TLP:AMBER

BOARDROOM EXECUTIVE REPORT

GLESEC

September 21, 2023

GLESEC 09/21/2023

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.

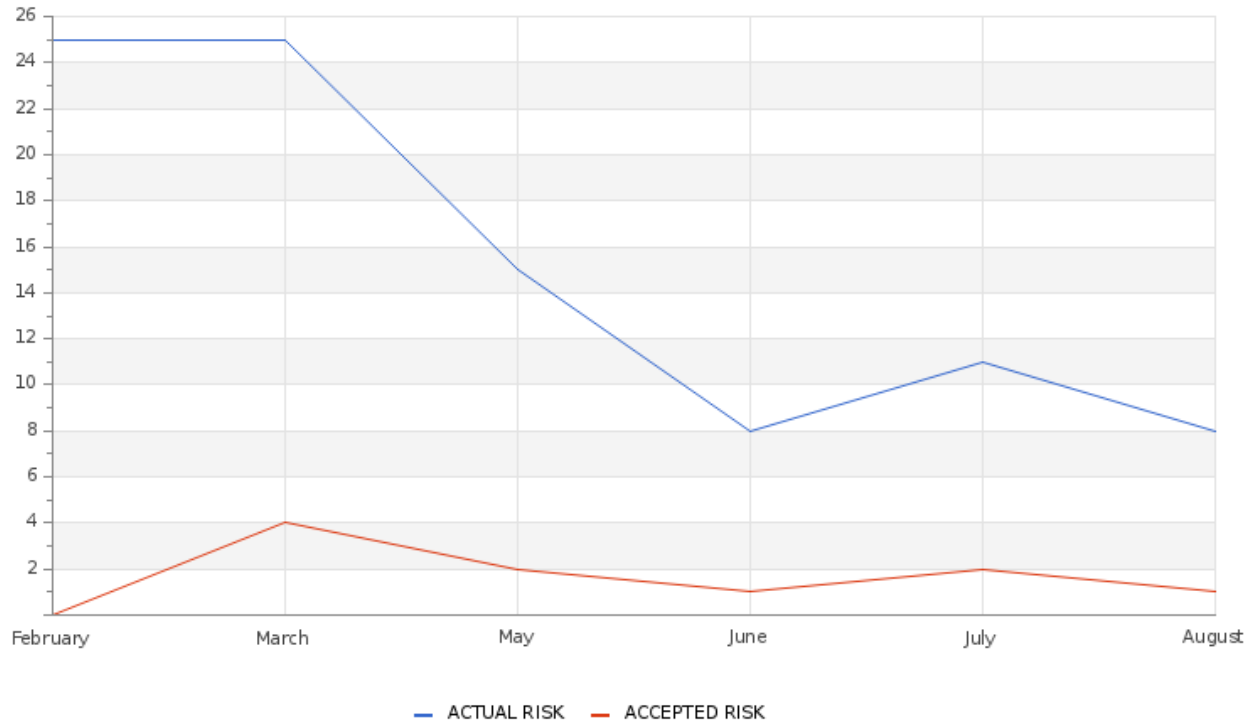
Actual Risk	Accepted Risk	Confidence
8%	1%	High

