TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

December 18, 2023

Organo Judicial 12/18/2023

TLP AMBER CISO

EXECUTIVE REPORT

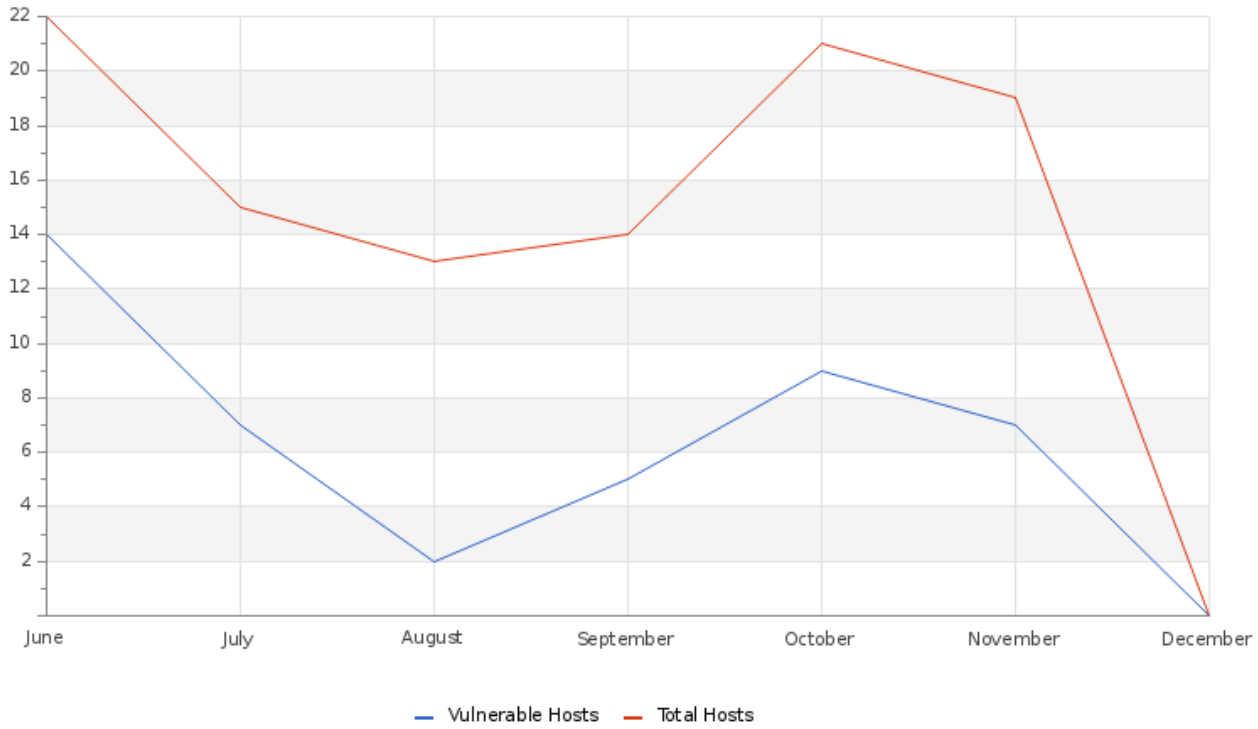
Este informe corresponde a "Noviembre" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades,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

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months



El gráfico muestra una leve disminución del número de hosts descubiertos, así como del número de vulnerabilidades descubiertas en ellos. Las vulnerabilidades que se han descubierto pertenecen al uso de protocolos obsoletos y al uso de un cifrado débil. Por lo tanto, recomendamos realizar los cambios oportunos para reforzar la seguridad.

Organo Judicial 12/18/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	45	45
Hosts Discovered	17	17
Vulnerable Hosts	2	7
Critical Vulnerabilities Count	0	2
High Vulnerabilities Count	0	2
Medium Vulnerabilities Count	4	13
Low Vulnerabilities Count	0	1
Phishing Score	0	0
Email Gateway Score	1	1
Web Application Firewall Score	0	0
Web Gateway Score	54	54
Endpoint Score	5	5
Hopper Score	0	0
DLP Score	0	0

La tabla muestra la comparación de los resultados del mes en curso con respecto al mes anterior. De los resultados se puede destacar el aumento de las vulnerabilidades medias y el valor obtenido para las pruebas del servicio MSS-BAS-WEB. Recomendamos revisar aquellas extensiones que no estén en uso y bloquearlas. Los resultados de las pruebas de servicio MSS-BAS han sido documentados y pueden ser consultados accediendo a la plataforma SKYWATCH.

