TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

January 31, 2024

Organo Judicial 01/31/2024

TLP AMBER CISO

EXECUTIVE REPORT

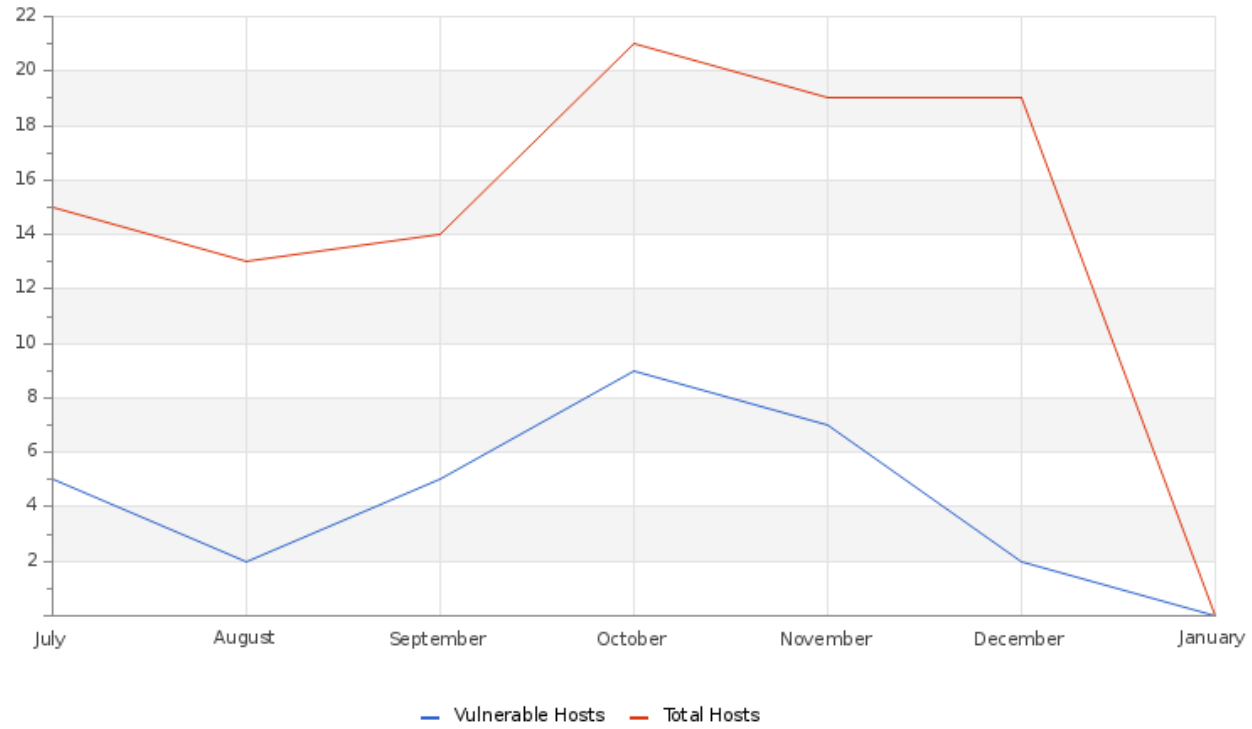
Este informe corresponde a "Diciembre" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, 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 un leve aumento en los host que han sido descubiertos a lo largo del mes, así como una disminución en las vulnerabilidades presentes en los hosts. Las vulnerabilidades descubiertas se deben al uso de protocolos obsoletos. Por lo que recomendamos llevar a cabo los cambios oportunos con el fin de robustecer su seguridad.

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

Organo Judicial 01/31/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	45	45
Hosts Discovered	17	18
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
Email Gateway Score		1
Web Application Firewall Score		0
Web Gateway Score		54
Endpoint Score		5
Hopper Score		0
DLP Score		0

La tabla muestra algunas variaciones en cuanto a los resultados que se han obtenido durante el mes actual en comparación al mes anterior. De los resultados obtenidos se puede destacar el puntaje que se ha obtenido en las pruebas del servicio MSS-BAS-WEB. Por lo que recomendamos realizar una revisión de aquellas extensiones de archivos que no se encuentran en uso y bloquearlas. Los resultados de las pruebas de servicio MSS-BAS han sido documentadas y pueden ser consultadas accediendo a la plataforma SKYWATCH.

