TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

November 21, 2023

GLESEC 11/21/2023

TLP AMBER CISO

EXECUTIVE REPORT

This report corresponds to October 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.

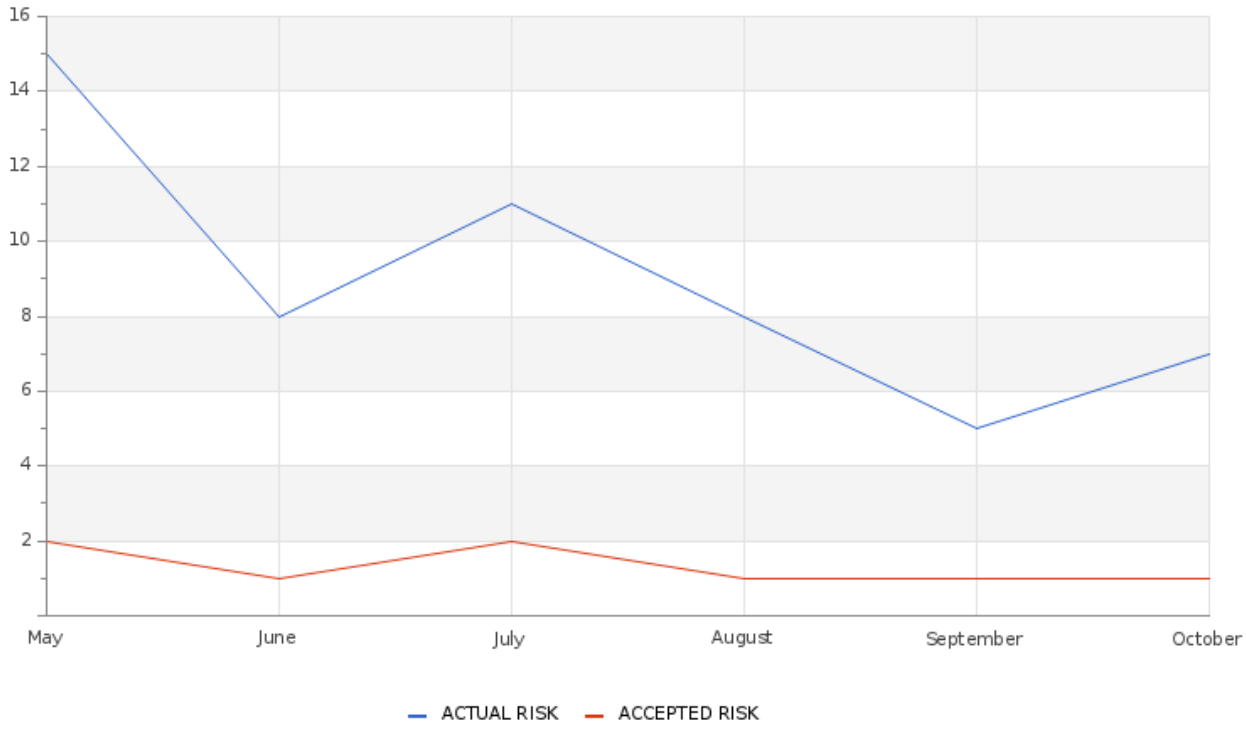
RISK

Actual Risk	Accepted Risk	Confidence
7%	1%	High

Accepted & Actual Risk

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

GLESEC 11/21/2023



The current level of risk has increased compared to the previous month. During the month, the risk stood at 7%, while the accepted risk remained at 1%. Compared to the previous month when the risk was 6%, there has been an increase of 1% when compared to the current risk as can be seen in the graph.

