GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

GLESEC

March 12, 2024

GLESEC 03/12/2024

TLP AMBER CISO

EXECUTIVE REPORT

This report corresponds to February 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

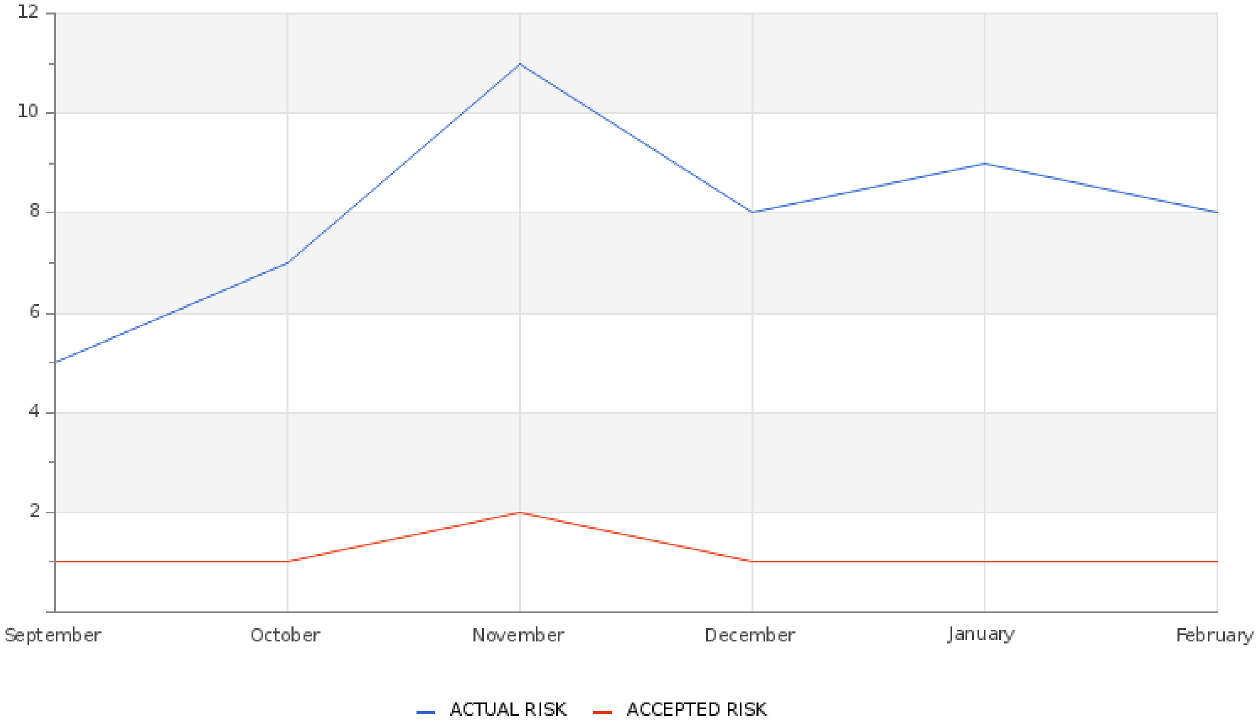
The purpose of this document is to report on the “state” of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed.

RISK

Actual Risk	Accepted Risk	Confidence
8%	1%	High

Accepted & Actual Risk

GLESEC 03/12/2024



Throughout this month, there has been a marked escalation in risk levels, with the current risk now evaluated at 8%, contrasted against an accepted risk of 0%. This indicates a noteworthy increase from last month's data, which documented the actual risk at 9% and the accepted risk at 1%.

