TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC

April 02, 2024

GLESEC 04/02/2024

TLP AMBER BOARDROOM

EXECUTIVE REPORT

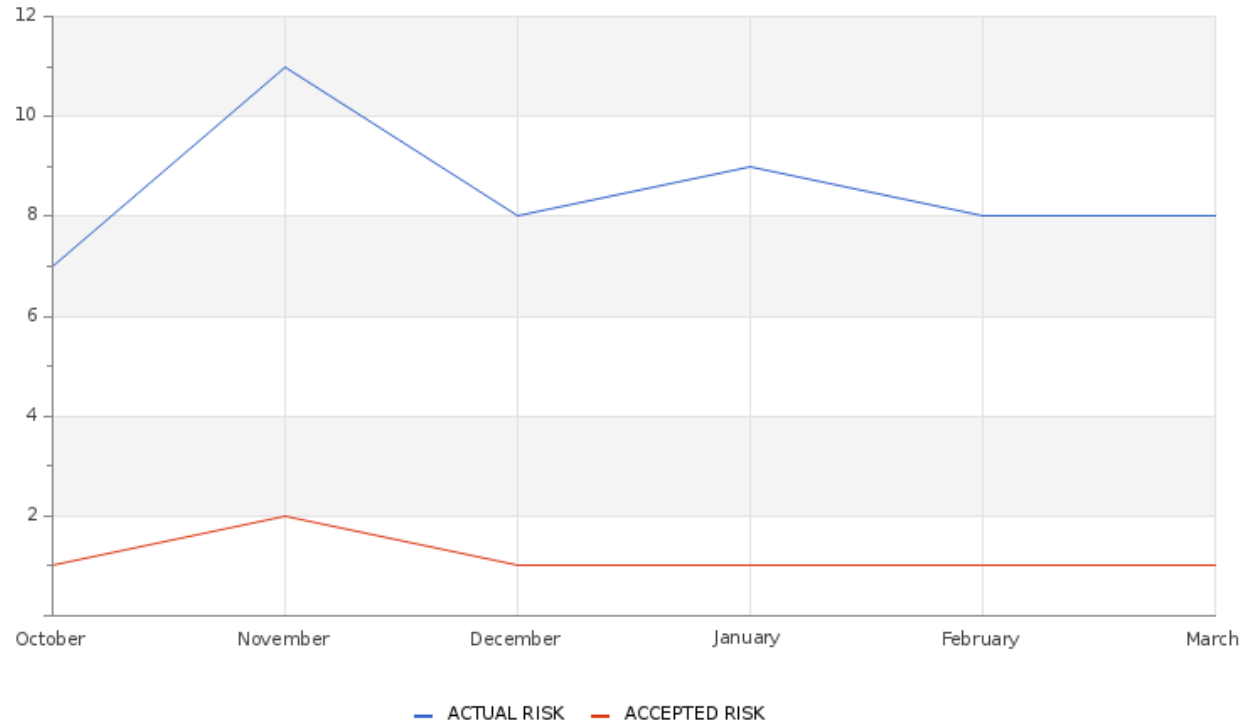
This report corresponds to THIS MONTH and it is directed to Director or VP of IT, Cyber Security, Cyber Security Compliance or equivalent. The information is delivered following the GLESEC`s Seven Elements Cyber Security Model (7eCSM TM), these elements are: Risk, Vulnerabilities, Threats, Assets, Compliance, 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
8%	1%	Medium

