TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

August 20, 2023

GLESEC 08/20/2023

TLP AMBER CISO

EXECUTIVE REPORT

This report corresponds to july 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.

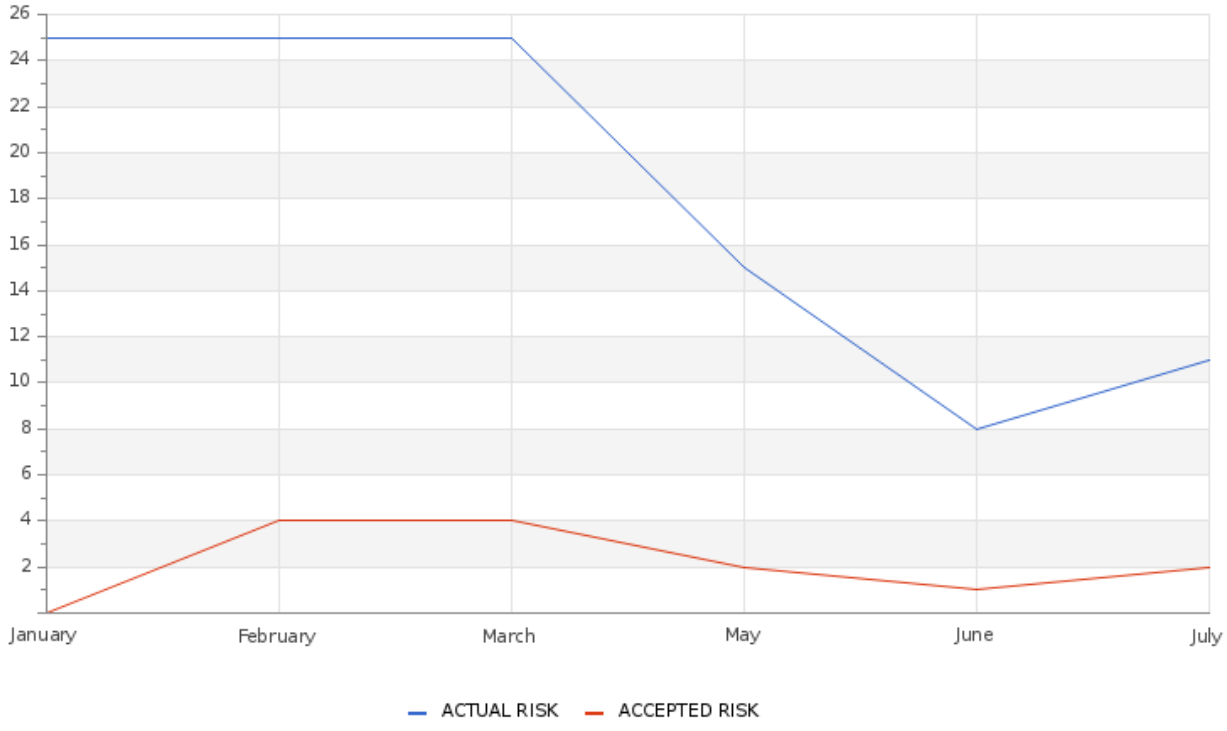
RISK

Actual Risk	Accepted Risk	Confidence
11%	**2%**	**High**
This is your company's current Actual Risk.	This is your company's current Accepted Risk.	The degree of confidence of the previous two figures.

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

GLESEC 08/20/2023

Accepted & Actual Risk



Accepted/Actual Risk has seen an increase in the month of July.