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

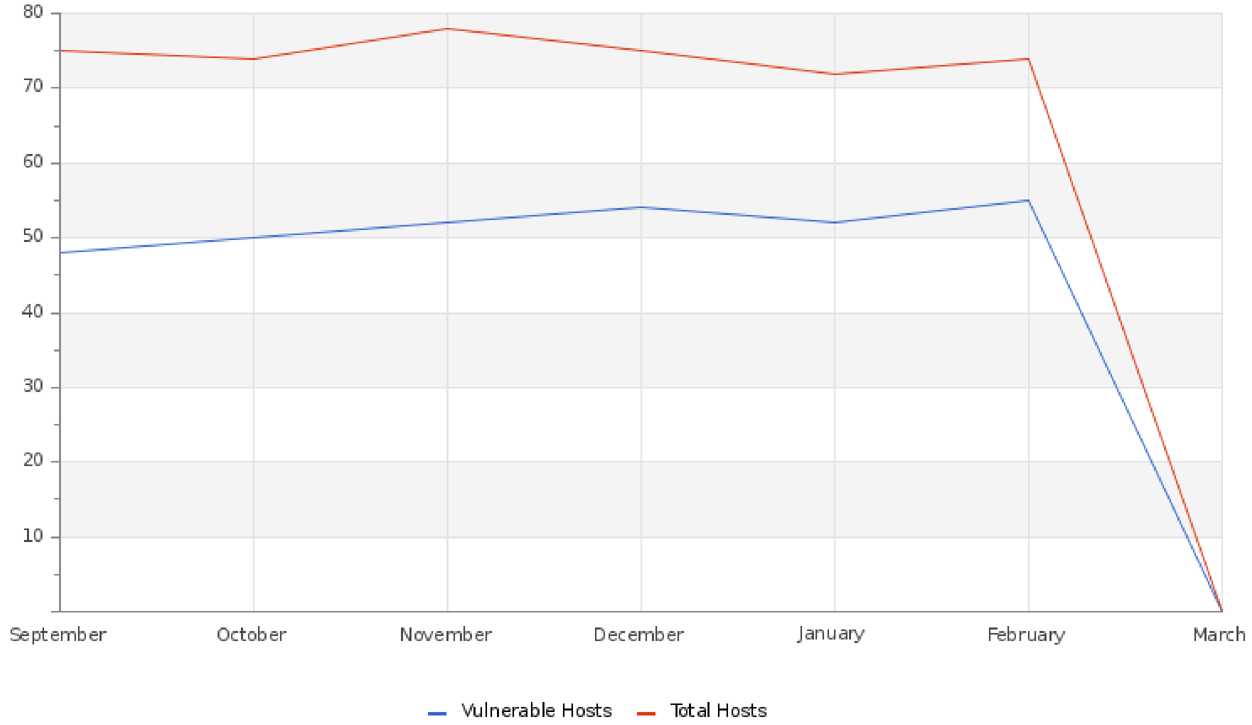
	Current Month	Previous Month
Actual Risk	8	9
Accepted Risk	0	1

The actual risk has risen by 1 percentage point compared to the previous month, while the accepted risk has decreased by 1 percentage point in the same period. These fluctuations within the cybersecurity landscape underscore the dynamic nature of our environment, emphasizing the critical importance of continuous vigilance and adaptability in response to the evolving challenges in information security.

VULNERABILITY

GLESEC 03/12/2024

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, hinting at possible breaches in the security perimeter. Noteworthy among the high-risk vulnerabilities are several iterations of Adobe Acrobat, each with distinct vulnerabilities. These are further elucidated in reports such as KB5034768, detailing a Security Update for Windows 10 version 1809 and Windows Server 2019 (February 2024), as well as the identification of a Heap Buffer Overflow vulnerability in libcurl versions 7.69 to below 8.4.0, and a Security Update for Microsoft Visual Studio Code (November 2023). Swift action in addressing these vulnerabilities is imperative to fortify the security landscape.

GLESEC 03/12/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	72	72
Hosts Discovered	0	65
Vulnerable Hosts	0	49
Critical Vulnerabilities Count	0	20
High Vulnerabilities Count	0	37
Medium Vulnerabilities Count	0	253
Low Vulnerabilities Count	0	45
Phishing Score	0	0
Email Gateway Score	8	8
Web Application Firewall Score	25	25
Web Gateway Score	64	63
Endpoint Score	37	37
Hopper Score	33	33
DLP Score	77	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 37, a Hopper Score of 33, and a DLP Score of 77. These scores show the areas of strength and those that require greater attention in our security infrastructure.

