TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

April 02, 2024

GLESEC 04/02/2024

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.

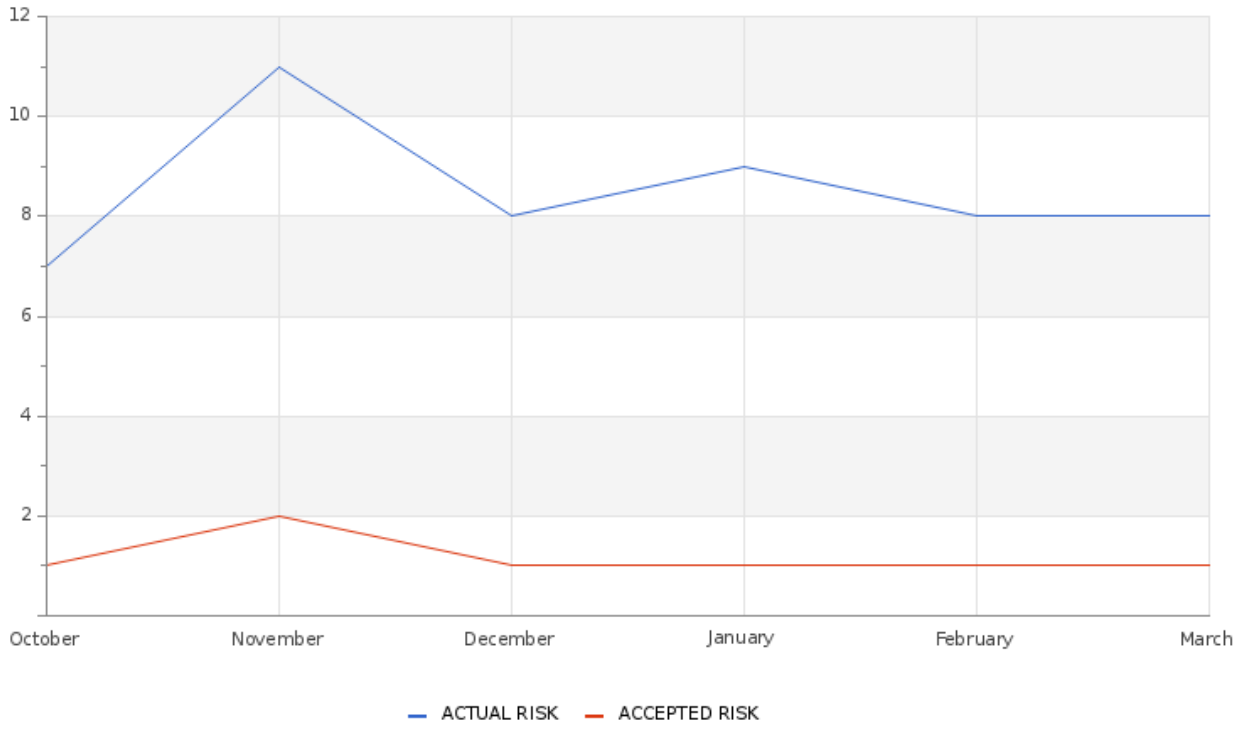
RISK

Actual Risk	Accepted Risk	Confidence
8%	1%	Medium

Accepted & Actual Risk

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

GLESEC 04/02/2024



Over this month, the observed increase in risk levels is noteworthy. The actual risk now is at 8%, with the accepted risk being 0%. This marks a notable change from last month, where the risk stood at 9% and the accepted risk was at 1%.