Table of Comparison of Actual and Acceptable Risk From Current to Previous Month

	Current Month	Previous Month
Actual Risk	11	10
Accepted Risk	2	2

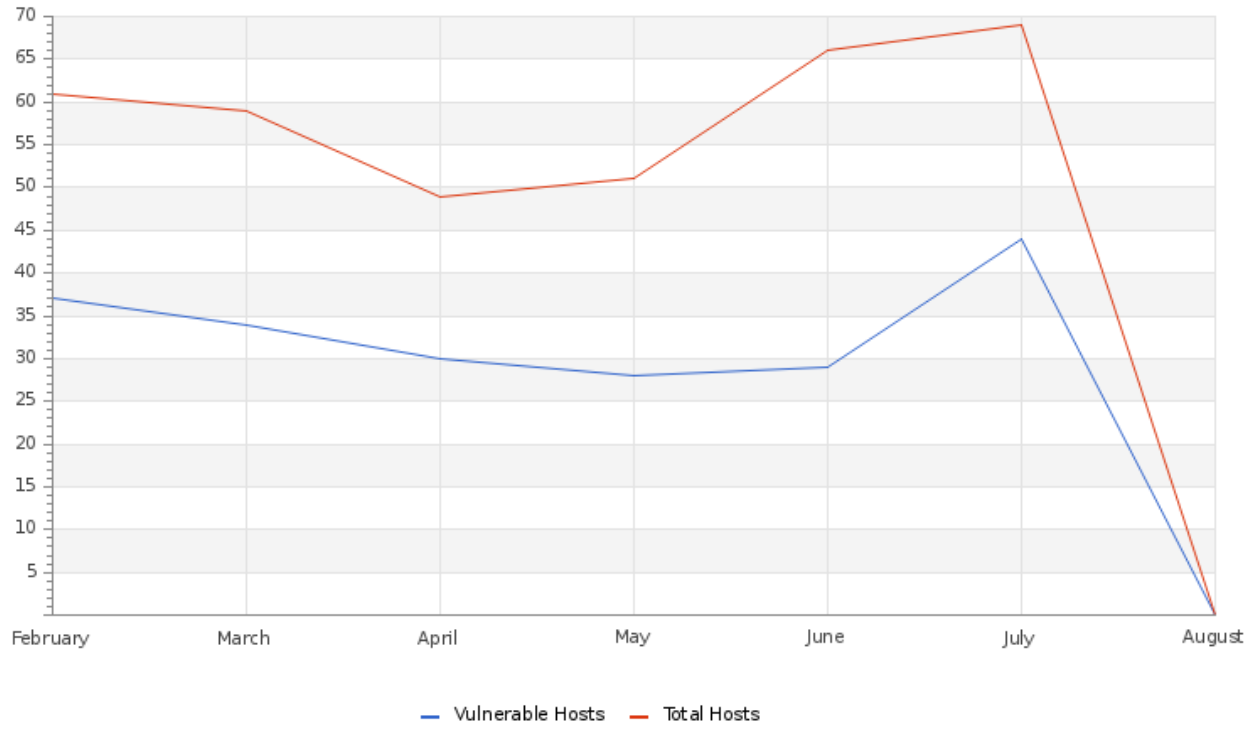
Your Actual Risk has gone up 1 point from the previous month;
Your Accepted Risk has remained the same since the previous month.

VULNERABILITY

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

GLESEC 08/20/2023

Hosts & Vulnerable Hosts In Last 6 Months



The number of Hosts discovered has increased slightly this month.
The number of Vulnerable Hosts has increased greatly this month.

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

GLESEC 08/20/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	56	56
Hosts Discovered	64	49
Vulnerable Hosts	40	27
Critical Vulnerabilities Count	0	0
High Vulnerabilities Count	2	4
Medium Vulnerabilities Count	115	89
Low Vulnerabilities Count	23	12
Phishing Score	0	0
Email Gateway Score	10	10
Web Application Firewall Score	24	24
Web Gateway Score	51	52
Endpoint Score	14	16
Hopper Score	0	0
DLP Score	79	79