Vulnerability Metric

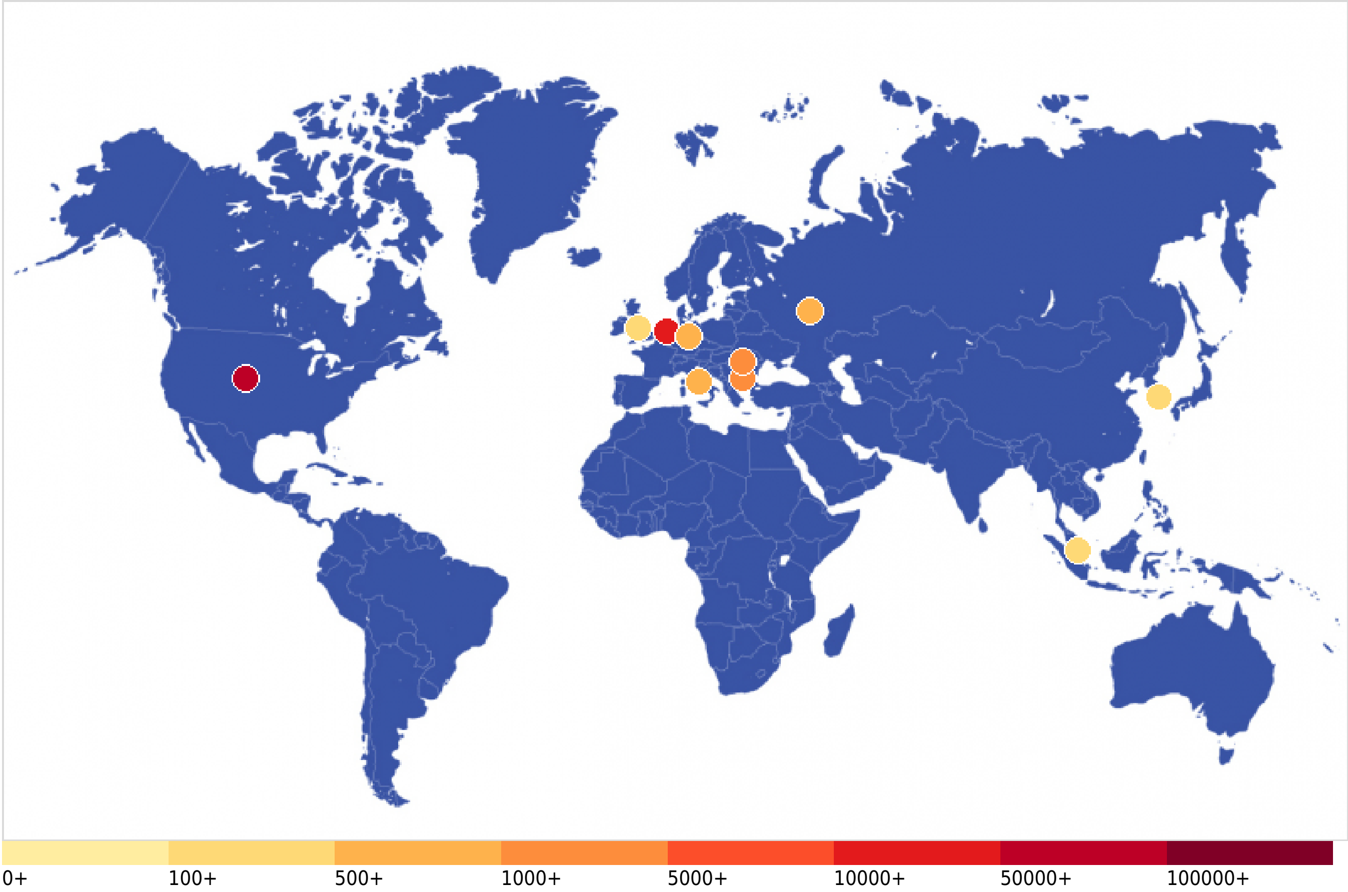
32

An analysis was conducted on 72 hosts based on their address range, revealing that 0 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, 0 medium-risk, and 0 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 32%.

