TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

April 05, 2024

Organo Judicial 04/05/2024

TLP AMBER CISO
EXECUTIVE REPORT

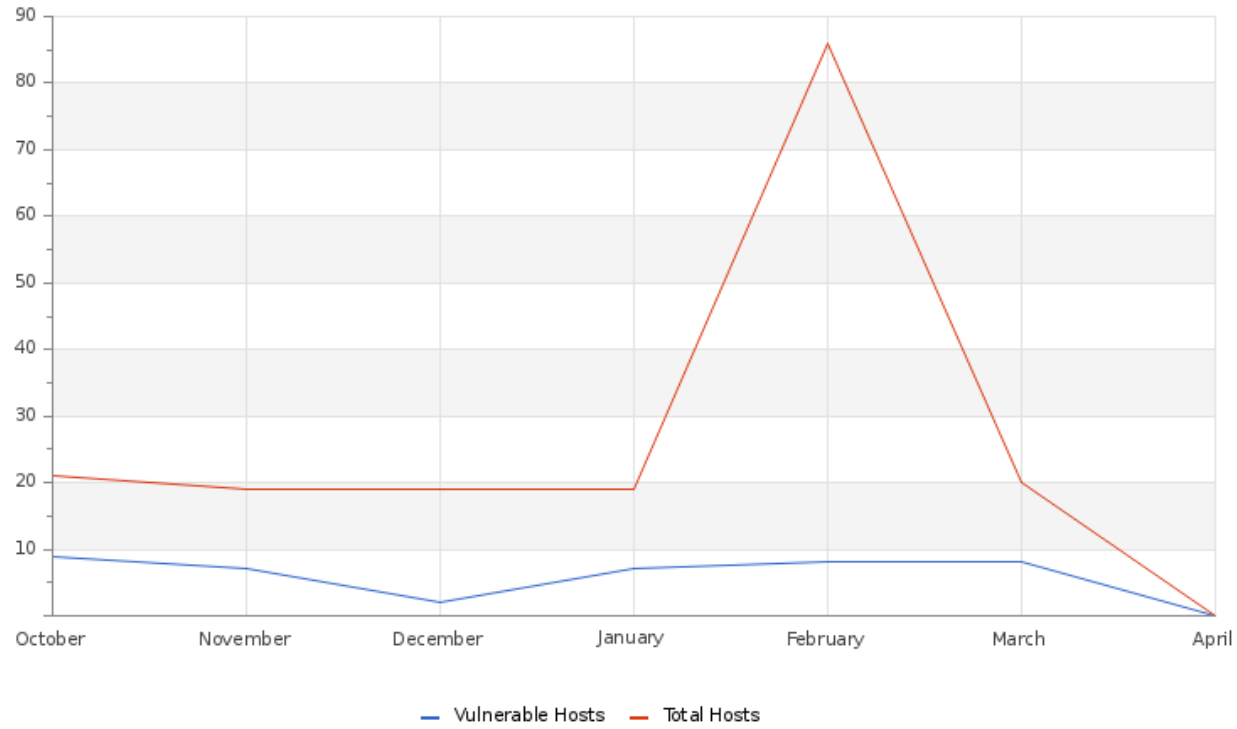
Este informe corresponde a Marzo y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades,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

ABOUT THIS REPORT

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 agregada, correlacionada y analizada.

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months



Para este mes se refleja un disminución significativa en la cantidad de host que han sido descubiertos, sin embargo se mantiene la cantidad de host vulnerables. Estas vulnerabilidades ya han sido documentadas y corresponden a vulnerabilidades de versiones obsoletas de servidores y protocolos en desuso.