Vulnerability Metric

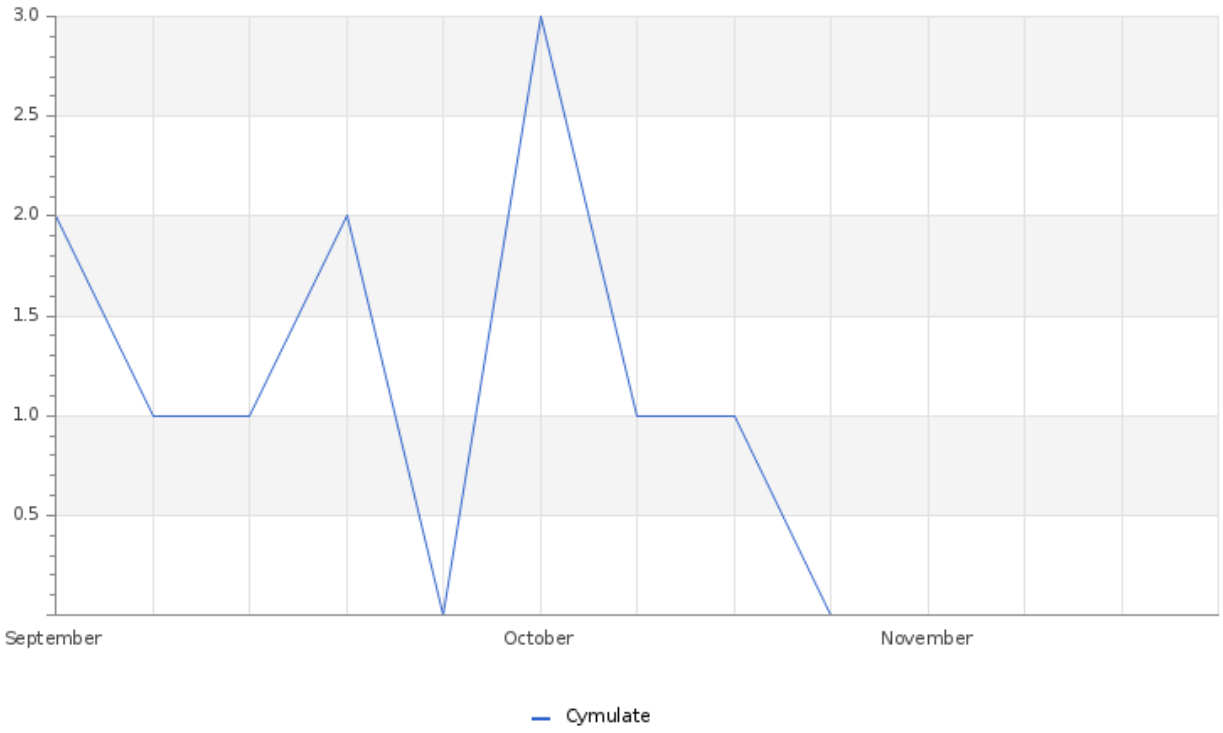
2

Se identificaron múltiples vulnerabilidades en sus sistemas. 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 12/18/2023