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

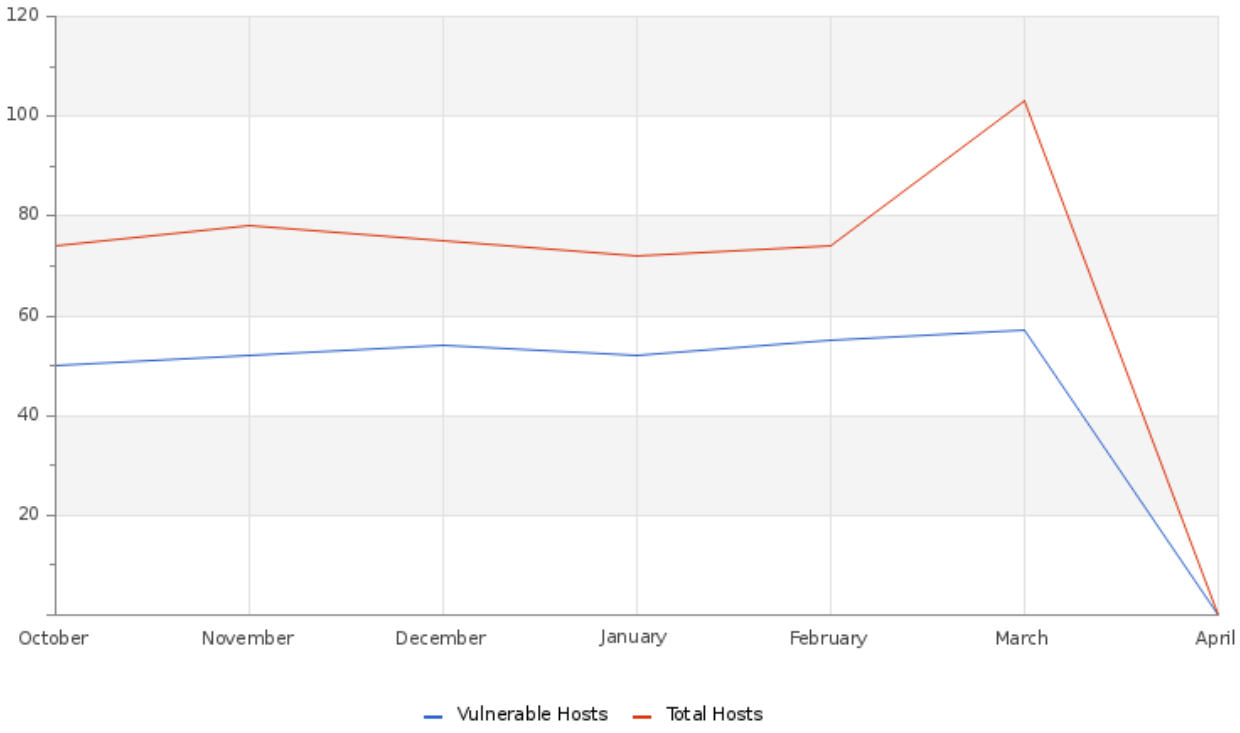
	Current Month	Previous Month
Actual Risk	8	8
Accepted Risk	1	0

This month, we've observed a 1-point increase in actual risk, bringing it to 8%, and a 1-point decrease in accepted risk, now at 0%, compared to last month's figures. Such shifts in cybersecurity metrics underscore the dynamic nature of our digital environment. They emphasize the imperative for continuous vigilance and the necessity to adapt to the ever-changing landscape of information security.

VULNERABILITY

GLESEC 04/02/2024

Hosts & Vulnerable Hosts In Last 6 Months



The graph displays an upward trend in the identification of hosts, alongside a reduction in vulnerabilities throughout the month. This pattern suggests potential breaches in the security framework. Particularly significant are high-risk vulnerabilities associated with different versions of Adobe Acrobat, each presenting unique security flaws. Additionally, multiple vulnerabilities were noted in Google Chrome versions prior to 123.0.6312.58, the security update KB5035849 for Windows 10 version 1809 and Windows Server 2019 released in March 2024, a specific vulnerability in OpenSSL versions earlier than 1.0.2zf, the security update for Microsoft Visual Studio Code released in November 2023, vulnerabilities in the Linux kernel for Ubuntu versions 22.04 LTS and 23.04 as documented in USN-6534-1, and a heap buffer overflow vulnerability in libcurl versions 7.69 to before 8.4.0. These details underscore the complexity and evolving nature of cybersecurity threats, highlighting the importance of proactive security measures and timely updates to mitigate these risks.