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

Organo Judicial 04/05/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	45	45
Hosts Discovered	17	15
Vulnerable Hosts	2	2
Critical Vulnerabilities Count	0	0
High Vulnerabilities Count	0	0
Medium Vulnerabilities Count	4	4
Low Vulnerabilities Count	0	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 que se han obtenido en las pruebas realizadas en comparación la mes anterior. Para este mes destaca la disminución en la cantidad de host descubiertos y el resultado de las pruebas para el servicio MSS-BAS-WEB, el cual ha mantenido su porcentaje. Recomendamos realizar el bloqueo de las extensiones que no se utilizan, esto ayudara a disminuir significativamente el puntaje que se obtiene en estas evaluaciones. Los resultados de las pruebas de servicio MSS-BAS han sido documentadas y pueden ser consultadas accediendo a la plataforma SKYWATCH.

Vulnerability Metric

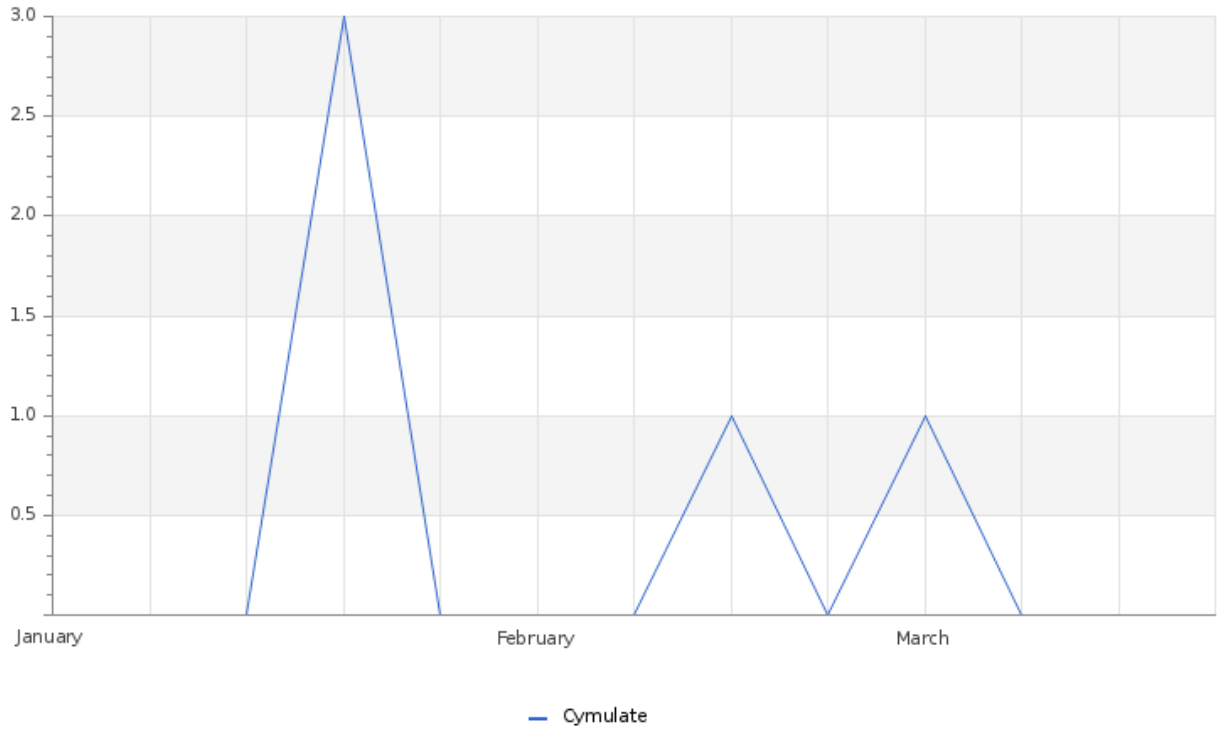
3

Se identificaron vulnerabilidades que se mantiene en sus sistemas, por lo que recomendamos acciones para abordar y mitigar estas vulnerabilidades. Las vulnerabilidades descubiertas, han sido documentadas y puede acceder a través de la sección C&RU de SKYWATCH.

