TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

May 26, 2024

Organo Judicial 05/26/2024

TLP AMBER CISO
EXECUTIVE REPORT

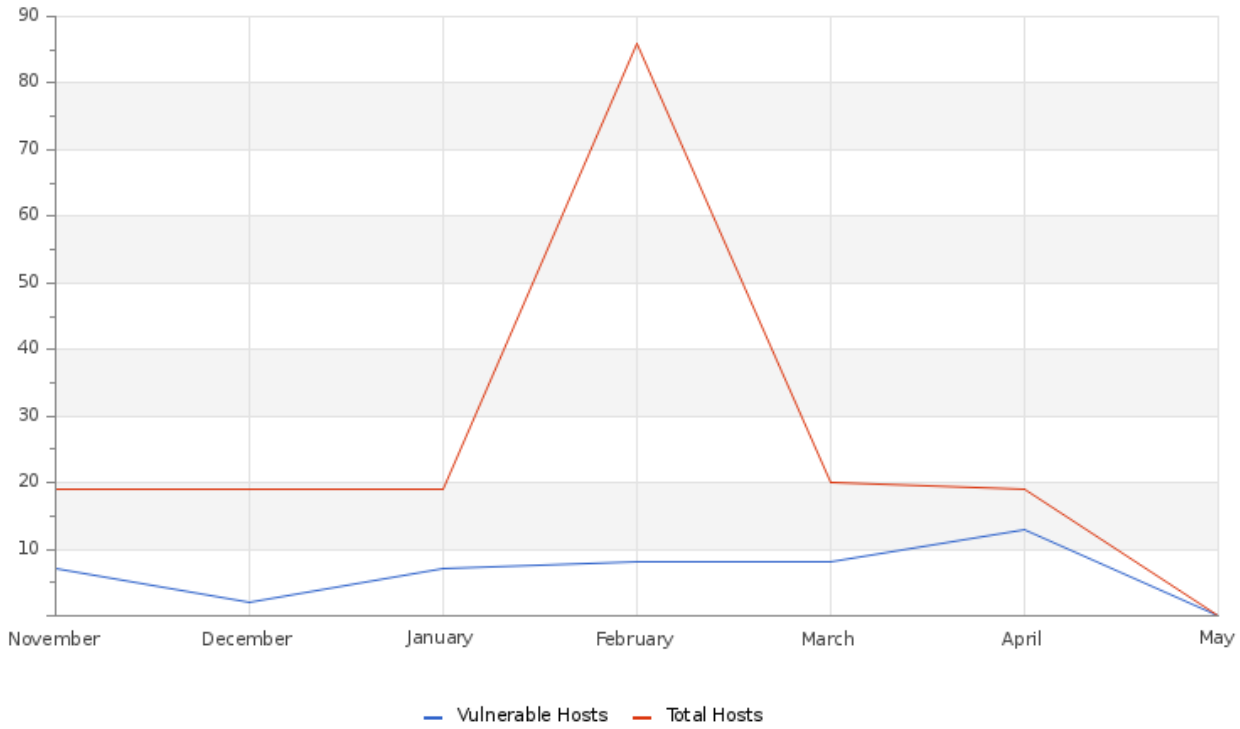
Este informe corresponde "Abril 2024" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, Amenazas, Activos, Cumplimiento, Validación de Ciberseguridad y Acceso.

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.

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months



Este mes, la cantidad de hosts descubiertos se ha mantenido estable; sin embargo, la cantidad de hosts vulnerables sigue siendo la misma. Estas vulnerabilidades han sido documentadas y corresponden a versiones obsoletas de servidores y protocolos en desuso.

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

Organo Judicial 05/26/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	45	45
Hosts Discovered	17	17
Vulnerable Hosts	8	2
Critical Vulnerabilities Count	0	0
High Vulnerabilities Count	0	0
Medium Vulnerabilities Count	10	4
Low Vulnerabilities Count	3	0
Phishing Score	0	-1
Email Gateway Score	1	0
Web Gateway Score	56	55
Endpoint Score	5	4
Hopper Score	0	-1

La tabla muestra los resultados obtenidos en las pruebas realizadas en comparación con el mes anterior. Este mes se destaca una disminución en la cantidad de hosts descubiertos y el mantenimiento del porcentaje en las pruebas del servicio MSS-BAS-WEB. Recomendamos bloquear las extensiones no utilizadas para reducir significativamente el puntaje en estas evaluaciones. Los resultados de las pruebas del servicio MSS-BAS han sido documentados y pueden consultarse en la plataforma SKYWATCH.