Vulnerability Metric

26

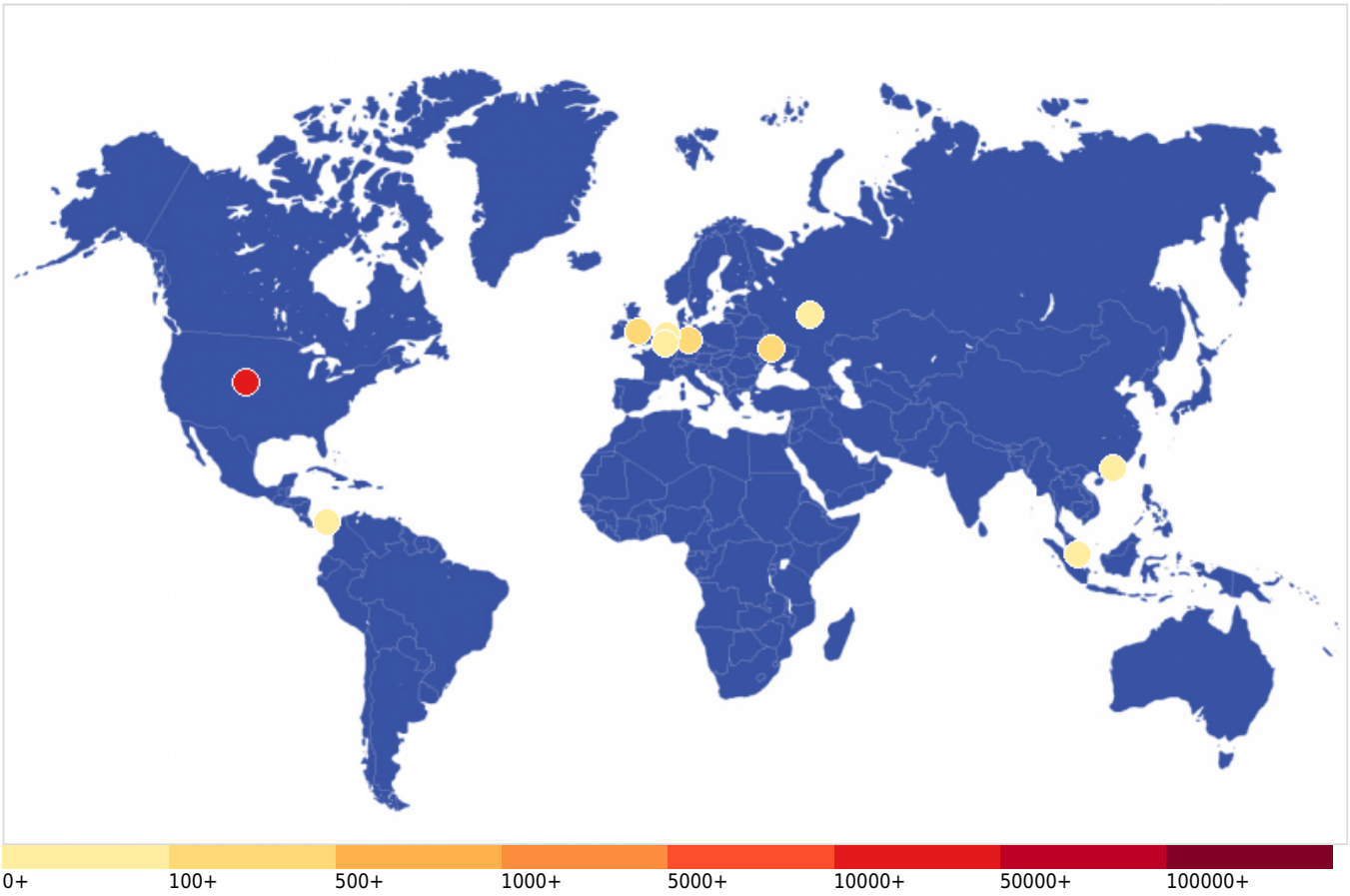
According to the range of addresses provided, the total number of hosts analyzed is 64, of which 40 are vulnerable. These vulnerabilities are divided into the following severities, as shown in the following table. For this period, there are 0 critical vulnerabilities, 2 high vulnerabilities, and 115 medium vulnerabilities. Thus, the vulnerability metric for your organization is 26%.

