TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

December 12, 2023

GLESEC 12/12/2023

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.

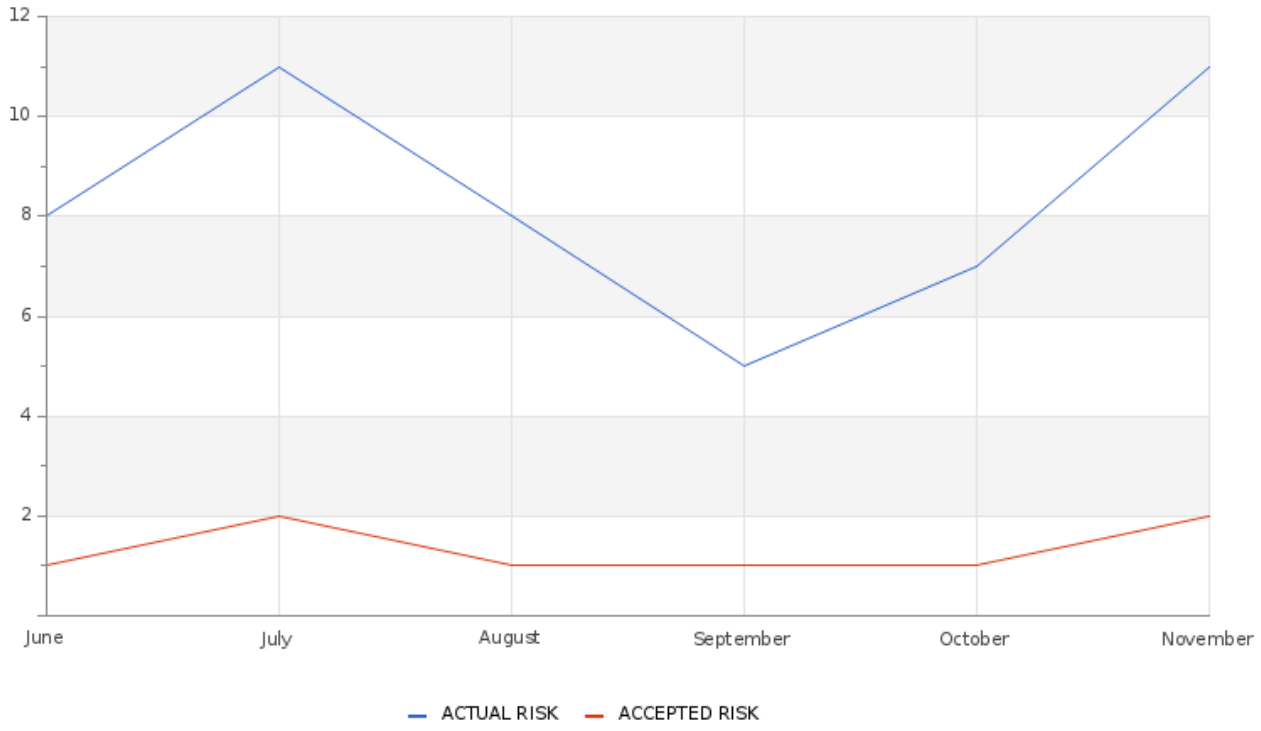
RISK

Actual Risk	Accepted Risk	Confidence
11%	2%	High

Accepted & Actual Risk

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

GLESEC 12/12/2023



Over the course of this month, there has been a noticeable increase in the risk levels. The current risk now sits at 11%, and the accepted risk at 2%. This represents a significant rise from the previous month's figures, where the actual risk was recorded at 7% and the accepted risk at 1%.

