TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

March 07, 2024

Organo Judicial 03/07/2024

TLP AMBER CISO
EXECUTIVE REPORT

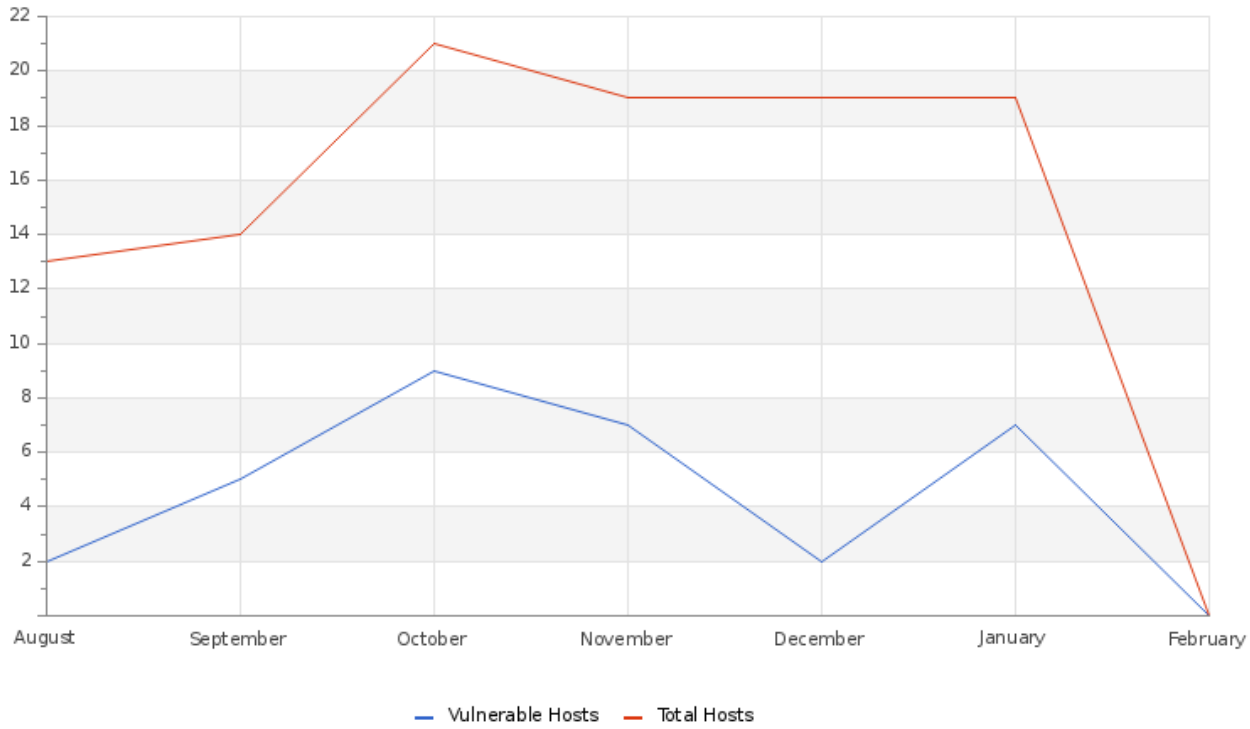
Este informe corresponde a "Enero" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades,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



El grafico muestra que la cantidad de host escaneados se mantiene, mientras que las vulnerabilidades presente en estos , presenta un aumento moderado. Las vulnerabilidades descubiertas durante el mes, la mayor parte pertenece al uso de protocolos en desuso, mientras que el resto corresponde al uso de sistemas operativos que ya no cuentan con soporte.