THREATS

Critical Attacks Per Country In Past Week

GLESEC 03/12/2024

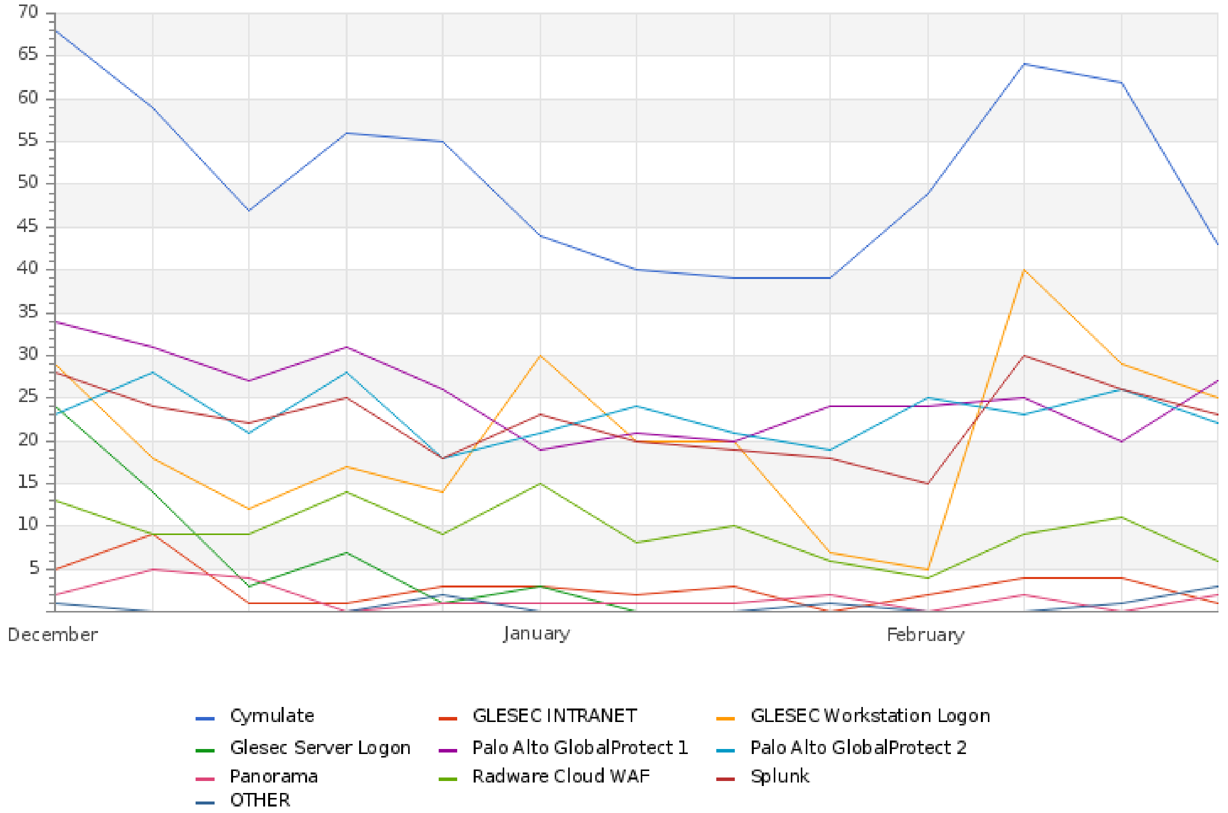


United States - 54377
Netherlands - 15309
Bulgaria - 2949
Romania - 2619
Germany - 706
Italy - 698
Russia - 668
Singapore - 439
United Kingdom - 430
South Korea - 407

The graph presents a breakdown of cyber attacks by country, emphasizing the United States' leading position with 54,377 attacks. The Netherlands ranks second with 15,309 attacks, followed by Bulgaria with 2,949. Lower incidence rates are reported in countries such as Romania, Germany, Ukraine, Italy, Russia, Singapore, and United Kingdom. This distribution signals a crucial need for prioritizing cybersecurity measures against threats emanating predominantly from the U.S., without neglecting the importance of a worldwide alertness.