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

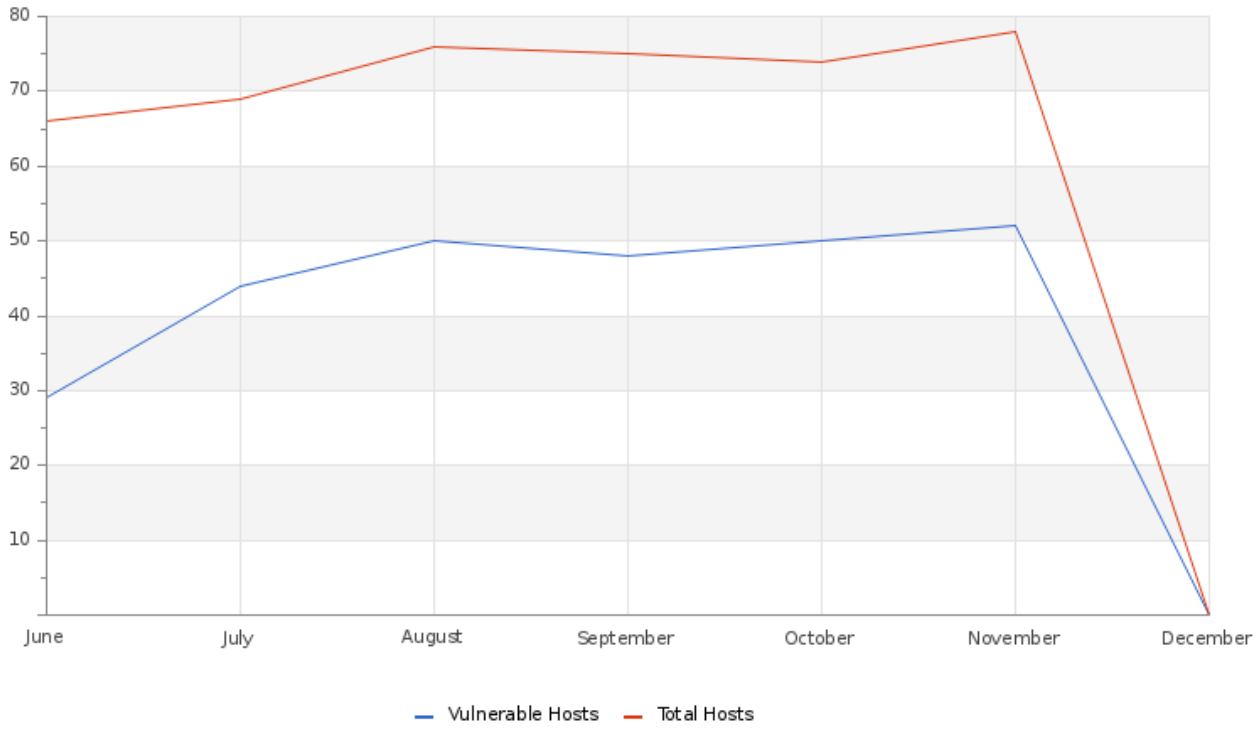
	Current Month	Previous Month
Actual Risk	11	9
Accepted Risk	2	1

Actual risk has increased by 2 points with respect to the previous month;
Accepted Risk has increased by 1 point with respect to the previous month.
These shifts in the realm of cybersecurity highlight how our environment is constantly evolving, underscoring the need for ongoing vigilance and adaptation to the emerging conditions in information security.

VULNERABILITY

GLESEC 12/12/2023

Hosts & Vulnerable Hosts In Last 6 Months



The graph shows an increase in the number of hosts identified and a decrease in vulnerabilities over the month, indicating potential breaches in the security perimeter. Among the most notable high-risk vulnerabilities are multiple versions of Adobe Acrobat with various vulnerabilities, as detailed in reports APSB22-32, APSB22-39, APSB22-46, APSB23-01, APSB23-24, APSB23-30, APSB23-34, and APSB23-54, as well as vulnerabilities in Adobe Reader according to report APSB17-24, and in 7-Zip prior to version 23.00. Prompt attention to these areas is crucial to ensure a more secure environment.

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

GLESEC 12/12/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	72	73
Hosts Discovered	74	72
Vulnerable Hosts	49	50
Critical Vulnerabilities Count	86	33
High Vulnerabilities Count	199	51
Medium Vulnerabilities Count	259	163
Low Vulnerabilities Count	35	32
Phishing Score	0	0
Email Gateway Score	9	9
Web Application Firewall Score	22	22
Web Gateway Score	61	57
Endpoint Score	38	36
Hopper Score	33	33
DLP Score	71	82

Our systems underwent simulations to assess various security facets. The ensuing scores were: Phishing - 0, Email Gateway - 9, Web Application Firewall - 22, Web Gateway - 61, Endpoint - 38, Hopper - 33, and DLP - 71. These results highlight the robust areas and those needing more focus in our security setup.