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 09/21/2023

Accepted & Actual Risk



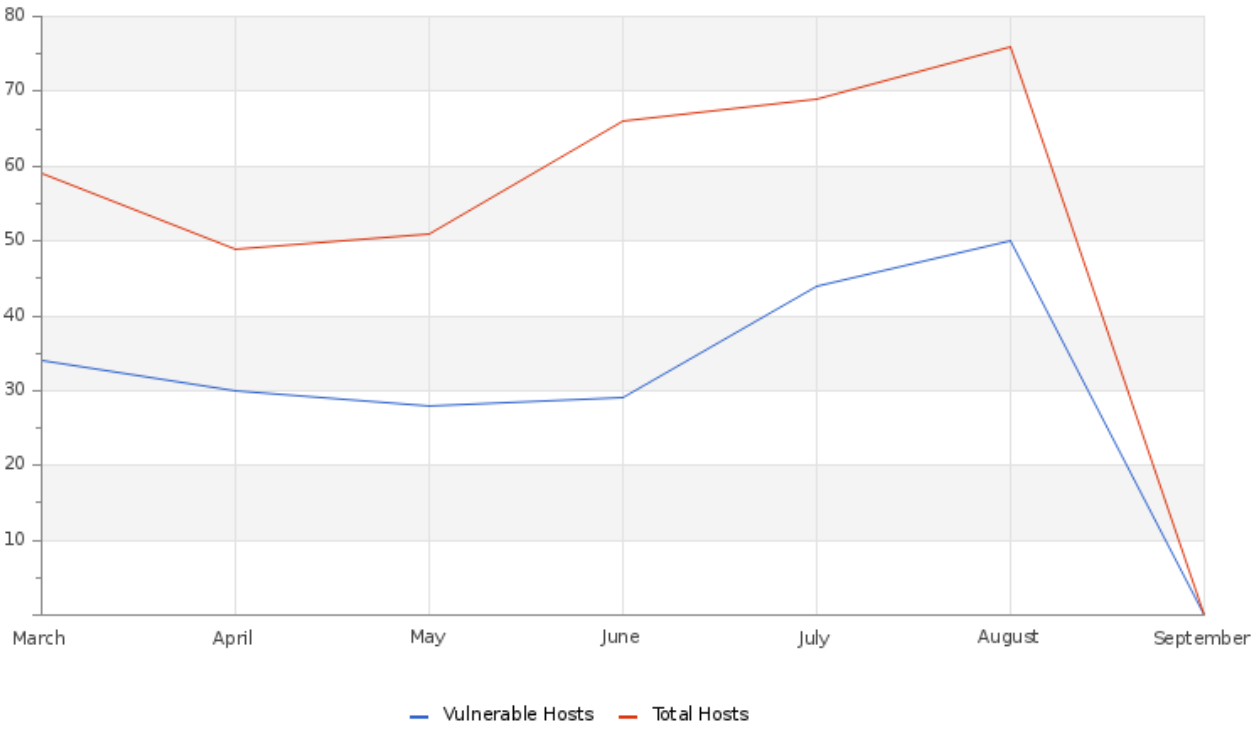
The current risk level has decreased. During this month, the current risk stands at 8, while the accepted risk remains at 1. Compared to the previous month, when the current risk was 10 and the accepted risk was 2, it is evident that the risk has decreased.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 09/21/2023

Hosts & Vulnerable Hosts In Last 6 Months



The graphic shows an increase in the number of hosts discovered and a decrease in vulnerabilities during the month. From this, we observe breaches in its security perimeter. Among the high-risk vulnerabilities, vulnerabilities in Apache POI, insecure Windows permissions, Cross-site scripting (DOM-based) and pending updates to Microsoft ASP.NET Core were identified. It is critical to also consider updating Palo Alto's GlobalProtect. To ensure a more secure environment, it is essential to address these areas promptly.

Total Attacks Successfully Blocked

180

During the month, our systems identified and neutralized 180 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.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

