TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC

March 12, 2024

GLESEC 03/12/2024

TLP AMBER BOARDROOM

EXECUTIVE REPORT

This report corresponds to February 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.

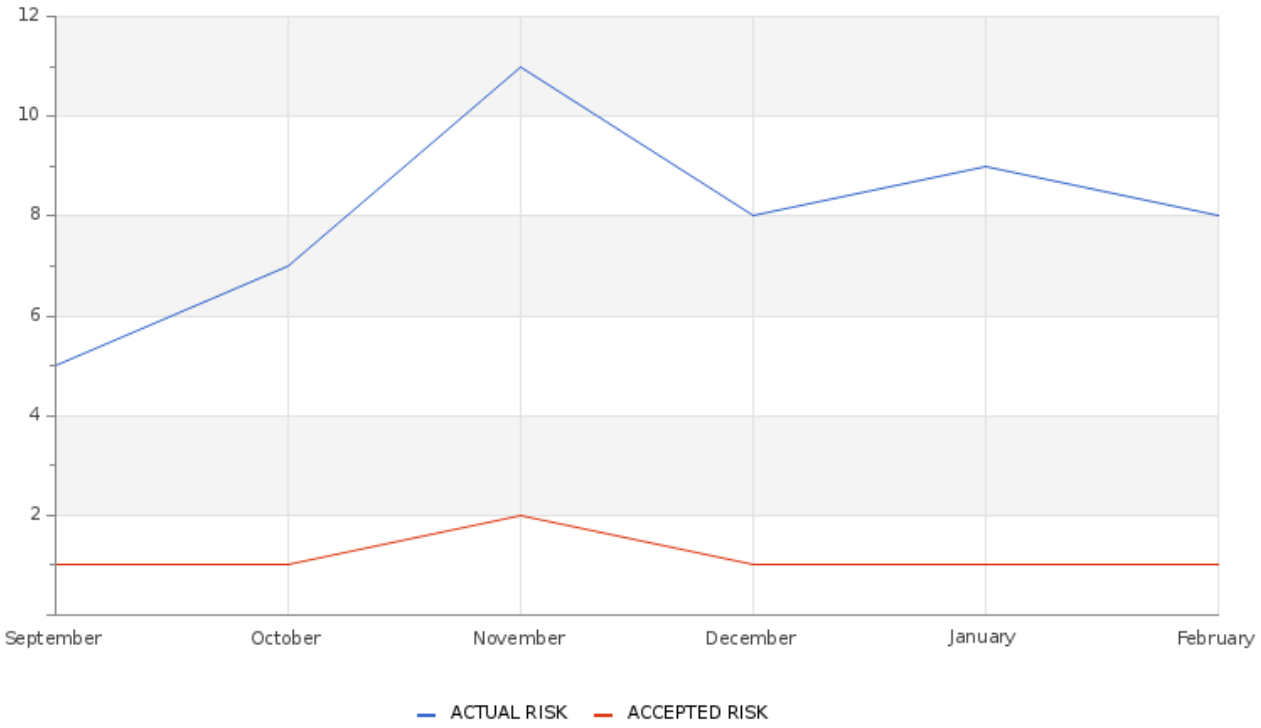
Actual Risk	Accepted Risk	Confidence
8%	1%	High

