TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

July 11, 2023

GLESEC 07/11/2023

TLP AMBER CISO

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.

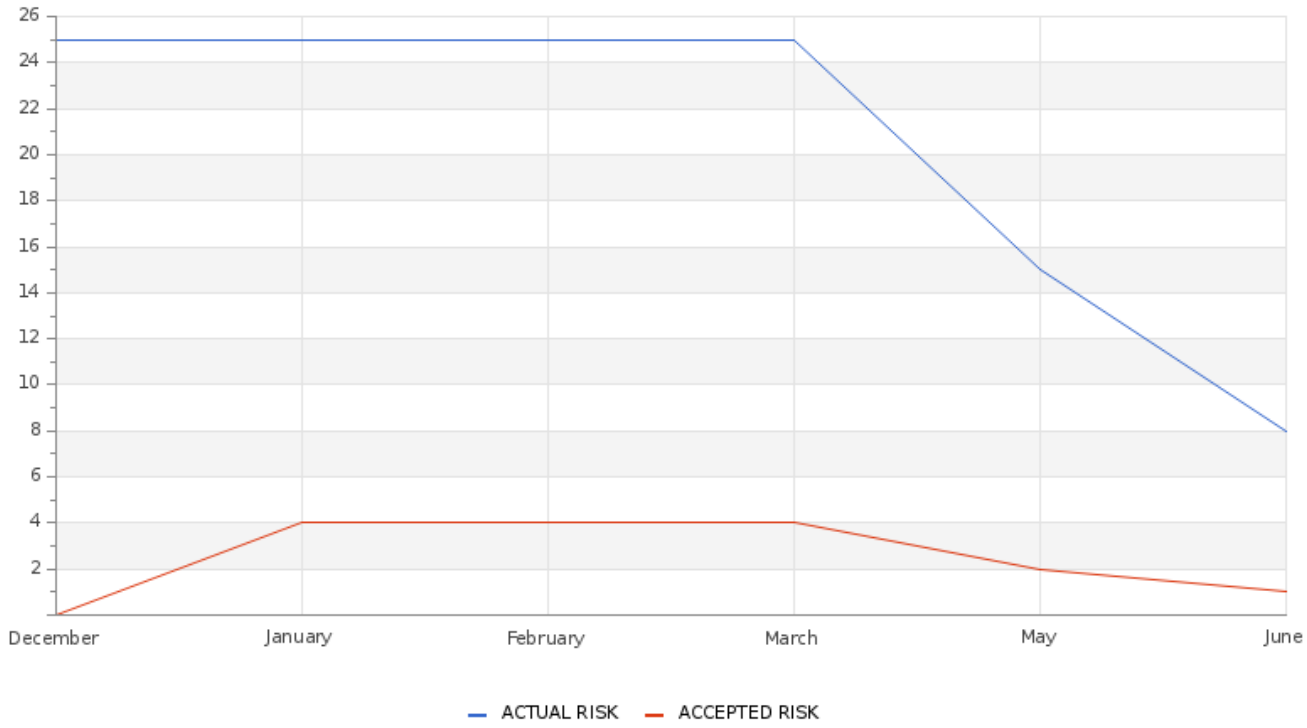
RISK

Actual Risk	Accepted Risk	Confidence
8%	**1%**	**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 07/11/2023

Accepted & Actual Risk



Your Actual/Accepted Risk level has decreased since the month of March.