Vulnerability Metric

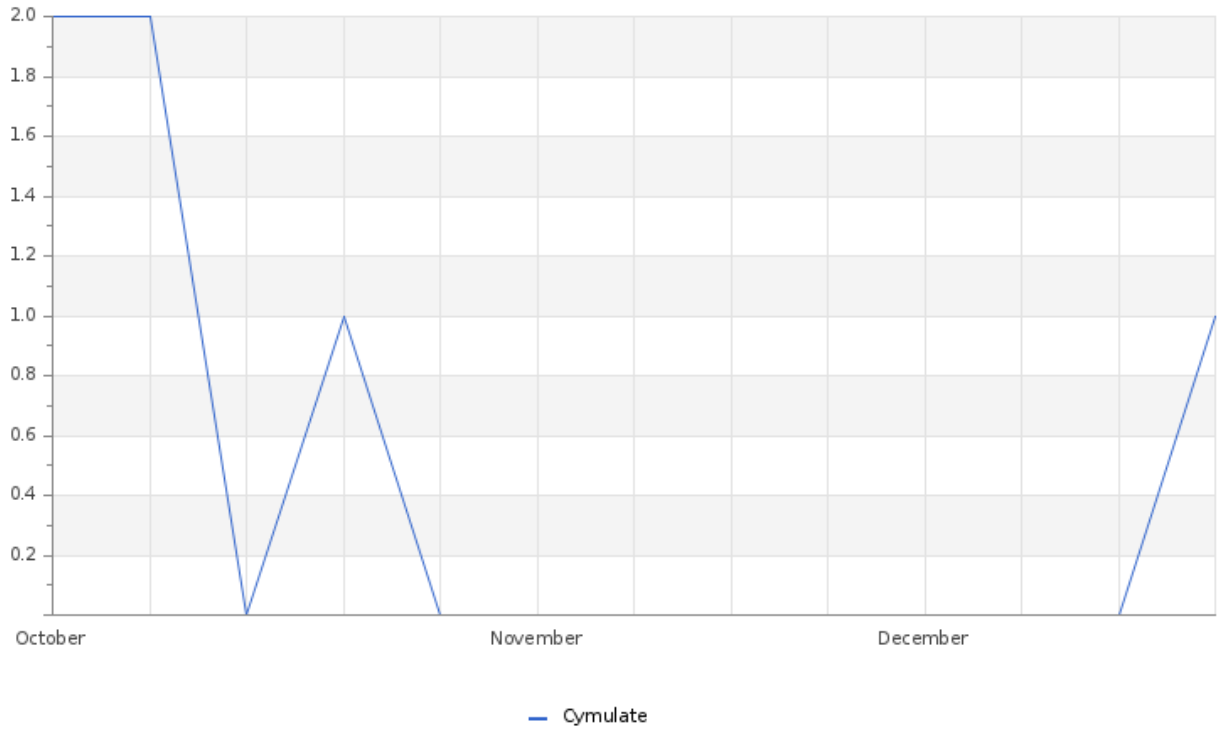
0

Se identificaron vulnerabilidades que persisten en sus sistemas, por lo que hemos recomendado acciones para abordar y mitigar estas vulnerabilidades. Además, cada una de estas vulnerabilidades se ha documentado y puede consultarse en la sección C&RU de SKYWATCH.

