TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

March 06, 2024

GLESEC 03/06/2024

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.

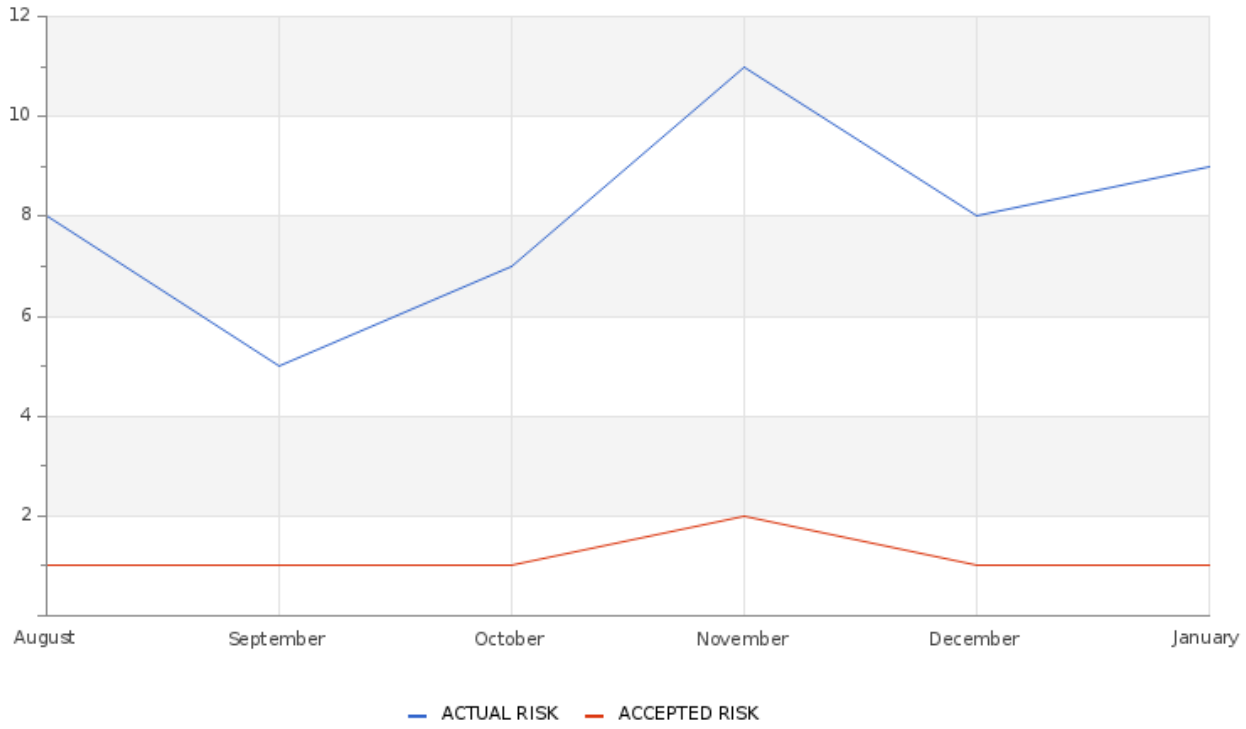
RISK

Actual Risk	Accepted Risk	Confidence
9%	1%	High

Accepted & Actual Risk

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

GLESEC 03/06/2024



Over the course of this month, there has been a noticeable increase in the risk levels. The current risk now sits at 9%, and the accepted risk at 1%. This represents a significant rise from the previous month's figures, where the actual risk was recorded at 8% and the accepted risk at 1%.