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 03/12/2024

Accepted & Actual Risk



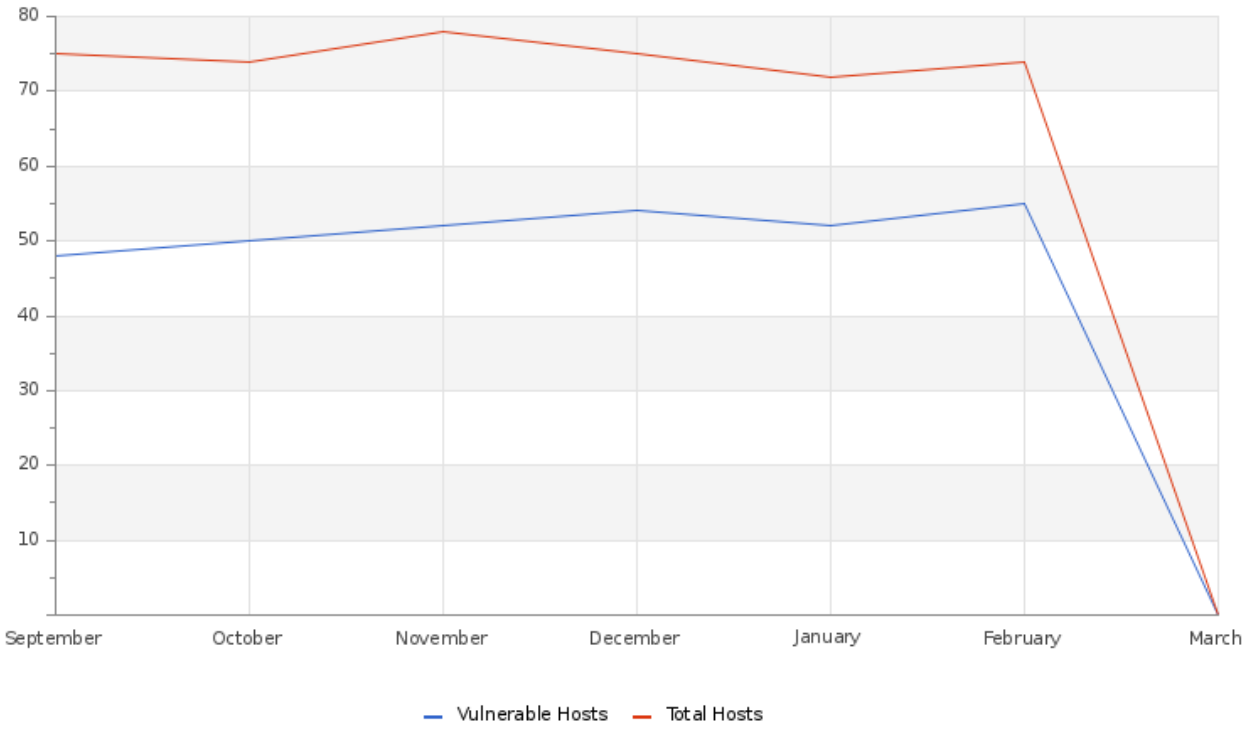
Throughout this month, there has been a marked escalation in risk levels, with the current risk now evaluated at 8%, contrasted against an accepted risk of 0%. This indicates a noteworthy increase from last month's data, which documented the actual risk at 9% and the accepted risk at 1%.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 03/12/2024

Hosts & Vulnerable Hosts In Last 6 Months



The graph illustrates a rise in the number of identified hosts coupled with a decline in vulnerabilities over the month, hinting at possible breaches in the security perimeter. Noteworthy among the high-risk vulnerabilities are several iterations of Adobe Acrobat, each with distinct vulnerabilities. These are further elucidated in reports such as KB5034768, detailing a Security Update for Windows 10 version 1809 and Windows Server 2019 (February 2024), as well as the identification of a Heap Buffer Overflow vulnerability in libcurl versions 7.69 to below 8.4.0, and a Security Update for Microsoft Visual Studio Code (November 2023). Swift action in addressing these vulnerabilities is imperative to fortify the security landscape.

Total Attacks Successfully Blocked

393

Throughout the month, our systems detected and neutralized 393 attempted attacks targeting your devices. Through unwavering vigilance and prompt response measures, we've deployed targeted strategies to thwart ongoing attacks effectively. It's noteworthy that a significant number of these attempts originated from compromised IP addresses and Botnets, which are infamous for their potential to disrupt. This highlights the critical importance of our continuous monitoring and adaptive security measures in safeguarding your digital assets.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

