
TLP:AMBER

# BOARDROOM EXECUTIVE REPORT

GLESEC

March 06, 2024

GLESEC 03/06/2024

# 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 |
|---|---|---|
| 9% | 1% | High |

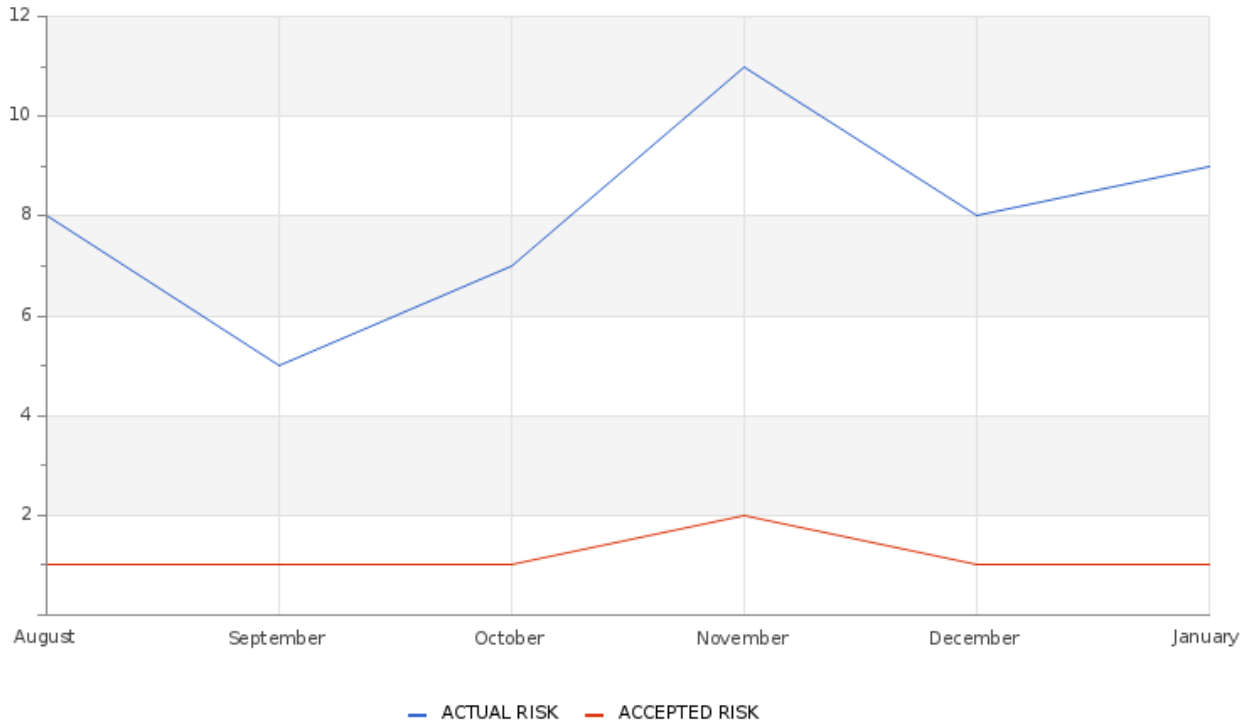


LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 03/06/2024

## 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 9%, and the accepted risk at 1%. This represents a significant rise from the previous month's figures, where the actual risk was recorded at 8% and the accepted risk at 1%.

