TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

July 09, 2024

GLESEC 07/09/2024

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.

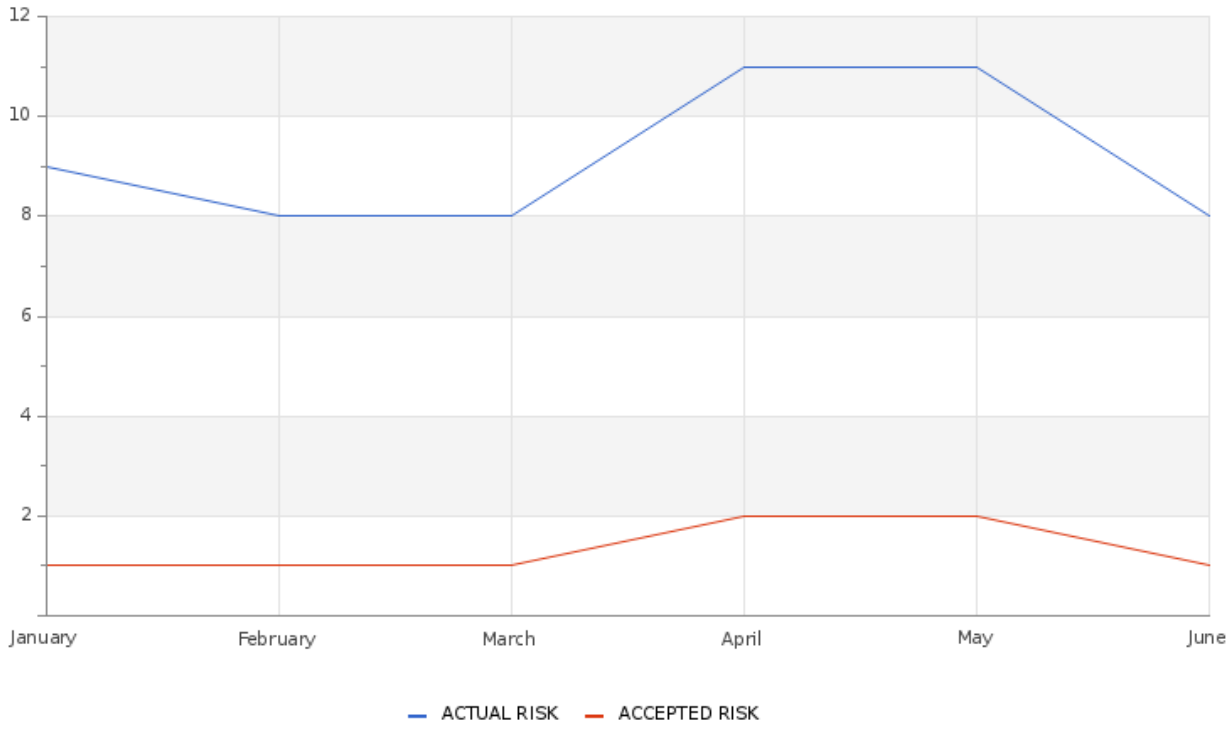
RISK

Actual Risk	Accepted Risk	Confidence
8%	1%	Medium

Accepted & Actual Risk

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

GLESEC 07/09/2024



During the past month, risk levels have remained stable. Currently, the actual risk stands at 8%, while the accepted risk is 1%. These figures indicate continuity with respect to the previous month, when the actual risk was also 11% and the accepted risk was 0%.

