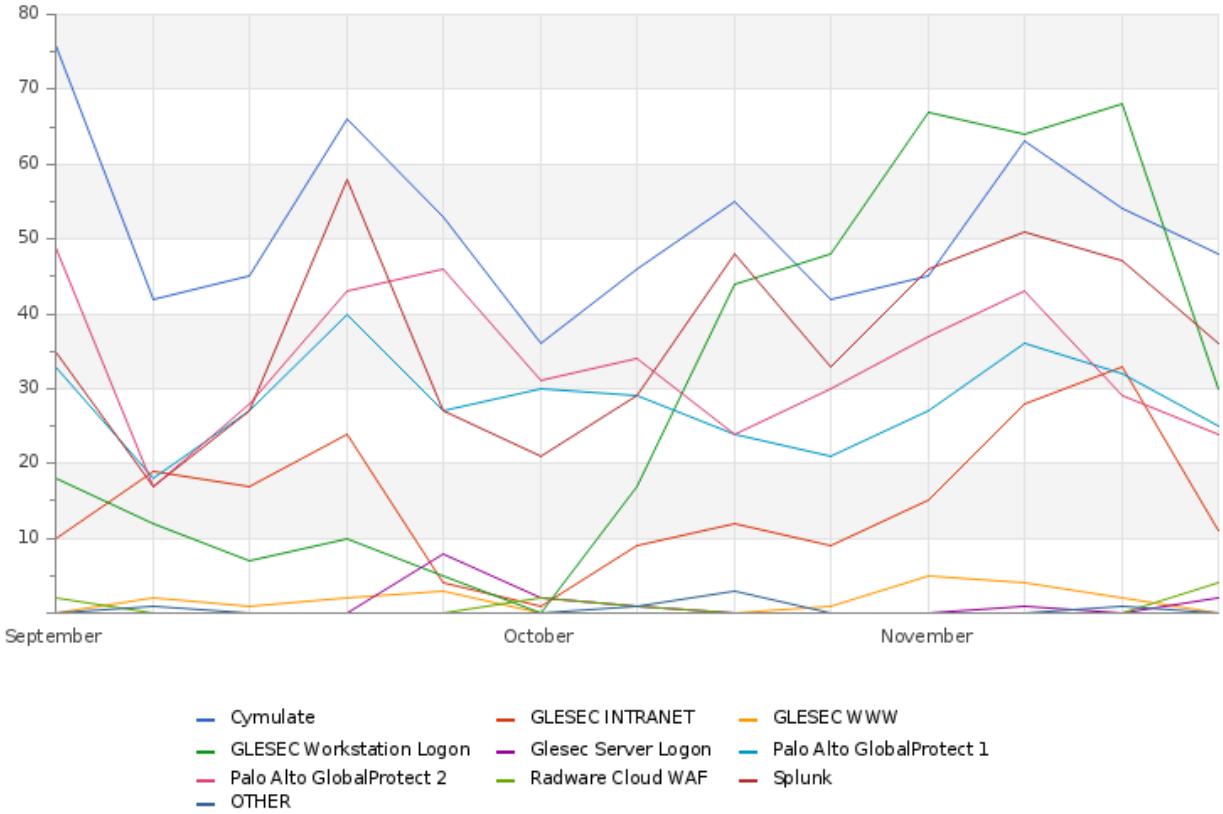
United States - 75650
Spain - 944
Hungary - 520
Romania - 3782
Panama - 835
United Kingdom - 351
Netherlands - 2395
Iran - 756
Russia - 1011
Singapore - 556

This graph illustrates the distribution of countries from which cyberattacks originate. The United States is the country with the highest number of attacks (75,650), followed by Romania (3,782), Netherlands (2,395), and Rusia (1,011). The map indicates the need to focus cybersecurity efforts primarily on threats emanating from the United States, while maintaining global vigilance.