Vulnerability Metric

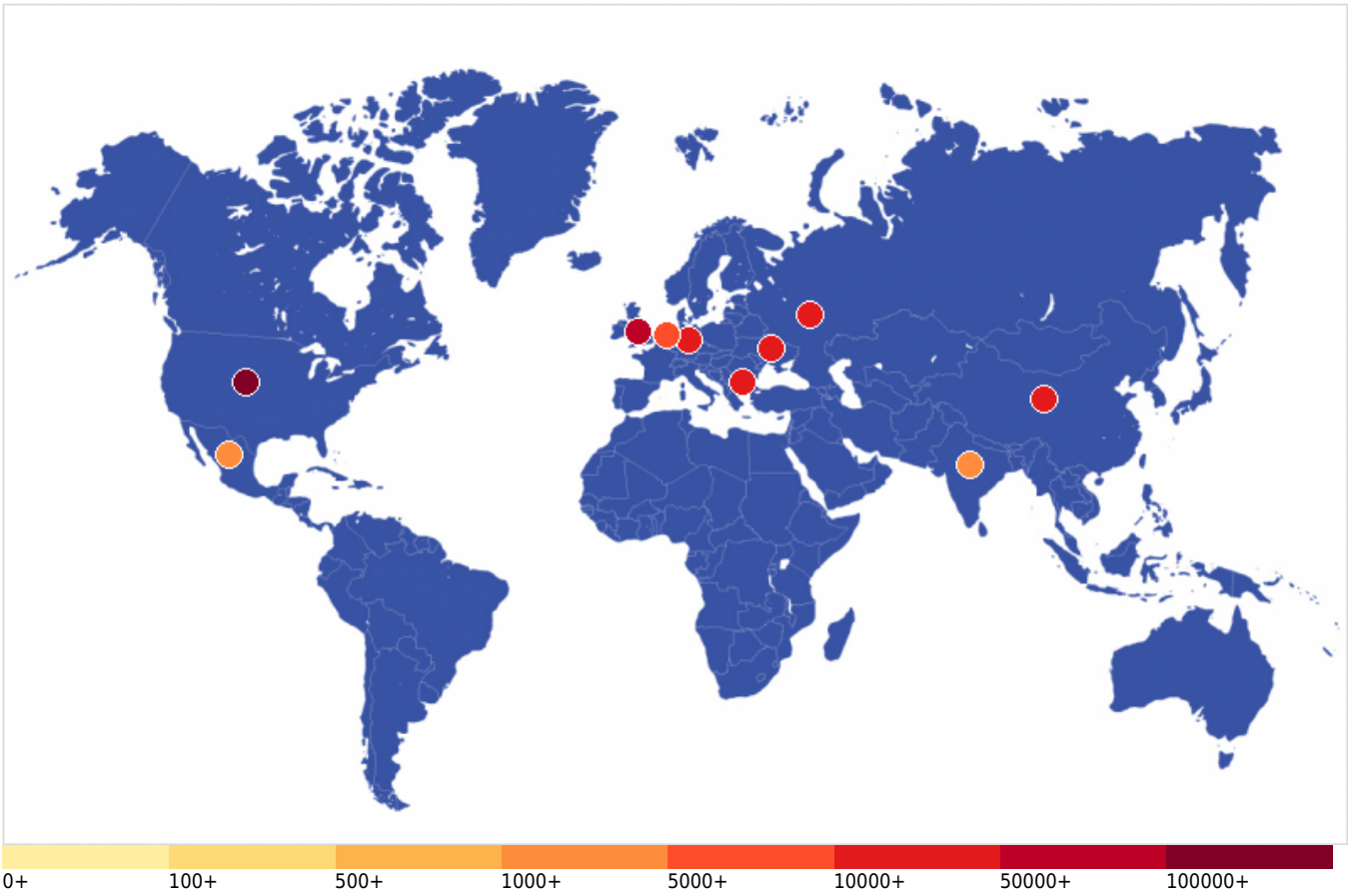
54

An analysis was conducted on 74 hosts based on their address range, revealing that 49 hosts are vulnerable. These vulnerabilities are categorized by severity, as outlined in the accompanying table. In this timeframe, we recorded 86 vulnerabilities of critical nature, 199 high-risk, 259 medium-risk, and 35 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 54%.

