TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

June 04, 2024

Organo Judicial 06/04/2024

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde a "Mayo 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

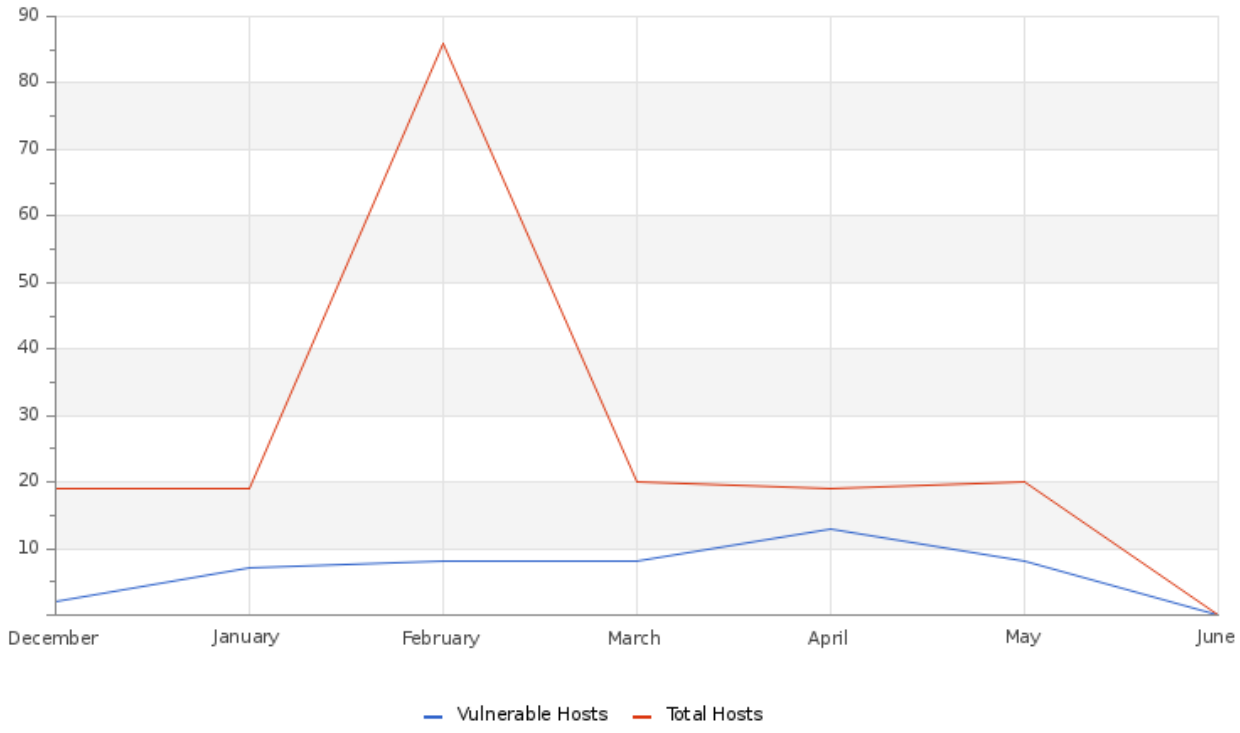
The purpose of this document is to report on the “state” of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed.

VULNERABILITY

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

Organo Judicial 06/04/2024

Hosts & Vulnerable Hosts In Last 6 Months



Nuestra gráfica refleja la cantidad de host con las que cuenta su empresa y cuánto de estos son vulnerables, para este mes podemos observar que la cantidad de host no ha variado si lo comparamos con los meses previos. En cuanto a sus host vulnerables la gráfica nos refleja una leve disminución en los mismos.

Si desea obtener mayor información, puede acceder a nuestra plataforma para clientes https://skywatch.glesec.com en la sección C&RU donde detallamos todos los eventos relacionados a su empresa y nuestras recomendaciones para robustecer la seguridad de la misma.

Si tiene alguna pregunta, no dude en ponerse en contacto con GLESEC GOC o Servicios profesionales.