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

	Current Month	Previous Month
Actual Risk	8	15
Accepted Risk	1	2

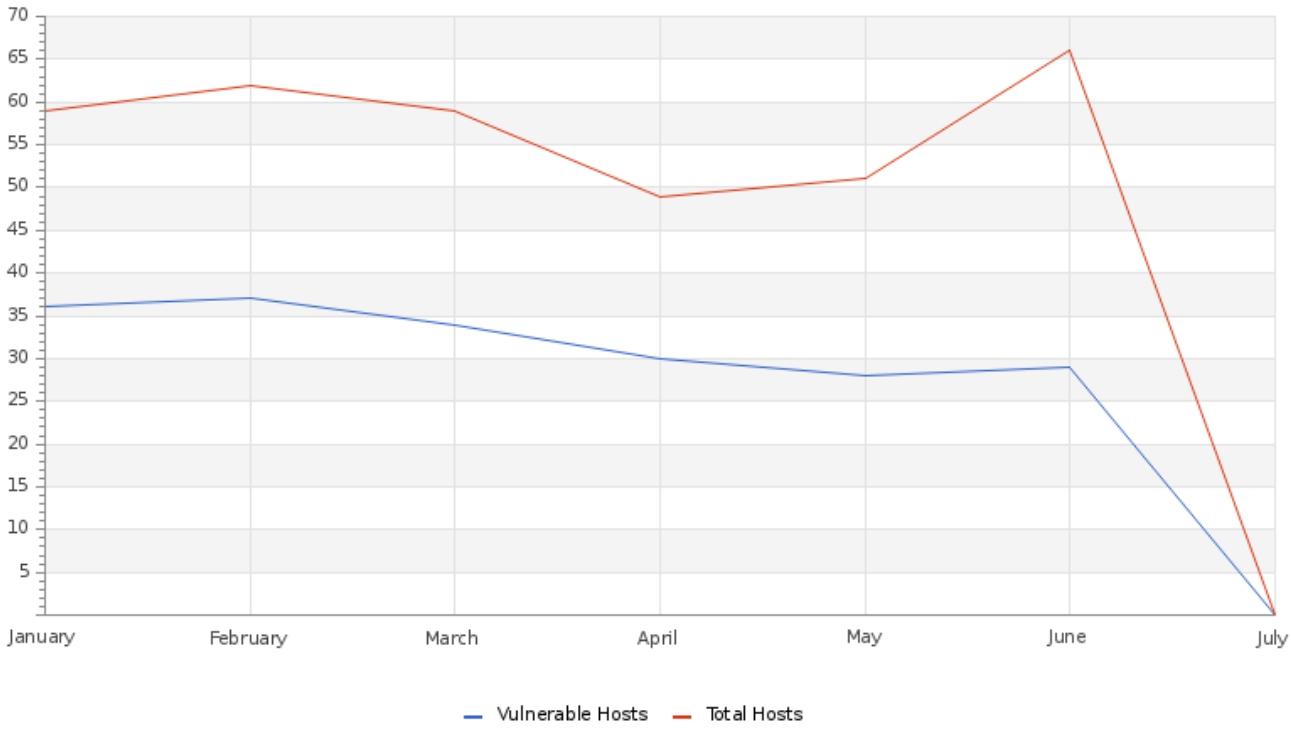
Your actual risk has gone down 7 points from the previous month.
Your accepted risk has also gone down 1 point from the previous month.

VULNERABILITY

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

GLESEC 07/11/2023

Hosts & Vulnerable Hosts In Last 6 Months



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

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

GLESEC 07/11/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	56	57
Hosts Discovered	61	44
Vulnerable Hosts	27	25
Critical Vulnerabilities Count	0	2
High Vulnerabilities Count	4	3
Medium Vulnerabilities Count	89	98
Low Vulnerabilities Count	12	10
Phishing Score	0	0
Email Gateway Score	10	10
Web Application Firewall Score	24	25
Web Gateway Score	52	52
Endpoint Score	16	18
Hopper Score	0	0
DLP Score	79	79