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

Organo Judicial 03/07/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	45	45
Hosts Discovered	15	17
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	0
Email Gateway Score	1	1
Web Application Firewall Score	0	0
Web Gateway Score	55	55
Endpoint Score	5	5
Hopper Score	0	0
DLP Score	0	0

La tabla muestra las comparaciones de los resultado que se han obtenido con respecto al mes anterior. Para este mes los resultados que se obtuvieron de las evaluaciones del servicio MSS-BAS no presentan cambios, de los resultados destaca el puntaje del servicio MSS-BAS-WEB. El bloqueo de las extensión que no están en uso 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

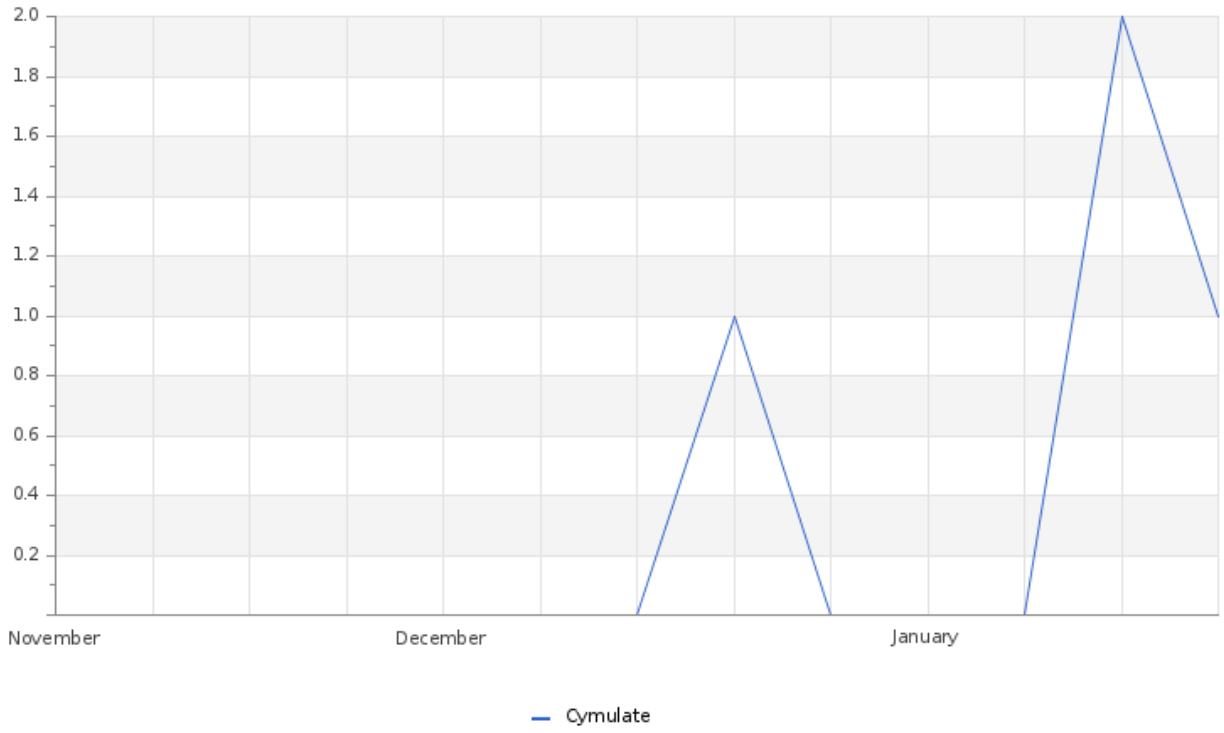
3

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

THREATS

Organo Judicial 03/07/2024

Total Number of Successful MFA authentications per application

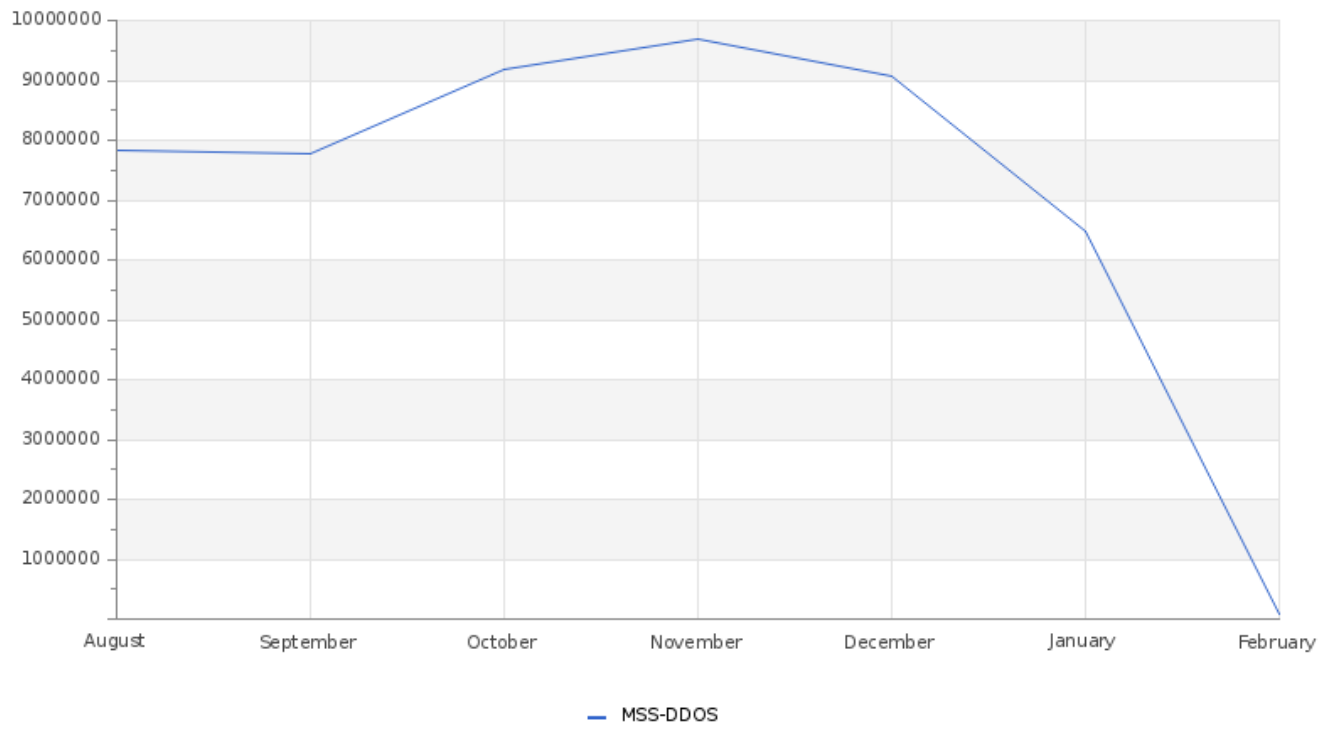


El gráfico muestra la interacción de los usuarios con las diferentes plataformas durante el mes. Se pueden observar un ligero aumento en los accesos durante el mes a la plataforma Cymulate.