THREATS

Critical Attacks Per Country In Past Week

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

GLESEC 08/20/2023



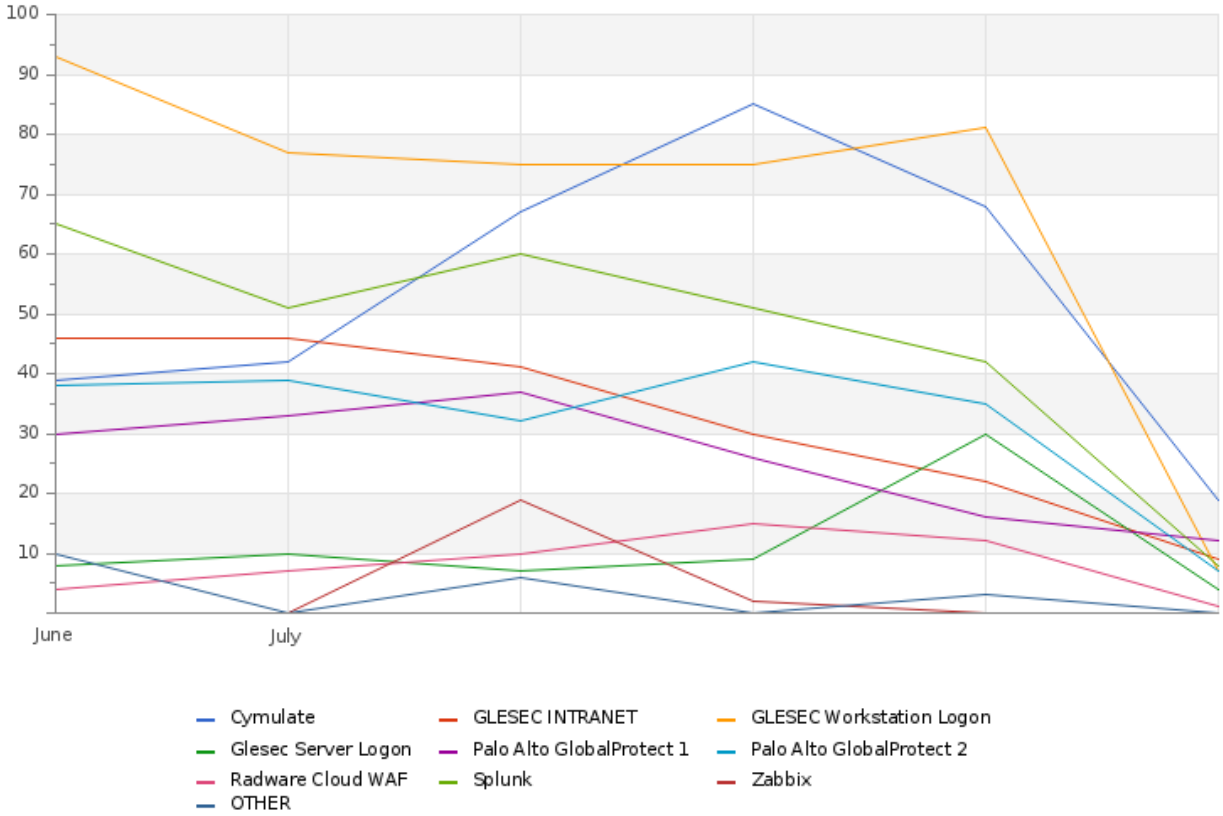
United States - 28824
Germany - 197
United Kingdom - 148
Ukraine - 132
Netherlands - 91
Russia - 74
Panama - 65
Singapore - 51
Hong Kong - 47
Belgium - 45

The vast majority of attacks are from the United States.