THREATS

Critical Attacks Per Country In Past Week

GLESEC 12/12/2023



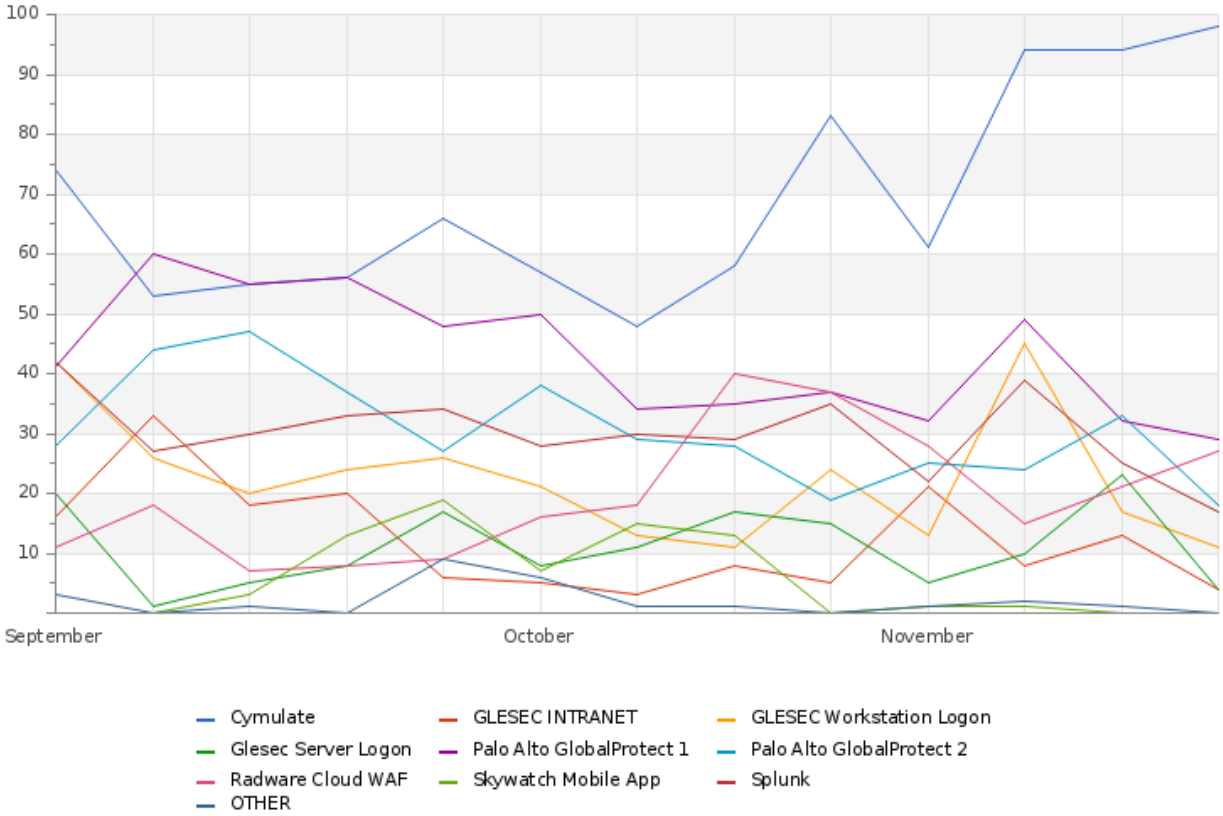
United States - 306582
Bulgaria - 13912
Mexico - 3053
United Kingdom - 86882
Ukraine - 13337
India - 3046
Germany - 25423
Russia - 10706
China - 13942
Netherlands - 8976

This graph displays the distribution of cyber attacks by country, highlighting the United States' dominance with 306,582 attacks. It is followed by the United Kingdom with 86,882 and Germany with 25,423. Other countries like China, Bulgaria, Ukraine, Russia, the Netherlands, Mexico, and India report lower figures. The map underscores the need to focus cybersecurity efforts mainly on threats originating from the U.S., while maintaining global vigilance.