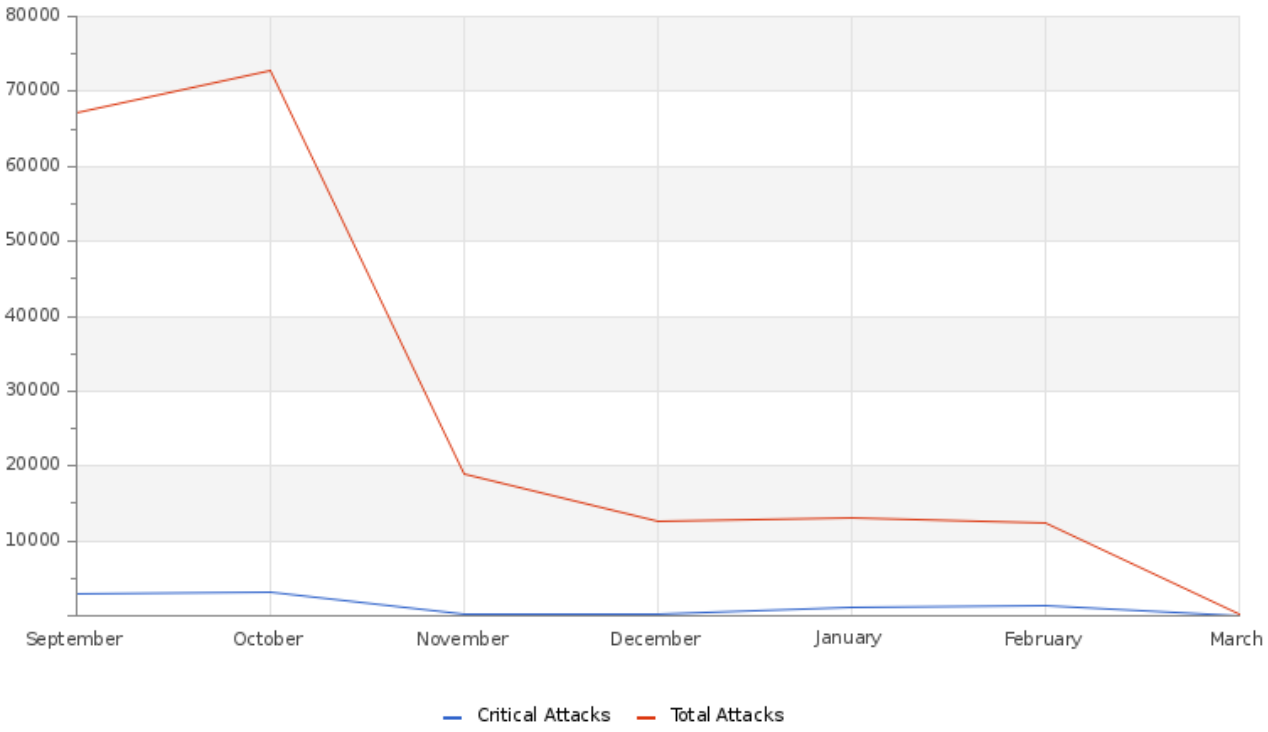
GLESEC 03/12/2024

Critical Attacks Successfully Blocked

0

Throughout this month, we managed to maintain the number at 0 critical attacks, in contrast to 393 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 showcases positive security trends, highlighting an increase in the number of attacks that have been successfully neutralized. This proactive stance enhances protection against emerging threats, such as Distributed Denial of Service (DDoS) attacks, Internet of Things (IoT) botnets, sophisticated phishing techniques, malware incursions, zero-day vulnerabilities, and intricate Domain Name System (DNS) spoofing strategies.

