TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC

June 10, 2024

GLESEC 06/10/2024

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.

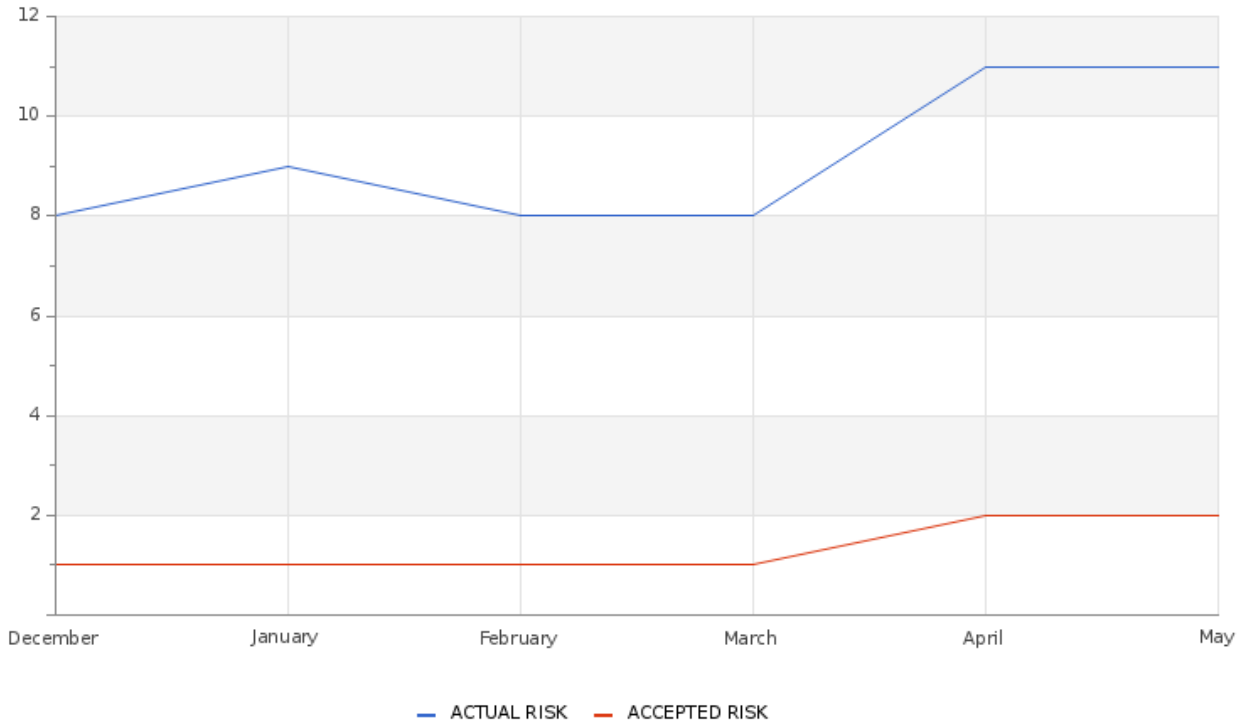
Actual Risk	Accepted Risk	Confidence
11%	2%	Medium