Vulnerability Metric

9

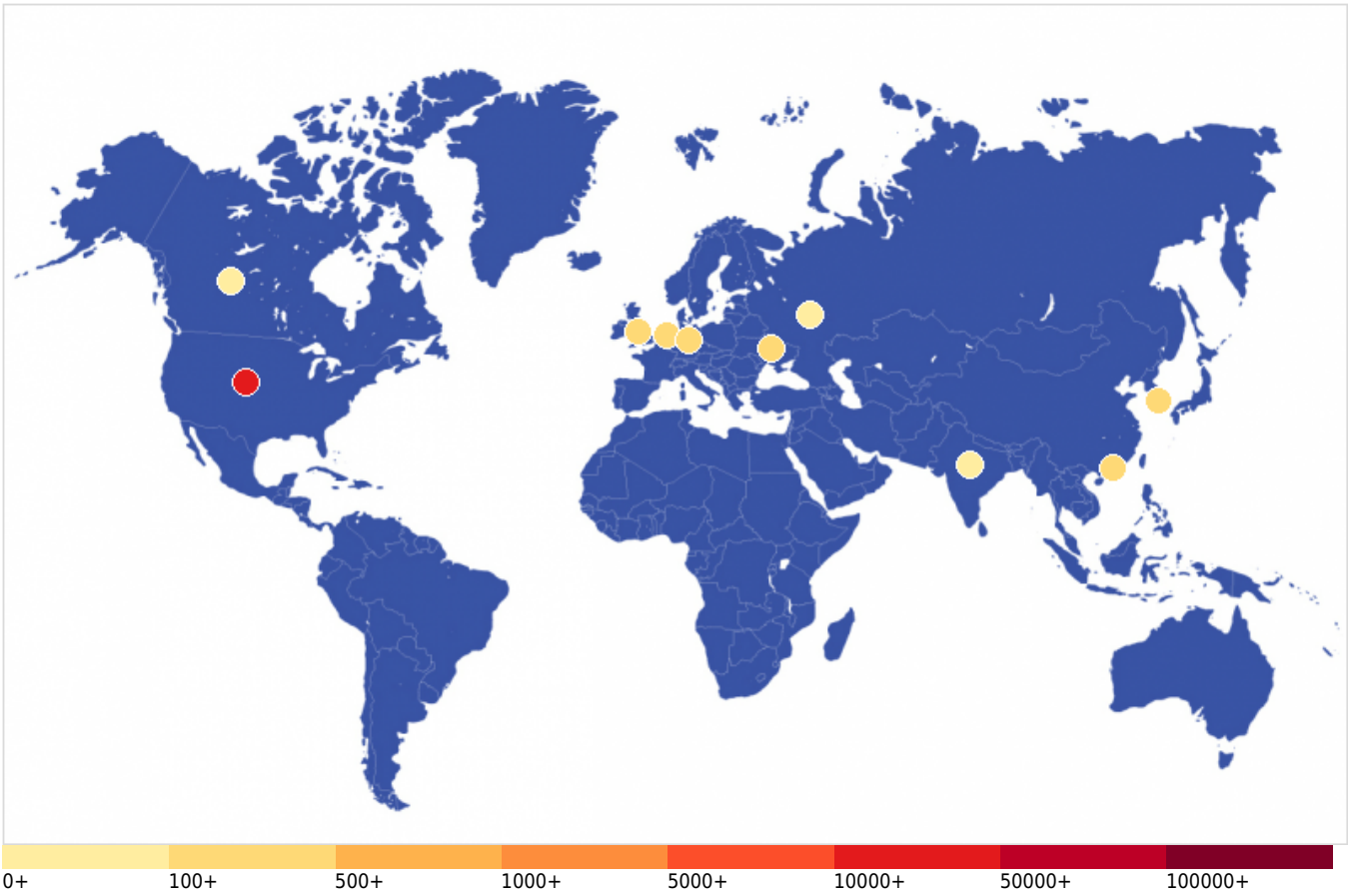
According to the range of addresses provided, the total number of hosts analyzed is 61, of which 27 are vulnerable. These vulnerabilities are divided into the following severities, as shown in the following table. For this period, there are 0 critical vulnerabilities and 4 high vulnerabilities. Thus, the vulnerability metric for your organization is 9%.

THREATS

Critical Attacks Per Country In Past Week

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

GLESEC 07/11/2023



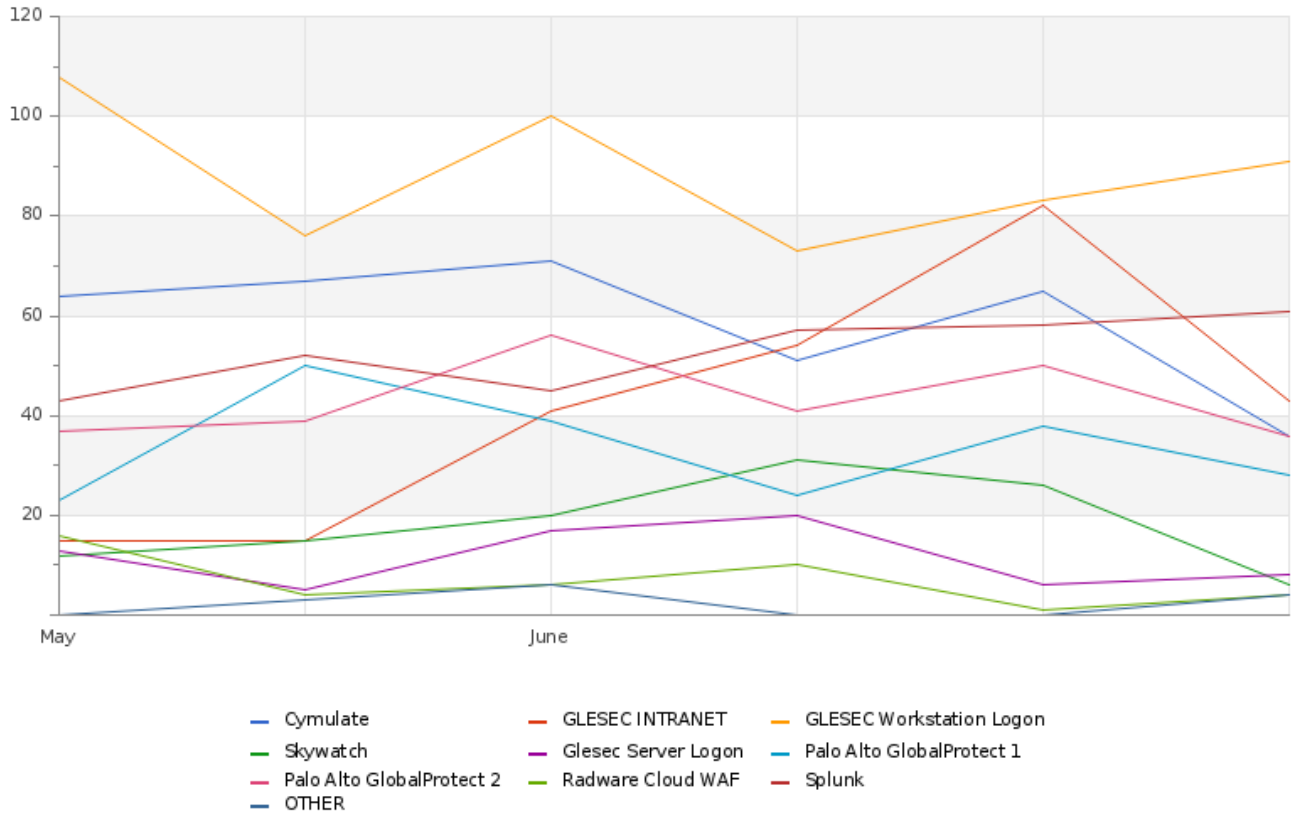
United States - 30112
Netherlands - 179
India - 62
South Korea - 369
Germany - 158
Russia - 62
Hong Kong - 350
Ukraine - 129
United Kingdom - 290
Canada - 95