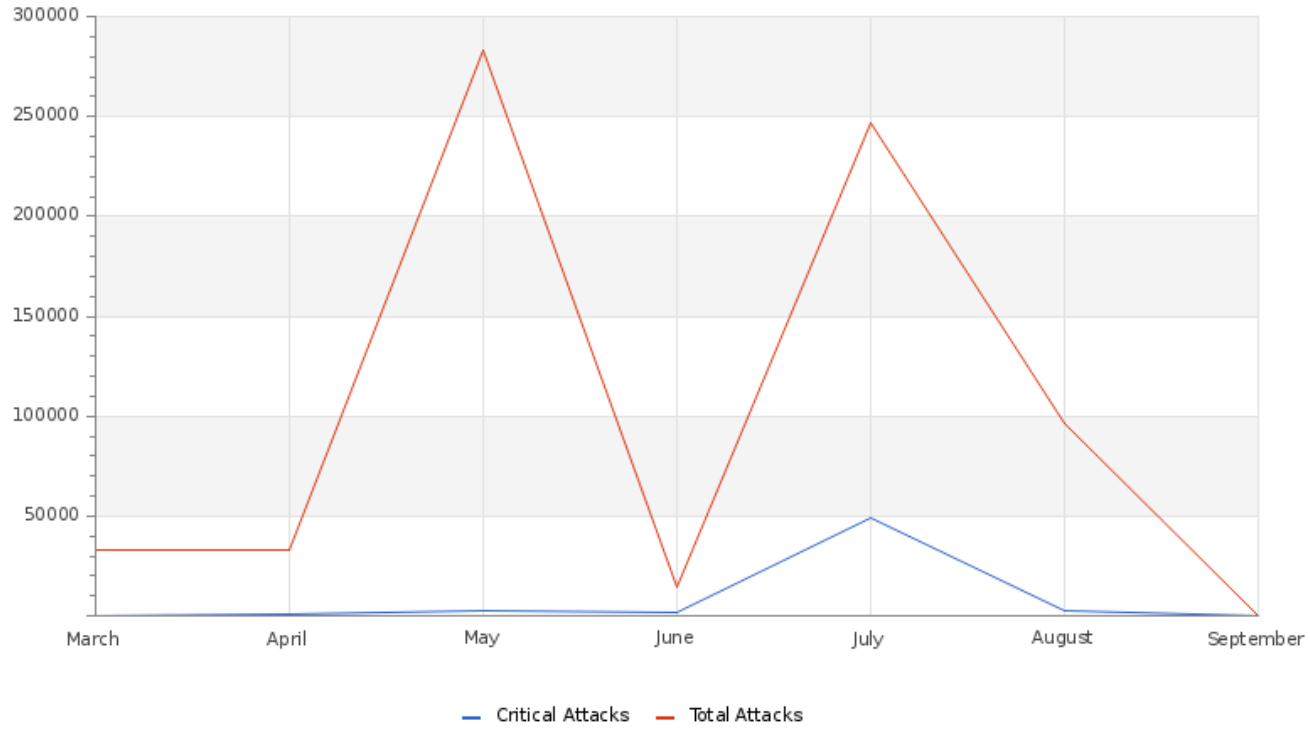
GLESEC 09/21/2023

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.

Attacks Successfully Blocked



The graph shows favorable results in terms of security, highlighting the increase in the number of successfully neutralized attacks. Proactively, it has protected against emerging risks, such as DDoS attacks, IoT botnets, advanced phishing techniques, malware intrusions, zero-day threats and sophisticated DNS spoofing attack strategies.