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 06/10/2024

Accepted & Actual Risk



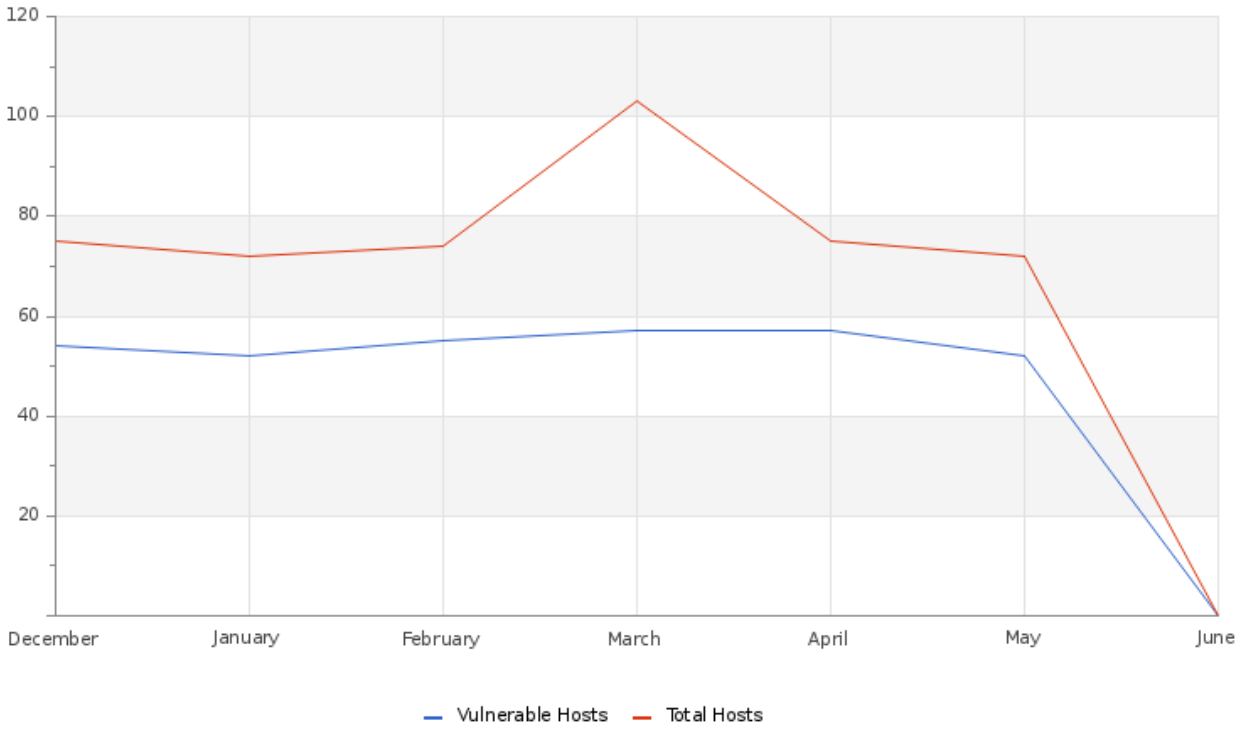
During the past month, risk levels have remained stable. Currently, the actual risk stands at 11%, while the accepted risk is 0%. These figures indicate continuity with respect to the previous month, when the actual risk was also 11% and the accepted risk was 2%.

Hosts & Vulnerable Hosts In Last 6 Months

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 06/10/2024



The graph illustrates a rise in the number of identified hosts coupled with a decline in vulnerabilities over the month, which may indicate potential breaches in the security perimeter. Noteworthy among the high-risk vulnerabilities are several iterations of Adobe Acrobat, each with distinct issues. Additionally, significant vulnerabilities include:
- Google Chrome < 123.0.6312.58 Multiple Vulnerabilities
- KB5035849: Windows 10 version 1809 / Windows Server 2019 Security Update (March 2024)
- OpenSSL 1.0.2 < 1.0.2zf Vulnerability
- Security Update for Microsoft Visual Studio Code (November 2023)
- Ubuntu 22.04 LTS / 23.04: Linux kernel vulnerabilities (USN-6534-1)
- libcurl 7.69 < 8.4.0 Heap Buffer Overflow

These vulnerabilities highlight the importance of continuous monitoring and timely updates to ensure the security of the infrastructure.

Total Attacks Successfully Blocked

399

During the month, our systems identified and neutralized 399 attempted attacks on your devices. Thanks to constant vigilance and rapid intervention, we have implemented specific strategies to counter ongoing threats. It is important to note that a significant proportion of these attempts originated from compromised IP addresses and botnets, which are known for their disruptive nature.