Accepted & Actual Risk

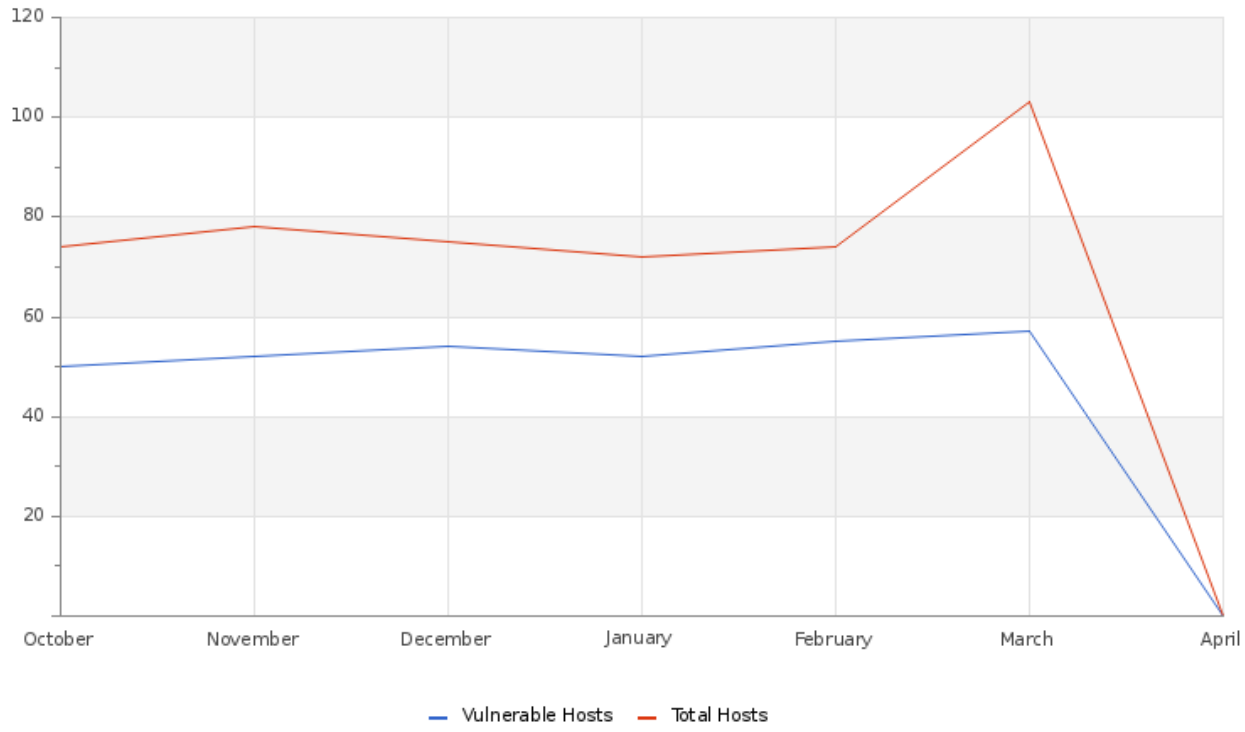


Over this month, the observed increase in risk levels is noteworthy. The actual risk now is at 8%, with the accepted risk being 1%. This marks a notable change from last month, where the risk stood at 8% and the accepted risk was at 0%.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Hosts & Vulnerable Hosts In Last 6 Months



This month, our observations indicate that the actual risk has remained stable at 8%, while there has been a 1-point increase in the accepted risk, now at 1%, compared to last month's figures. These developments in cybersecurity metrics highlight the fluid nature of our digital environment. They underscore the need for constant vigilance and the importance of adapting to the continuously evolving landscape of information security.

Total Attacks Successfully Blocked

677

The chart showcases positive security outcomes, highlighting an increase in successfully neutralized attacks. It reflects the effectiveness of proactive measures in guarding against emerging threats, such as DDoS attacks, IoT botnets, sophisticated phishing techniques, malware intrusions, zero-day vulnerabilities, and intricate DNS spoofing strategies.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