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

	Current Month	Previous Month
Actual Risk	8	11
Accepted Risk	1	0

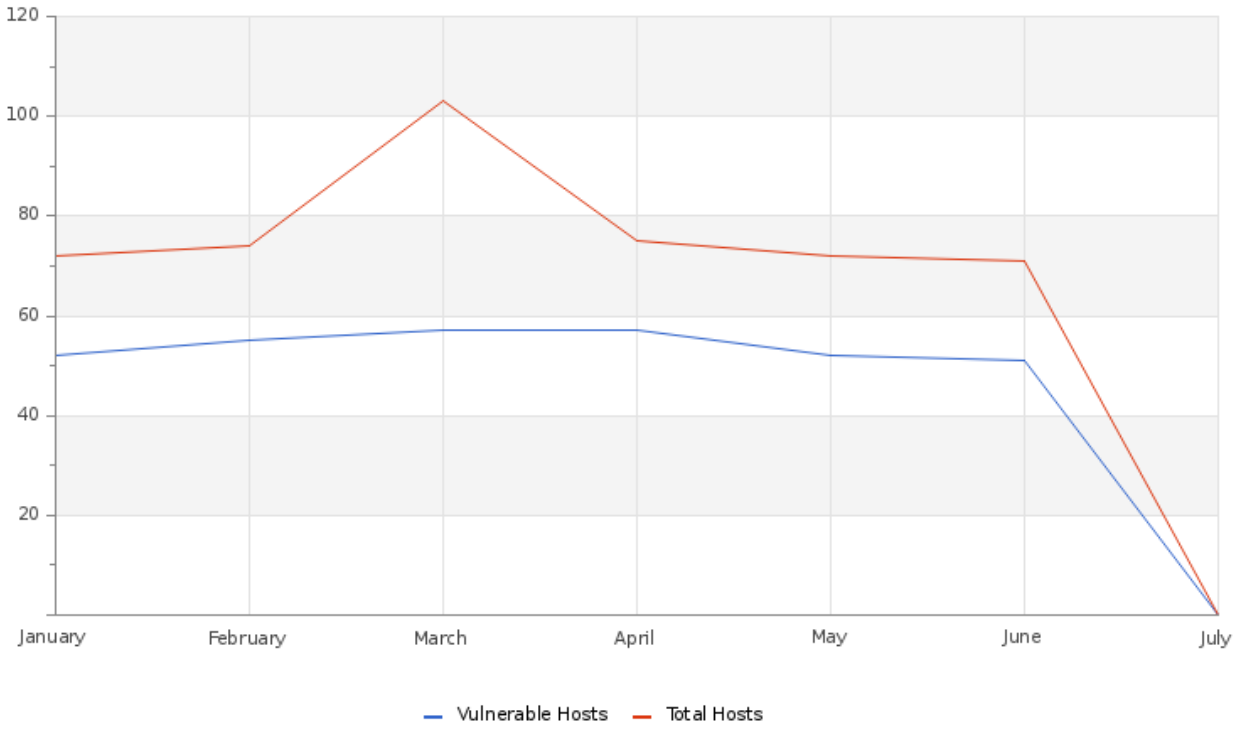
Actual risk has decreased by 2 percentage points. However, accepted risk has increased by 1 percentage point. These changes in cybersecurity highlight the dynamic nature of our environment and underscore the need for constant vigilance and adaptation to changing conditions in information security.

VULNERABILITY

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

GLESEC 07/09/2024

Hosts & Vulnerable Hosts In Last 6 Months



The graph illustrates a rise in the number of identified hosts coupled with a decline in vulnerabilities over the month, which may indicate potential breaches in the security perimeter. Noteworthy among the high-risk vulnerabilities are several iterations of Adobe Acrobat, each with distinct issues. Additionally, significant vulnerabilities include:

- Google Chrome < 123.0.6312.58 Multiple Vulnerabilities
- KB5035849: Windows 10 version 1809 / Windows Server 2019 Security Update (March 2024)
- OpenSSL 1.0.2 < 1.0.2zf Vulnerability
- Security Update for Microsoft Visual Studio Code (November 2023)
- Ubuntu 22.04 LTS / 23.04: Linux kernel vulnerabilities (USN-6534-1)
- libcurl 7.69 < 8.4.0 Heap Buffer Overflow

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

GLESEC 07/09/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	73	73
Hosts Discovered	64	68
Vulnerable Hosts	4	49
Critical Vulnerabilities Count	0	35
High Vulnerabilities Count	0	55
Medium Vulnerabilities Count	7	332
Low Vulnerabilities Count	5	64
Phishing Score	0	-1
Email Gateway Score	7	6
Web Application Firewall Score	24	23
Web Gateway Score	62	61
Endpoint Score	49	48
Hopper Score	33	32
DLP Score	79	78

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 7, a Web Application Firewall Score of 24, a Web Gateway Score of 62, an Endpoint Score of 49, a Hopper Score of 33, and a DLP Score of 79. These scores show the areas of strength and those that require greater attention in our security infrastructure.