GLESEC 03/12/2024

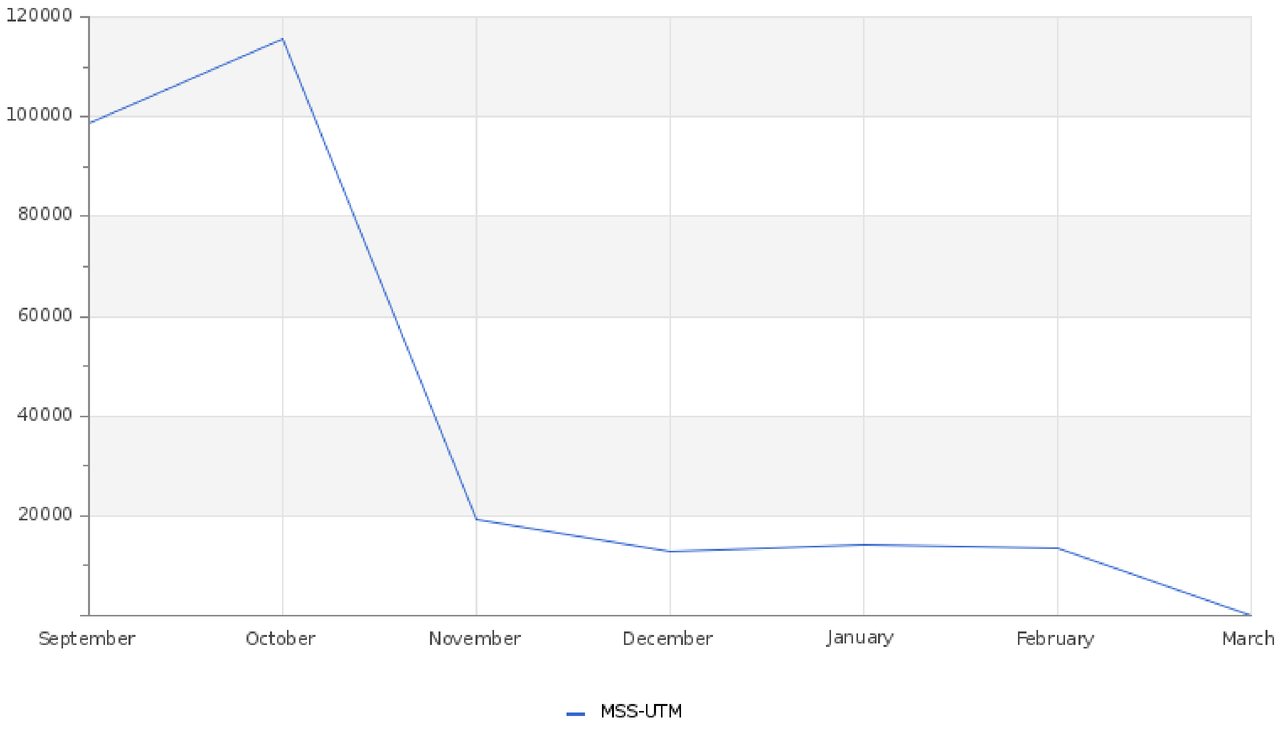
Total Number of Successful MFA authentications per application



The graph highlights a noticeable trend in authentication practices, showcasing workstations and Cymulate as the primary applications utilized for logins. This pattern accentuates the crucial role these two facets occupy in everyday operations, potentially pinpointing vital points of interaction or significant areas within the organizational framework.