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

Organo Judicial 06/04/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	45	45
Hosts Discovered	17	17
Vulnerable Hosts	8	10
Critical Vulnerabilities Count	0	2
High Vulnerabilities Count	0	2
Medium Vulnerabilities Count	10	19
Low Vulnerabilities Count	3	1
Phishing Score	0	-1
Email Gateway Score	1	0
Web Gateway Score	57	56
Endpoint Score	5	4
Hopper Score	0	-1

En la tabla podemos observar una comparación de vulnerabilidad correspondiente a los dos últimos meses, para el último mes podemos observar una leve disminución en los hosts vulnerables y sus severidades correspondientes. Para el servicio MSS-BAS podemos observar que existe persistencia en los porcentajes de las diversas pruebas, recomendamos revisar la documentación suministrada en la plataforma Skywatch sobre estos servicios para robustecer su seguridad frente a nuevas amenazas.

Vulnerability Metric

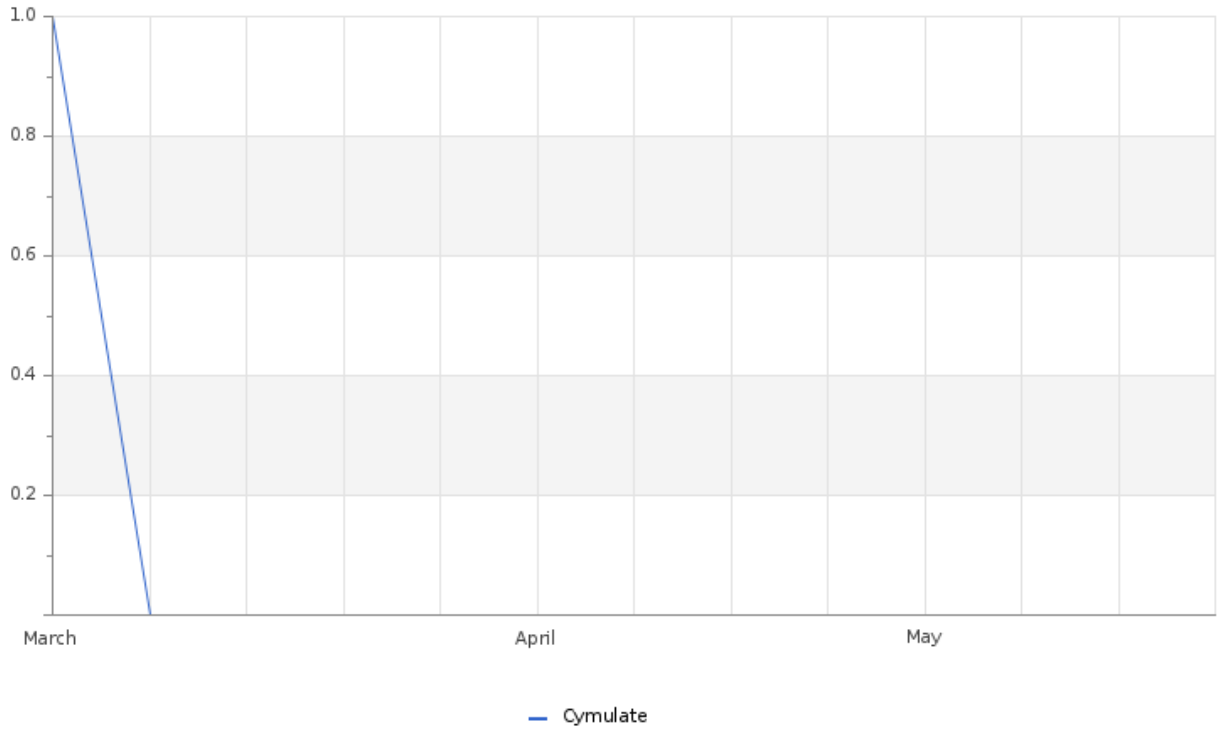
2

Se mantienen casos abiertos del servicio MSS-VM donde se han realizado recomendaciones para abordar y mitigar las diferentes vulnerabilidades que se han identificado en sus sistemas externos previamente. La documentación de las vulnerabilidades se encuentra en la plataforma Skywatch en el apartado de casos (C&RU).