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

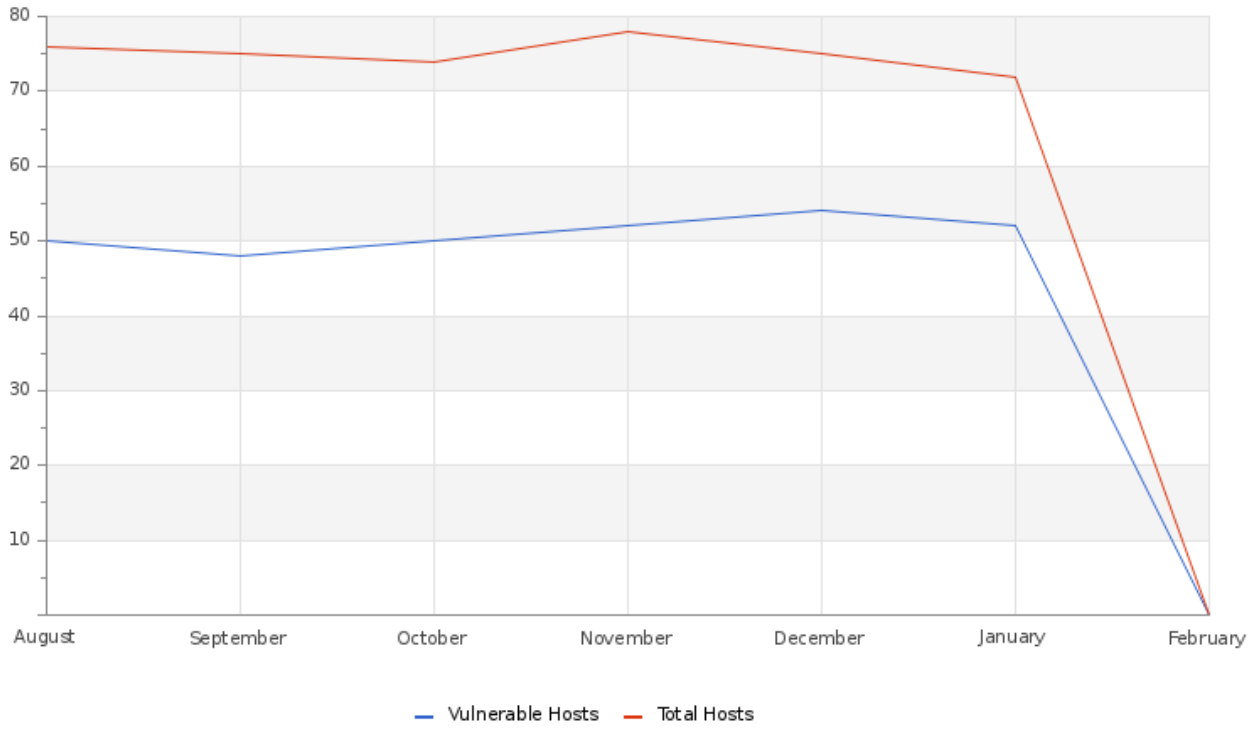
	Current Month	Previous Month
Actual Risk	9	8
Accepted Risk	1	1

Actual risk has increased by 1 points with respect to the previous month;
Accepted Risk has remained at 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 03/06/2024

Hosts & Vulnerable Hosts In Last 6 Months



The graph reveals a decrease in the number of hosts detected over the month, accompanied by a slight increase in the number of vulnerabilities identified in those hosts. The most notable vulnerabilities were related to the lack of security updates and the use of unsupported software versions. Prompt mitigation of these vulnerabilities is crucial to ensure security, thus minimizing the risk of intrusions and data breaches.

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

GLESEC 03/06/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	72	72
Hosts Discovered	66	69
Vulnerable Hosts	46	51
Critical Vulnerabilities Count	19	6
High Vulnerabilities Count	37	17
Medium Vulnerabilities Count	249	159
Low Vulnerabilities Count	41	39
Phishing Score	0	
Email Gateway Score	8	
Web Application Firewall Score	25	
Web Gateway Score	64	
Endpoint Score	39	
Hopper Score	33	
DLP Score	73	

Simulations were carried out on our systems to evaluate different security aspects. The results obtained were as follows: a Phishing Score of 0, an Email Gateway Score of 8, a Web Application Firewall Score of 25, a Web Gateway Score of 64, an Endpoint Score of 39, a Hopper Score of 33, and a DLP Score of 73. These scores show the areas of strength and those that require greater attention in our security infrastructure.

