TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

August 22, 2023

GLESEC 08/22/2023

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.

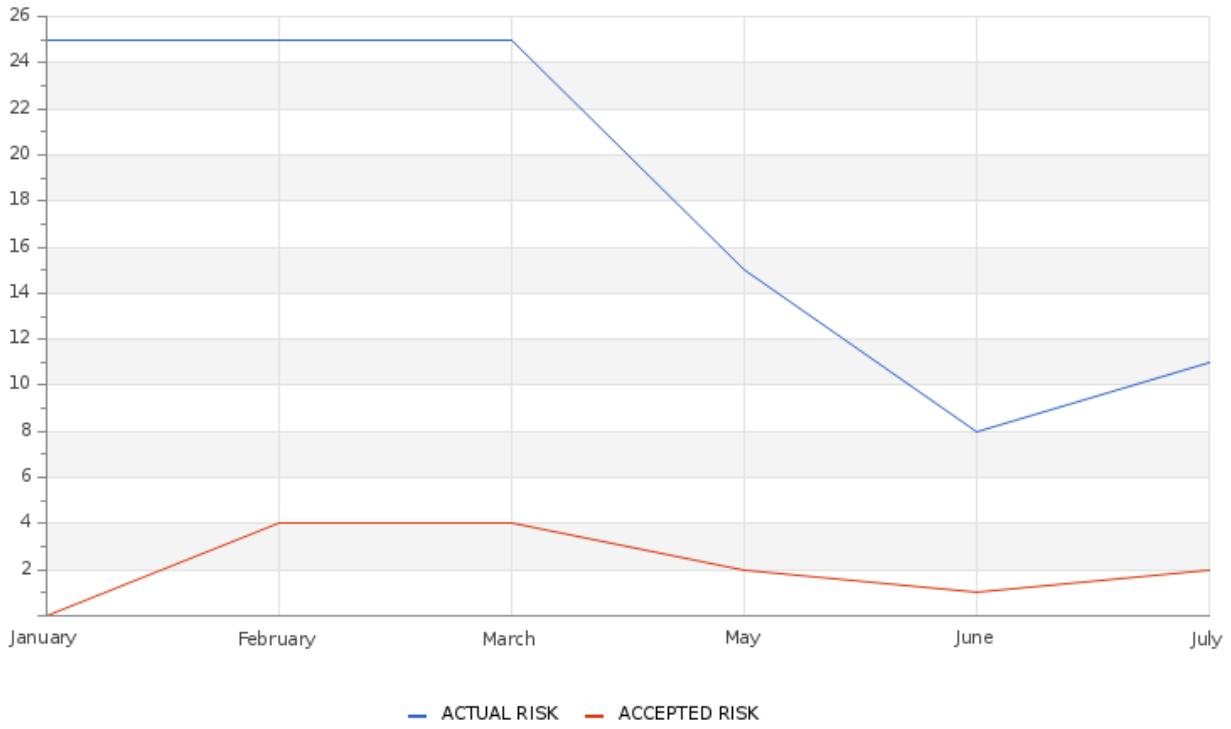
RISK

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.

Accepted & Actual Risk

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

GLESEC 08/22/2023



The current risk level has increased in the month of July. During this month, the current risk stands at 11, while the accepted risk remains at 2. Compared to the previous month, where the current risk was 10 and the accepted risk was also 2, it is evident that the risk has increased.