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

GLESEC 04/02/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	72	72
Hosts Discovered	72	69
Vulnerable Hosts	51	49
Critical Vulnerabilities Count	23	21
High Vulnerabilities Count	35	47
Medium Vulnerabilities Count	273	262
Low Vulnerabilities Count	52	45
Phishing Score	0	-1
Email Gateway Score	7	6
Web Application Firewall Score	25	24
Web Gateway Score	63	62
Endpoint Score	16	15
Hopper Score	33	32
DLP Score	79	78

The conducted simulations to assess various security dimensions of our systems yielded insightful results: a Phishing Score of 0, indicating no vulnerability detected in phishing attempts; an Email Gateway Score of 7, suggesting moderate robustness against email-based threats; a Web Application Firewall (WAF) Score of 25, showing a level of effectiveness in protecting web applications; a Web Gateway Score of 54, reflecting a stronger defense against web-based threats; an Endpoint Score of 16, indicating a solid defense at individual network entry points; a Hopper Score of 33, which implies no risk from internal network hopping threats; and a Data Loss Prevention (DLP) Score of 79, showcasing a high level of protection against data breaches.

Vulnerability Metric

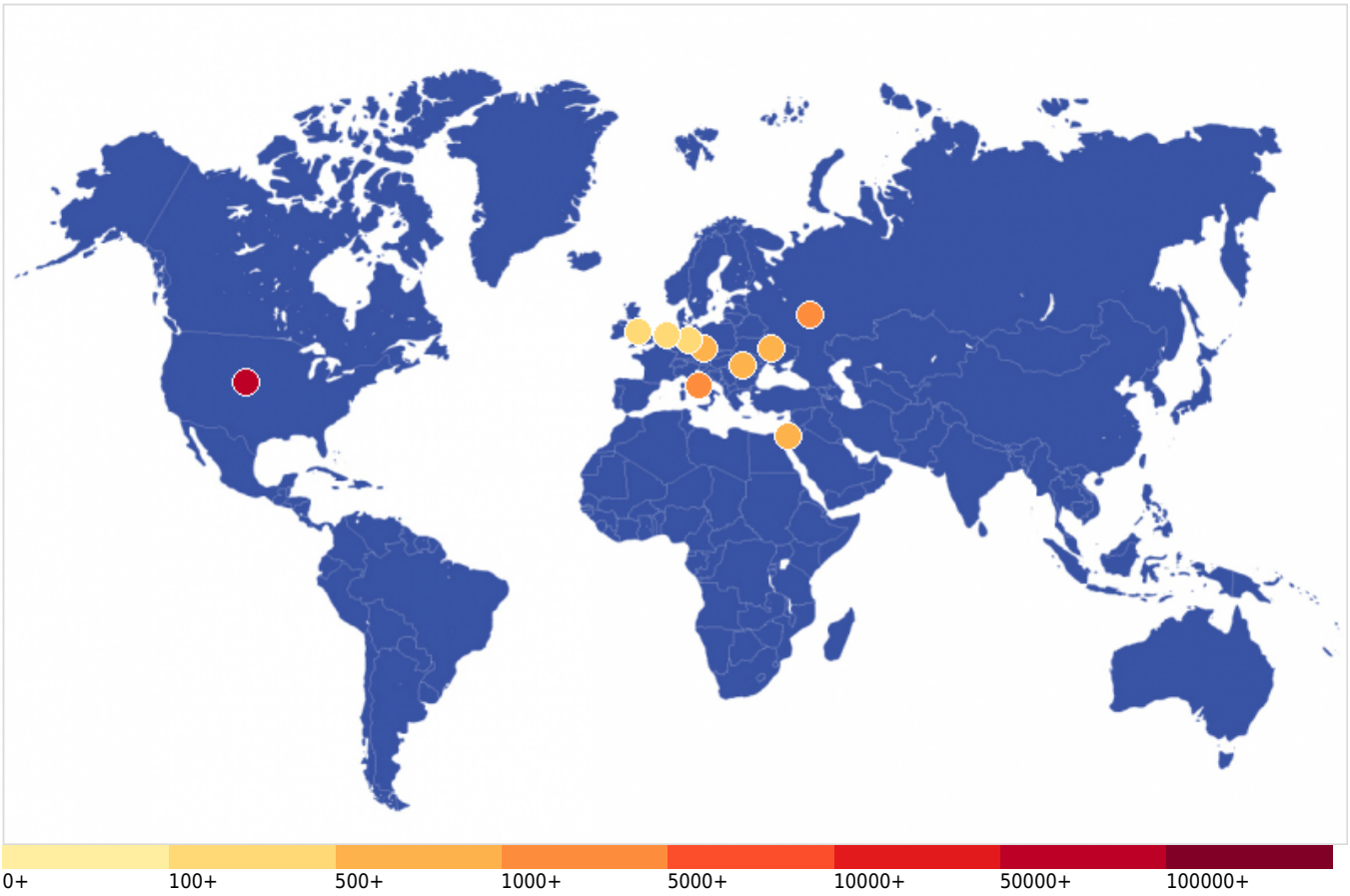