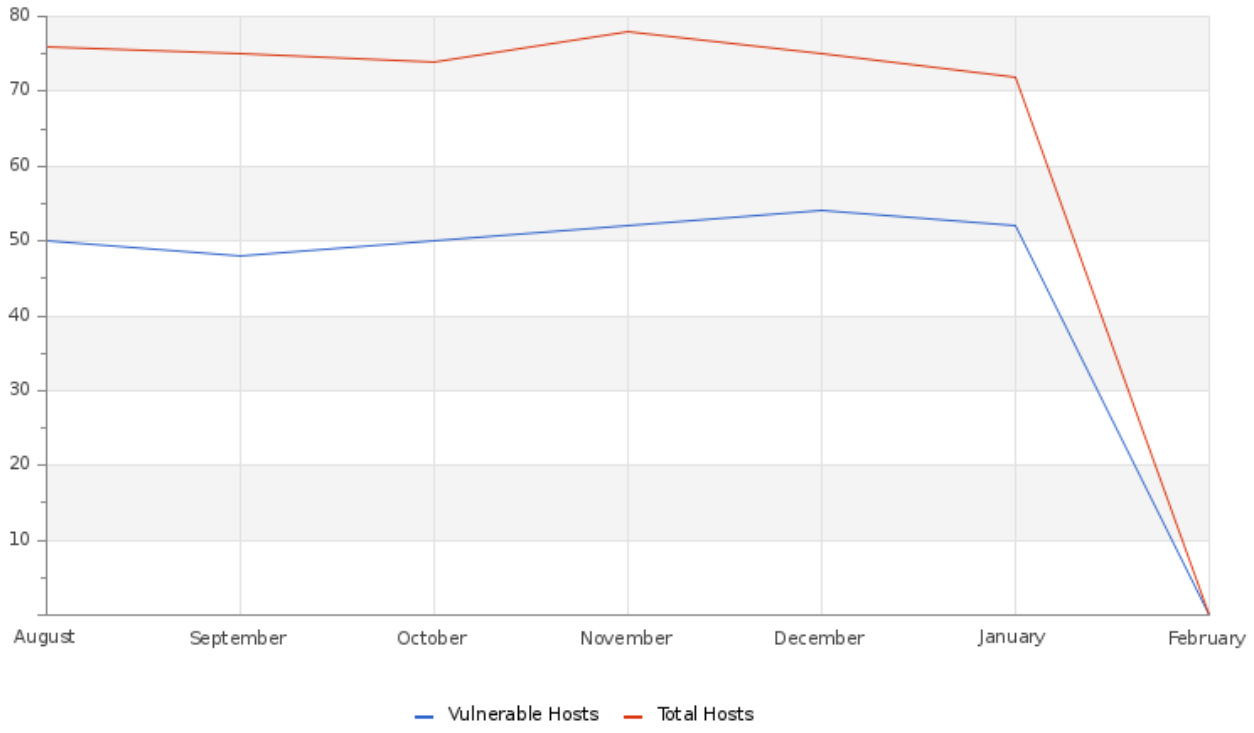


LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 03/06/2024

## Hosts & Vulnerable Hosts In Last 6 Months




The graph reveals a decrease in the number of hosts detected over the month, accompanied by a slight increase in the number of vulnerabilities identified in those hosts. The most notable vulnerabilities were related to the lack of security updates and the use of unsupported software versions. Prompt mitigation of these vulnerabilities is crucial to ensure security, thus minimizing the risk of intrusions and data breaches.

## Total Attacks Successfully Blocked

**360**

During the month, our systems identified and neutralized 360 attempted attacks on your devices. Thanks to constant vigilance and rapid intervention, we have implemented specific strategies to counter continued attacks. It is important to note that a large proportion of these attempts came from compromised IP addresses and Botnets, known for their disruptive nature.