Vulnerability Metric

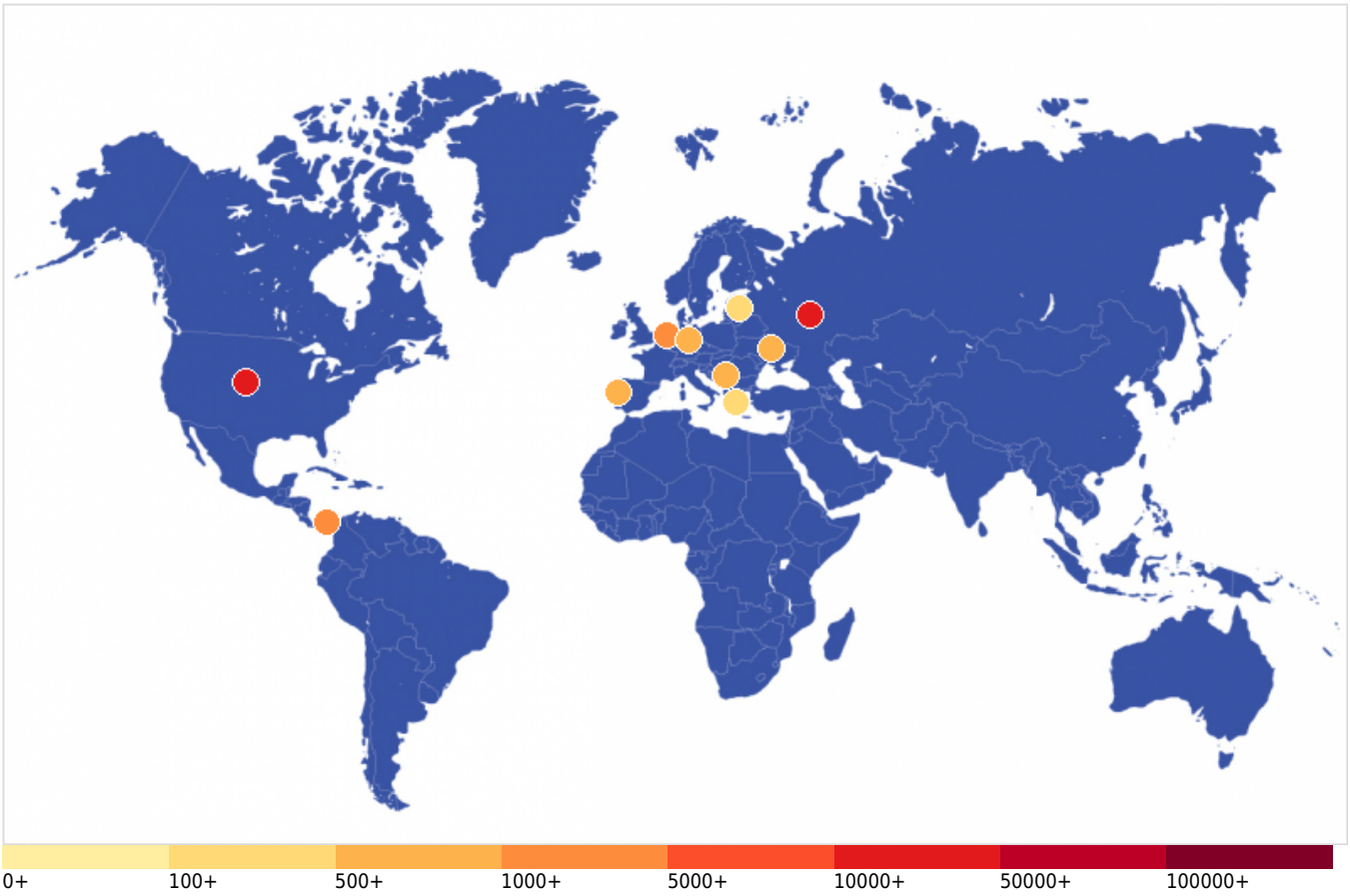
46

An analysis was conducted on 73 hosts based on their address range, revealing that 4 hosts are vulnerable. These vulnerabilities are categorized by severity, as outlined in the accompanying table. In this timeframe, we recorded 0 vulnerabilities of critical nature, 0 high-risk, 7 medium-risk, and 5 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 46%.