Vulnerability Metric

37

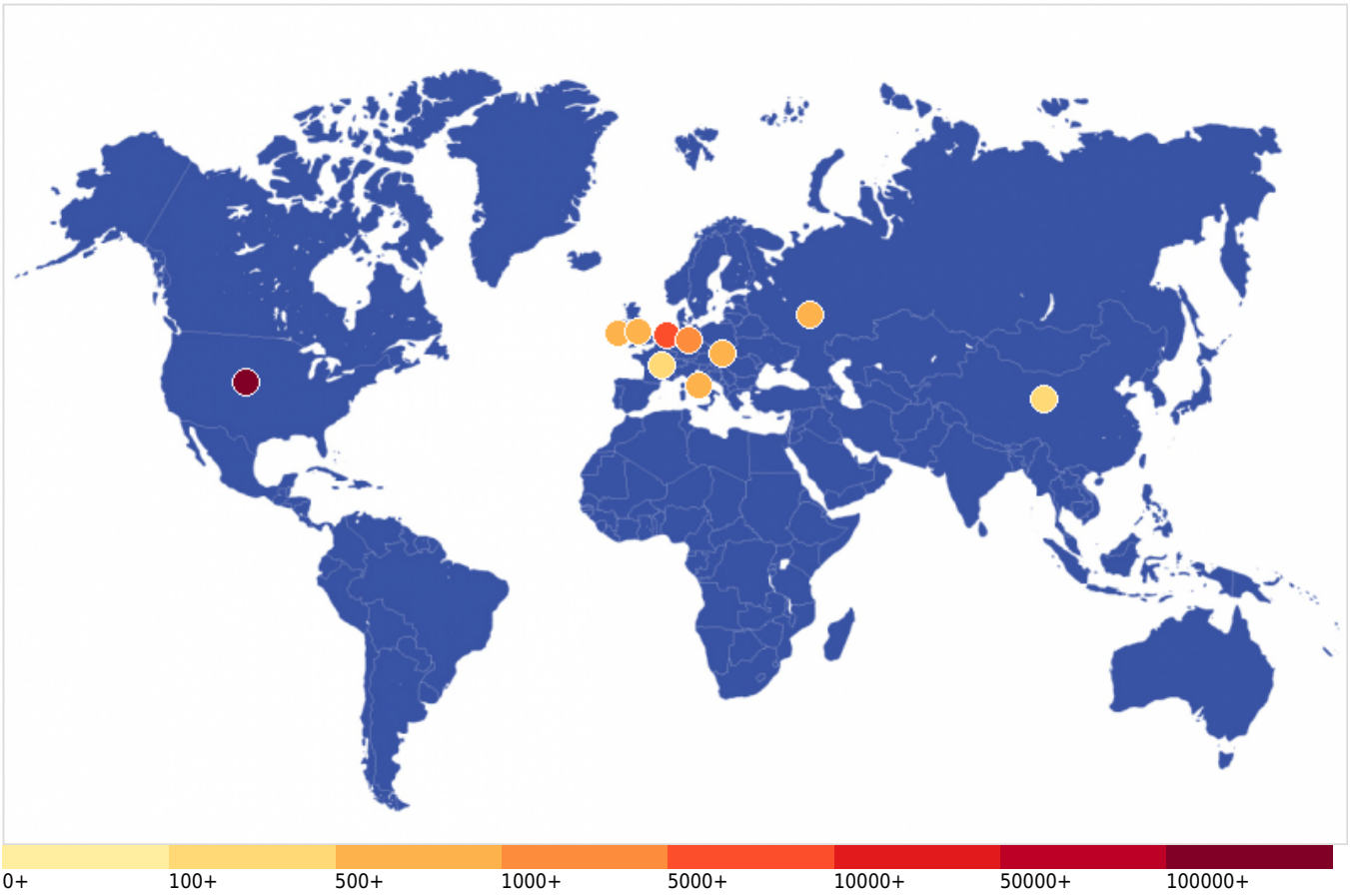
An analysis was conducted on 72 hosts based on their address range, revealing that 66 hosts are vulnerable. These vulnerabilities are categorized by severity, as outlined in the accompanying table. In this timeframe, we recorded 46 vulnerabilities of critical nature, 37 high-risk, 249 medium-risk, and 41 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 37%.