THREATS

Organo Judicial 04/05/2024

Total Number of Successful MFA authentications per application

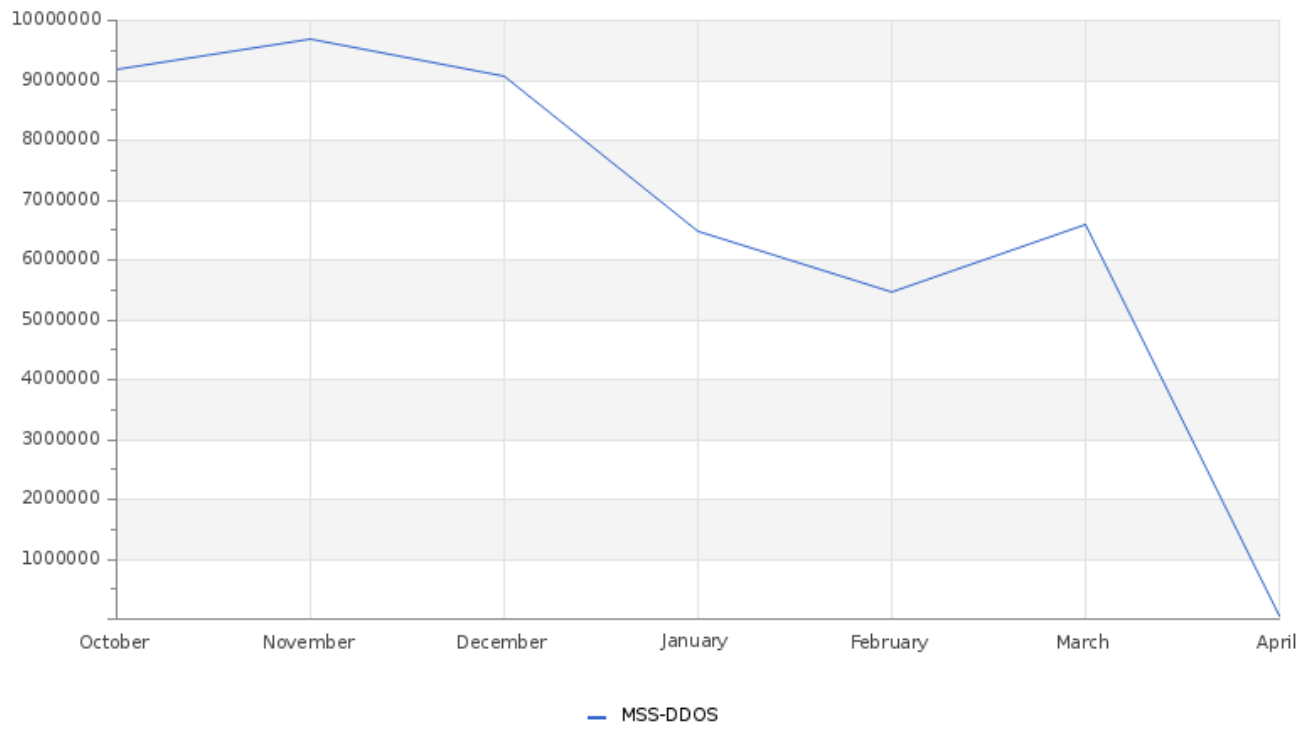


La grafica muestra la actividad de los usuarios en las diferentes plataformas. Se puede observar que el ingreso a la plataforma de Cymulate se mantiene.