Vulnerability Metric

6

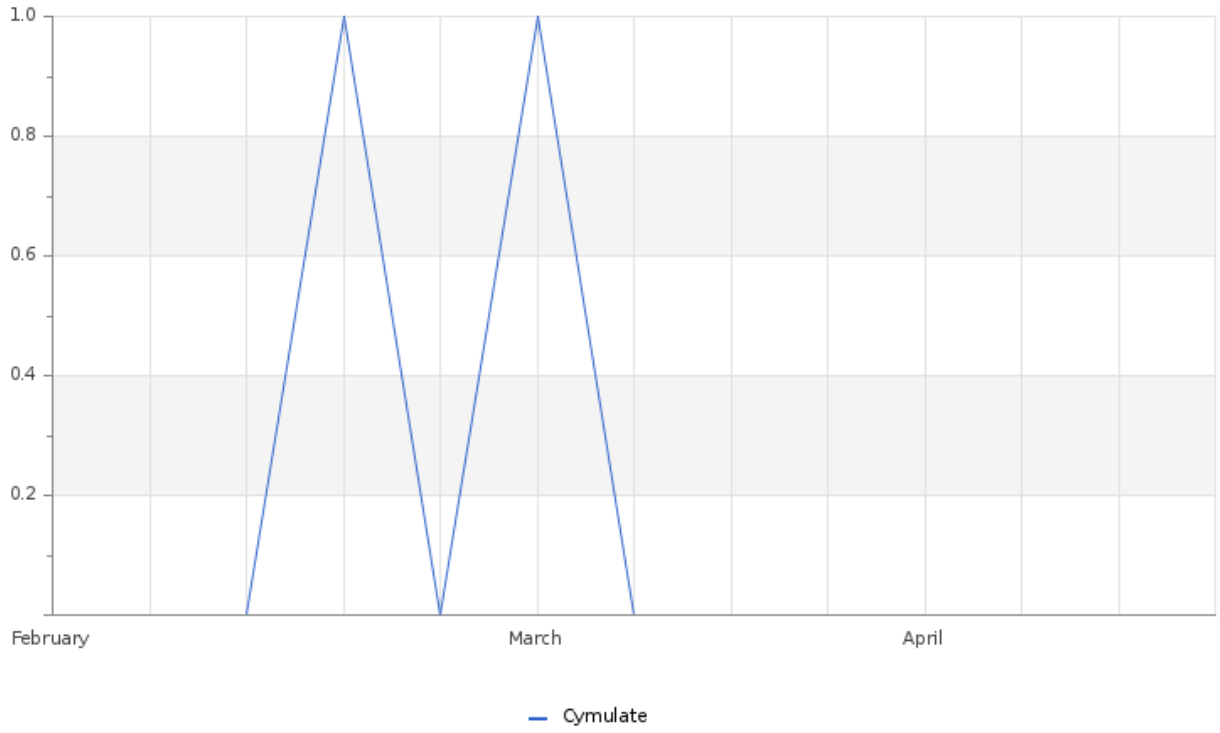
El análisis realizado sobre 45 hosts dentro de un rango de direcciones especificado mostró una disminución en los niveles de vulnerabilidad, según la categorización detallada de severidad en la tabla adjunta. Durante este período de evaluación, los hallazgos destaca una ausencia total de vulnerabilidades críticas y de alto riesgo: se registraron 0 críticas, 0 de alto riesgo, 10 de riesgo medio y 3 de bajo riesgo. A pesar del reducido número de vulnerabilidades identificadas, el índice de vulnerabilidad de su organización se sitúa en el 6%.