THREATS

Critical Attacks Per Country In Past Week

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

GLESEC 03/06/2024



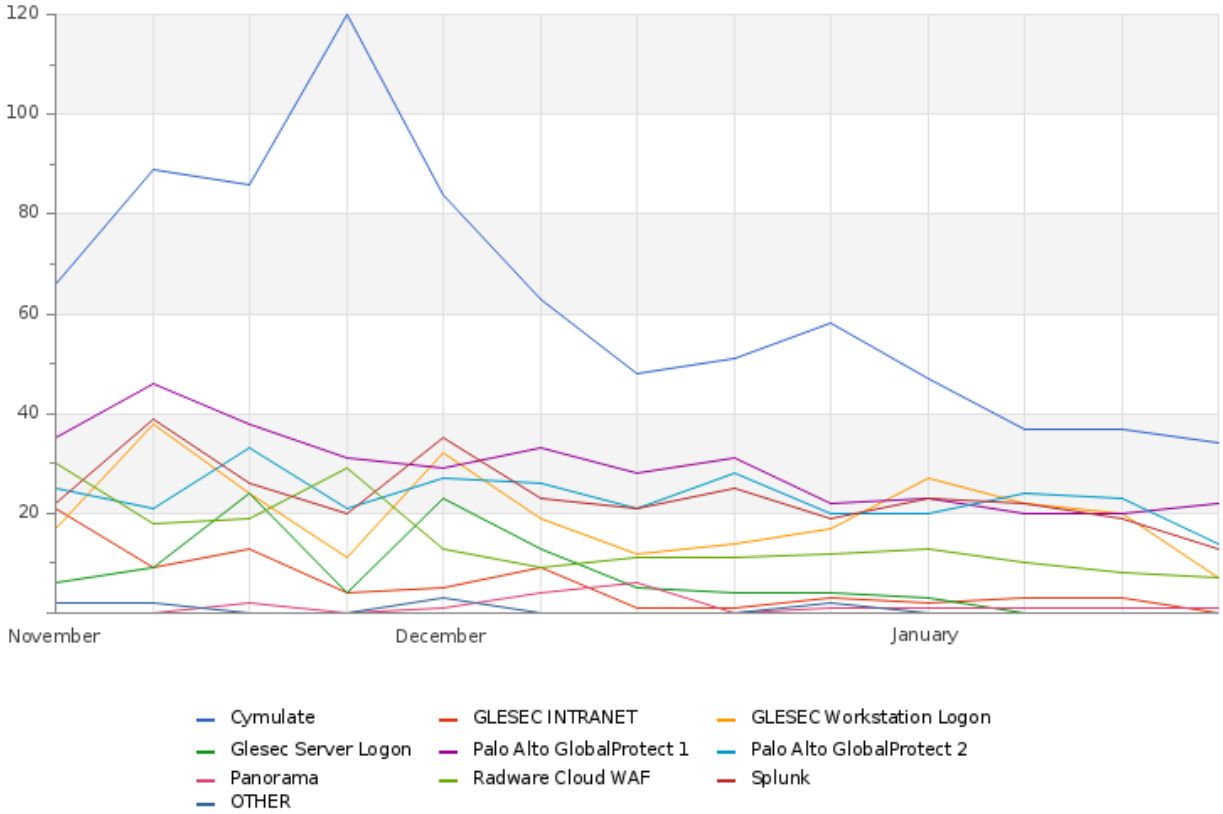
United States - 140595
Ireland - 852
France - 452
Netherlands - 7924
United Kingdom - 826
China - 443
Germany - 1099
Russia - 514
Italy - 908
Slovakia - 504

