TLP:AMBER

CISO EXECUTIVE REPORT

BLADEX

May 21, 2024

BLADEX 05/21/2024

TLP AMBER CISO
EXECUTIVE REPORT

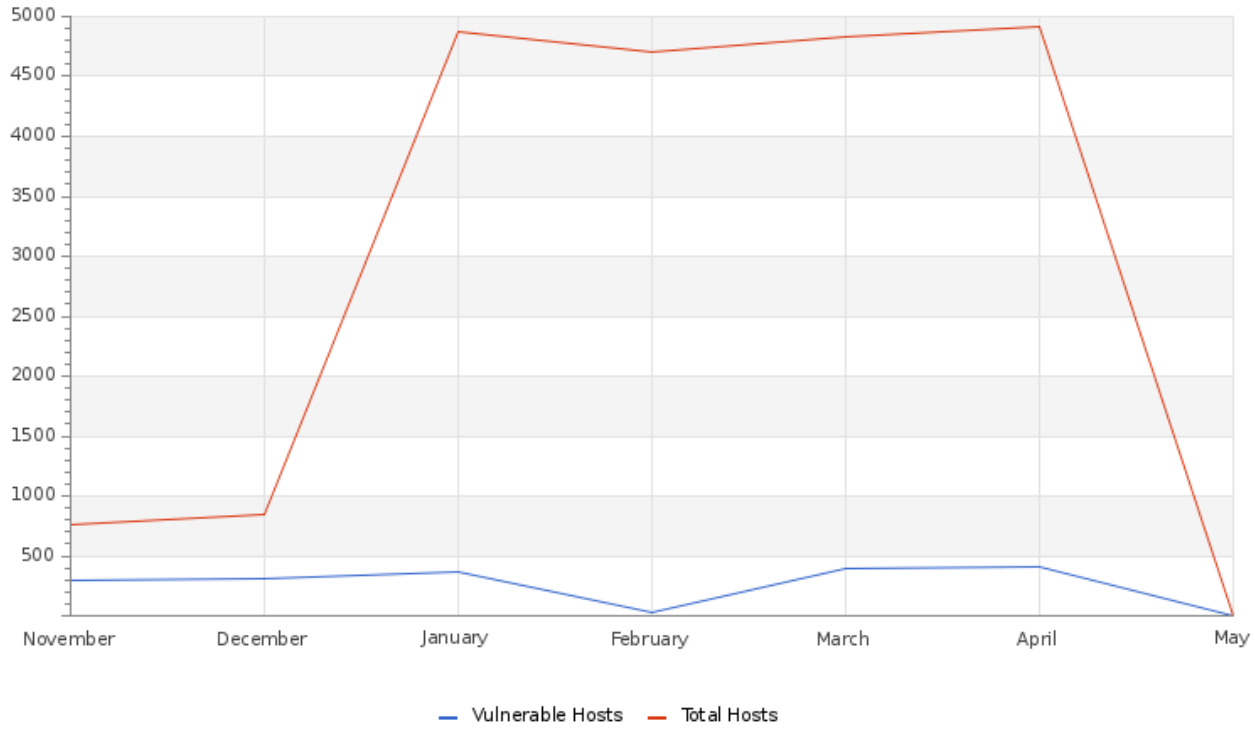
Este informe corresponde "EDIT MONTH" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, Amenazas, Activos, Cumplimiento, Validación de Ciberseguridad y Acceso.

SOBRE ESTE INFORME

El propósito de este documento es informar sobre el estado" de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months



The graph indicates a steady increase in the number of Total Hosts and Vulnerable Hosts. We are working together with the customer to resolve any issues identified. For more details, please visit our customer platform at [Skywatch Glesec](https://skywatch.glesec.com), in the C&RU section, where you will find detailed information about this event and the updates made. If you have any questions, please do not hesitate to contact the GLESEC GOC or Professional Services team.

BLADEX 05/21/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	925	925
Hosts Discovered	4446	4636
Vulnerable Hosts	355	34
Critical Vulnerabilities Count	146	0
High Vulnerabilities Count	570	20
Medium Vulnerabilities Count	2022	87
Low Vulnerabilities Count	332	45

The table presents a vulnerability comparison for the last two months. In the last month, an increase in the number of vulnerable hosts and in the severity of these vulnerabilities is observed. Our team has worked closely with the customer to verify the changes observed in the Total Hosts and Vulnerable Hosts. In the MSS-BAS service, there has also been a slight increase in the values. We recommend reviewing the documentation available on the Skywatch platform on these services to strengthen your security against new threats.