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

GLESEC 12/17/2025

Total Number of Successful MFA authentications per application

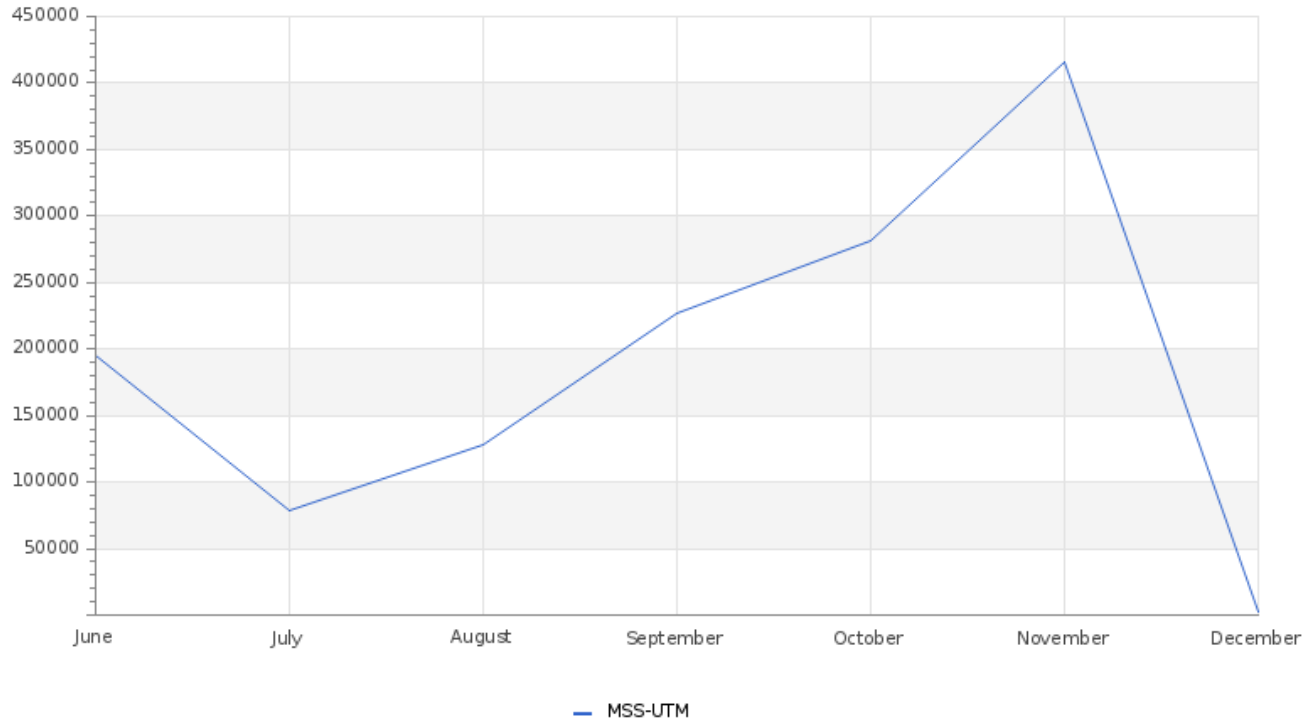


The graph shows login activity during November, demonstrating user interaction across platforms and highlighting the significance of each.