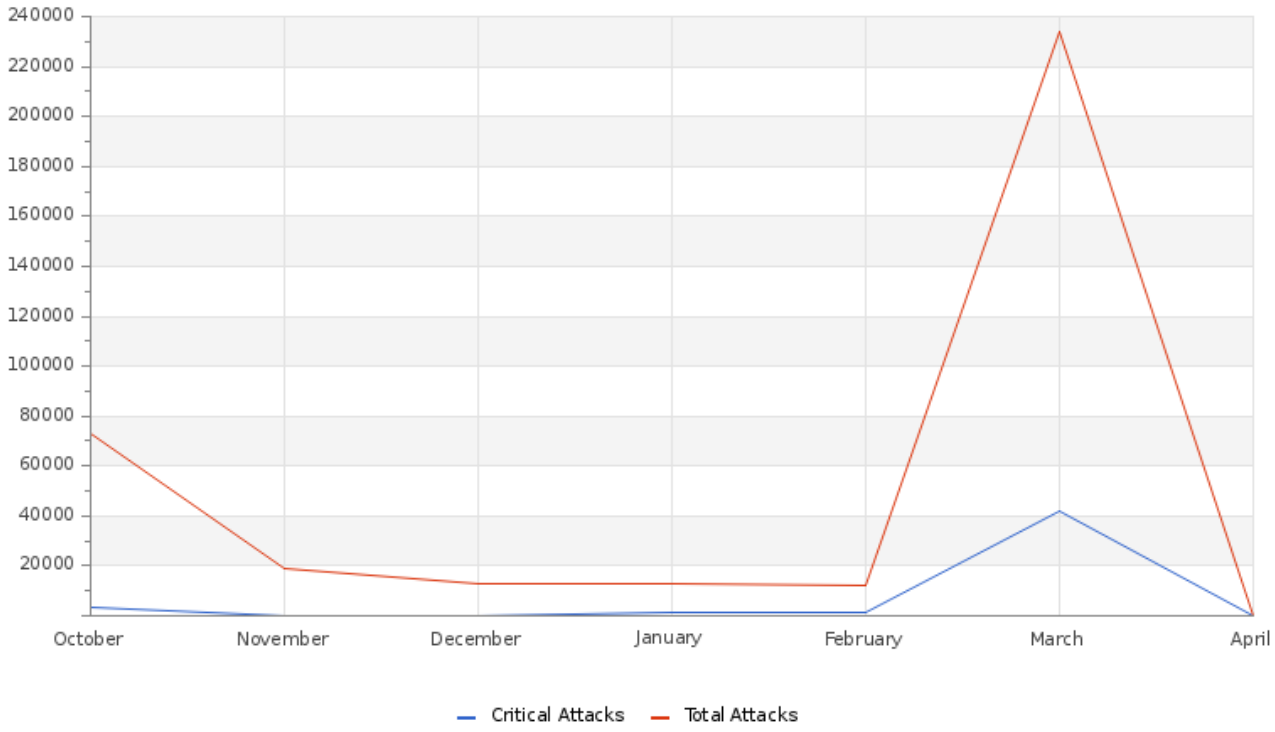
GLESEC 04/02/2024

Critical Attacks Successfully Blocked

10

Throughout this month, we managed to maintain the number at 10 critical attacks, in contrast to 677 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.

Attacks Successfully Blocked



The chart vividly illustrates the positive impact of enhanced security measures through a detailed breakdown by severity of neutralized attacks. This distinction allows for a clear view of how well the security infrastructure is performing against threats of varying levels of danger. By categorizing the thwarted attacks as critical, high, medium, or low severity, the data provides insights into the robustness of the defensive strategies employed. It reveals not only the capability to manage the most severe threats but also the thoroughness in addressing lesser risks, ensuring comprehensive protection.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