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

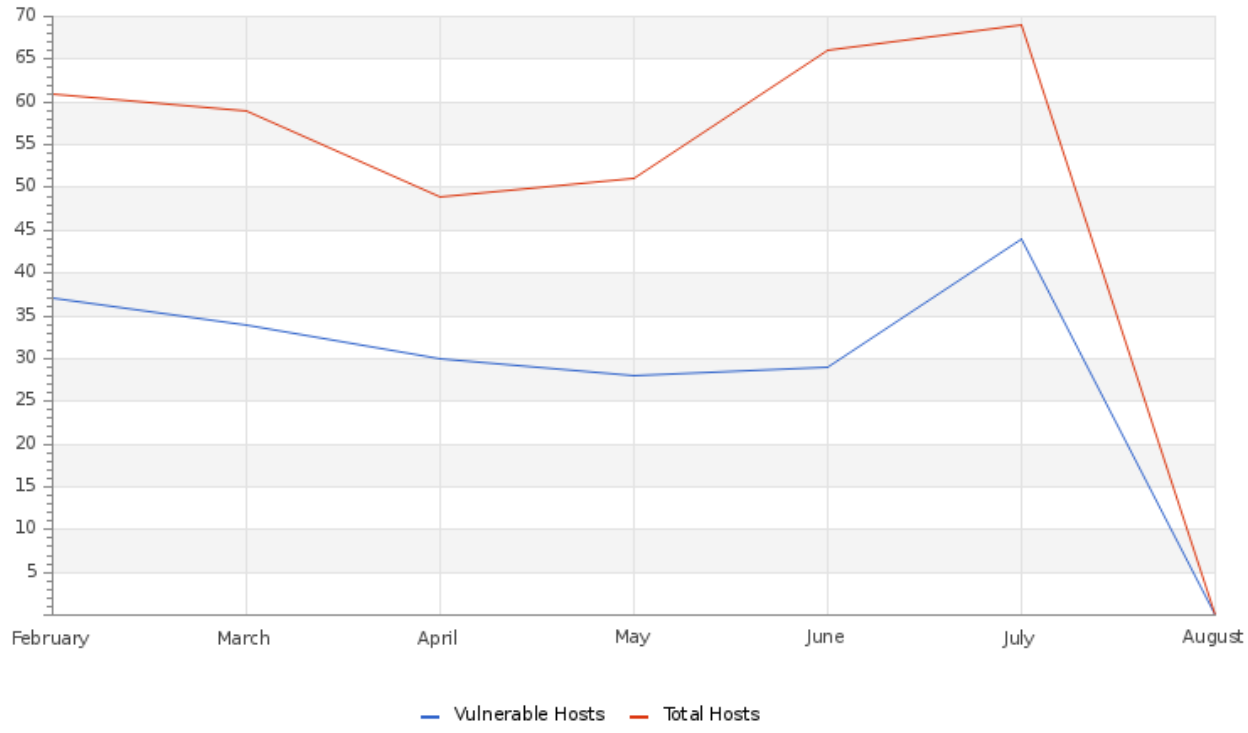
	Current Month	Previous Month
Actual Risk	11	10
Accepted Risk	2	2

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

VULNERABILITY

GLESEC 08/22/2023

Hosts & Vulnerable Hosts In Last 6 Months



The graph shows a marked increase in vulnerabilities and hosts discovered during the month, pointing to security deficiencies. Critical flaws in Google Chrome and Windows permissions issues are fixable with updates, while vulnerabilities in Apache Log4j and Palo Alto GlobalProtect Agent need specific attention. The remaining vulnerabilities are largely associated with outdated software and protocols. It is recommended that these risks be addressed immediately to strengthen organizational security.