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

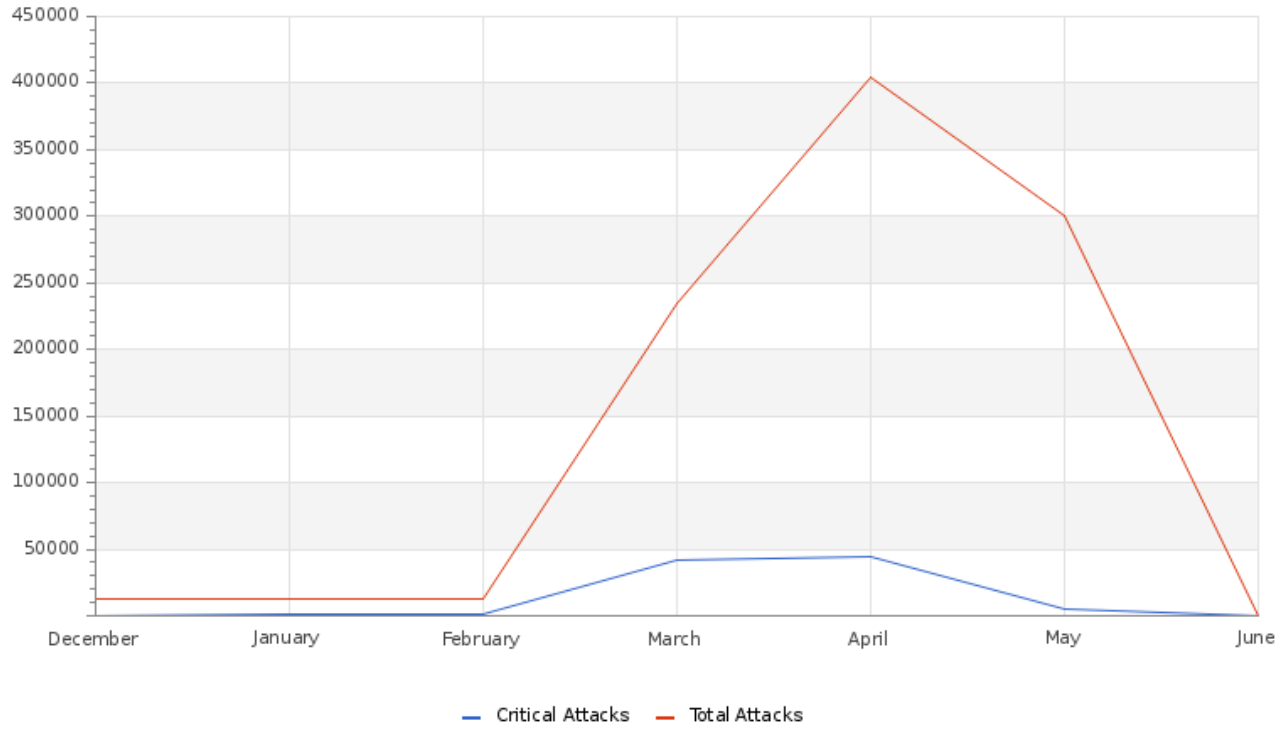
GLESEC 06/10/2024

Critical Attacks Successfully Blocked

10

Throughout this month, we successfully maintained the number of critical attacks at ten, a significant improvement compared to the 399 incidents in the previous month. Our strategy, based on real-time intelligence, continues to provide robust defense against emerging threats, including DDoS attacks, evolving IoT threats, and novel DNS attack vectors. This demonstrates the effectiveness and adaptability of our system in the face of a constantly changing threat landscape.

Attacks Successfully Blocked



The chart presents encouraging security outcomes, highlighting the rise in successfully countered attacks. These measures proactively safeguard against emerging threats, including DDoS attacks, IoT botnets, advanced phishing methods, malware infiltrations, zero-day vulnerabilities, and sophisticated DNS spoofing tactics.