## Critical Attacks Successfully Blocked

**0**

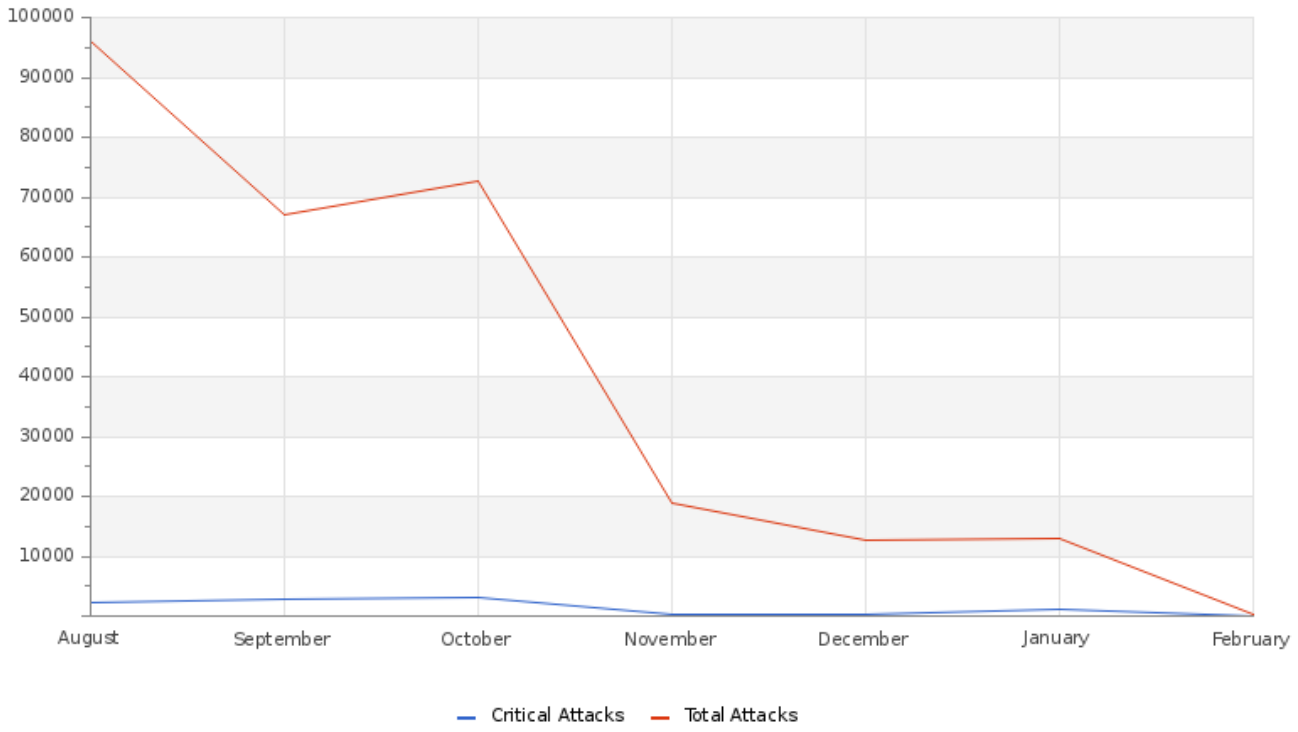
Throughout this month, we managed to maintain the number at 0 critical attacks, in contrast to 309 incidents in the previous month. Our strategy, based on real-time intelligence, continues to provide a robust defense against emerging threats, including DDoS attacks, evolving IoT and novel DNS attack vectors. This is a clear demonstration of the effectiveness and adaptability of our system in the face of the changing threat landscape.



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

## Attacks Successfully Blocked




The chart 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

**37**

An analysis was conducted on 72 hosts based on their address range, revealing that 66 hosts are vulnerable. These vulnerabilities are categorized by severity, as outlined in the accompanying table. In this timeframe, we recorded 46 vulnerabilities of critical nature, 37 high-risk, 249 medium-risk, and 41 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 37%.