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

GLESEC 08/20/2023

Total Number of Successful MFA authentications per application

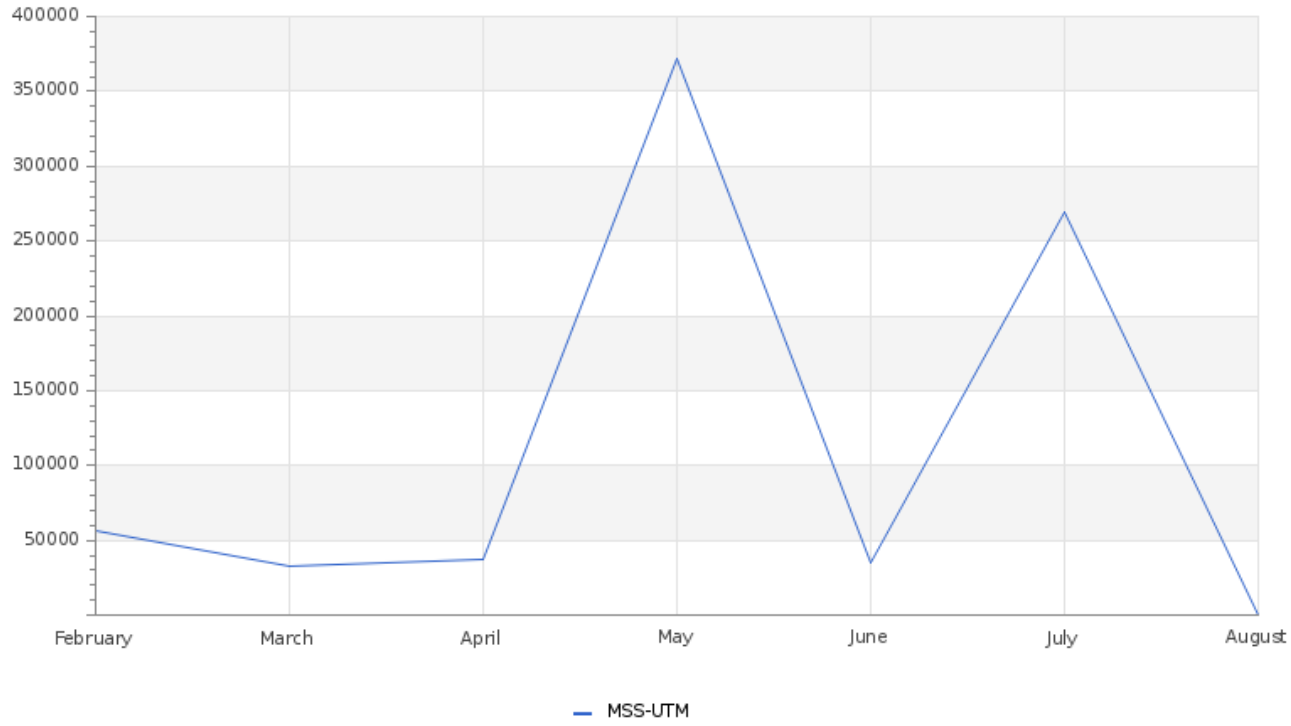


The most authenticated application was the logins to the workstation and the Cymulate.