GLESEC 03/12/2024

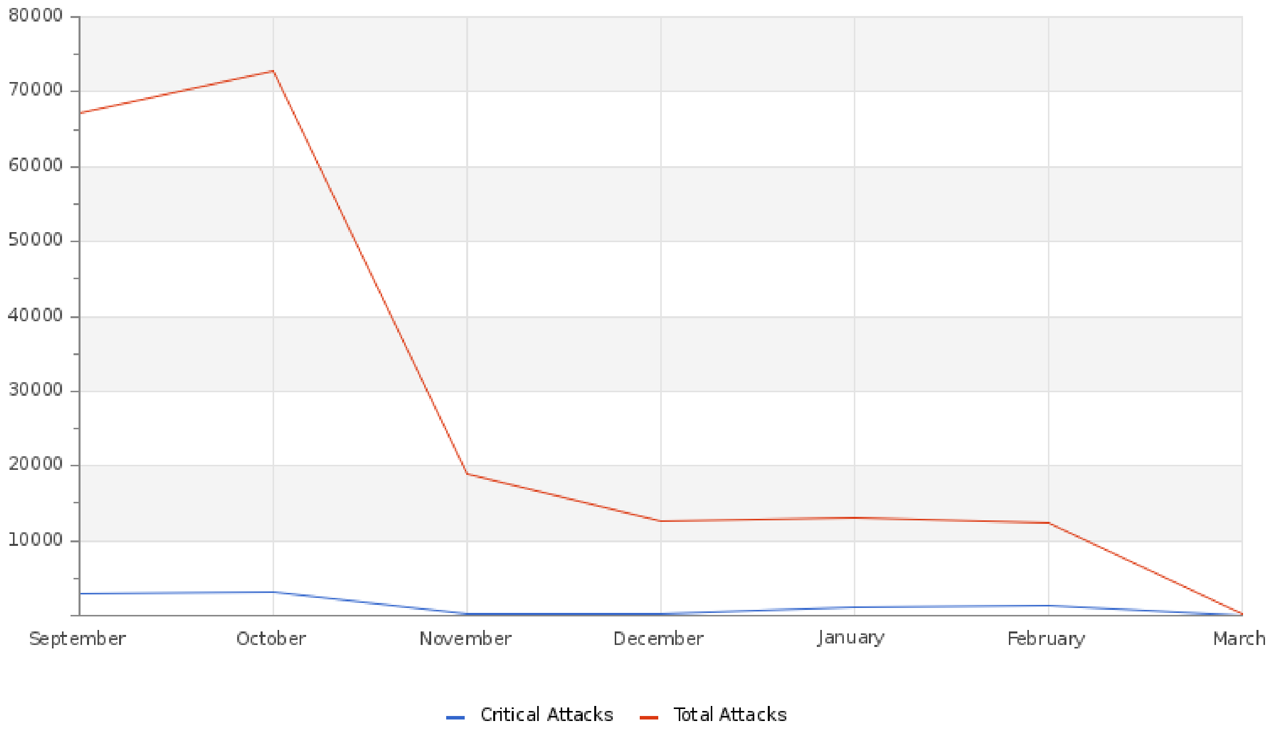
Total Attacks Successfully Blocked Per Service



The chart clearly demonstrates the beneficial impact of the security measures that have been put into place. Relative to the prior month, there's a noticeable decrease in the overall count of attacks, alongside an uptick in the number of attacks that have been effectively repelled.

GLESEC 03/12/2024

Attacks Successfully Blocked by Severity



The chart showcases positive security trends, highlighting an increase in the number of attacks that have been successfully neutralized. This proactive stance enhances protection against emerging threats, such as Distributed Denial of Service (DDoS) attacks, Internet of Things (IoT) botnets, sophisticated phishing techniques, malware incursions, zero-day vulnerabilities, and intricate Domain Name System (DNS) spoofing strategies.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	8	1
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.

GLESEC 03/12/2024

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
26,555	0	0	22,544

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 #
BAS Immediate Threat	59
BAS DLP	5
BAS Endpoint Security	8
BAS Web Security	24
EDR Alerts	169
Monitoring Event for SPLUNK CLOUD	2
Change in High or Critical Vulnerabilities	2
Immediate Threat System Vulnerable and Remediation by Patch Management	1
Change in Baseline Systems Discovered	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 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.**

GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on our services and security solutions.