THREATS

Critical Attacks Per Country In Past Week

GLESEC 07/09/2024



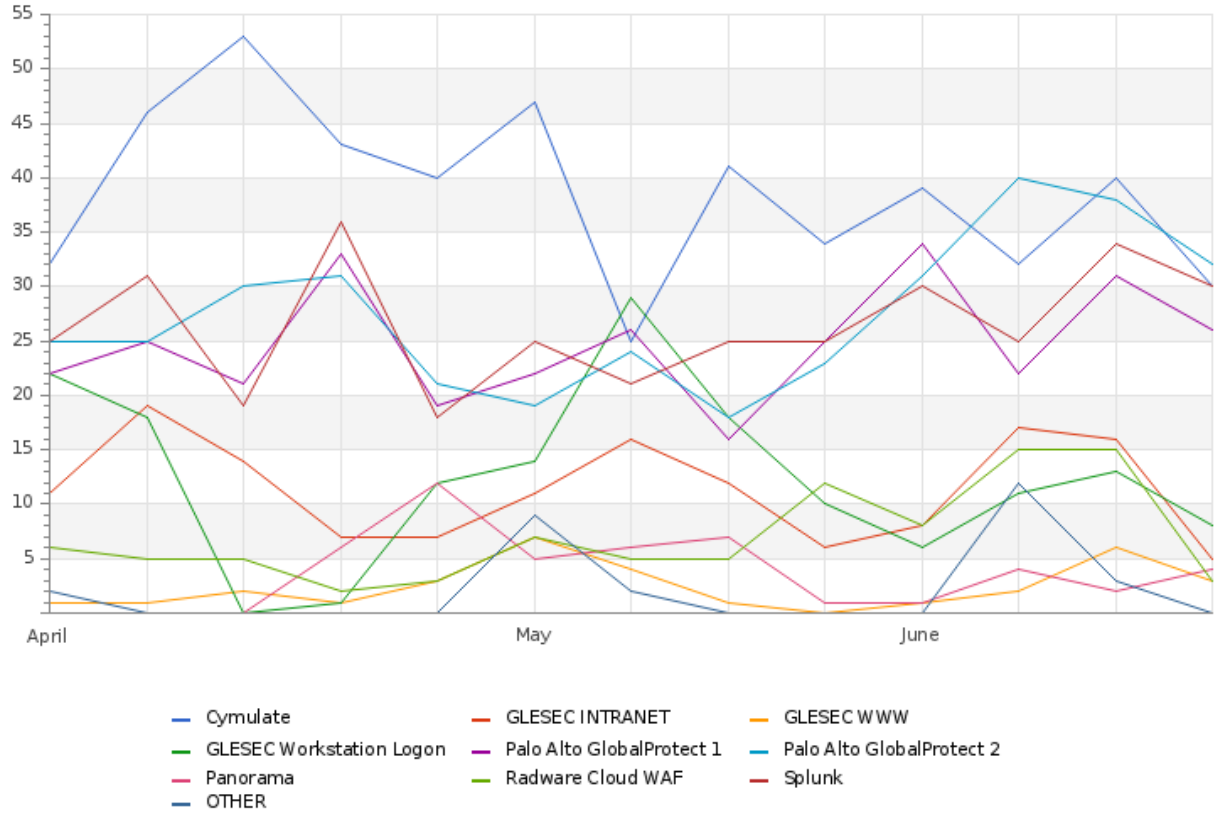
United States - 49340
Germany - 856
Greece - 456
Russia - 47052
Portugal - 622
Latvia - 395
Panama - 2281
Ukraine - 544
Netherlands - 1460
Serbia - 500

This graph displays the distribution of cyber attacks by country, highlighting the United States' dominance with 49,340 attacks. It is followed by the Russia with 47,052 and Panama with 2,281. Other countries like Netherlands, Germany, Portugal, Ukraine, Serbia, Greece, and Latvia 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 07/09/2024