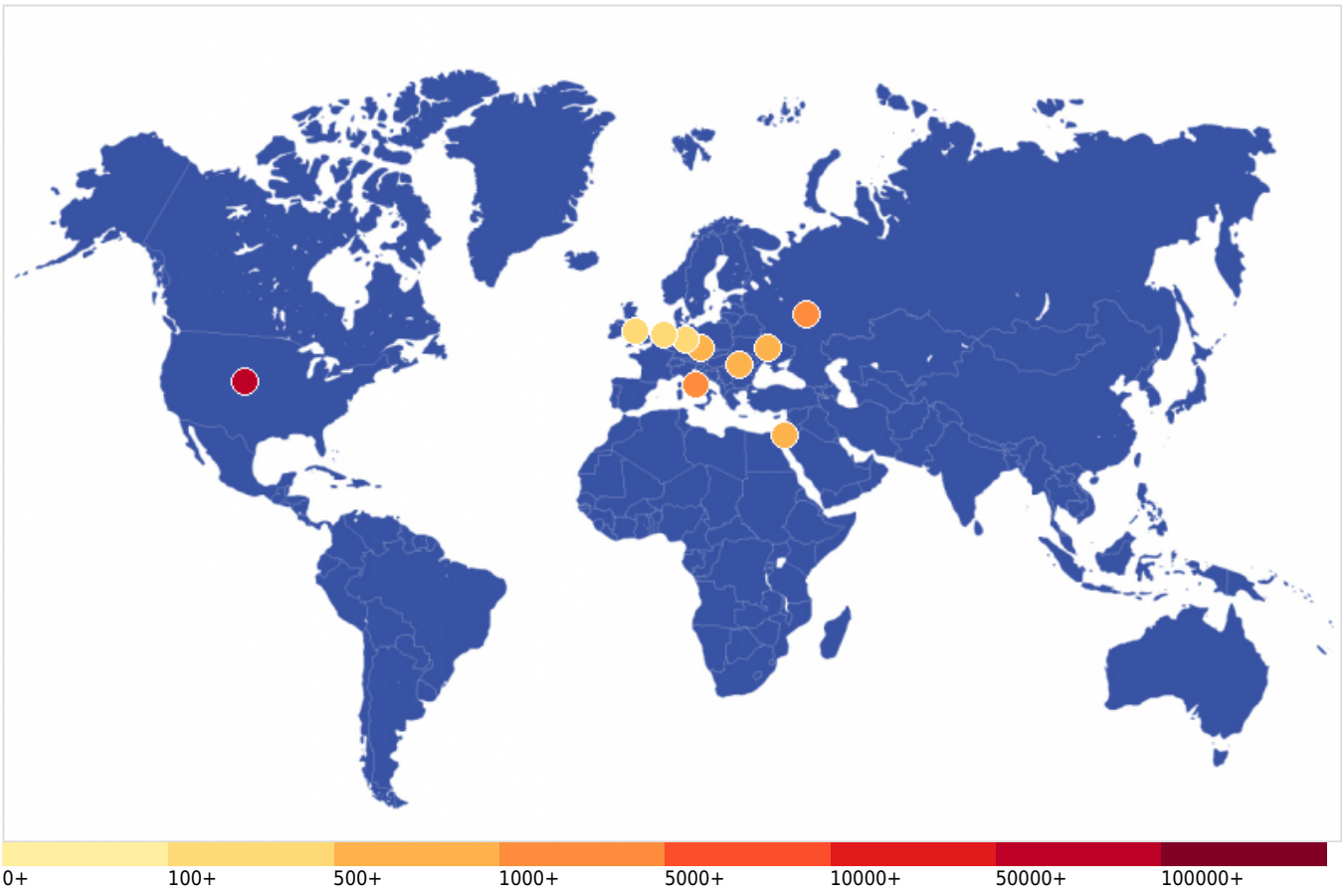
GLESEC 04/02/2024

Vulnerability Metric

23

The analysis performed on 72 hosts within a specified address range showed that none of the hosts are vulnerable, as indicated by the detailed severity categorization in the accompanying table. During this assessment period, the findings highlighted a total absence of vulnerabilities across all severity levels: 23 critical, 35 high-risk, 273 medium-risk, and 52 low-risk vulnerabilities were recorded. Despite the absence of identified vulnerabilities, your organization's vulnerability index stands at 23%.

Critical Attacks Per Country In Past Week



United States - 55744
Israel - 635
United Kingdom - 261
Italy - 2072
Czechia - 631
Netherlands - 250
Russia - 1263
Romania - 548
Ukraine - 678
Germany - 272

This graph illustrates the cyber attack distribution across countries, with the United States leading significantly at 55,744 attacks. The Italy comes next with 2072 attacks, followed by Russia with 1263. Lower attack numbers are reported in China, Bulgaria, Ukraine, Russia, the Netherlands, Mexico, and India. The data emphasizes the importance of concentrating cybersecurity efforts on threats emanating from the U.S., while still keeping a watchful eye on global cybersecurity challenges.

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

GLESEC 04/02/2024

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

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