TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC

December 12, 2023

GLESEC 12/12/2023

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.

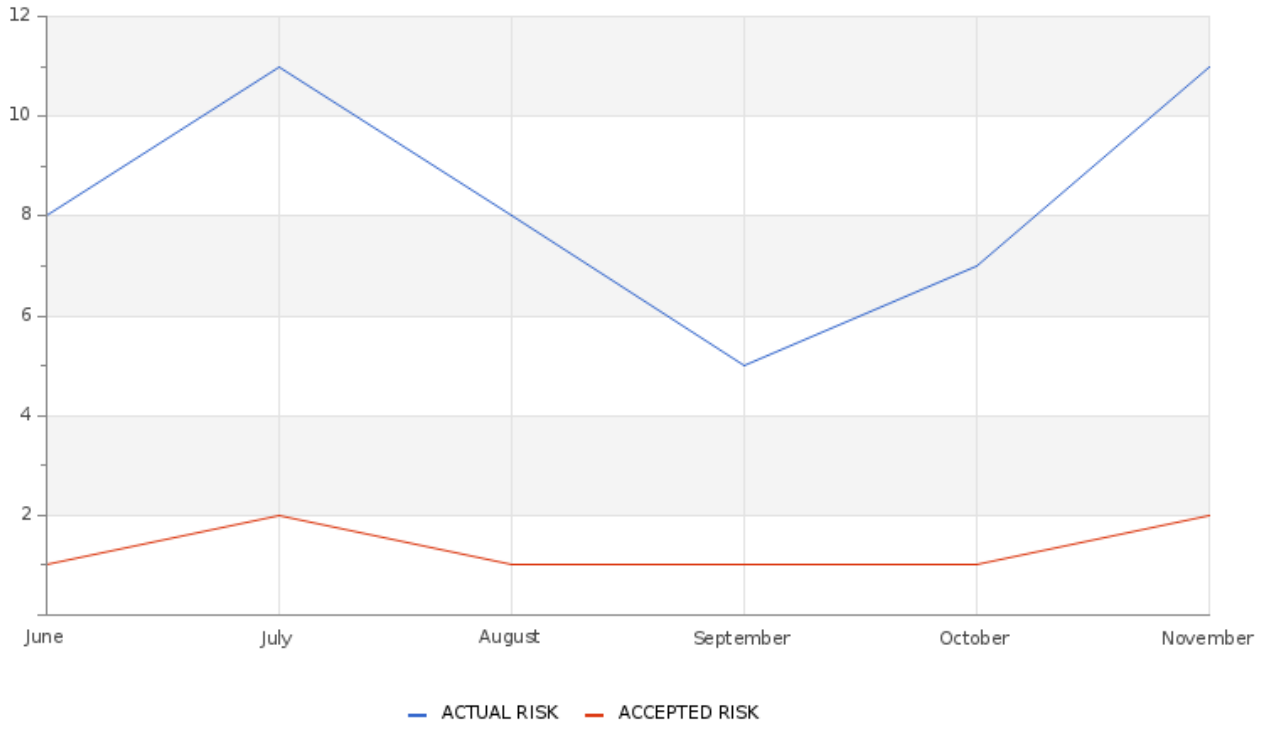
Actual Risk	Accepted Risk	Confidence
11%	2%	High