23

The analysis performed on 72 hosts within a specified address range showed that none of the hosts are vulnerable, as indicated by the detailed severity categorization in the accompanying table. During this assessment period, the findings highlighted a total absence of vulnerabilities across all severity levels: 23 critical, 35 high-risk, 273 medium-risk, and 52 low-risk vulnerabilities were recorded. Despite the absence of identified vulnerabilities, your organization's vulnerability index stands at 32%.

THREATS

Critical Attacks Per Country In Past Week

GLESEC 04/02/2024



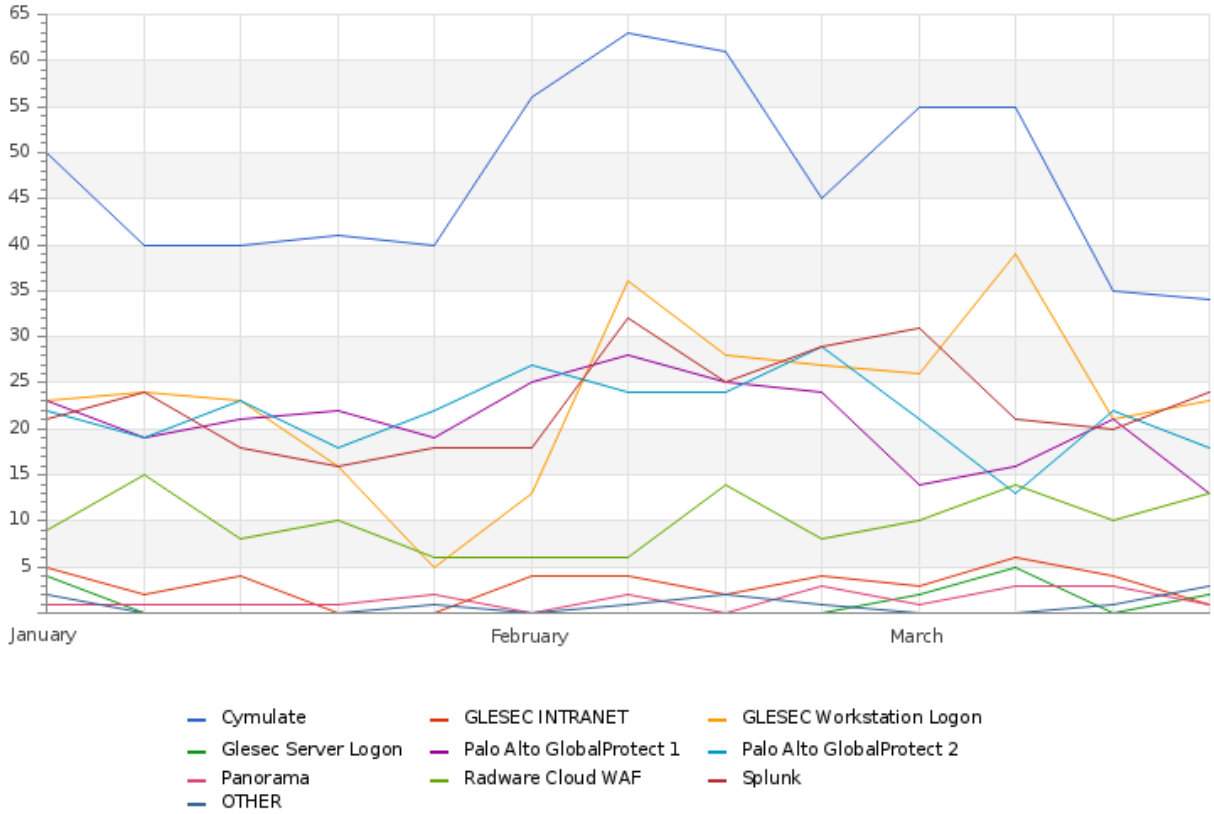
United States - 55744
Israel - 635
United Kingdom - 261
Italy - 2072
Czechia - 631
Netherlands - 250
Russia - 1263
Romania - 548
Ukraine - 678
Germany - 272

This graph illustrates the cyber attack distribution across countries, with the United States leading significantly at 55,744 attacks. The Italy comes next with 2072 attacks, followed by Russia with 1263. Lower attack numbers are reported in China, Bulgaria, Ukraine, Russia, the Netherlands, Mexico, and India. The data emphasizes the importance of concentrating cybersecurity efforts on threats emanating from the U.S., while still keeping a watchful eye on global cybersecurity challenges.

