TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

January 31, 2024

GLESEC 01/31/2024

TLP AMBER CISO

EXECUTIVE REPORT

This report corresponds to December 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.

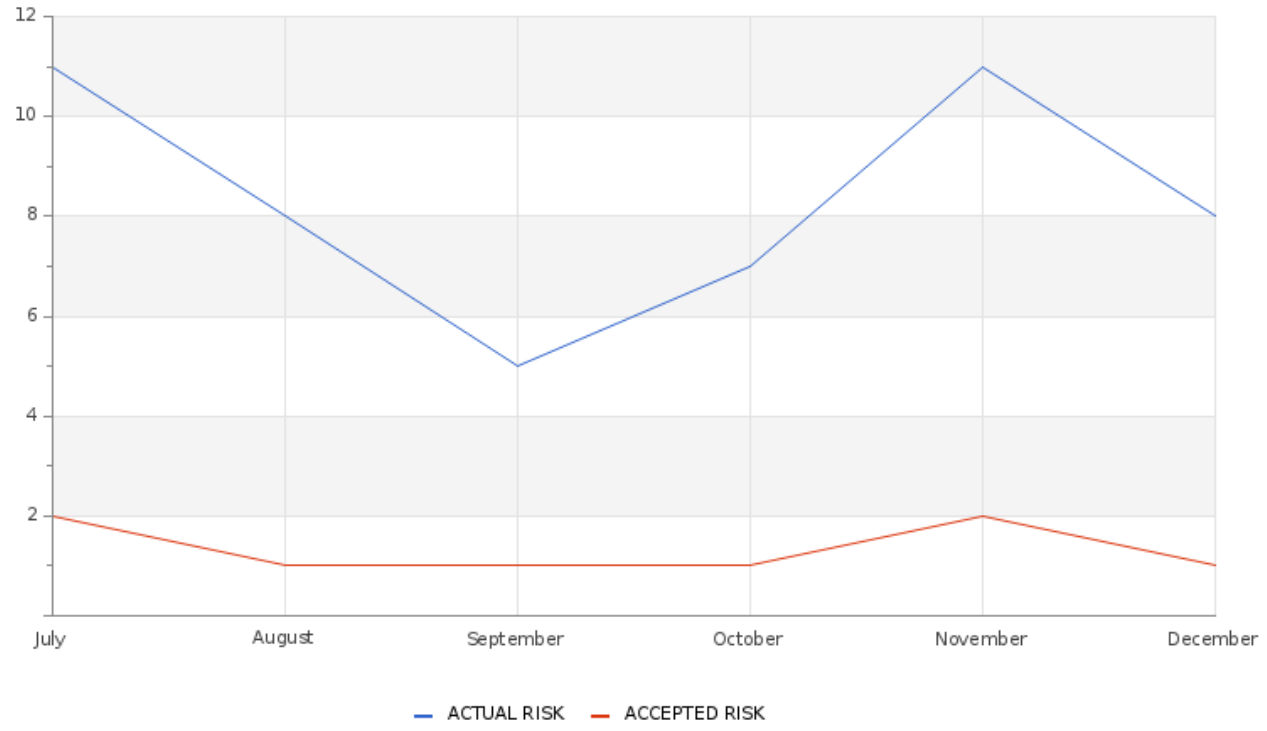
RISK

Actual Risk	Accepted Risk	Confidence
8%	1%	High

Accepted & Actual Risk

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

GLESEC 01/31/2024



During this month there has been a slight decrease in risk levels. The current risk is 8%, and the accepted risk is 1%. Compared to the previous month the risk figures have decreased, the actual risk has decreased by 3%, while the accepted risk decreased by 1%.