THREATS

Organo Judicial 06/04/2024

Total Number of Successful MFA authentications per application

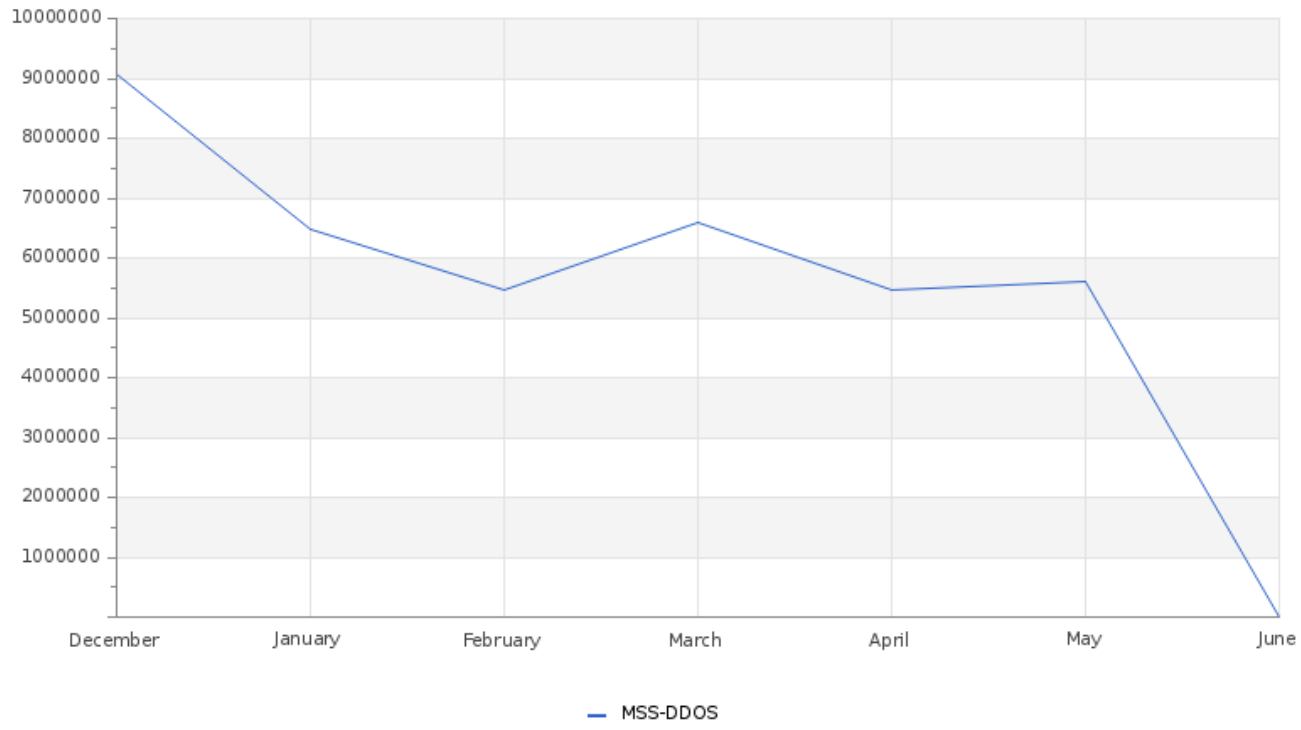


La gráfica nos permite visualizar la actividad que ha mantenido el cliente en las diferentes plataformas a las que tiene acceso. La gráfica refleja actividad en nuestra plataforma Cymulate, esta plataforma brinda información relacionada a nuestro servicio MSS-BAS; nos permite validar los controles de ciberseguridad y proporciona evaluaciones continuas las cuales les detallamos en los diversos casos relacionados a este servicio. En Skywatch puede encontrar documentación detallada sobre los casos, incidentes, reportes, etc., que les brindan información útil que permite robustecer la seguridad de su empresa.