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

Organo Judicial 04/05/2024

Total Attacks Successfully Blocked Per Service

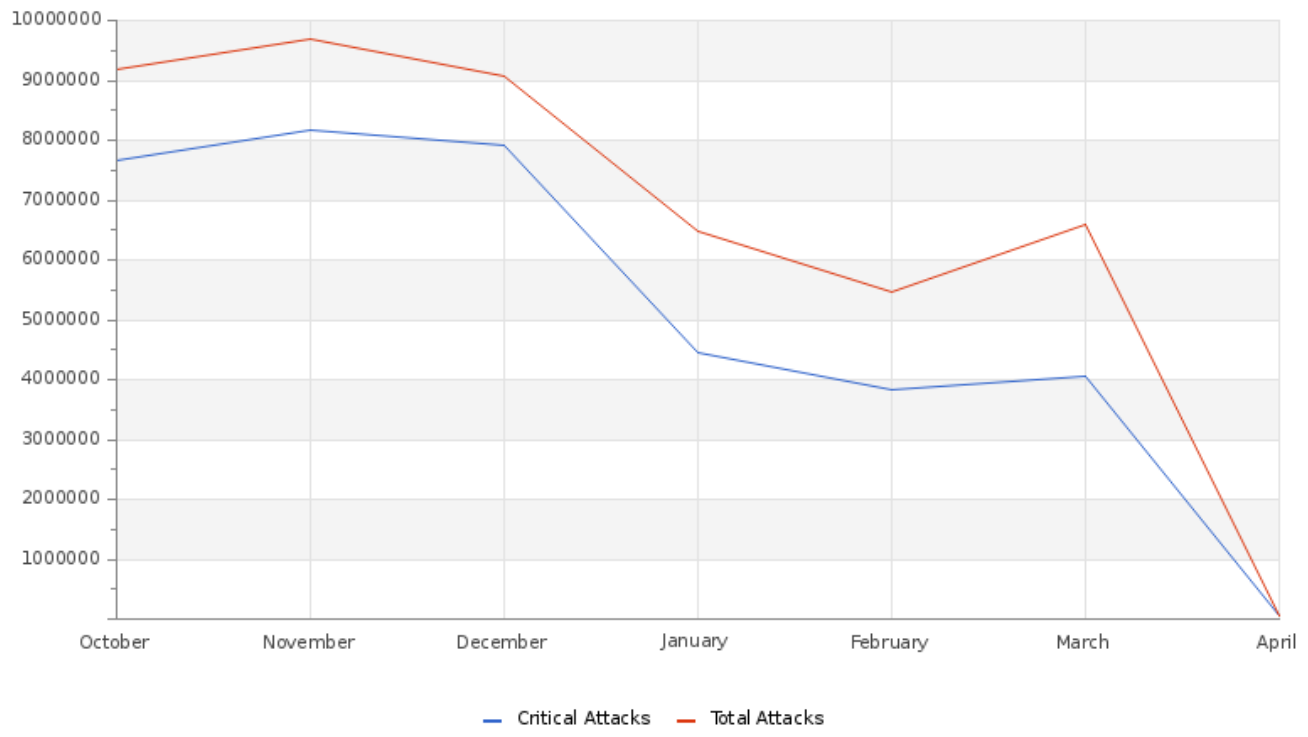


Durante el mes se registraron un total de 6,574,325 ataques, estos tenían como objetivos múltiples sistemas de su organización. Se identificaron múltiples ataques persistentes provenientes de direcciones IP catalogadas como maliciosas y que contaban con múltiples reportes de ataques contra otros sistemas.

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

Organo Judicial 04/05/2024

Attacks Successfully Blocked by Severity



Un total de 4,060,949 fueron catalogados como ataques críticos, sus sistemas lograron bloquear con éxito todos estos ataques. La mayor parte de estos ataques son clasificados como ErtFeed y GeoFeed, estas clasificaciones se deben a que son configuraciones adicionales que se realizan en los equipos DefensePro con el fin de robustecer 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 observadas en los estados del otros sistemas. Estos eventos fueron notificados y documentados respectivamente.

Histogram of Total and Critical Device Outages

Organo Judicial 04/05/2024

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Non Baselined Discovered System	54
Change in Critical Perimeter Attacks	1
BAS Immediate Threat	44
BAS Web Security	9
Change in Systems Performance	1

Se documentaron múltiples casos para el servicio MSS-BAS, la mayor parte de esto casos corresponde al servicio BAS-IMTHREAT, el cual realiza evaluaciones diariamente de amenazas emergentes. Fueron documentados ataques de persistencia observados durante el mes y se actualizo el estado de las vulnerabilidades persistentes en sus sistemas. Recomendamos llevar a cabo una revisión de cada uno de estos casos y aplicar las recomendaciones y mitigaciones correspondientes. Para más información puede acceder a nuestra plataforma para clientes 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