Total Number of Successful MFA authentications per application

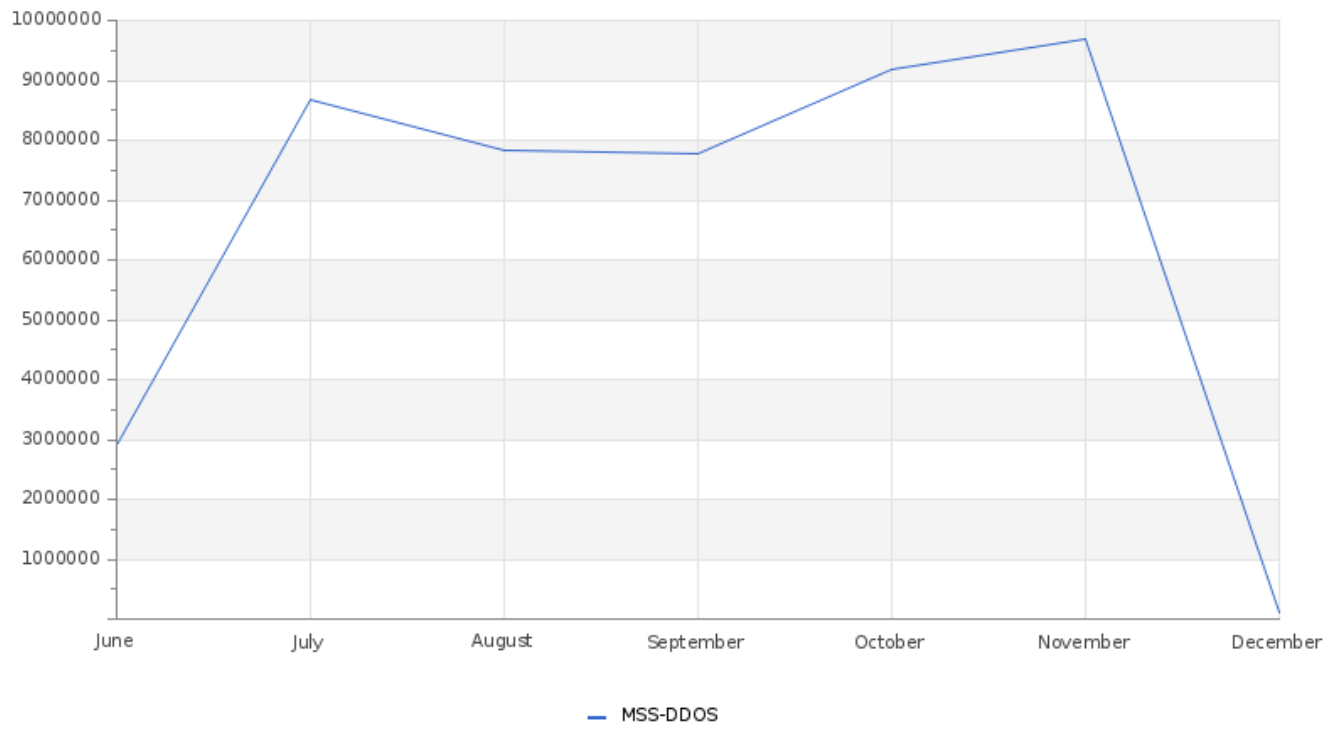


El gráfico muestra la interacción de los usuarios con las diferentes plataformas durante el mes. Se pueden observar los accesos durante el mes a la plataforma Cymulate.

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

Organo Judicial 12/18/2023

Total Attacks Successfully Blocked Per Service

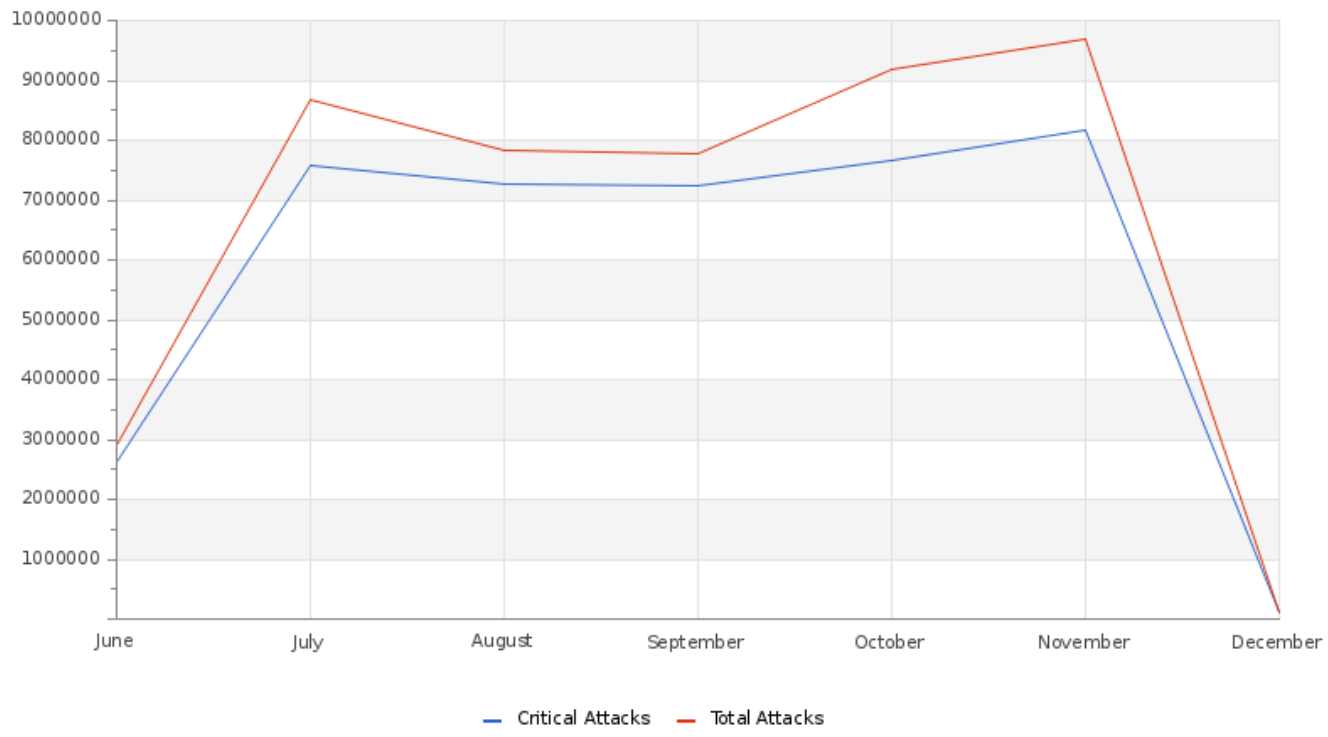


Durante el mes se registraron un total de 9,697,603 ataques dirigidos a sus sistemas. Se identificaron ataques persistentes contra múltiples sistemas de sus organización. La mayor parte de estos ataques provienen de IP's maliciosas y Botnets.

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

Organo Judicial 12/18/2023

Attacks Successfully Blocked by Severity



Un total de 301,045 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 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	4
Critical Device Outages	0	0

Durante el mes se presentaron anomalías relacionadas con el sitio web, estas fueron reportadas de manera inmediata al personal encargado.

Histogram of Total and Critical Device Outages

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

Organo Judicial 12/18/2023

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	57
Change in Critical Perimeter Attacks	3
EDR Alerts	3
Change in Systems Performance	3
BAS Web Security	6

Durante el mes fueron documentados múltiples casos relacionados con el servicio MSS-BAS, alertas de ataques persistentes 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