THREATS

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

Organo Judicial 05/26/2024

Total Number of Successful MFA authentications per application

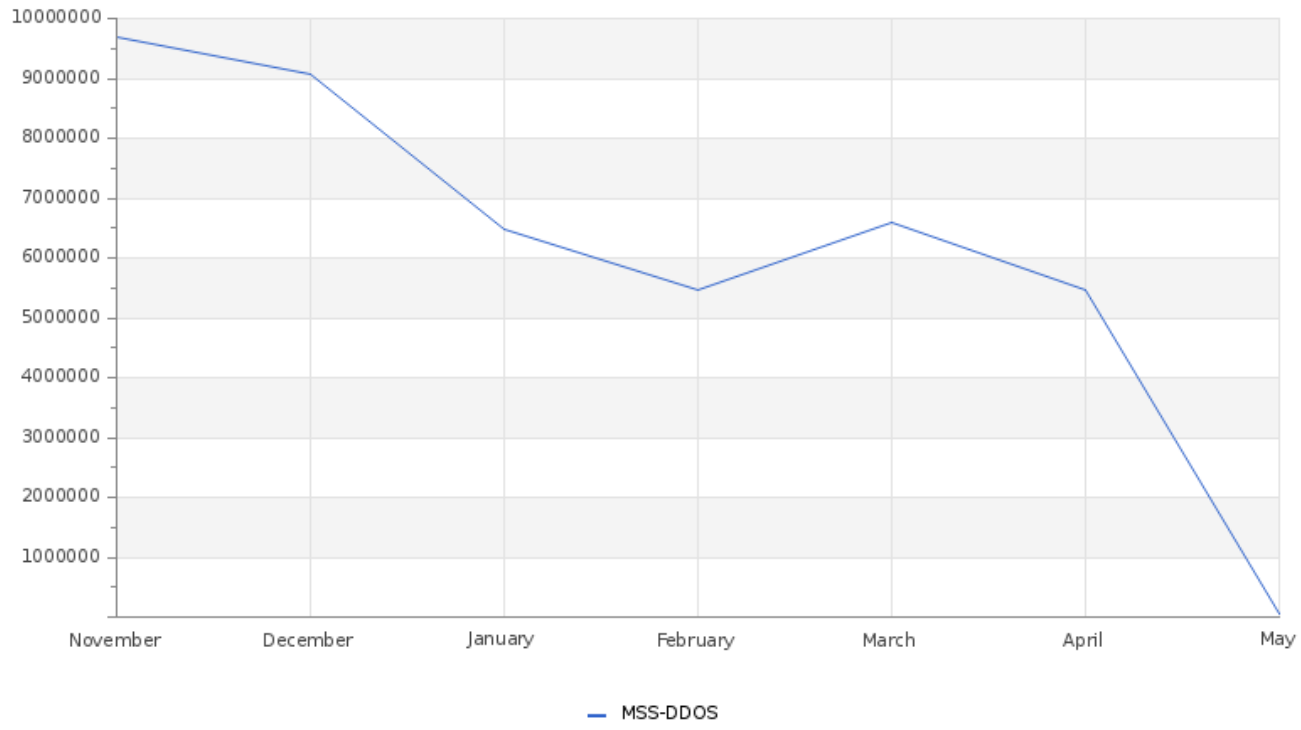


La gráfica muestra la actividad de los usuarios en las diferentes plataformas. Se observa que el uso de la plataforma Cymulate ha permanecido estable.