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

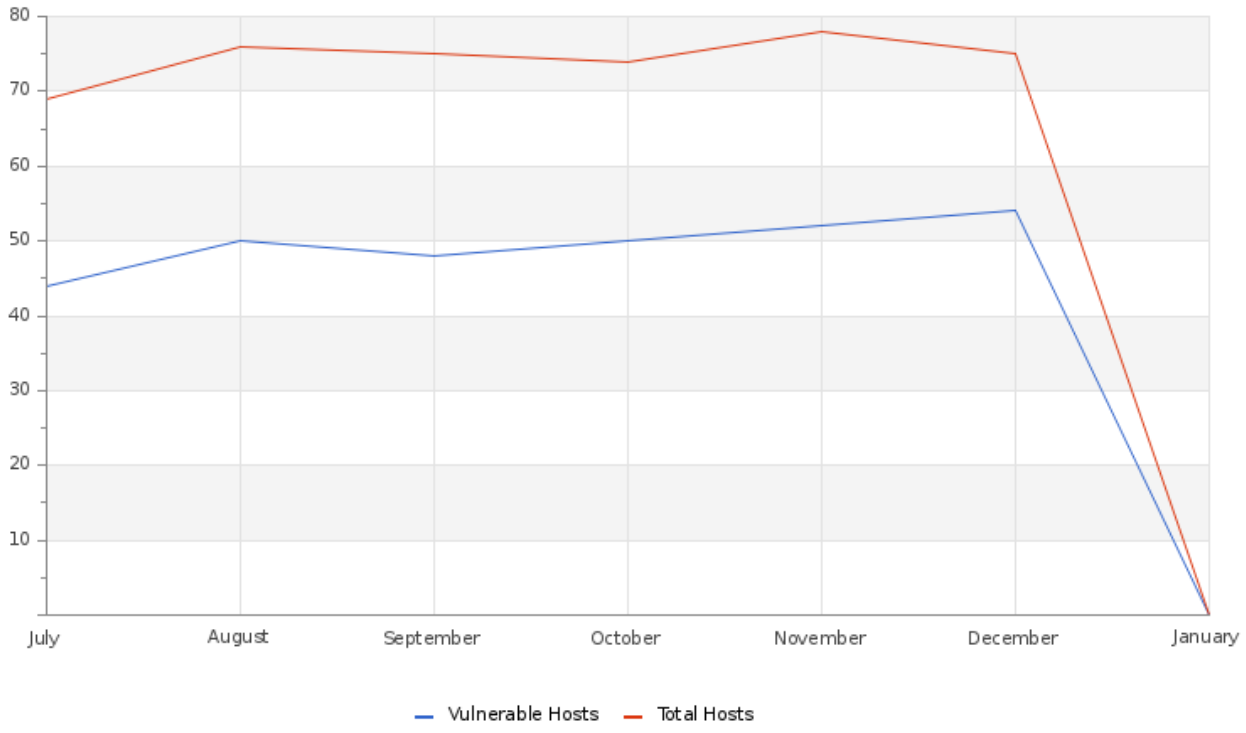
	Current Month	Previous Month
Actual Risk	8	11
Accepted Risk	1	2

The comparative table shows a 3% reduction with respect to the Actual Risk of the previous month. As for the Accepted Risk, the reduction with respect to the previous month is 1%.
This information shows us how our security posture is currently, with respect to threats and vulnerabilities and the impact they can have.

VULNERABILITY

GLESEC 01/31/2024

Hosts & Vulnerable Hosts In Last 6 Months



The graph shows a decrease in the number of hosts identified during the month and a slight increase in the number of vulnerabilities present in the hosts. Among the most prominent vulnerabilities were vulnerabilities related to security updates and unsupported versions of software. Prompt remediation of these vulnerabilities is essential to ensure security, reducing the risk of intrusions and breaches.

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

GLESEC 01/31/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	72	72
Hosts Discovered	68	75
Vulnerable Hosts	49	48
Critical Vulnerabilities Count	6	148
High Vulnerabilities Count	17	198
Medium Vulnerabilities Count	156	233
Low Vulnerabilities Count	39	35
Phishing Score		0
Email Gateway Score		9
Web Application Firewall Score		22
Web Gateway Score		61
Endpoint Score		38
Hopper Score		33
DLP Score		71

The table shows the results obtained as a result of the evaluations performed in different security areas. The results of the assessments are as follows: Phishing - 0, Email Gateway- 8, Web Application Firewall - 25, Web Gateway - 64, Endpoint - 39, Hopper - 33, and DLP - 73. The results show those areas that need more attention and need to be addressed promptly.