THREATS

Organo Judicial 01/31/2024

Total Number of Successful MFA authentications per application

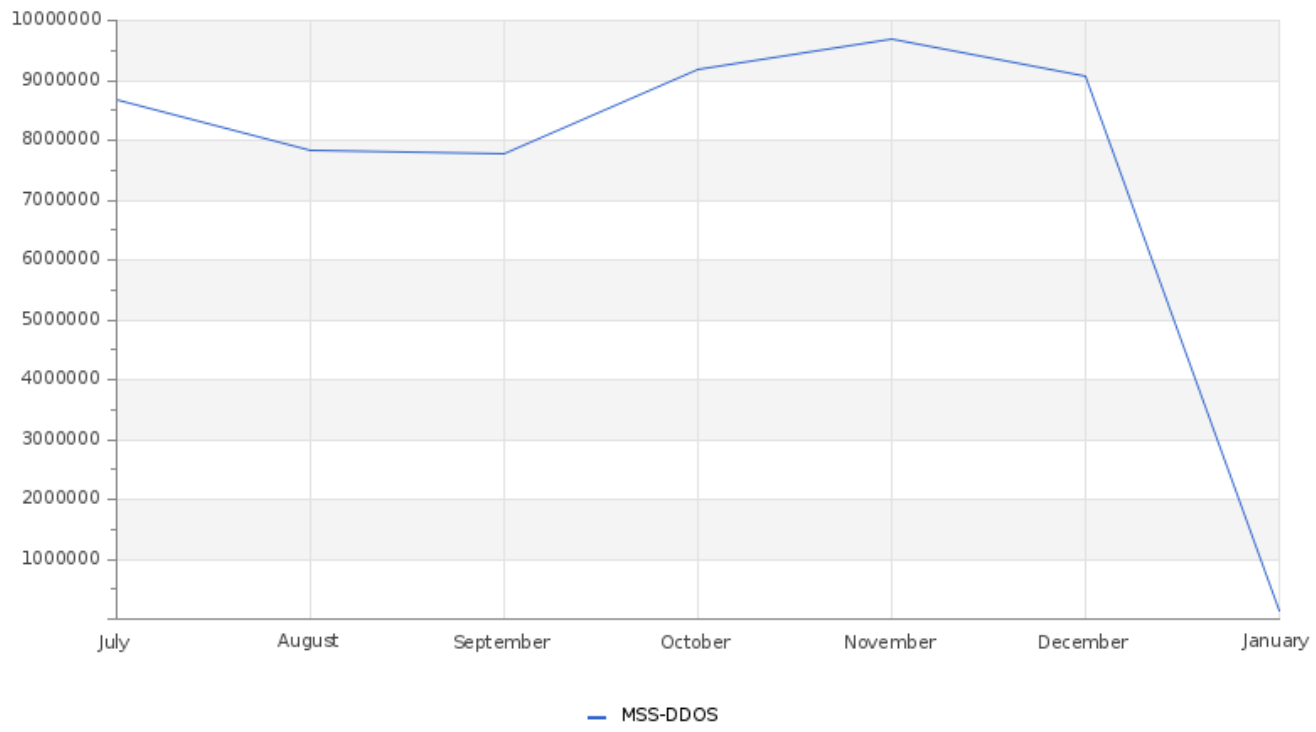


El gráfico muestra la interacción de los usuarios con las diferentes plataformas durante el mes. Se pueden observar los accesos durante el mes a la plataforma Cymulate.

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

Organo Judicial 01/31/2024

Total Attacks Successfully Blocked Per Service

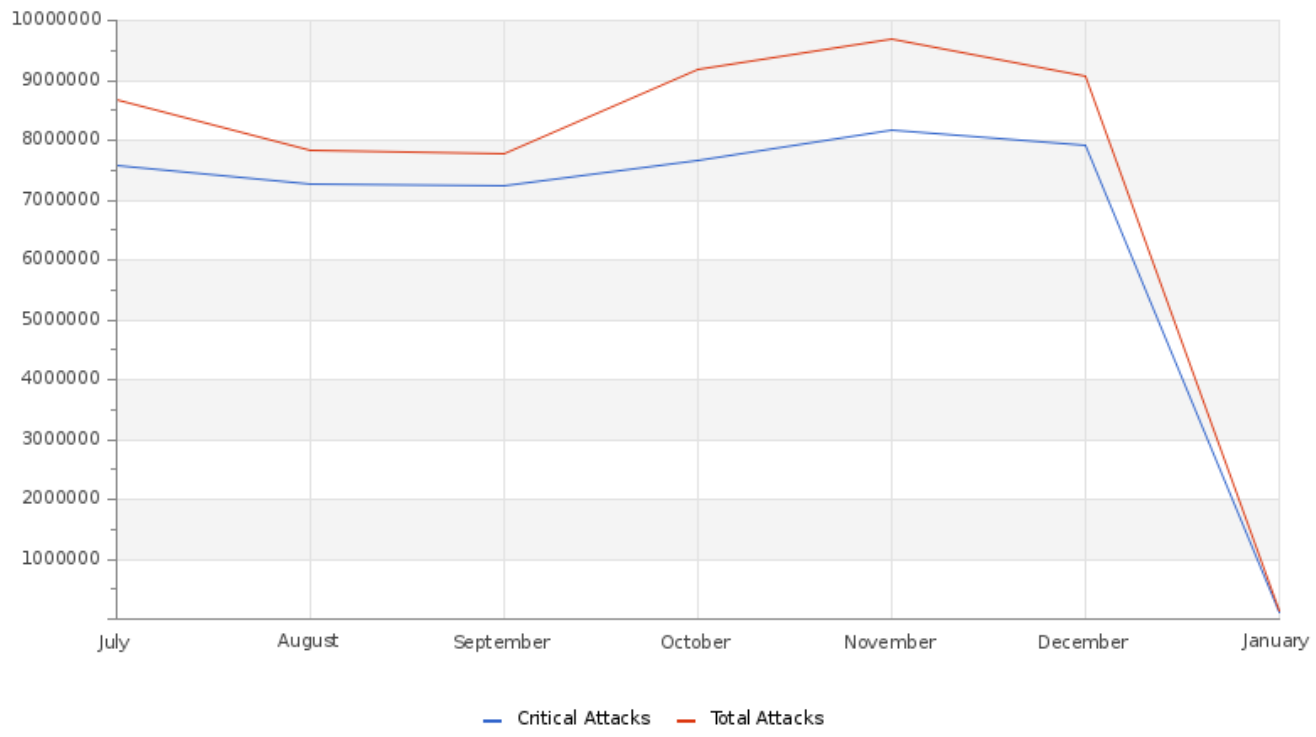


Durante el mes se registraron un total de 9,069,354 ataques los cuales fueron dirigidos contra sus sistemas. Se identificaron ataques de persistencia contra múltiples sistemas de su organización. Cabe destacar que la mayor parte de estos ataques provienen de IP's maliciosas y Botnets.

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

Organo Judicial 01/31/2024

Attacks Successfully Blocked by Severity



Un total de 7,912,450 ataques críticos fueron bloqueados de manera exitosa a lo largo del mes. 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	1	0
Critical Device Outages	0	0

Durante el mes no se presentaron anomalías en sus sistemas.

Histogram of Total and Critical Device Outages

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

Organo Judicial 01/31/2024

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	64
BAS Web Security	16
Change in Critical Perimeter Attacks	5
EDR Alerts	2

Durante el mes fueron documentados múltiples casos relacionados con el servicio MSS-BAS, alertas de ataques persistentes que fueron registrados por el servicio MSS-DDoS. 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