This graph displays the distribution of cyber attacks by country, highlighting the United States' dominance with 140,595 attacks. It is followed by the Netherlands with 7,924 and Germany with 1,099. 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 03/06/2024

Total Number of Successful MFA authentications per application

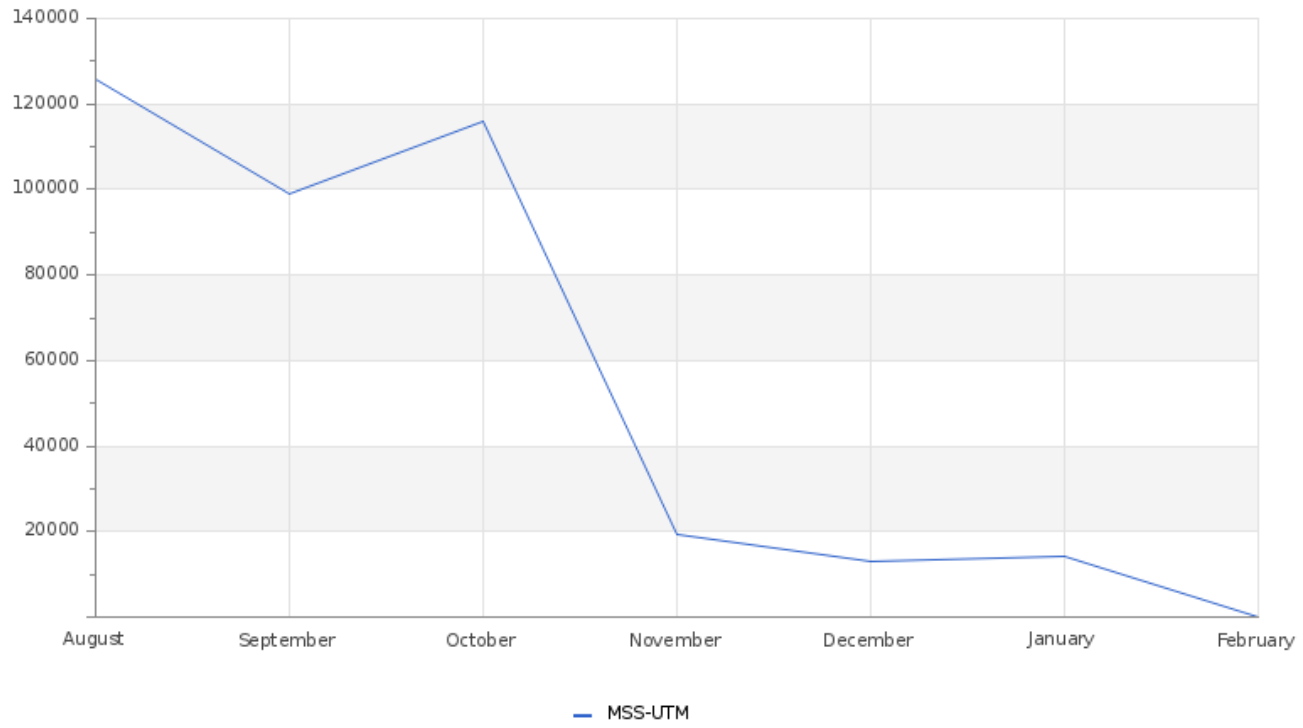


The graph reveals a distinct trend in authentication patterns, with workstations and Cymulate emerging as the predominant applications for logins. This trend underscores the significant role these two areas play in daily activities, possibly indicating key interaction points or areas of importance within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