Vulnerability Metric

29

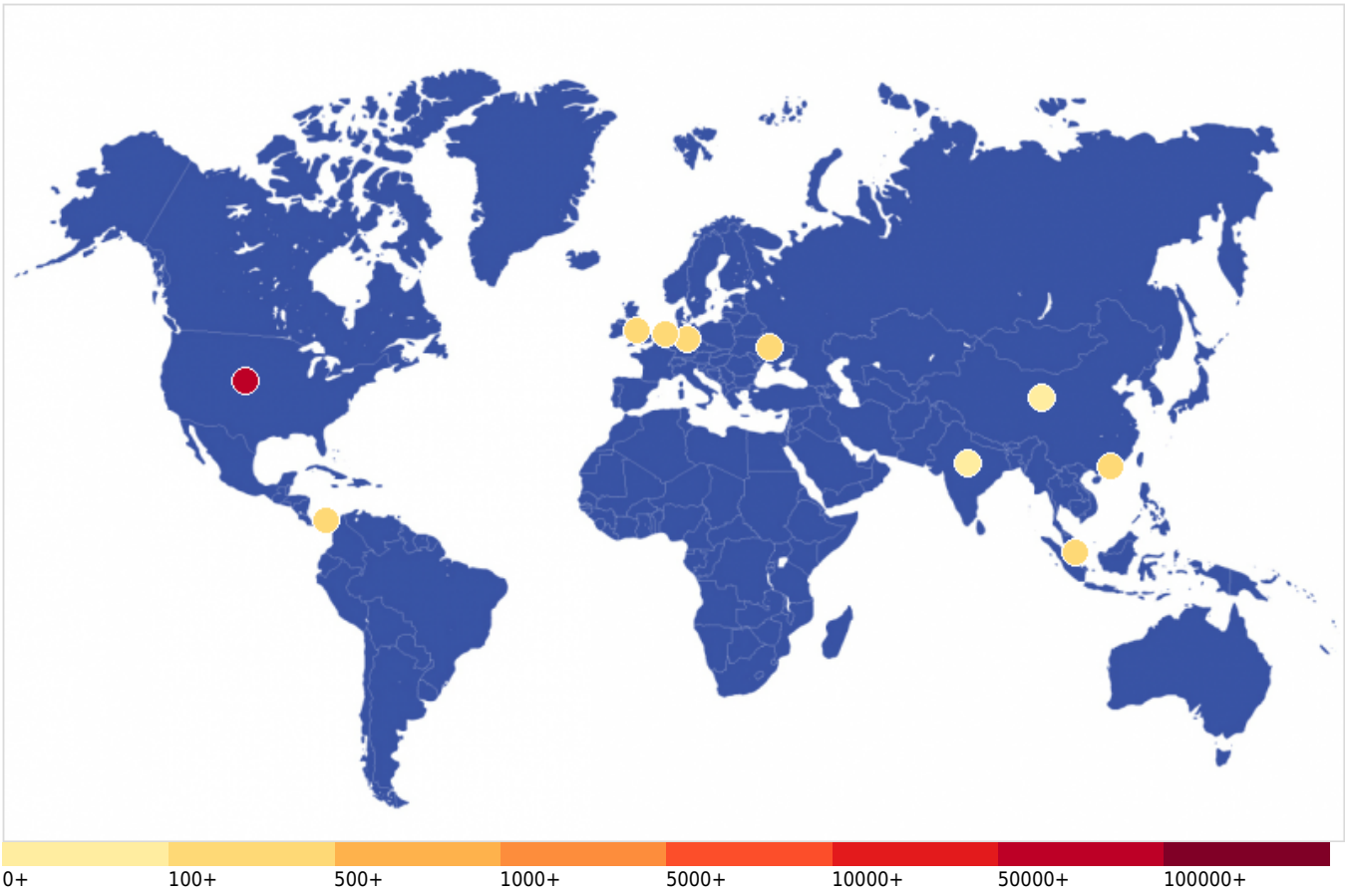
According to the range of addresses, a total of 67 hosts were analyzed, of which 34 were found to be vulnerable. Vulnerabilities are categorized according to their severity, as detailed in the table below. During this period, no critical vulnerabilities were recorded, but 8 high-risk vulnerabilities, 103 medium-risk vulnerabilities and 22 low-ranking vulnerabilities were recorded. Based on this data, the vulnerability index of your organization stands at 29%.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

GLESEC 09/21/2023

Critical Attacks Per Country In Past Week



United States - 52880
Ukraine - 152
China - 97
Germany - 190
Singapore - 146
India - 59
Panama - 183
Netherlands - 107
United Kingdom - 160
Hong Kong - 100

The graph shows that the vast majority of attacks, with a total of 52,880, originate in the United States. In contrast, Germany, the UK and Ukraine show considerably lower numbers, with fewer than 200 attacks per country. Given such an imbalance, cybersecurity strategies should focus primarily on threats originating in the United States.

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