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

	Current Month	Previous Month
Actual Risk	7	6
Accepted Risk	1	1

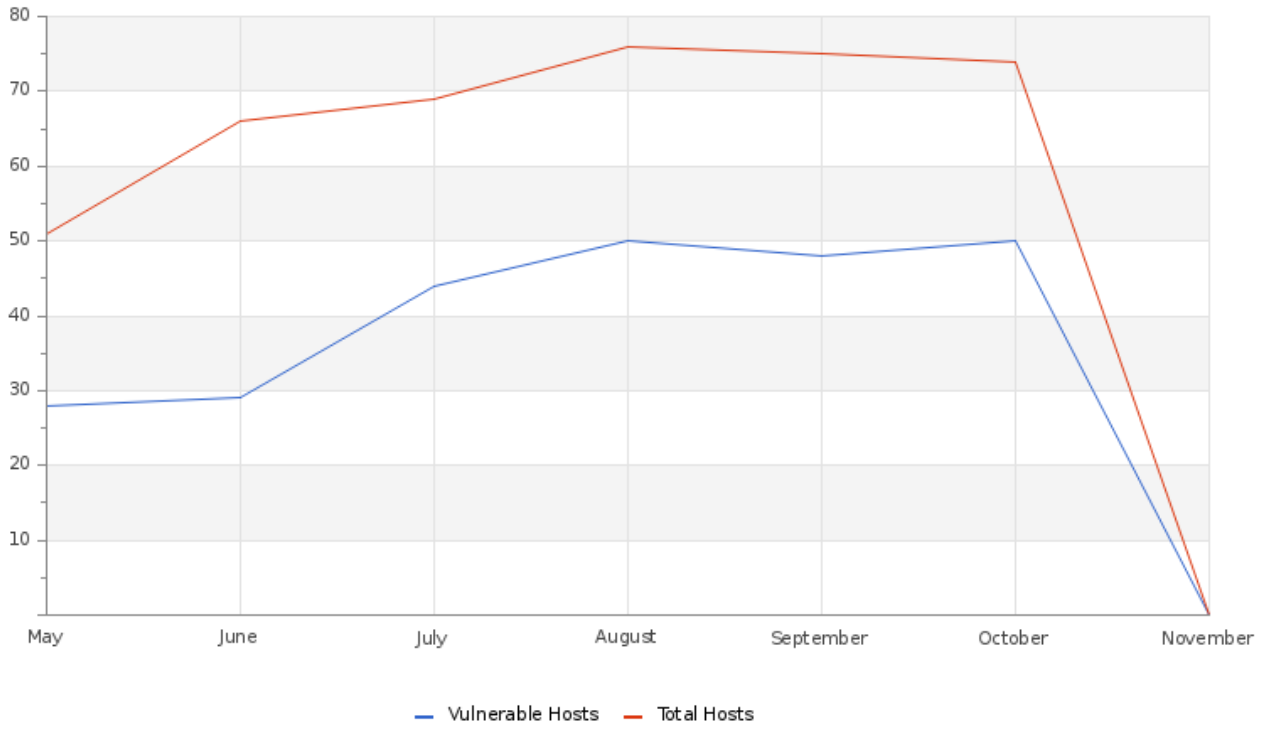
The comparison shows a slight increase of 1% in the current risk compared to the previous month, while the accepted risk remains at 1%. The variations indicate the constant changes in the environment and the importance of adapting the security systems to these changes.

VULNERABILITY

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

GLESEC 11/21/2023

Hosts & Vulnerable Hosts In Last 6 Months



During the month the number of hosts discovered was maintained, and there was a slight increase in the number of vulnerabilities present on hosts. Most of the vulnerabilities correspond to application updates and new system patches that need to be applied. The vulnerabilities include security updates to ASP.NET Core, Windows and Linux kernel updates. There are also other lower priority vulnerabilities such as GlobalProtect agent updates, but these need to be addressed as they are an essential part of maintaining enterprise security.

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

GLESEC 11/21/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	73	73
Hosts Discovered	73	71
Vulnerable Hosts	50	34
Critical Vulnerabilities Count	49	2
High Vulnerabilities Count	51	17
Medium Vulnerabilities Count	153	96
Low Vulnerabilities Count	32	27
Phishing Score	0	0
Email Gateway Score	9	9
Web Application Firewall Score	22	22
Web Gateway Score	58	57
Endpoint Score	36	44
Hopper Score	33	33
DLP Score	82	82

The comparison of the results obtained during the month for the MSS-VM and MSS-BAS services shows an increase in the number of hosts with vulnerabilities as well as the number of vulnerabilities. For the MSS-BAS service tests, it can be observed that some values are maintained, while others show a slight increase or decrease in the results. We recommend that you carefully review the cases created for the MSS-BAS service tests and carry out appropriate mitigations to reduce the vulnerabilities present in your systems.