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

Organo Judicial 06/04/2024

Total Attacks Successfully Blocked Per Service

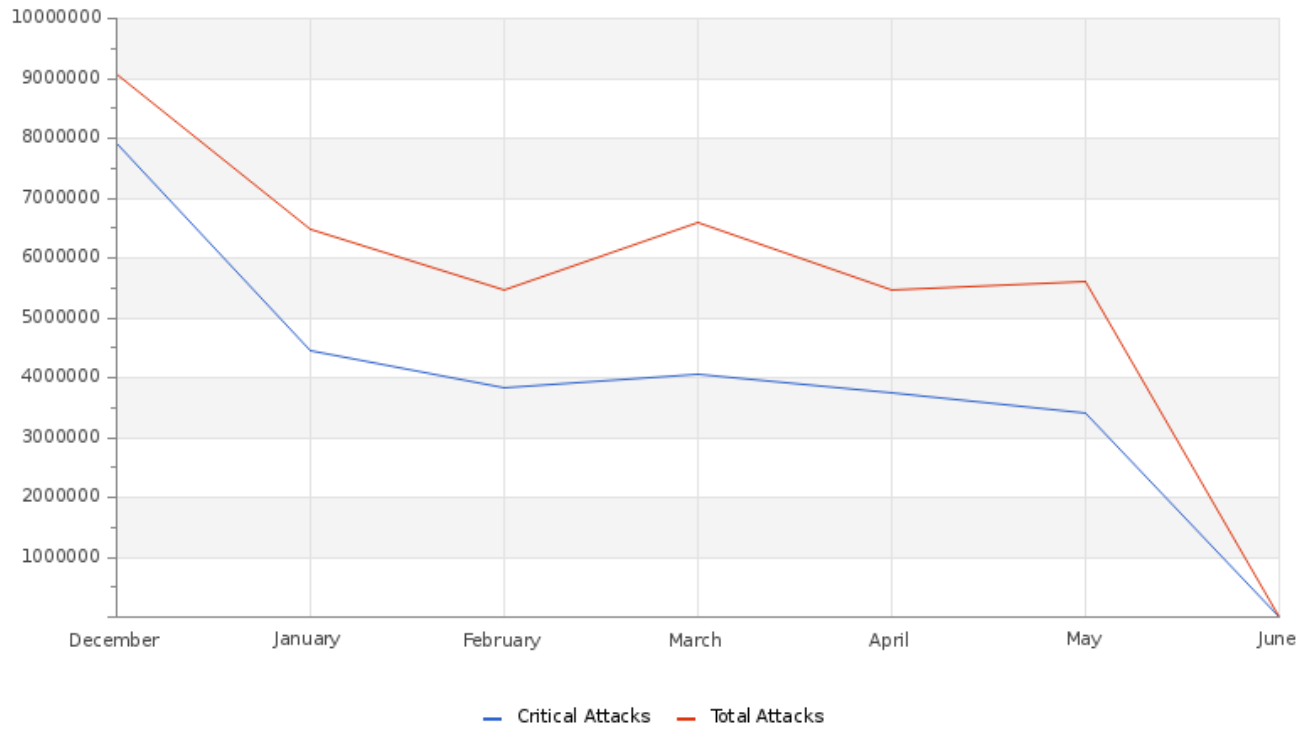


Durante el mes se registraron un total de 5,573,458 ataques dirigidos a múltiples sistemas de su organización. Se identificaron numerosos ataques persistentes provenientes de direcciones IP catalogadas como maliciosas, con múltiples reportes de ataques contra otros sistemas.

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

Organo Judicial 06/04/2024

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	0
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 06/04/2024

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	43
BAS Web Security	20
Change in Critical Perimeter Attacks	1
Change in Systems Performance	1
Immediate Threat System Vulnerable and Remediation by Patch Management	2

Para el servicio MSS-BAS se realizaron documentaciones detalladas que le permiten conocer el estado de la seguridad de su empresa; se han abierto casos que se deben tomar en cuenta ya que estos han logrado eludir sus contramedidas de seguridad. Para el servicio MSS-VME, mantenemos casos abiertos relacionados a las vulnerabilidades presentadas y el caso de seguimiento relacionado a un número significativo de direcciones IP descubiertas. Se recomienda realizar una revisión de estos casos y aplicar las mitigaciones correspondientes para salvaguardar la seguridad de su empresa. Para más información puede acceder a nuestra plataforma para clientes https://skywatch.glesec.com en la sección C&RU.

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