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

GLESEC 08/22/2023

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

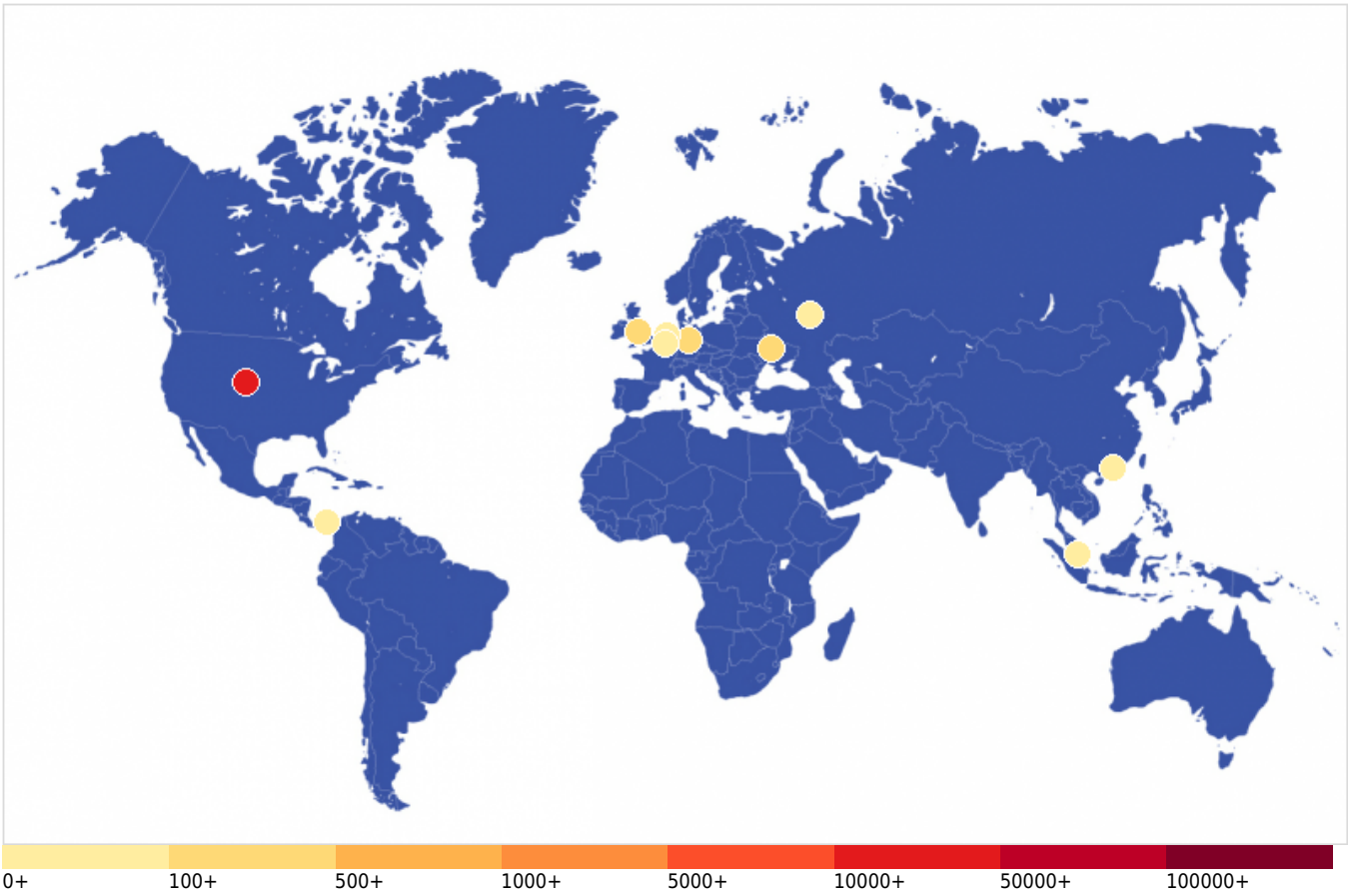
According to the range of addresses provided, the total number of hosts analyzed is 64, of which 40 are vulnerable. These vulnerabilities are divided into the following severities, as shown in the following table. For this period, there are 0 critical vulnerabilities, 2 high vulnerabilities, and 115 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 08/22/2023



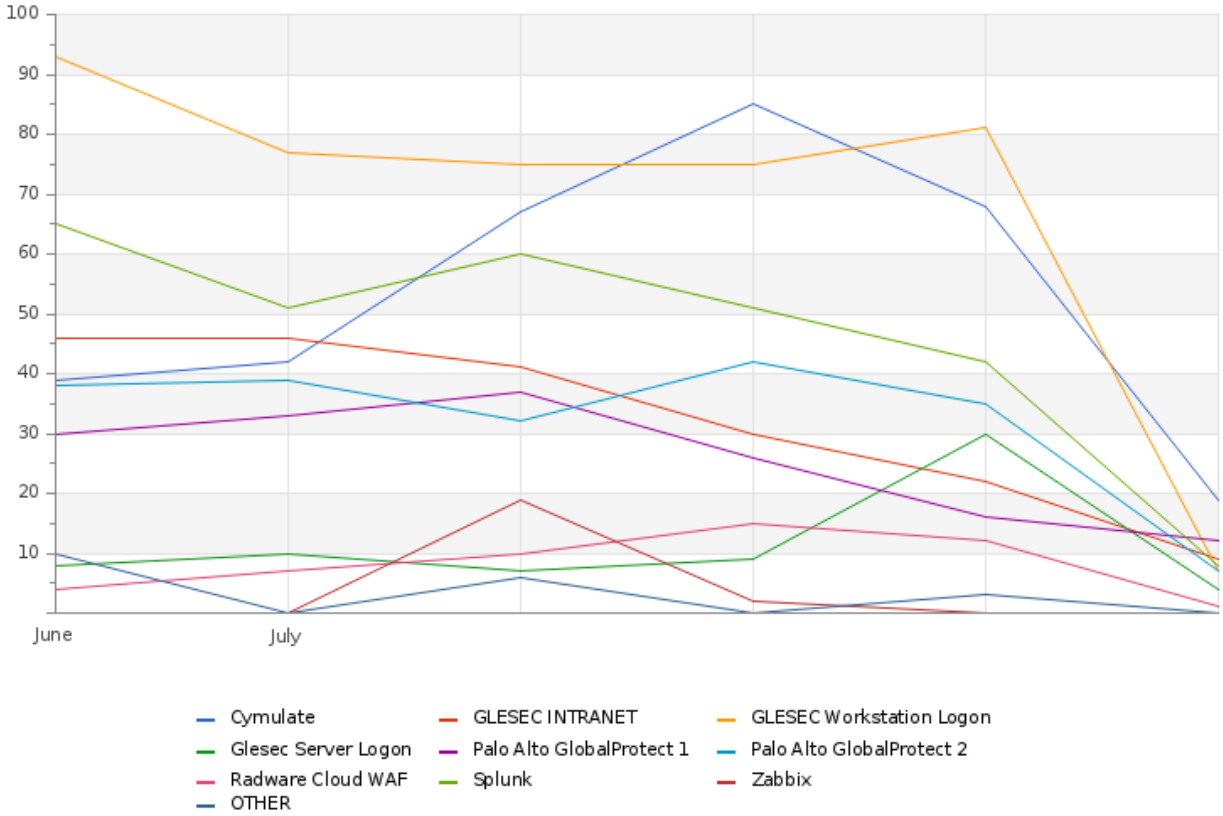
United States - 28824
Germany - 197
United Kingdom - 148
Ukraine - 132
Netherlands - 91
Russia - 74
Panama - 65
Singapore - 51
Hong Kong - 47
Belgium - 45