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

GLESEC 04/02/2024

Total Number of Successful MFA authentications per application

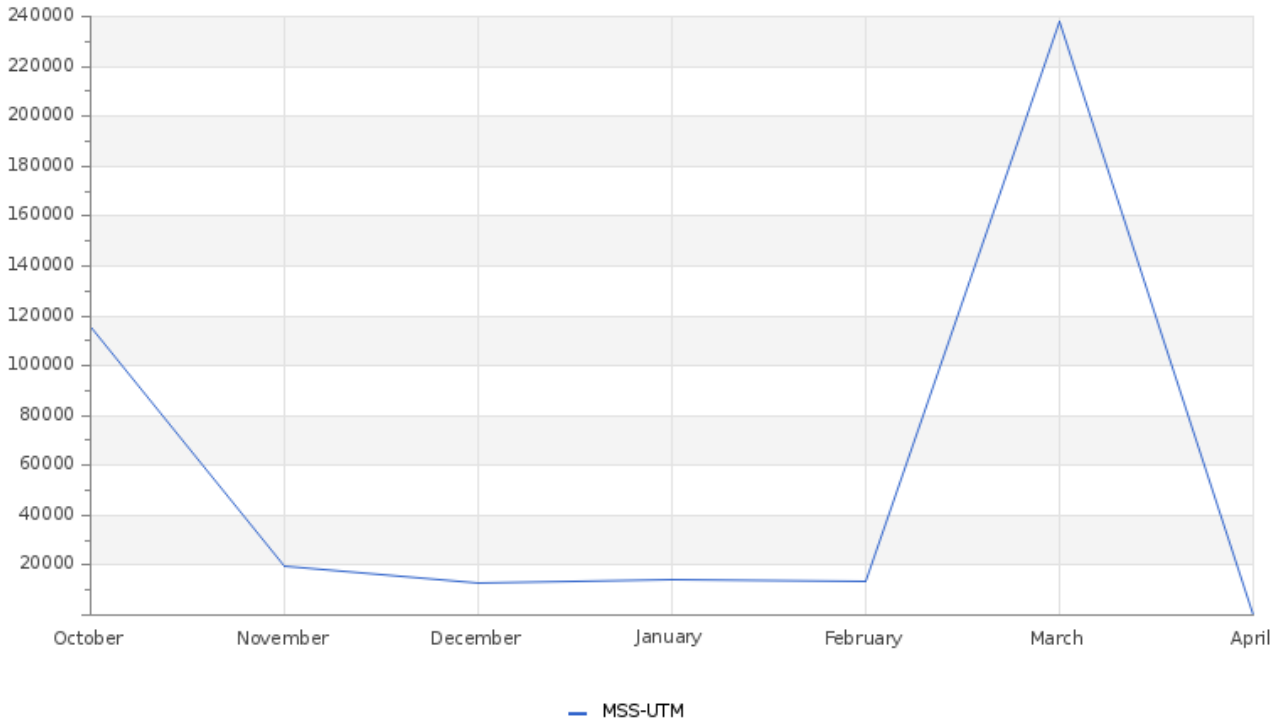


The chart clearly demonstrates the beneficial impact of the security measures that were implemented. There's a noticeable decline in the total number of attacks compared to the previous month, alongside a rise in the number of attacks that were successfully repelled. This trend indicates that the security enhancements have not only reduced the overall threat level but have also significantly improved the system's ability to prevent potential cyber threats from succeeding.