This graph shows the amount of attack per country in the last week of May. Most attacks are generated from the United States.

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

GLESEC 07/11/2023

Total Number of Successful MFA authentications per application

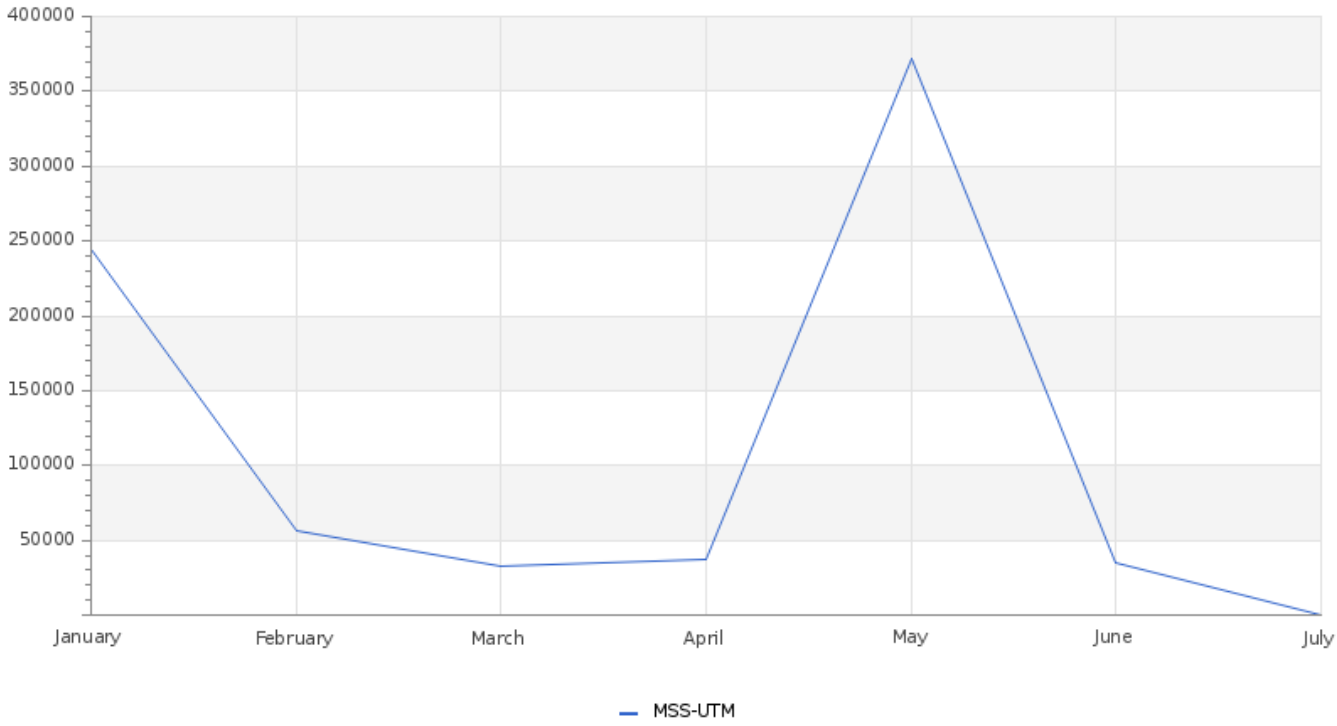


The most authenticated application was the logins to the workstation and the Intranet. There were 77 different endpoints used to authenticate during this period.