Total Number of Successful MFA authentications per application

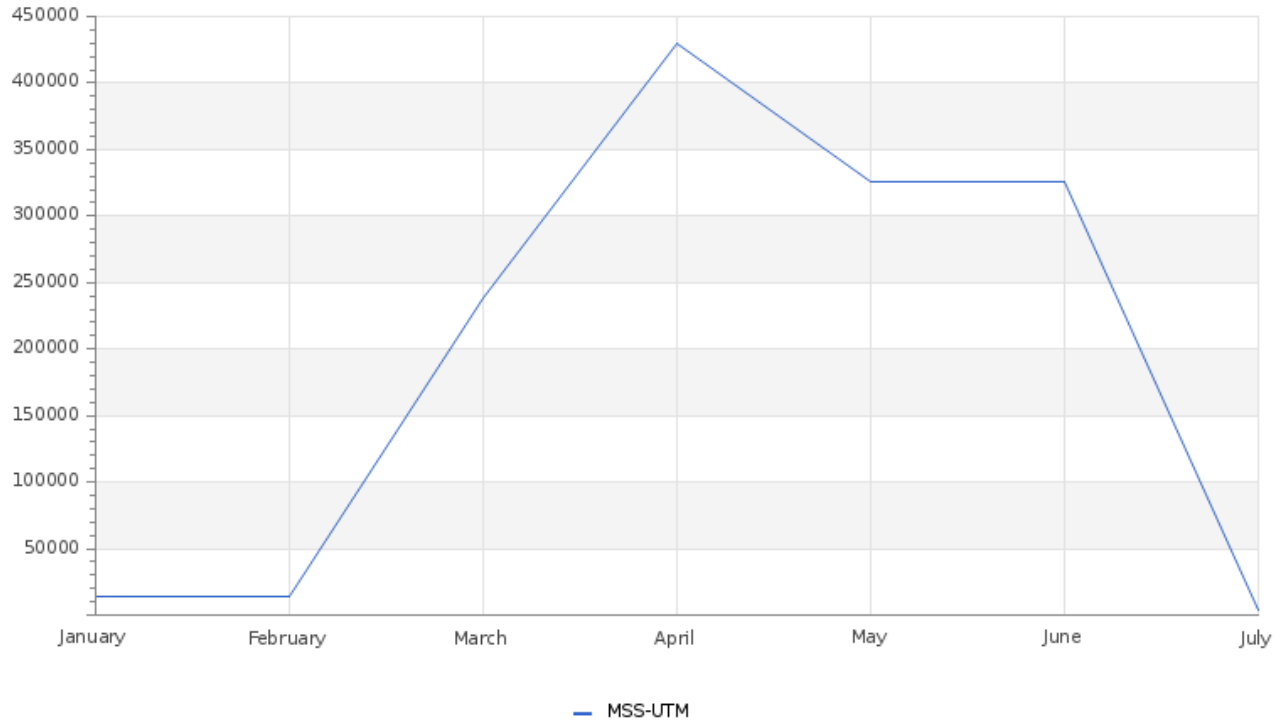


The graph highlights a clear trend in authentication patterns, showing that workstations and Cymulate are the primary applications for logins. This trend emphasizes the crucial role these two areas play in daily operations, possibly indicating key interaction points or areas of significance within the organizational environment.