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 12/12/2023

Accepted & Actual Risk



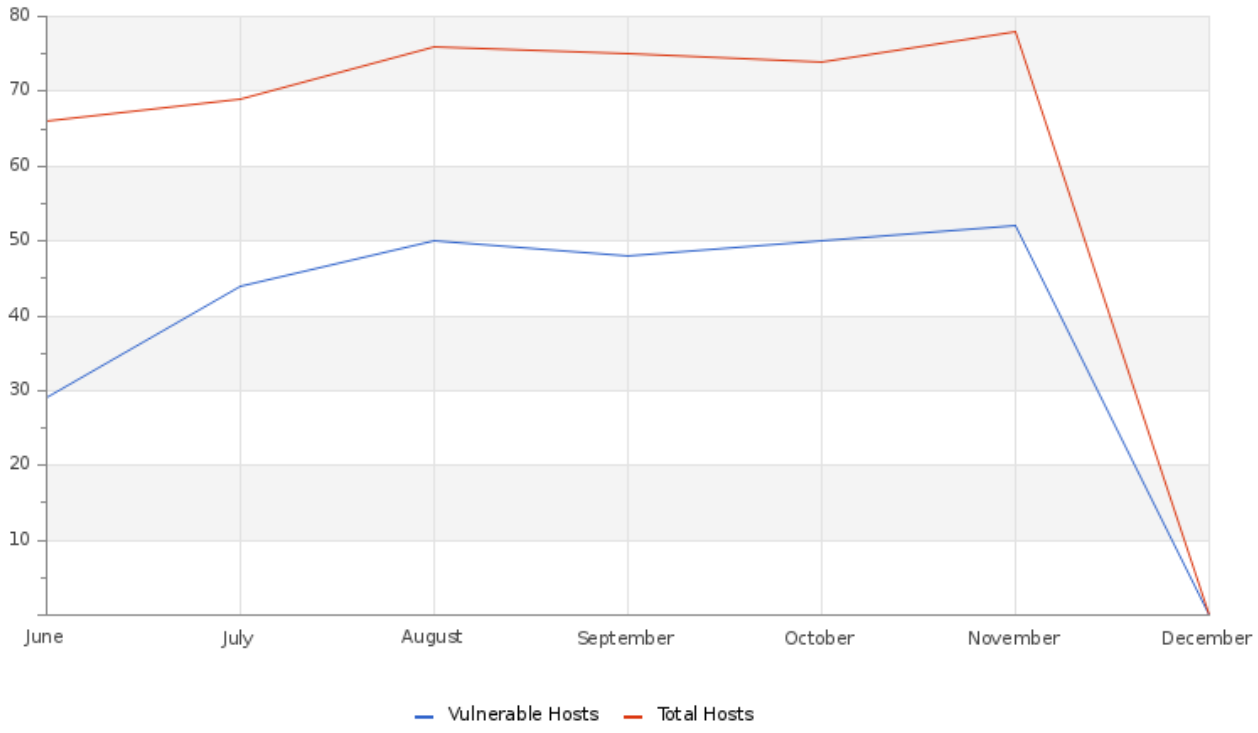
Over the course of this month, there has been a noticeable increase in the risk levels. The current risk now sits at 11%, and the accepted risk at 2%. This represents a significant rise from the previous month's figures, where the actual risk was recorded at 7% and the accepted risk at 1%.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 12/12/2023

Hosts & Vulnerable Hosts In Last 6 Months



The graph shows an increase in the number of hosts identified and a decrease in vulnerabilities over the month, indicating potential breaches in the security perimeter. Among the most notable high-risk vulnerabilities are multiple versions of Adobe Acrobat with various vulnerabilities, as detailed in reports APSB22-32, APSB22-39, APSB22-46, APSB23-01, APSB23-24, APSB23-30, APSB23-34, and APSB23-54, as well as vulnerabilities in Adobe Reader according to report APSB17-24, and in 7-Zip prior to version 23.00. Prompt attention to these areas is crucial to ensure a more secure environment.

Total Attacks Successfully Blocked

527

Throughout the month, 527 critical attacks were successfully blocked. This achievement stems from our unique real-time intelligence-based approach, which provides robust protection against emerging threats. This includes DDoS attacks, evolving threats targeting IoT devices, and new DNS attack vectors.