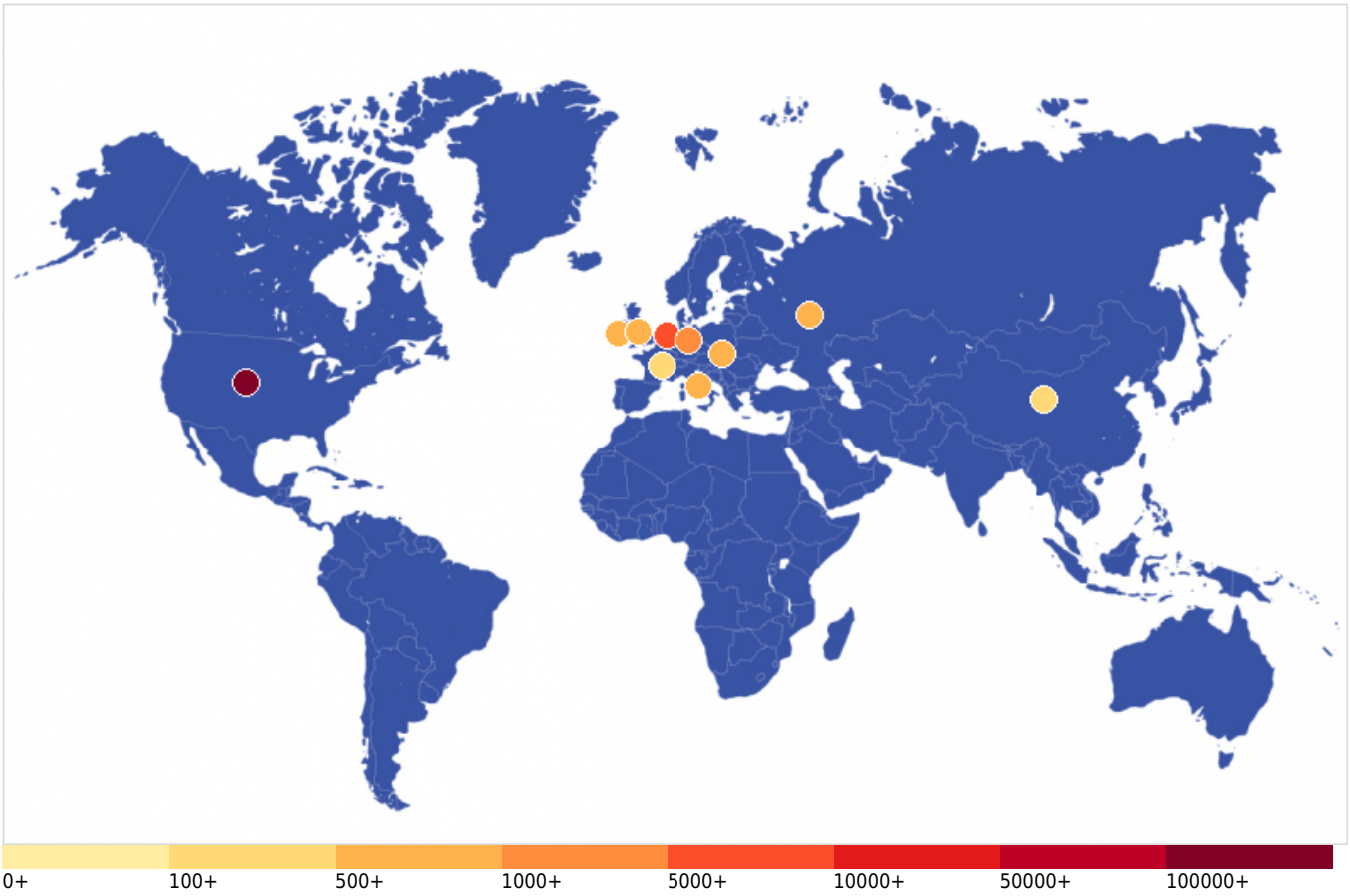
## Critical Attacks Per Country In Past Week



LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 03/06/2024




United States - 140595
Ireland - 852
France - 452
Netherlands - 7924
United Kingdom - 826
China - 443
Germany - 1099
Russia - 514
Italy - 908
Slovakia - 504

This graph displays the distribution of cyber attacks by country, highlighting the United States' dominance with 140,595 attacks. It is followed by the Netherlands with 7,924 and Germany with 1,099. 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