Vulnerability Metric

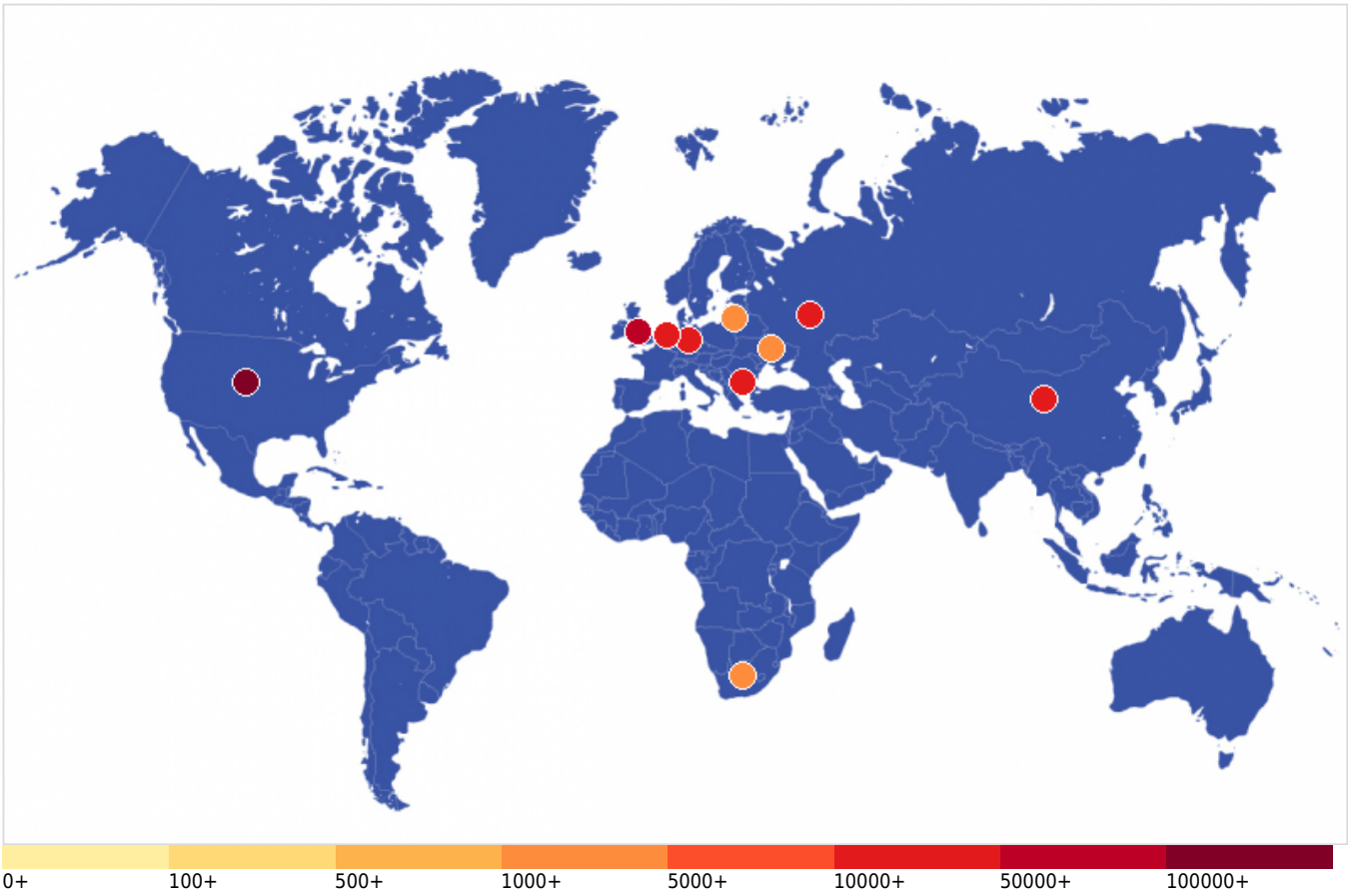
36

The number of hosts analyzed during the month was 69, of which 50 had vulnerabilities. The vulnerabilities are classified as follows: 55 critical risk, 58 high risk, 164 medium risk and 30 low risk. According to the data provided, the current vulnerability index of your organization is 36%.