Vulnerability Metric

35

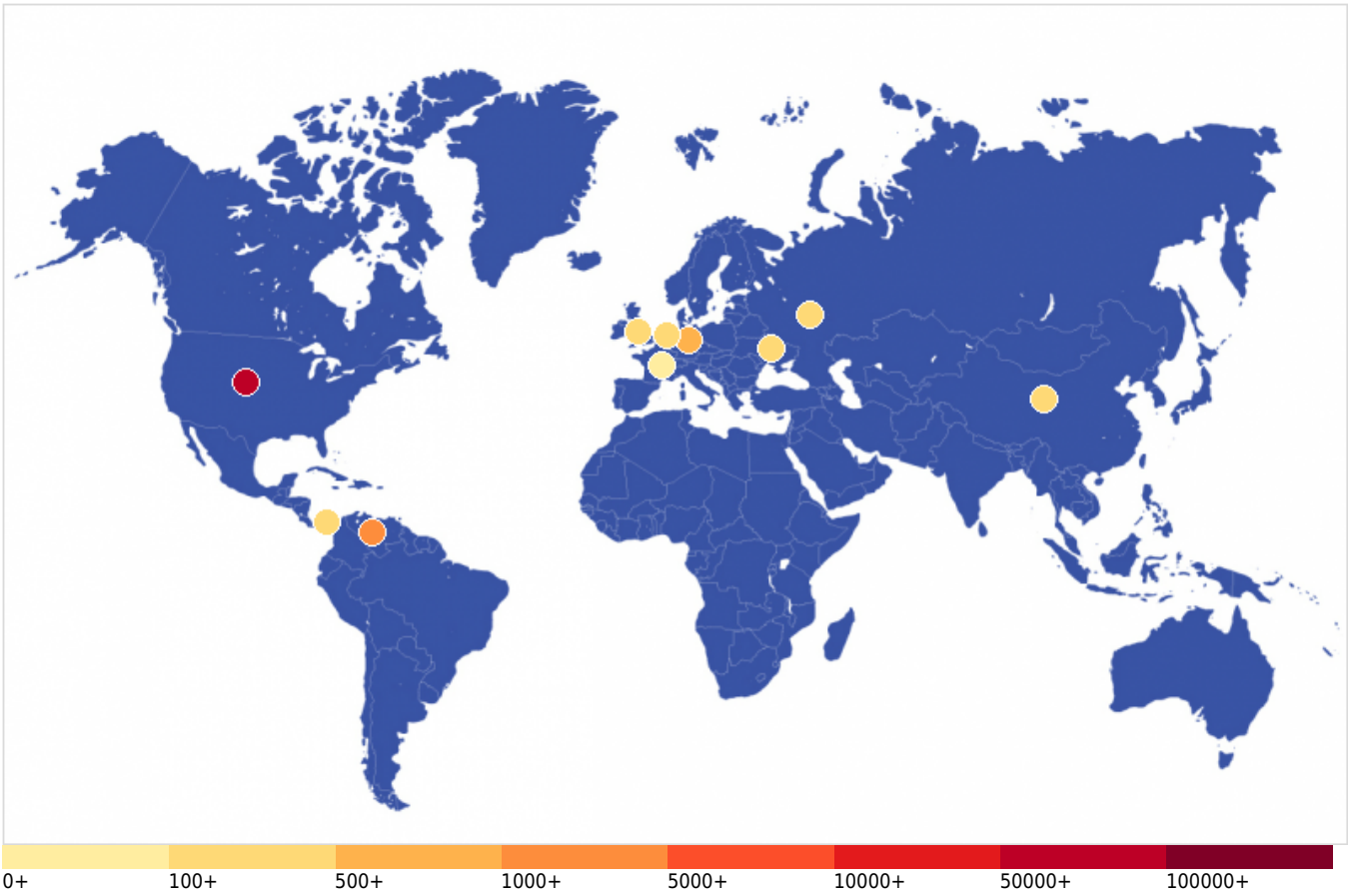
During the month a total of 70 hosts were analyzed, of which 54 were identified as vulnerable. These vulnerabilities are classified by severity, during this period 91 critical, 137 high, 223 medium and 37 low vulnerabilities were identified. The current vulnerability index for your organization is 35%.