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

GLESEC 08/20/2023

Total Attacks Successfully Blocked Per Service

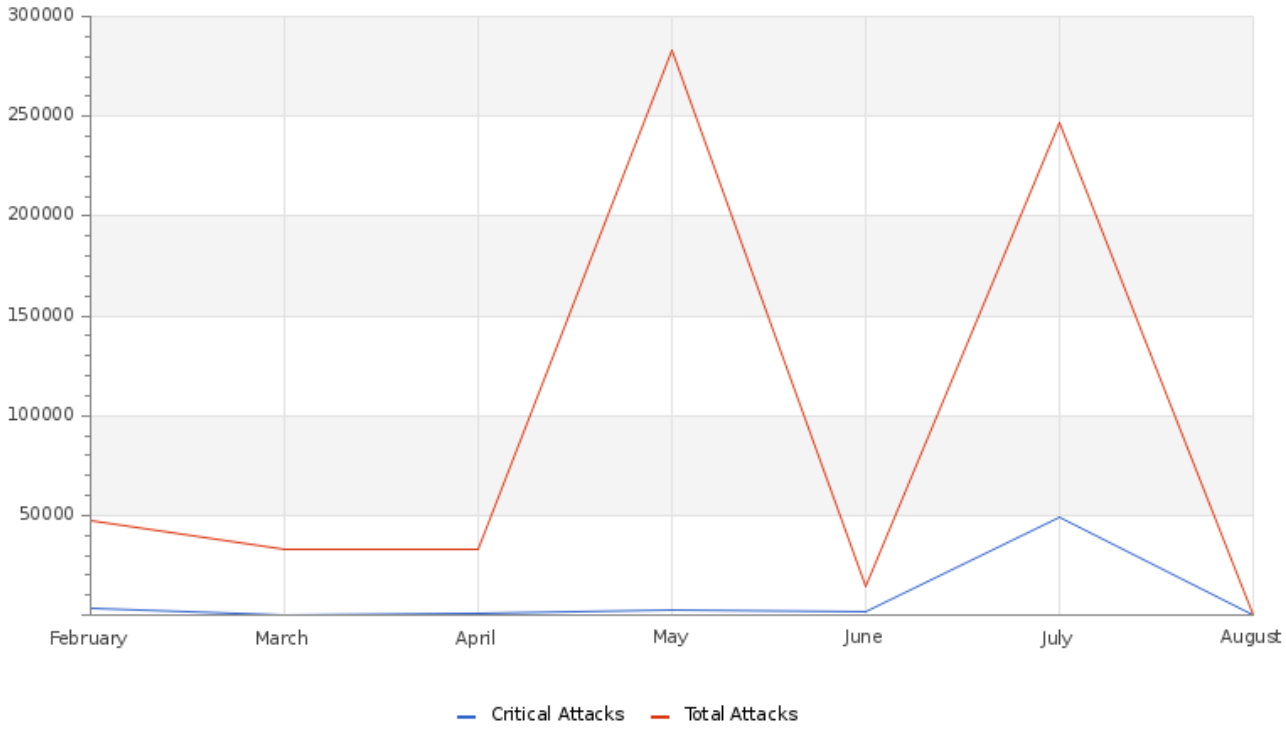


Due to Firewalls being configured during the month of June, your Firewalls are successfully blocking significantly more attacks in the month of July.

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

GLESEC 08/20/2023

Attacks Successfully Blocked by Severity



Due to Firewalls being configured during the month of June, your Firewalls are successfully blocking significantly more attacks in the month of July.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Down Devices	15	5
Critical Down Devices	0	0

The devices that were down only lasted a few seconds before appearing again. These are false positives from a momentary lost of connection.

Histogram of Total and Critical Device Outages

Device outages were minimal in the month of June. These devices were only down momentarily.

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

GLESEC 08/20/2023

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
356	0	0	24,718

The numbers for MSS-EDR are inflated due to the BAS assessments conducted through our MSS-BAS service.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Baseline Systems Discovered	2
BAS Immediate Threat	53
Monitoring Event for SPLUNK CLOUD	28
Change in High or Critical Vulnerabilities	27
Change in Systems Performance	10
EDR Alerts	398
Change in Systems Availability	2
FW Alerts	9
BAS DLP	2
BAS Web Security	2
Non Baselined Discovered System	1

For more information about the individual cases, please visit the Skywatch platform and filter the C&RU by the specific type you'd like more information on.

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

CISO 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