THREATS

Critical Attacks Per Country In Past Week

GLESEC 11/21/2023



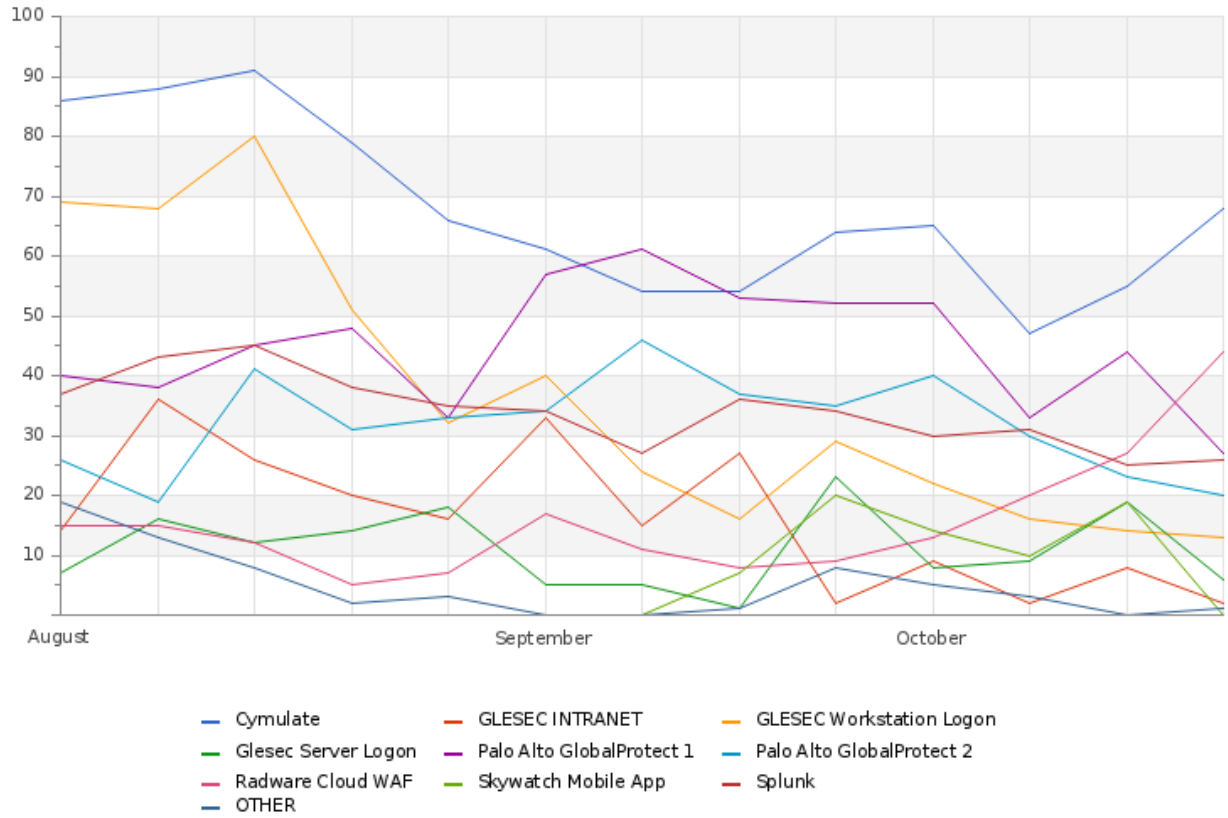
United States - 266541
Germany - 20885
Lithuania - 3748
United Kingdom - 62984
Netherlands - 20528
South Africa - 3341
Bulgaria - 28361
China - 14723
Russia - 28112
Ukraine - 4179

The graph shows the origin of the attacks that have been carried out against the company. Most of these attacks come from the United States, which ranks first with more than 200,000 attacks, followed by the United Kingdom, Bulgaria and Russia, which do not exceed 100,000 attacks. Security strategies should therefore focus primarily on threats originating in the United States, as it accounts for the majority of attacks against the company.