THREATS

Critical Attacks Per Country In Past Week

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

GLESEC 01/31/2024



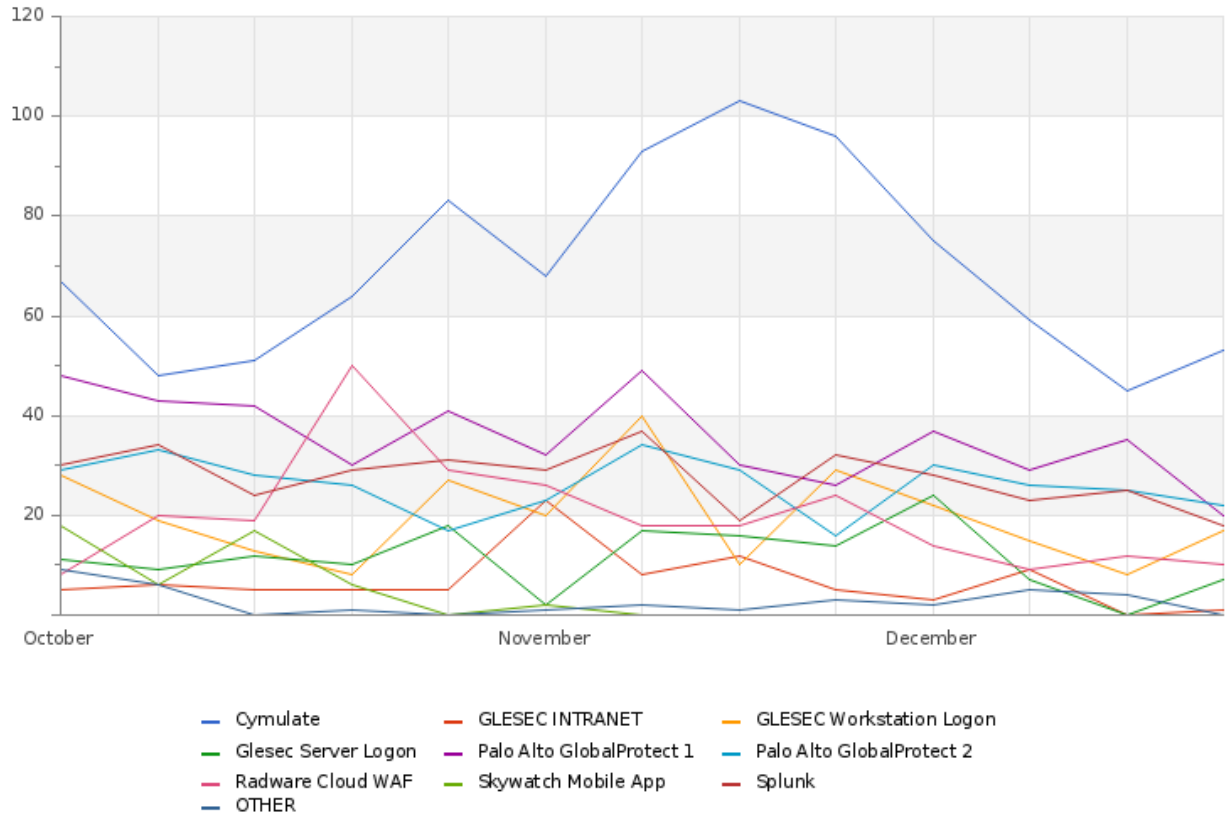
United States - 59290
Netherlands - 351
Panama - 116
Venezuela - 3608
Ukraine - 183
France - 84
Germany - 907
Russia - 158
United Kingdom - 372
China - 128

The graph shows the distribution of attacks classified by country, it can be seen that most attacks come from the United States with a total of 306,582 attacks, followed by Venezuela with 3,608 and Germany with 907 attacks. Other countries, such as the United Kingdom, the Netherlands, Ukraine and Russia, registered less than 500 attacks. The results indicate that we should focus our cybersecurity efforts on the main source of attacks, while maintaining a more generalized vigilance.