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

Organo Judicial 03/07/2024

Total Attacks Successfully Blocked Per Service

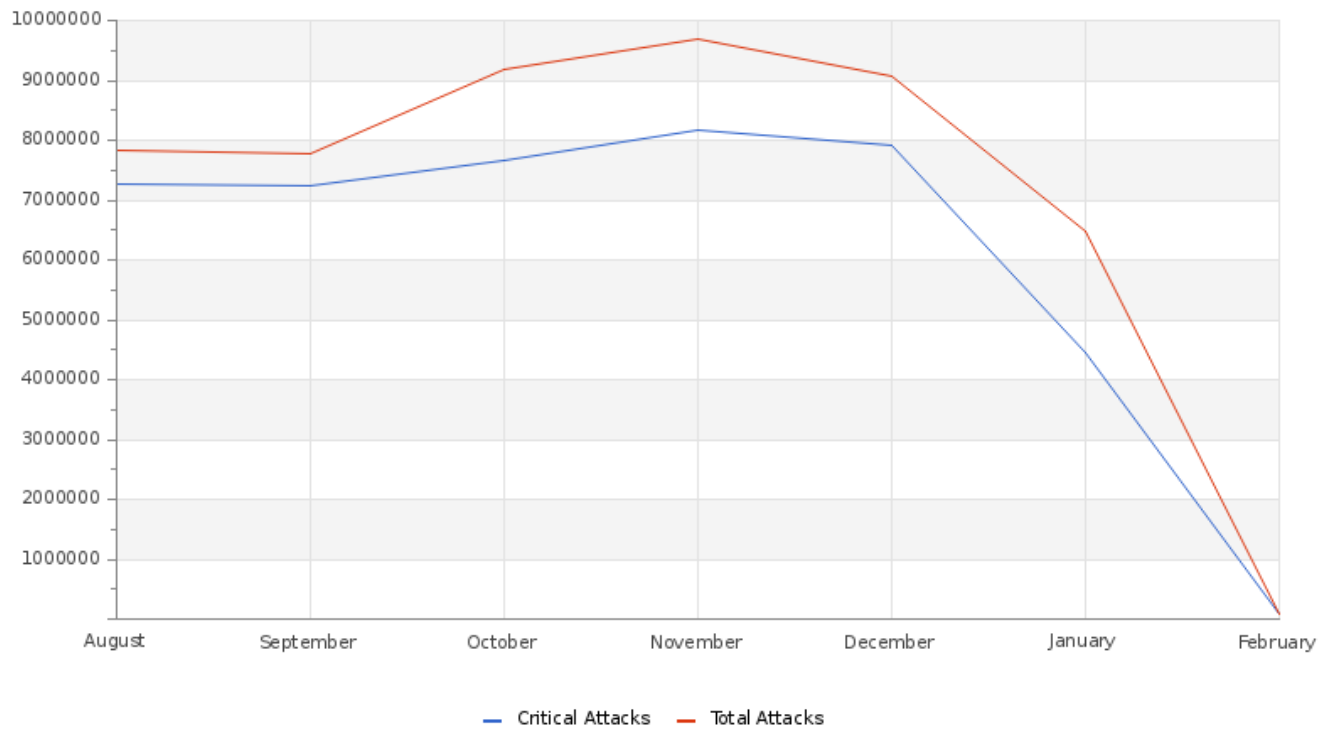


Durante el mes se registraron un total de 6,461,542 ataques los cuales tenían como objetivo múltiples sistemas de su organización. También se identificaron múltiples ataques de persistencia. Cabe destacar que la mayor parte de estos ataques provienen de IP's maliciosas y Botnets.

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

Organo Judicial 03/07/2024

Attacks Successfully Blocked by Severity



De los 6,461,542 ataques totales, fueron identificados 4,461,515 como críticos, los cuales fueron bloqueados de manera exitosa. . La mayor parte de estos ataques han sido clasificados como ErtFeed y GeoFeed. Estas son configuraciones adicionales que se realizan en los equipos con el fin de robustecer la seguridad.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	3	0
Critical Device Outages	0	0

Durante el mes se presento una caída del sitio web https://www.organojudicial.gob.pa/ por un corto lapso de tiempo, esto fue reportado y los eventos fueron documentados.

Histogram of Total and Critical Device Outages

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

Organo Judicial 03/07/2024

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	76
EDR Alerts	3
BAS Web Security	21
Change in Critical Perimeter Attacks	6
Change in High or Critical Vulnerabilities	2
Non Baselined Discovered System	54

Durante el mes se documentaron múltiples casos para el servicio MSS-BAS. También fueron documentaron ataques de persistencia registrados por el servicio MSS-DDoS, los cuales fueron llevados a cabo por IP's maliciosas las cuales contaban con múltiples reportes. También se han realizado actualizaciones de los casos relacionados con vulnerabilidades que aun persisten en sus sistemas. Recomendamos realizar 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