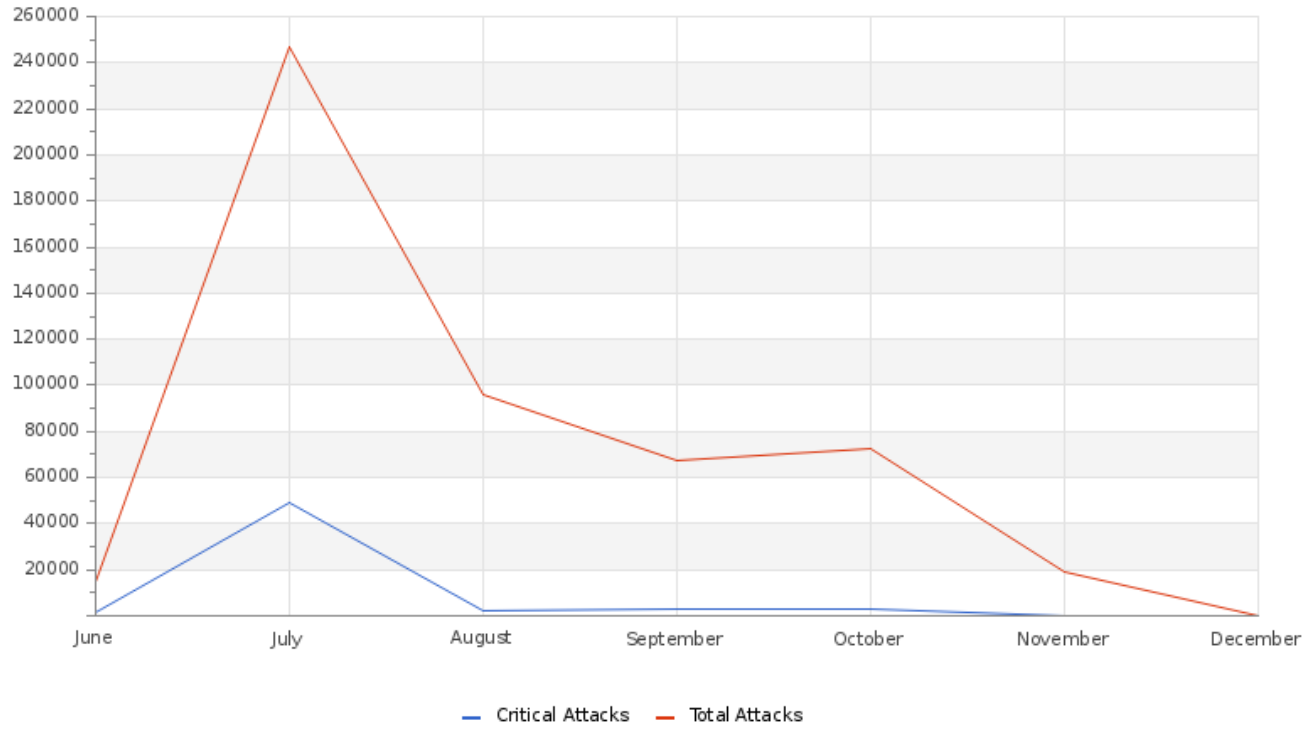
GLESEC 12/12/2023

Critical Attacks Successfully Blocked

0

This month stood out in terms of security with zero critical attacks recorded, marking a significant improvement compared to the 5 blocked last month. This achievement highlights the effectiveness of our advanced security technologies and suggests a decrease in attack attempts against our systems, thereby reinforcing the strength of our protective measures against emerging threats.

Attacks Successfully Blocked



The graph presents encouraging security outcomes, emphasizing the rise in successfully countered attacks. It proactively safeguards against emerging threats, including DDoS attacks, IoT botnets, advanced phishing methods, malware infiltrations, zero-day vulnerabilities, and complex DNS spoofing tactics.