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

GLESEC 01/31/2024

Total Number of Successful MFA authentications per application

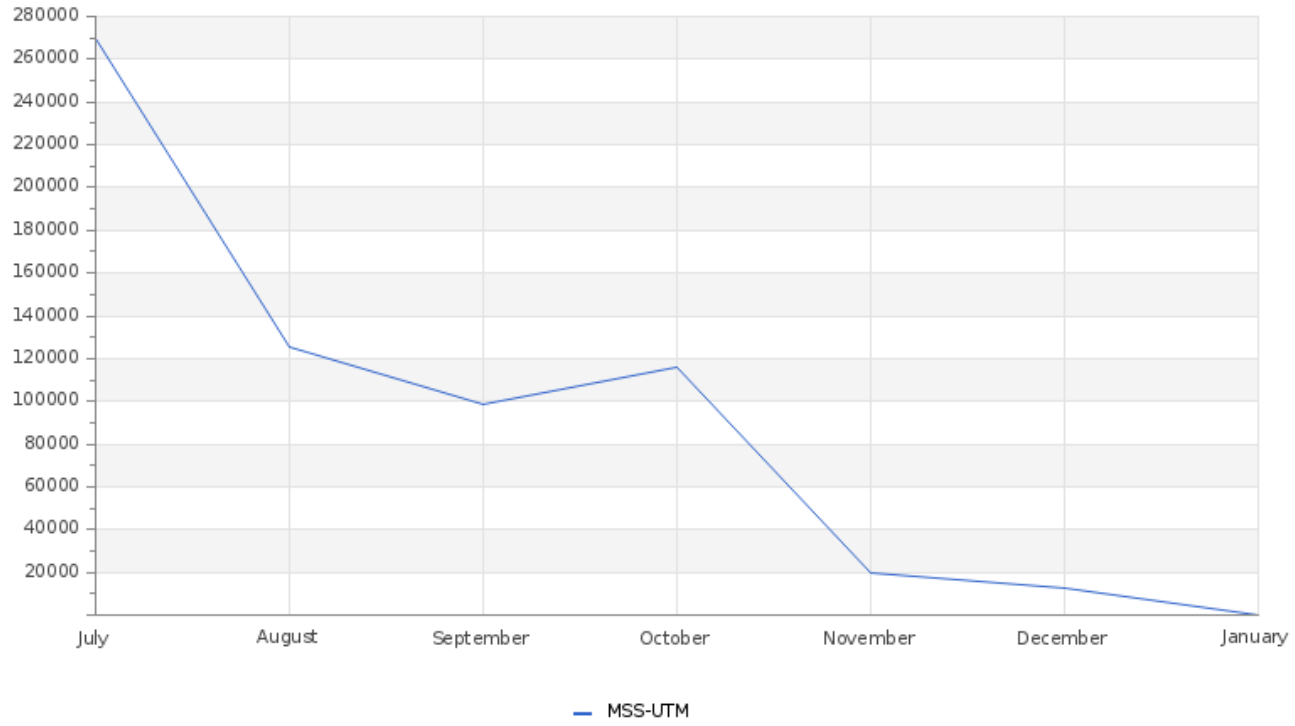


The graph shows a clear trend in authentication patterns for workstations and the Cymulate platform, with the latter recording the most authentications during the month. This is a product of the evaluations that are carried out on a daily basis.