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

GLESEC 11/21/2023

Total Number of Successful MFA authentications per application

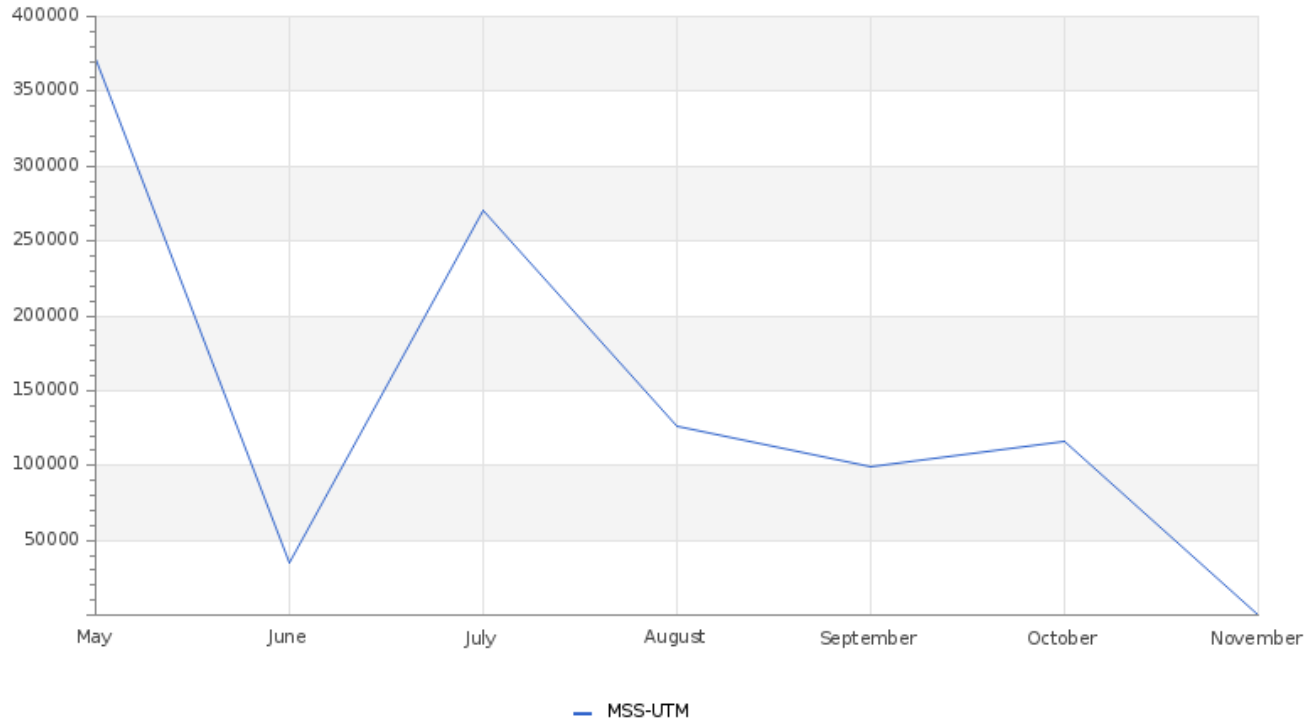


The graph shows a predominance of authentications performed on the GlobalProtect and Cymulate application. This information coincides with the events of the month, and the constant evaluations that are performed on a weekly basis to customers through the Cymulate application.