The graph indicates that the vast majority of attacks, 28,824 in total, come from the United States. By comparison, Germany, the UK and the Ukraine all record much lower numbers, with fewer than 200 attacks each. Given this disparity, cybersecurity measures should especially focus on threats originating in the United States.

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

GLESEC 08/22/2023

Total Number of Successful MFA authentications per application

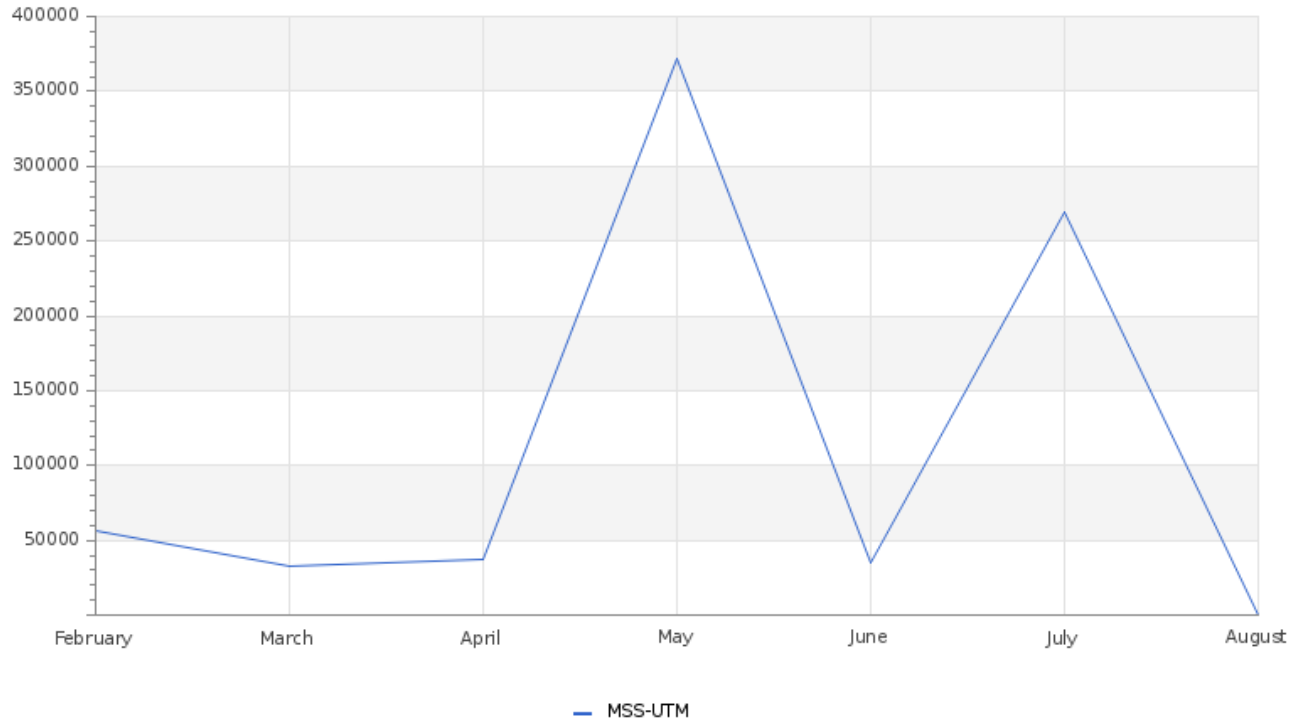


The graph shows that the most authenticated applications are the workstation and Cymulate logins.