Vulnerability Metric

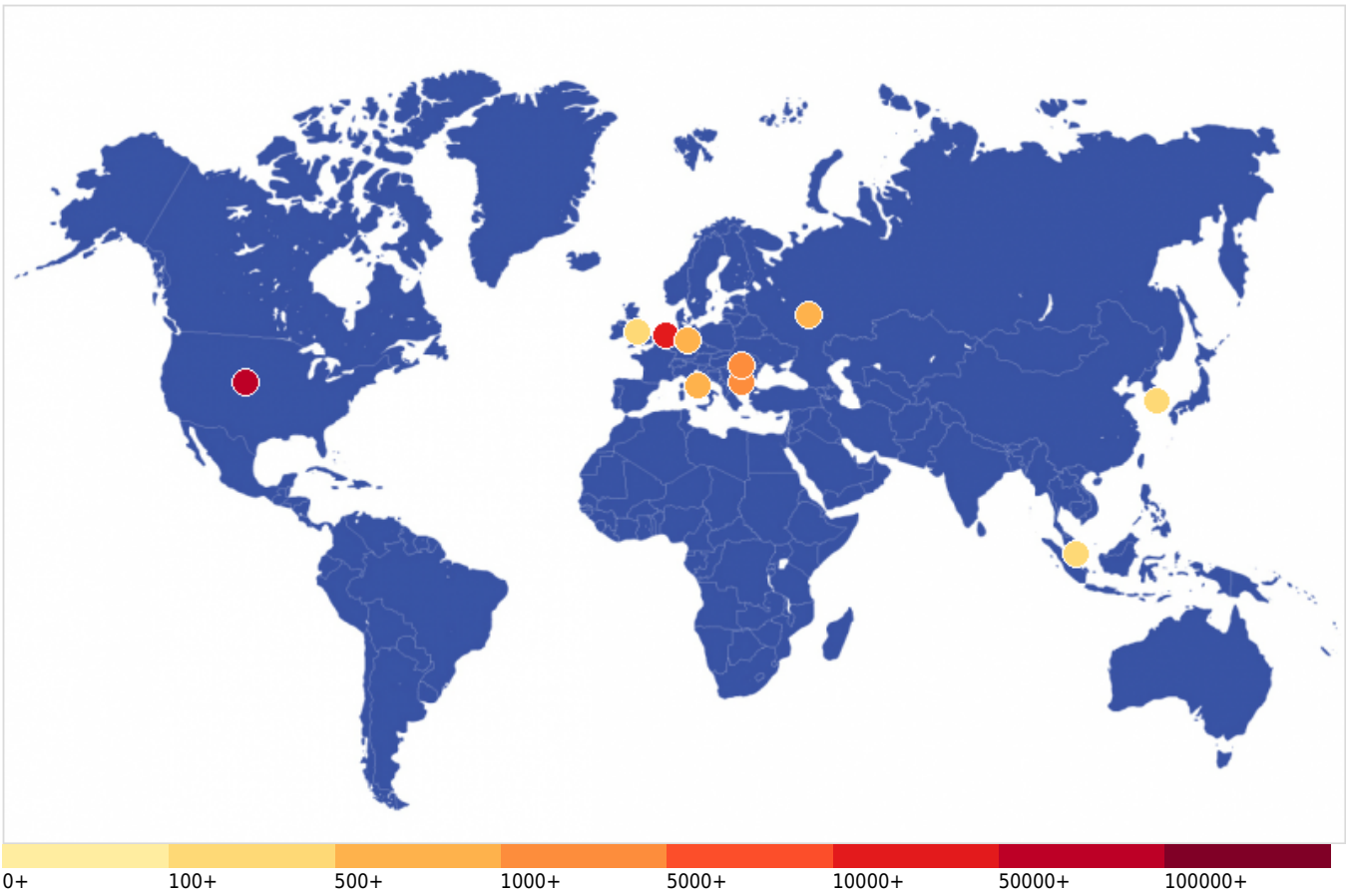
32

An analysis was conducted on 72 hosts based on their address range, revealing that 0 hosts are vulnerable. These vulnerabilities are categorized by severity, as outlined in the accompanying table. In this timeframe, we recorded 0 vulnerabilities of critical nature, 0 high-risk, 0 medium-risk, and 0 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 32%.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Critical Attacks Per Country In Past Week



United States - 54377
Germany - 706
United Kingdom - 430
Netherlands - 15309
Italy - 698
South Korea - 407
Bulgaria - 2949
Russia - 668
Romania - 2619
Singapore - 439

The graph presents a breakdown of cyber attacks by country, emphasizing the United States' leading position with 54,377 attacks. The Netherlands ranks second with 15,309 attacks, followed by Bulgaria with 2,949. Lower incidence rates are reported in countries such as Romania, Germany, Ukraine, Italy, Russia, Singapore, and United Kingdom. This distribution signals a crucial need for prioritizing cybersecurity measures against threats emanating predominantly from the U.S., without neglecting the importance of a worldwide alertness.

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

GLESEC 03/12/2024

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