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

GLESEC 12/12/2023

Total Number of Successful MFA authentications per application

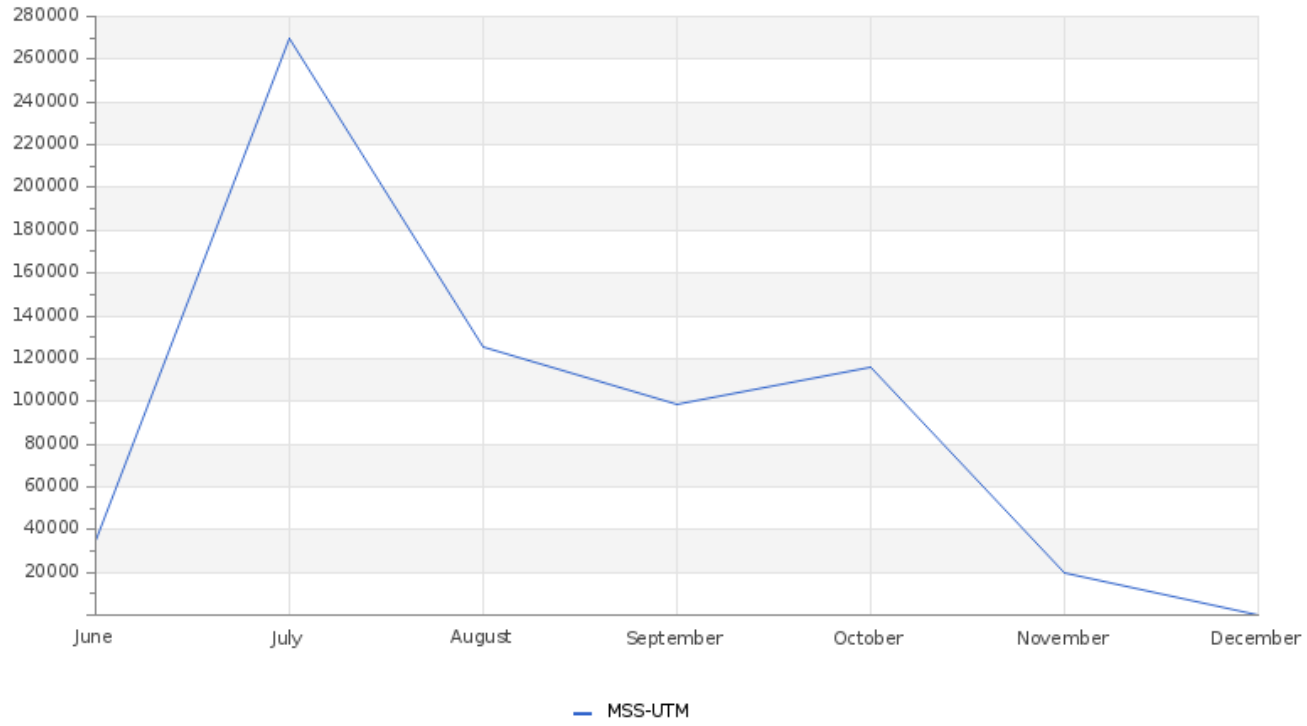


The graph reveals a distinct trend in authentication patterns, with workstations and Cymulate emerging as the predominant applications for logins. This trend underscores the significant role these two areas play in daily activities, possibly indicating key interaction points or areas of importance within the organizational environment.