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

GLESEC 07/09/2024

Total Attacks Successfully Blocked Per Service

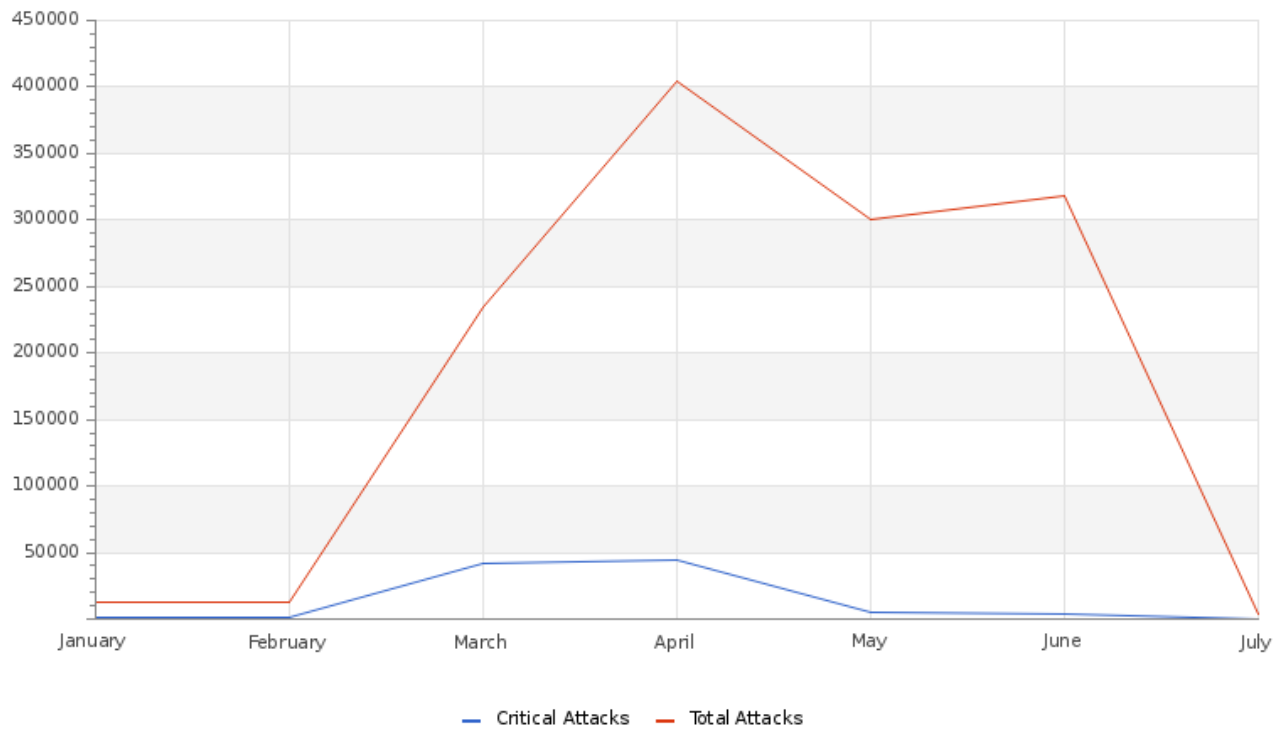


The chart distinctly illustrates the positive effect of implemented security measures. Compared to the previous month, there has been a reduction in the total number of attacks, accompanied by an increase in the number of successfully thwarted attacks

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

GLESEC 07/09/2024

Attacks Successfully Blocked by Severity



The chart presents encouraging security outcomes, highlighting the rise in successfully countered attacks. These measures proactively safeguard against emerging threats, including DDoS attacks, IoT botnets, advanced phishing methods, malware infiltrations, zero-day vulnerabilities, and sophisticated DNS spoofing tactics.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	10	0
Critical Device Outages	0	0

Devices impacted by outages experienced swift recovery, with functionality being restored within seconds. These incidents primarily originated from false positives, attributed to transient disconnections.

Histogram of Total and Critical Device Outages

Devices experiencing downtime were swiftly brought back online within seconds, ensuring rapid recovery and minimal disruption. These incidents involved sensors that were reported and momentarily disconnected, highlighting the need for continuous monitoring and immediate response mechanisms to maintain operational efficiency and security.

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

GLESEC 07/09/2024

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
22,606	0	0	0

The elevated statistics from the Managed Security Service - Endpoint Detection and Response (MSS-EDR) are largely due to the Breach and Attack Simulation (BAS) assessments conducted through our specialized Managed Security Service - Breach and Attack Simulation (MSS-BAS) service. Acknowledging this distortion is crucial for a more accurate and contextual evaluation of the security landscape when analyzing the data.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
FW Alerts	5
BAS Immediate Threat	71
BAS DLP	2
BAS Web Security	12
BAS WAF	6
Immediate Threat System Vulnerable and Remediation by Patch Management	7
EDR Alerts	37
Monitoring Event for SPLUNK CLOUD	6
BAS Endpoint Security	10
Change in Baseline Systems Discovered	2
Change in Systems Performance	1
MSS-DLP - External File access	5
Change in High or Critical Vulnerabilities	1
High Persistency Detection	1

For a closer look at specific instances, I recommend visiting the Skywatch platform. By applying the C&RU (Create & Review Update) filter there, you can choose the category that interests you the most. This approach will allow you to uncover the insights that Skywatch provides!

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

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

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