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

GLESEC 07/11/2023

Total Attacks Successfully Blocked Per Service

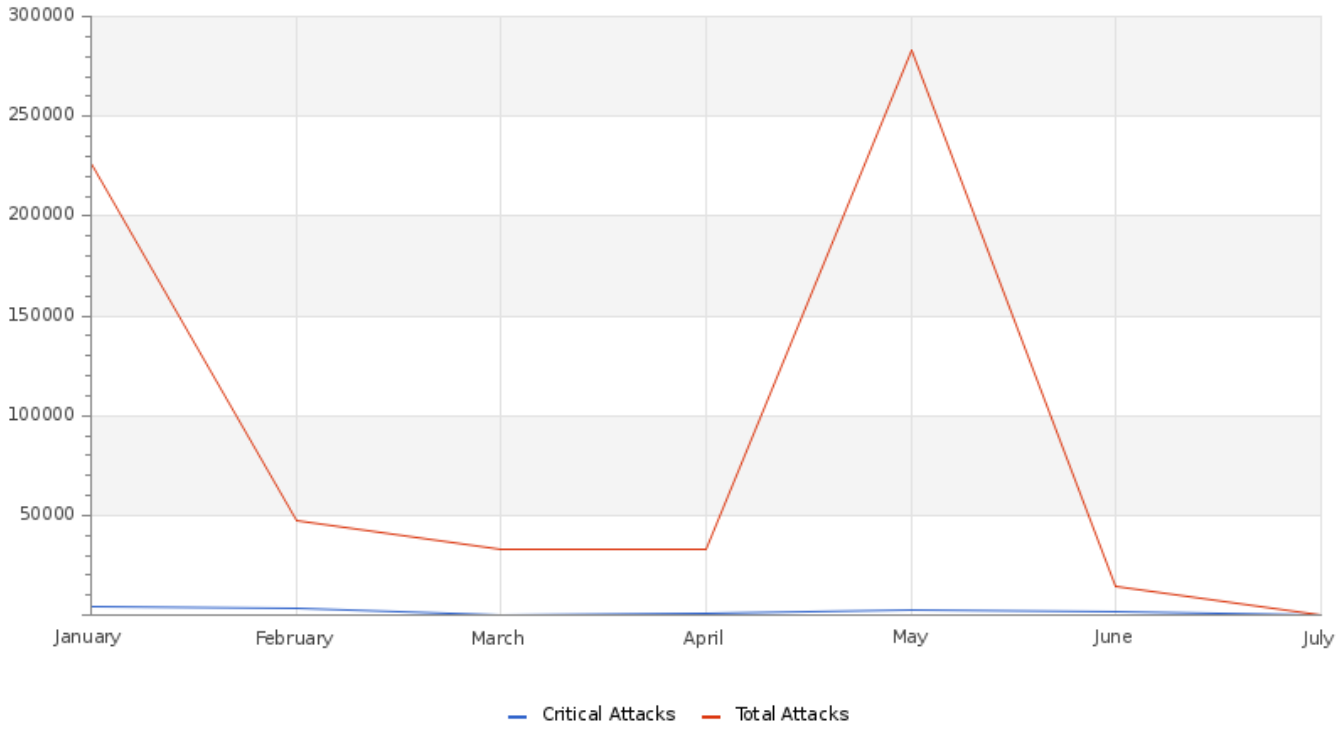


Threat information for this period was collected from the MSS-UTM services. For this period, the firewall was not properly uploading data due to other issues, and is the reason why the June figure is low.

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

GLESEC 07/11/2023

Attacks Successfully Blocked by Severity



For this period, the firewall was not properly uploading data due to other issues, and is the reason why the June figure is low.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Down Devices	11	6
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 07/11/2023

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
983	0	0	23,375

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 #
BAS Immediate Threat	37
Non Baselined Discovered System	2
FW Alerts	3
BAS DLP	1
Change in Systems Performance	2
Monitoring Event for SPLUNK CLOUD	20
Change in Baseline Systems Discovered	1
Change in High or Critical Vulnerabilities	3

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