Vulnerability Metric

54

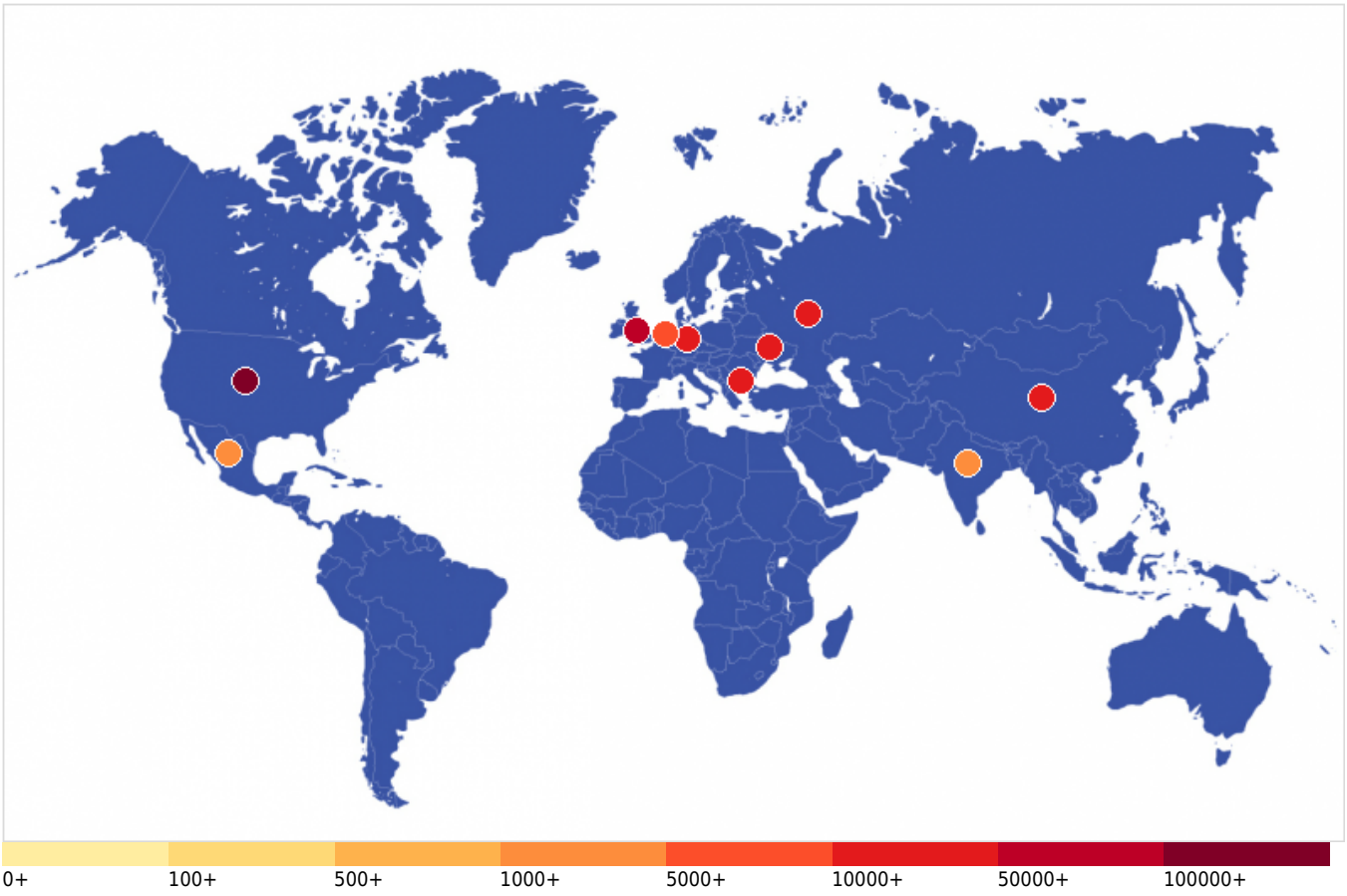
An analysis was conducted on 74 hosts based on their address range, revealing that 49 hosts are vulnerable. These vulnerabilities are categorized by severity, as outlined in the accompanying table. In this timeframe, we recorded 86 vulnerabilities of critical nature, 199 high-risk, 259 medium-risk, and 35 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 54%.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 12/12/2023

Critical Attacks Per Country In Past Week



United States - 306582
Bulgaria - 13912
Mexico - 3053

United Kingdom - 86882
Ukraine - 13337
India - 3046

Germany - 25423
Russia - 10706

China - 13942
Netherlands - 8976

This graph displays the distribution of cyber attacks by country, highlighting the United States' dominance with 306,582 attacks. It is followed by the United Kingdom with 86,882 and Germany with 25,423. Other countries like China, Bulgaria, Ukraine, Russia, the Netherlands, Mexico, and India report lower figures. The map underscores the need to focus cybersecurity efforts mainly on threats originating from the U.S., while maintaining global vigilance.

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