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

GLESEC 03/06/2024

Total Attacks Successfully Blocked Per Service

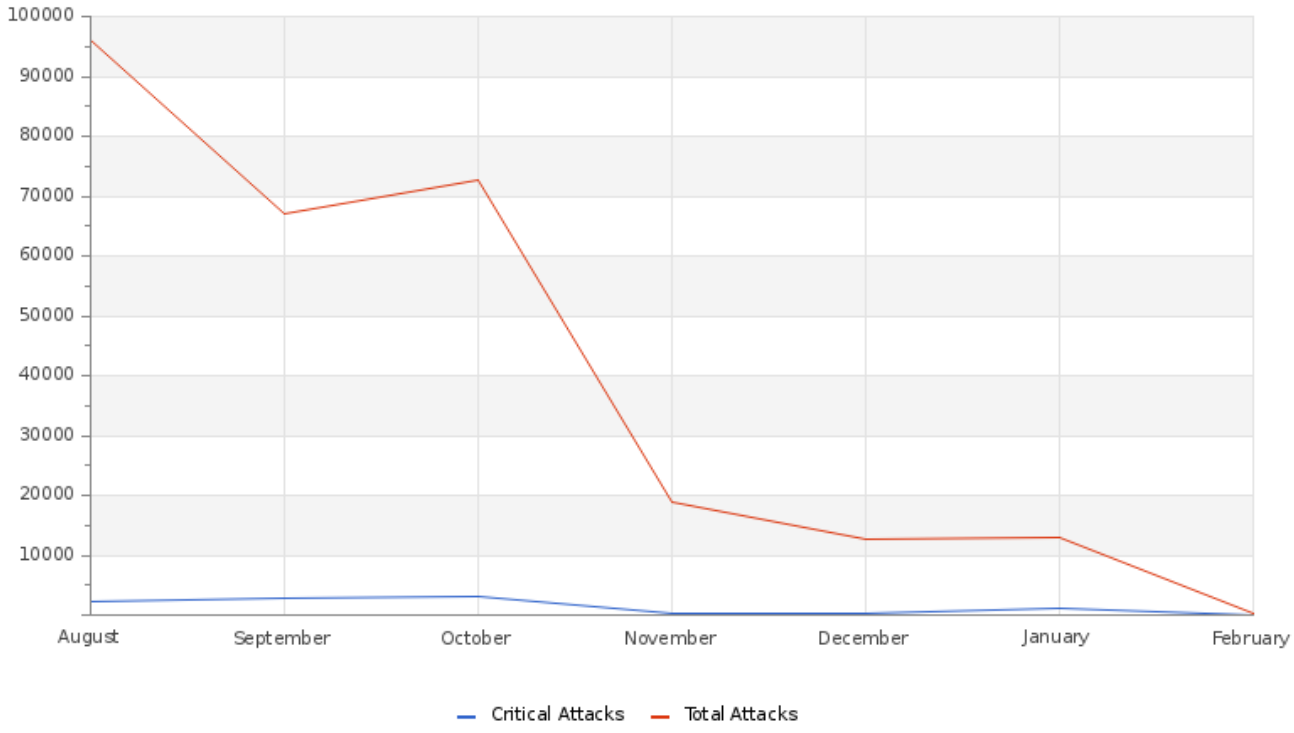


The graph clearly illustrates the positive effect of the security measures implemented. Compared to the previous month, there has been stability in the total number of attacks, accompanied by an increase in the number of successfully thwarted attacks.

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

GLESEC 03/06/2024

Attacks Successfully Blocked by Severity



The chart 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	1
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 03/06/2024

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
22,257	0	0	21,788

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	86
BAS DLP	8
Monitoring Event for SPLUNK CLOUD	9
Change in High or Critical Vulnerabilities	15
EDR Alerts	322
BAS Endpoint Security	10
BAS Web Security	28
Immediate Threat System Vulnerable and Remediation by Patch Management	1
Change in Baseline Systems Discovered	1

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