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

GLESEC 04/02/2024

Total Attacks Successfully Blocked Per Service

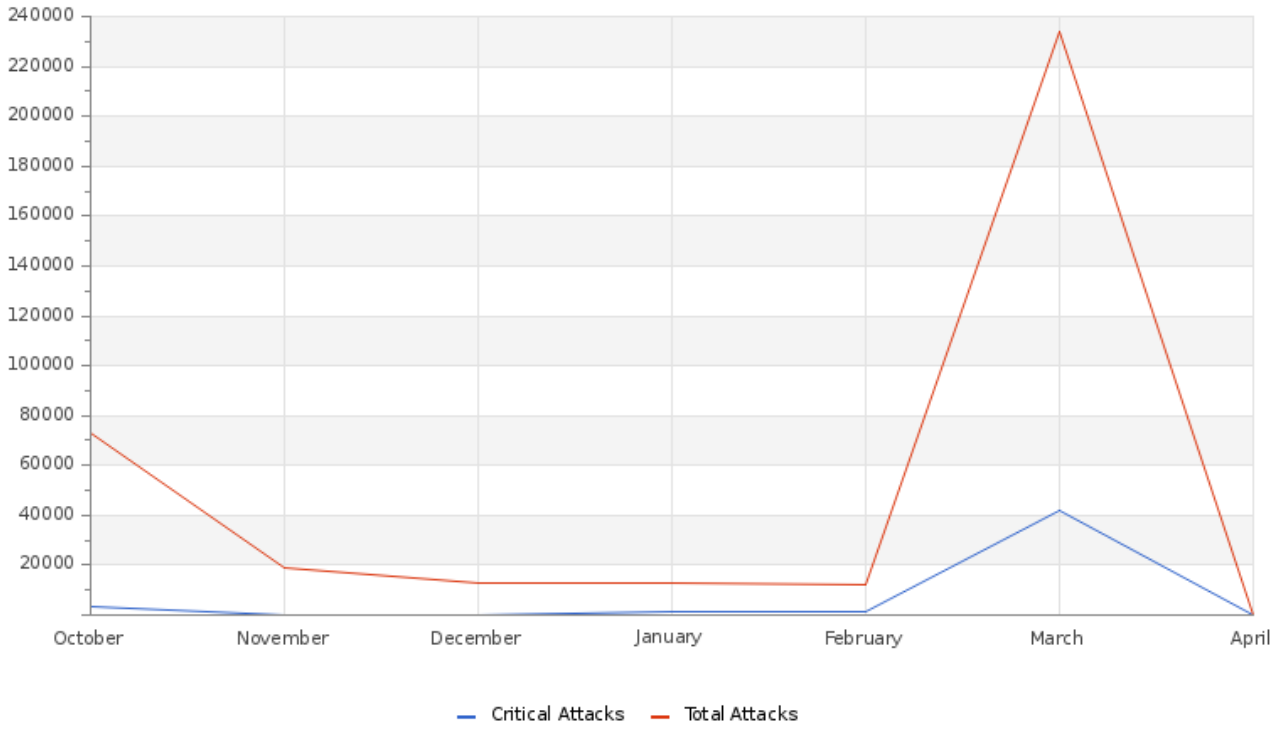


The chart showcases positive security outcomes, highlighting an increase in successfully neutralized attacks. It reflects the effectiveness of proactive measures in guarding against emerging threats, such as DDoS attacks, IoT botnets, sophisticated phishing techniques, malware intrusions, zero-day vulnerabilities, and intricate DNS spoofing strategies.

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

GLESEC 04/02/2024

Attacks Successfully Blocked by Severity



The chart vividly illustrates the positive impact of enhanced security measures through a detailed breakdown by severity of neutralized attacks. This distinction allows for a clear view of how well the security infrastructure is performing against threats of varying levels of danger. By categorizing the thwarted attacks as critical, high, medium, or low severity, the data provides insights into the robustness of the defensive strategies employed. It reveals not only the capability to manage the most severe threats but also the thoroughness in addressing lesser risks, ensuring comprehensive protection.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	9	1
Critical Device Outages	0	0

The devices affected by outages witnessed rapid recovery, with their functionality being reinstated within seconds. These incidents were mainly due to false positives, stemming from brief disconnections. This swift return to normal operations highlights the efficiency of the system's response mechanisms to temporary disruptions, ensuring minimal impact on overall performance and reliability.

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

GLESEC 04/02/2024

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.

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
26,702	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 #
Change in Baseline Systems Discovered	1
BAS Immediate Threat	53
BAS DLP	5
BAS Endpoint Security	2
BAS Web Security	17
Monitoring Event for SPLUNK CLOUD	3
Change in Systems Performance	2
BAS WAF	3
FW Alerts	2

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.**

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