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

GLESEC 11/21/2023

Total Attacks Successfully Blocked Per Service

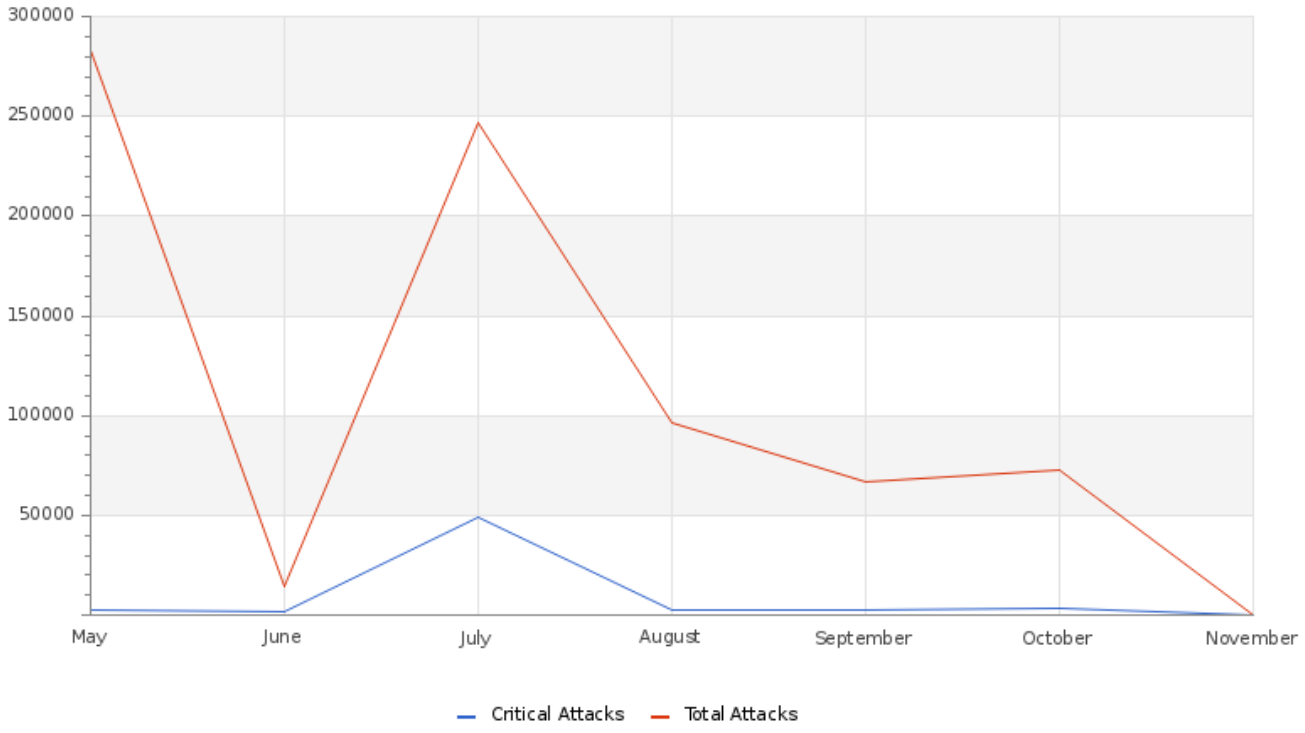


The graph shows a slight increase in attacks received compared to the previous month, through monitoring in conjunction with the security systems have allowed each of the attacks to be successfully blocked.

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

GLESEC 11/21/2023

Attacks Successfully Blocked by Severity



The graph shows a slight increase in the number of attacks recorded during the month and in attacks classified as critical. Our security systems have been consistently protecting against DDoS attacks, IoT botnets, phishing, intrusions, zero-day threats, among others.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Down Devices	7	3
Critical Down Devices	0	0

Some devices presented momentary crashes, which were immediately reported to corroborate that they were false positives.

Histogram of Total and Critical Device Outages

Some devices exhibited momentary outages, while others pertain to false positives related to monitoring sensors. Constant monitoring is necessary to provide a quick and effective solution to any outages that may occur.

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

GLESEC 11/21/2023

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
760,746	0	0	26,821

Most of the attacks blocked by the MSS-EDR service belong to attacks originating from the MSS-BAS service. This should be taken into account when performing an in-depth analysis of the security status.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
EDR Alerts	298
BAS Immediate Threat	54
Change in High or Critical Vulnerabilities	25
BAS DLP	7
BAS Endpoint Security	8
BAS Web Security	28
Change in Systems Performance	4
Monitoring Event for SPLUNK CLOUD	3
Change in Systems Availability	1

We recommend reviewing in detail the results of the tests performed on the MSS-BAS service, as well as the cases of vulnerabilities that have been discovered in your systems. All events recorded during the month have been documented and can be viewed in the C&RU section of our Skywatch platform.

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