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

GLESEC 12/12/2023

Total Attacks Successfully Blocked Per Service

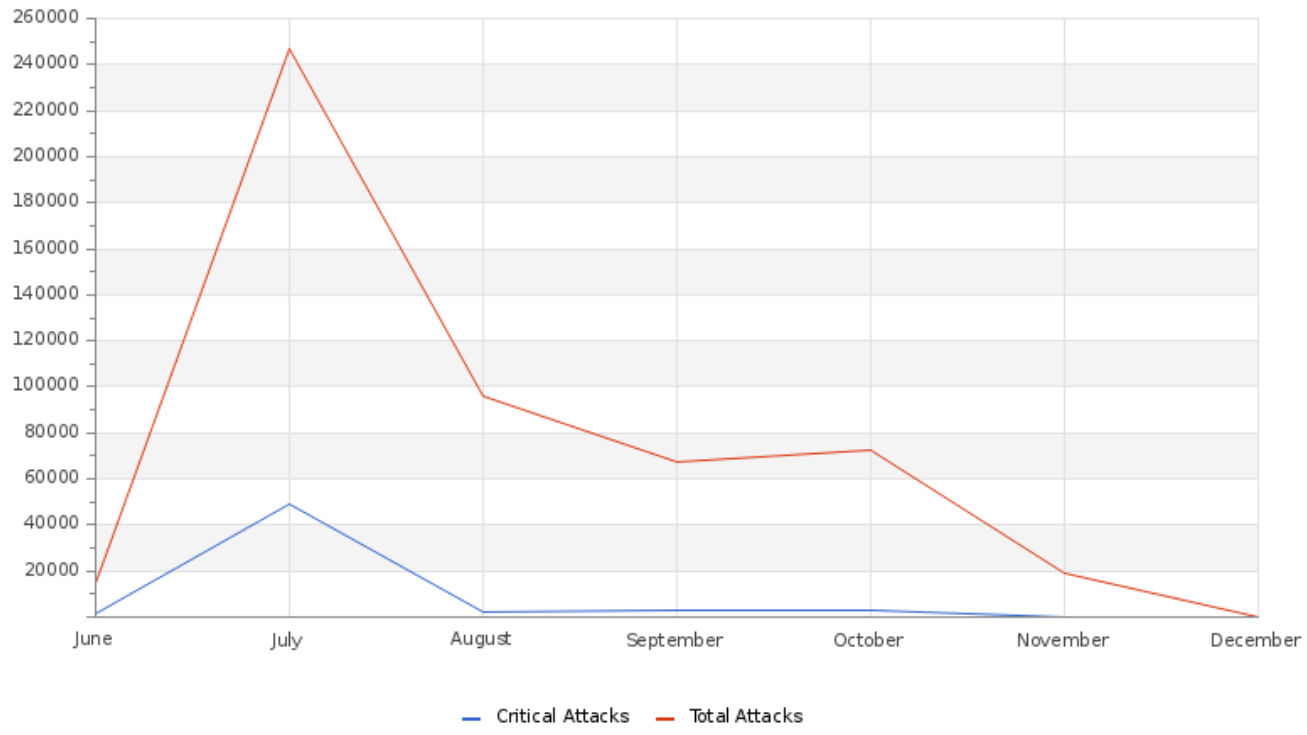


The graph distinctly illustrates the positive effect of implemented security measures. Compared to the previous month, there has been a reduction in the total number of attacks, accompanied by an increase in the number of successfully thwarted attacks

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

GLESEC 12/12/2023

Attacks Successfully Blocked by Severity



The graph presents encouraging security outcomes, emphasizing the rise in successfully countered attacks. It proactively safeguards against emerging threats, including DDoS attacks, IoT botnets, advanced phishing methods, malware infiltrations, zero-day vulnerabilities, and complex DNS spoofing tactics.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	8	4
Critical Device Outages	0	0

Devices affected by outages were quickly restored in a matter of seconds. These occurrences stemmed from false positives due to brief disconnections.

Histogram of Total and Critical Device Outages

Devices undergoing downtime achieved swift restoration within seconds, ensuring prompt recovery. These brief incidents are attributed to false positives from short-term disconnections. Understanding and monitoring these events is crucial for seamless operation and reducing future outages.

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

GLESEC 12/12/2023

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
813,381	0	0	27,230

The statistics from MSS-EDR are elevated, primarily because of the BAS assessments carried out via our dedicated MSS-BAS service. Considering this distortion is vital for a more precise and contextual analysis of the security landscape when reviewing the data.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	36
EDR Alerts	265
BAS DLP	6
BAS Endpoint Security	5
BAS Web Security	16
Change in High or Critical Vulnerabilities	14
Monitoring Event for SPLUNK CLOUD	2
Change in Systems Availability	2
Change in Systems Performance	4

To delve into particular instances, I encourage you to visit the Skywatch platform. There, by applying the C&RU filter, you can select the category that sparks your interest - uncover the insights Skywatch offers!

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