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

GLESEC 01/31/2024

Total Attacks Successfully Blocked Per Service

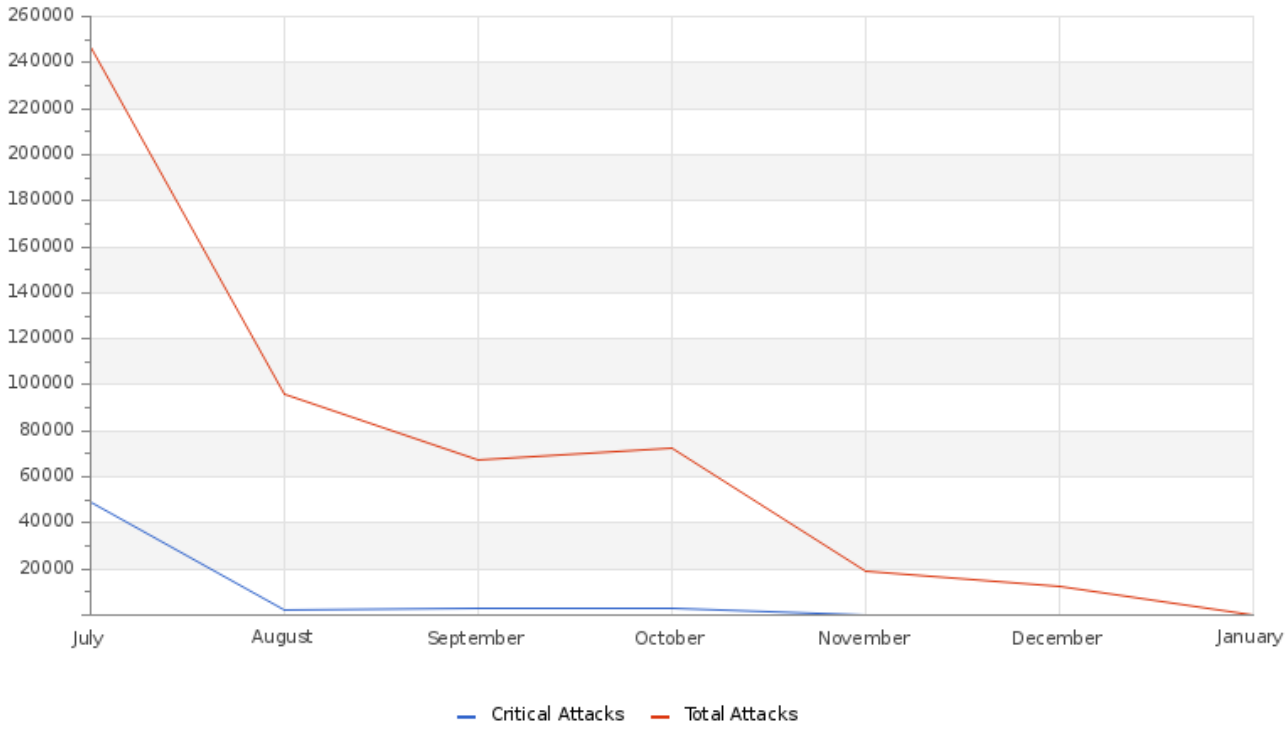


The graph shows a decrease in the number of attacks carried out against company systems compared to the previous month's attacks. The result reflects the effectiveness of the security measures that have been implemented.

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

GLESEC 01/31/2024

Attacks Successfully Blocked by Severity



System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	7	6
Critical Device Outages	0	0

Devices affected during the month had momentary outages, whereby the connection was restored immediately, others were caused by alerts related to device performance.

Histogram of Total and Critical Device Outages

Affected devices during the month had momentary outages, for which the connection was immediately restored, others were caused by alerts related to device performance. Understanding and controlling these issues is crucial for smooth operation and to reduce future outages..

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

GLESEC 01/31/2024

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
22,601	0	0	20,100

The results shown in the table for the MSS-EDR service are due to the BAS assessments carried out by the MSS-BAS service. Knowing this information is vital for a more accurate analysis.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	60
BAS DLP	8
EDR Alerts	366
Change in Systems Performance	2
Change in High or Critical Vulnerabilities	17
BAS WAF	2
BAS Endpoint Security	7
BAS Web Security	16
Monitoring Event for SPLUNK CLOUD	8

During the month, multiple cases were documented, which included detailed information to address and mitigate vulnerabilities present in their systems, as well as recommendations to help strengthen their security against emerging threats. You can access this documentation through our Skywatch platform in the C&RU section.

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.**

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