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

Organo Judicial 05/26/2024

Total Attacks Successfully Blocked Per Service

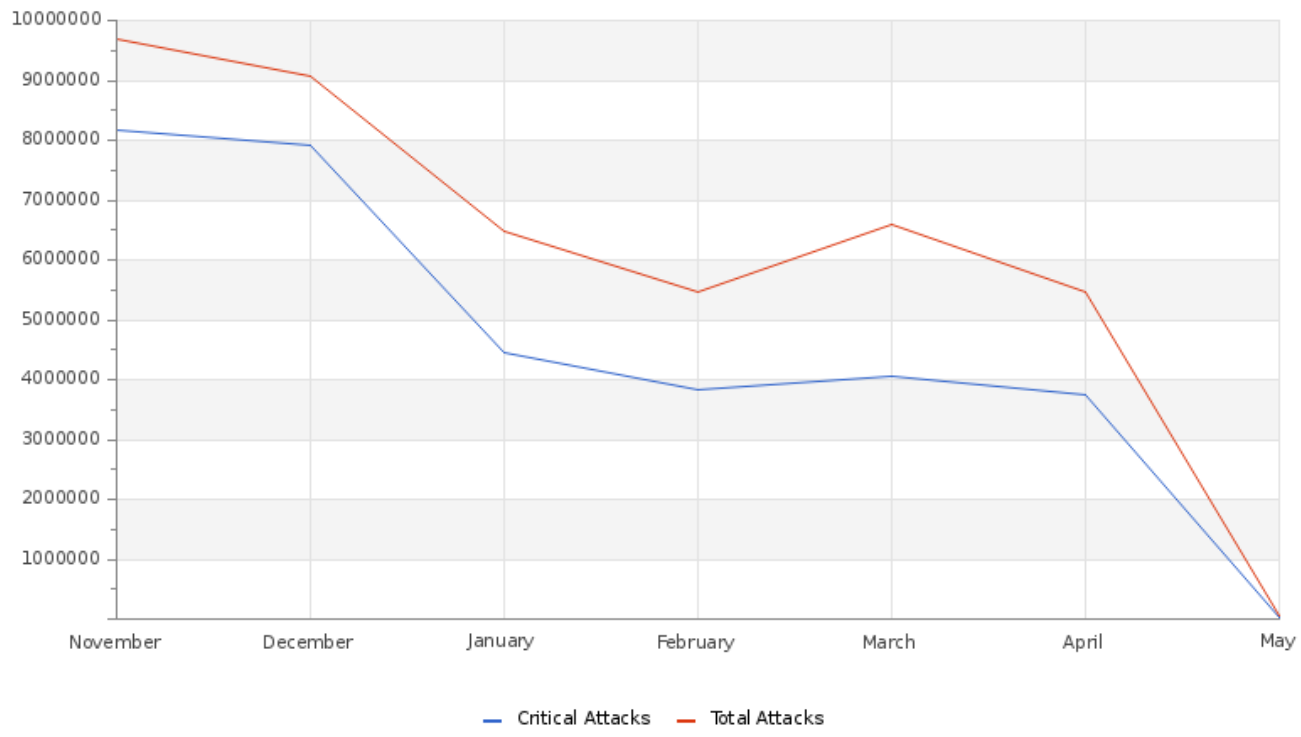


Durante el mes se registraron un total de 5,564,225 ataques dirigidos a múltiples sistemas de su organización. Se identificaron numerosos ataques persistentes provenientes de direcciones IP catalogadas como maliciosas, con múltiples reportes de ataques contra otros sistemas.

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

Organo Judicial 05/26/2024

Attacks Successfully Blocked by Severity



La gráfica muestra la actividad de los ataques dirigidos a múltiples sistemas de su organización durante el mes. Estos ataques fueron catalogados como críticos, pero sus sistemas lograron bloquear con éxito todos ellos. La mayoría de los ataques se clasificaron como ErtFeed y GeoFeed, gracias a las configuraciones avanzadas en los equipos DefensePro, implementadas para fortalecer la seguridad.

System Availability and Performance in current & previous month

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

Durante el mes, se reportaron caídas en el sitio web y anomalías en el estado de otros sistemas. Estos eventos fueron notificados y documentados adecuadamente.

Histogram of Total and Critical Device Outages

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

Organo Judicial 05/26/2024

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	60
BAS Web Security	28
Immediate Threat System Vulnerable and Remediation by Patch Management	4
Change in Critical Perimeter Attacks	1
Change in Systems Performance	1

Durante el mes, se documentaron varios eventos notables relacionados con la seguridad de su organización. El servicio MSS-BAS identificó un total de 58 amenazas inmediatas y 28 eventos relacionados con la seguridad web. Además, se detectaron 4 vulnerabilidades críticas que fueron mitigadas mediante la gestión de parches. Hubo un cambio significativo en los ataques al perímetro crítico y se observó una variación en el rendimiento de los sistemas, con un evento reportado en cada categoría. Estos hallazgos subrayan la importancia de revisar y aplicar las recomendaciones y mitigaciones necesarias para fortalecer la seguridad de su organización. Para obtener más información, puede acceder a nuestra plataforma para clientes en [Skywatch Glesec](https://skywatch.glesec.com) en la sección CR&U.

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