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

GLESEC 08/22/2023

Total Attacks Successfully Blocked Per Service

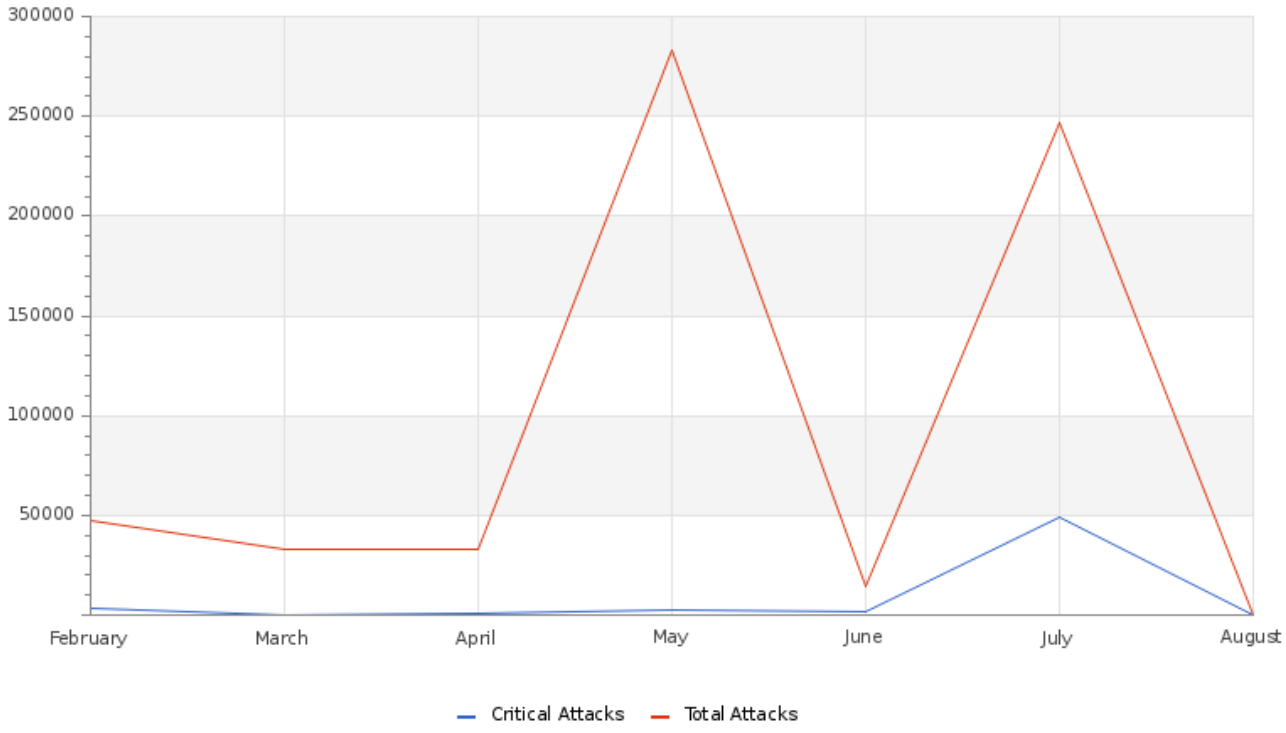


The implementation of firewalls in the month of June has had a positive impact on security, as evidenced by the graph showing a significant increase in the number of attacks successfully blocked in July.

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

GLESEC 08/22/2023

Attacks Successfully Blocked by Severity



Firewall configuration in June has generated positive security results, which is reflected in the graph with an increase in attacks successfully neutralized in July. These Firewalls also provide a preemptive defense against emerging risks like DDoS attacks, ever-evolving IoT botnets, and new DNS attack methods.

System Availability and Performance in current & previous month

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

Devices that experienced interruptions reappeared within seconds. These incidents are due to false positives caused by brief interruptions in the connection.

Histogram of Total and Critical Device Outages

Devices that suffered brief interruptions were quickly restored, reappearing in just a few seconds. These incidents are attributable to false positives caused by momentary loss of connection.

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

GLESEC 08/22/2023

Total and Critical Attacks Successfully Blocked by Security Layer and Department

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

MSS-EDR statistics are overestimated due to BAS evaluations performed through our specialized 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	57
Monitoring Event for SPLUNK CLOUD	30
Change in High or Critical Vulnerabilities	27
Change in Systems Performance	10
EDR Alerts	402
Change in Systems Availability	2
FW Alerts	9
BAS DLP	2
BAS Web Security	2
Non Baselined Discovered System	1

For additional details on individual cases, access the Skywatch platform and use the C&RU filter to select the specific type that is of interest to you.

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