Vulnerability Metric

60

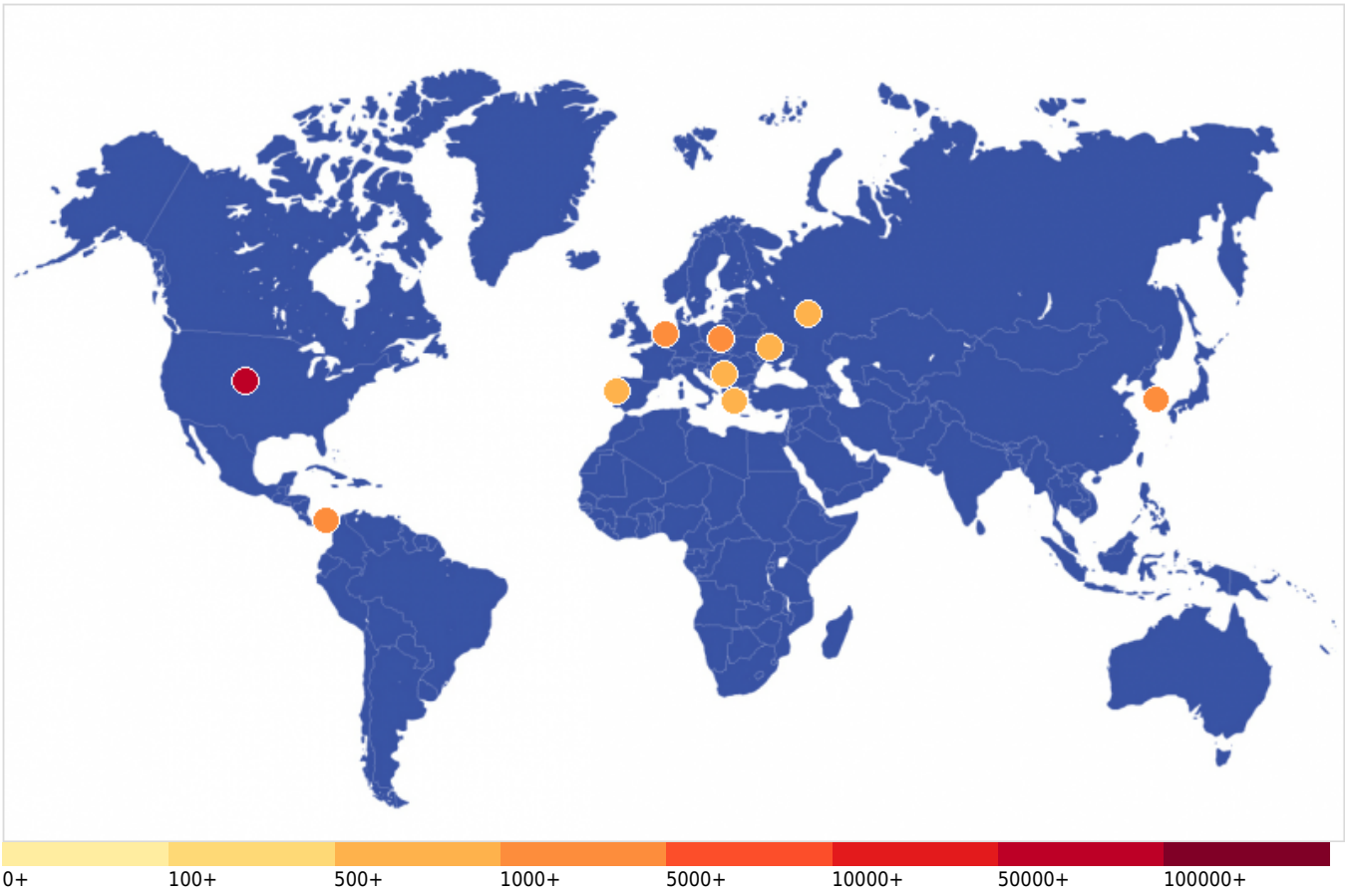
An analysis was conducted on 73 hosts based on their address range, revealing that 49 hosts are vulnerable. These vulnerabilities are categorized by severity, as outlined in the accompanying table. In this timeframe, we recorded 56 vulnerabilities of critical nature, 56 high-risk, 332 medium-risk, and 63 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 60%.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 06/10/2024

Critical Attacks Per Country In Past Week



United States - 59985
Poland - 1188
Serbia - 740

Panama - 2509
Russia - 852
Greece - 738

Netherlands - 2113
Ukraine - 852

South Korea - 1296
Portugal - 773

This graph displays the distribution of cyber attacks by country, highlighting the United States' dominance with 59,985 attacks. It is followed by the Panama with 2,509 and Netherlands with 2113. Other countries like South Korea, Poland, Russia, Ukraine, Portugal, Serbia, and Greece 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

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