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

GLESEC 12/17/2025

Total Attacks Successfully Blocked Per Service

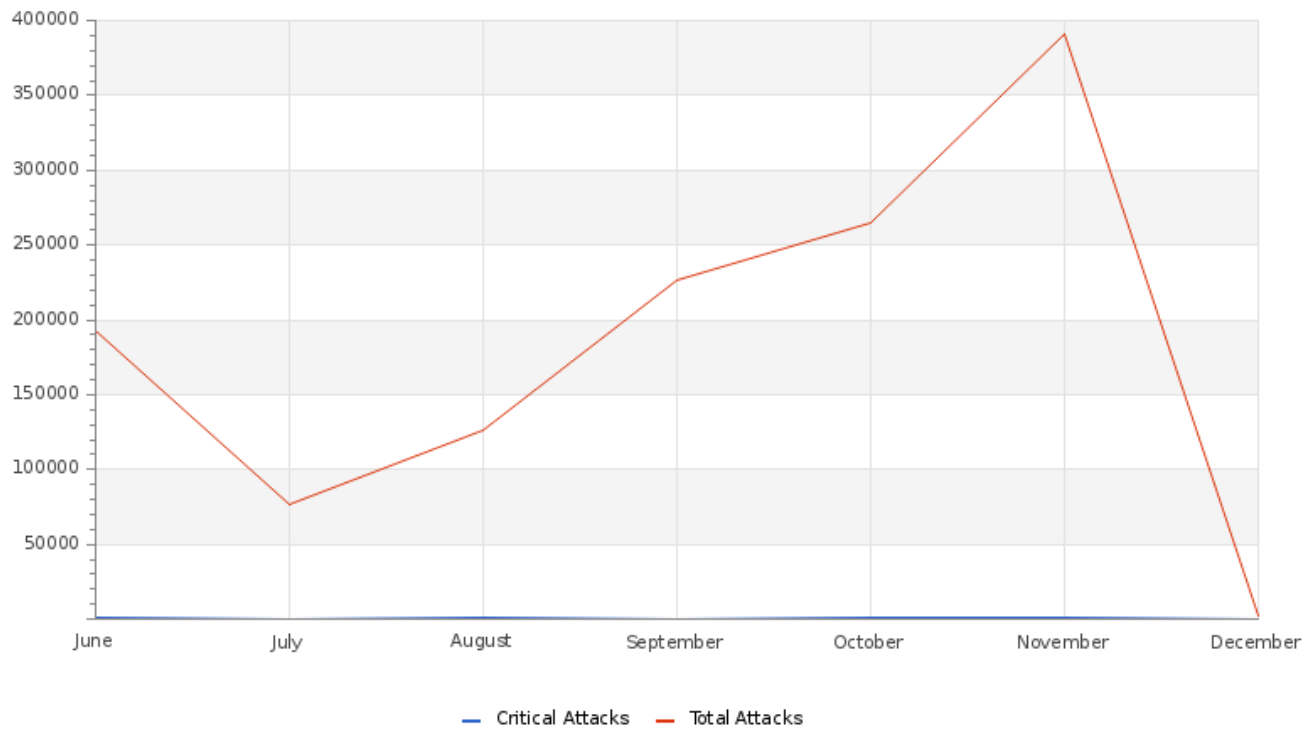


In November, UTM activity increased significantly to over 400,000 events, rising sharply from approximately 280,000 events in October. This notable month-over-month increase represents a clear escalation in detected activity and marks the highest level observed during the period. The sharp rise suggests either heightened threat activity or increased network utilization, reinforcing the need for continued vigilance and proactive monitoring to ensure timely detection and response to potential risks.

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

GLESEC 12/17/2025

Attacks Successfully Blocked by Severity



In this month, the number of blocked attacks increased significantly compared to the previous period, reaching nearly 400,000. This surge may reflect either a large-scale malicious campaign or improved detection and response capabilities. Notably, no critical incidents were reported, confirming that all threats were successfully contained.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	14	11
Critical Device Outages	0	0

During the month, 14 devices went down, but none of them were critical. This indicates that, although there was an interruption due to the failure of these devices, they did not represent critical problems in the performance of the system. This reflects consistent monitoring and preventive response measures.

Histogram of Total and Critical Device Outages

In November, there was 14 total device outages in comparison to the previous month, those was due to the relocation, but none were classified as critical or posed a significant operational risk. This reflects consistent monitoring and preventive response measures.

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

GLESEC 12/17/2025

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
6,958	0	0	19,675

Both MSS-UTM and MSS-EDR successfully blocked 26,633 attacks each. The DDOS and DLP layers reported no detected or mitigated incidents, underscoring the effectiveness of the security layers in place.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
FW Alerts	7
BAS Immediate Threat	27
BAS Web Security	21
Monitoring Event for SPLUNK CLOUD	6
Change in High or Critical Vulnerabilities	10
MSS-DLP - Abnormal activity in the file system(s)	5
BAS WAF	1
Change in Systems Performance	6
BAS Endpoint Security	1

During November, a total of 83 notable events were recorded. The BAS Immediate Threat category remained the most active with 27 cases, although this represents a decrease compared to the previous month (39)., followed by the BAS Web Security (21) and Change in High or Critical Vulnerabilities (10). These categories represented the most significant events during the month. Importantly, all incidents were addressed and resolved within the established response times, ensuring timely delivery back to the client.

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.**

TLP:AMBER

CISO 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