Vulnerability Metric

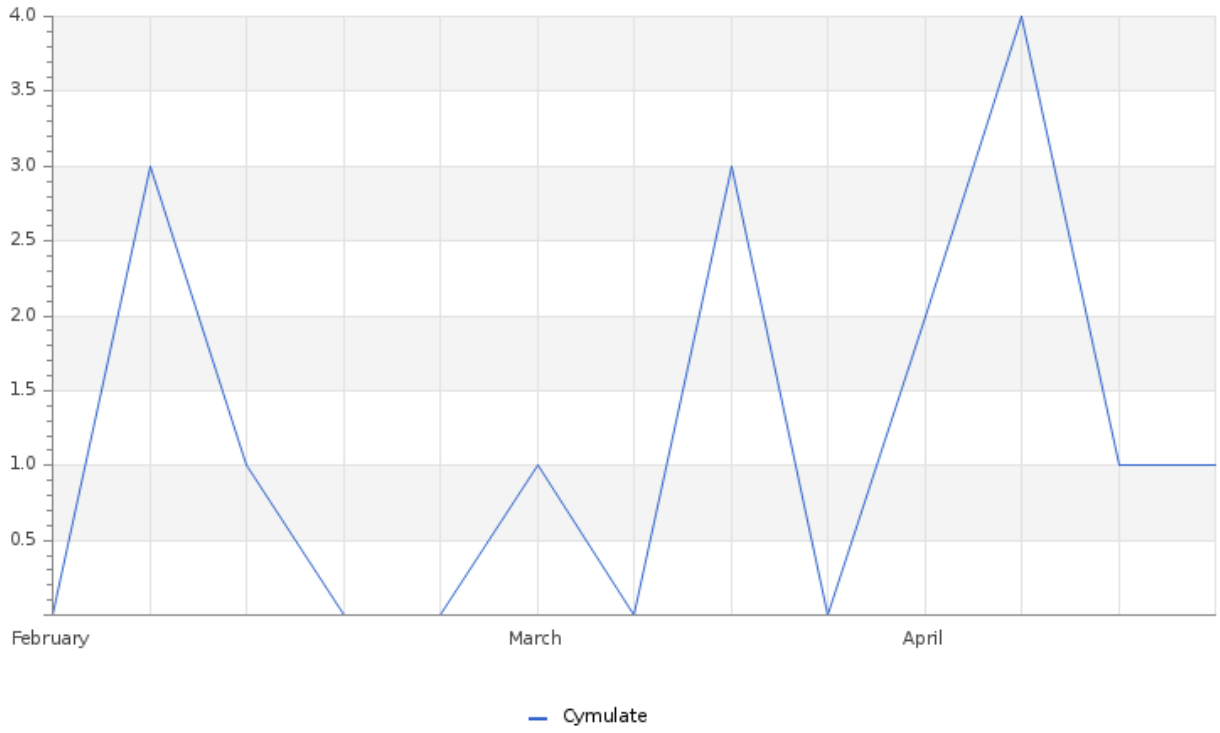
1

An analysis of 925 hosts based on their address range revealed that 355 hosts are vulnerable. These vulnerabilities are categorized by severity, as shown in the accompanying table. During this timeframe, we recorded 146 critical vulnerabilities, 570 high-risk, 2022 medium-risk, and 332 low-risk vulnerabilities. Based on these findings, your organization's vulnerability index is currently at 1%.

THREATS

BLADEX 05/21/2024

Total Number of Successful MFA authentications per application



The graph allows us to visualize the client's activity on the different platforms to which it has access. In particular, it shows the activity on our Cymulate platform, which provides information related to our MSS-BAS service. This platform allows us to validate cybersecurity controls and provides ongoing, detailed assessments on the various cases related to this service. On Skywatch, you can find detailed documentation on cases, incidents, reports and other useful resources to strengthen your company's security.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	4	1
Critical Device Outages	0	0

During the month, our MSS-CSM service reported alerts related to CPU performance and connection anomalies, which could be due to network congestion issues. Our team documented these events and an email was sent notifying the situation.

Histogram of Total and Critical Device Outages

BLADEX 05/21/2024

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
0	0	0	0

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	50
BAS Endpoint Security	6
BAS Web Security	6
BAS WAF	7
Change in High or Critical Vulnerabilities	36
Immediate Threat System Vulnerable and Remediation by Patch Management	2

For the MSS-BAS service, detailed documentations have been made that allow you to know the security status of your company. Cases have been opened that should be taken into account, as they have managed to circumvent more than 50% of your security countermeasures.

As for the MSS-VME service, we continue to work together to address events related to the significant increase in the total number of hosts. It is recommended to review these cases and apply the corresponding mitigations to safeguard your company's security.

For more information, you can access our customer platform at [Skywatch Glesec](https://skywatch.glesec.com) in the C&RU section.

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