TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

August 18, 2023

Organo Judicial 08/18/2023

TLP AMBER CISO
EXECUTIVE REPORT

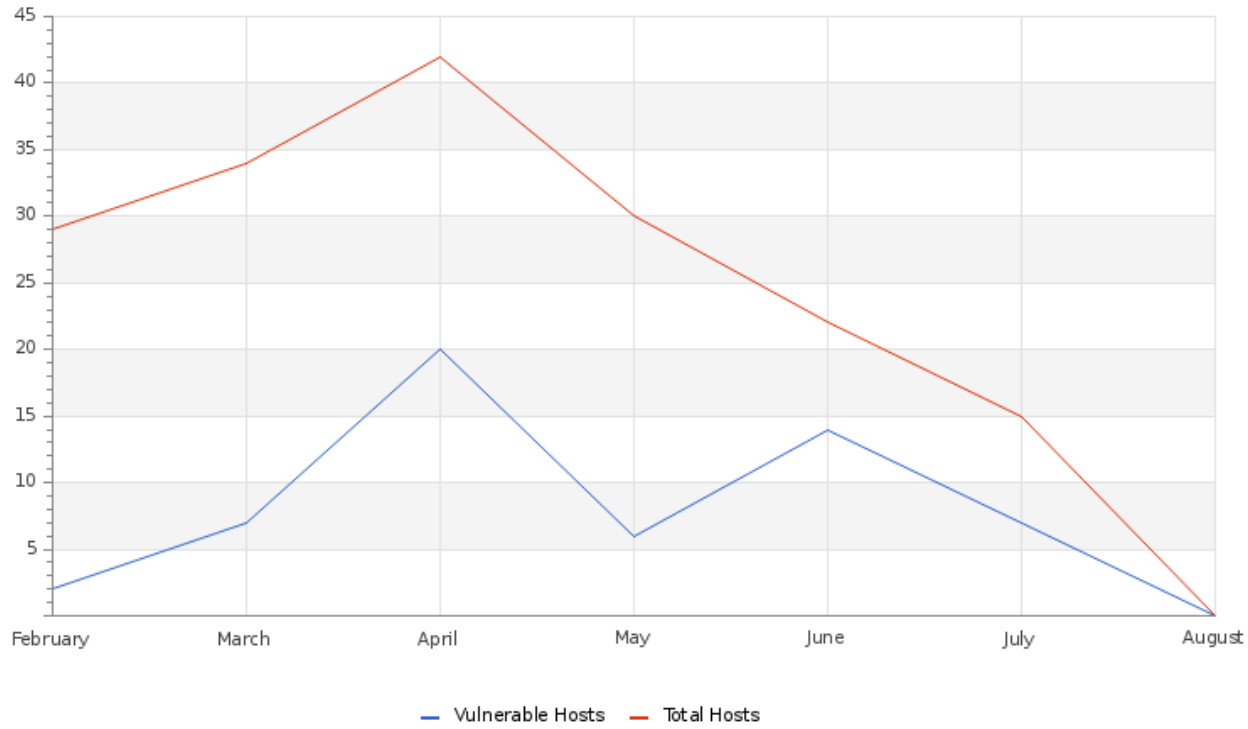
Este informe corresponde "julio" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades,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



En la gráfica podemos observar un decremento en las vulnerabilidades que se han descubierto durante el mes. Las vulnerabilidades presentes en sus dispositivos están relacionadas con el uso de protocolos y software que están en desuso. Recomendamos que estas vulnerabilidades sean solucionadas, para mejorar la seguridad de su empresa u organización.

Organo Judicial 08/18/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	38	38
Hosts Discovered	13	21
Vulnerable Hosts	5	13
Critical Vulnerabilities Count	2	19
High Vulnerabilities Count	2	41
Medium Vulnerabilities Count	9	120
Low Vulnerabilities Count	1	10
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

En la tabla de puede observar la comparación con el mes anterior de los puntajes obtenidos en las pruebas realizadas por el servicio MSS-BAS, en los resultados de las pruebas destaca el puntaje que se obtuvo para el BAS Web Gateway, recomendamos verificar aquellas extensiones que no utiliza y bloquearlas. Los resultados obtenidos en las simulaciones realizadas por el servicio MSS-BAS han sido documentadas y pueden ser visualizadas en la plataforma SKYWATCH.

Vulnerability Metric

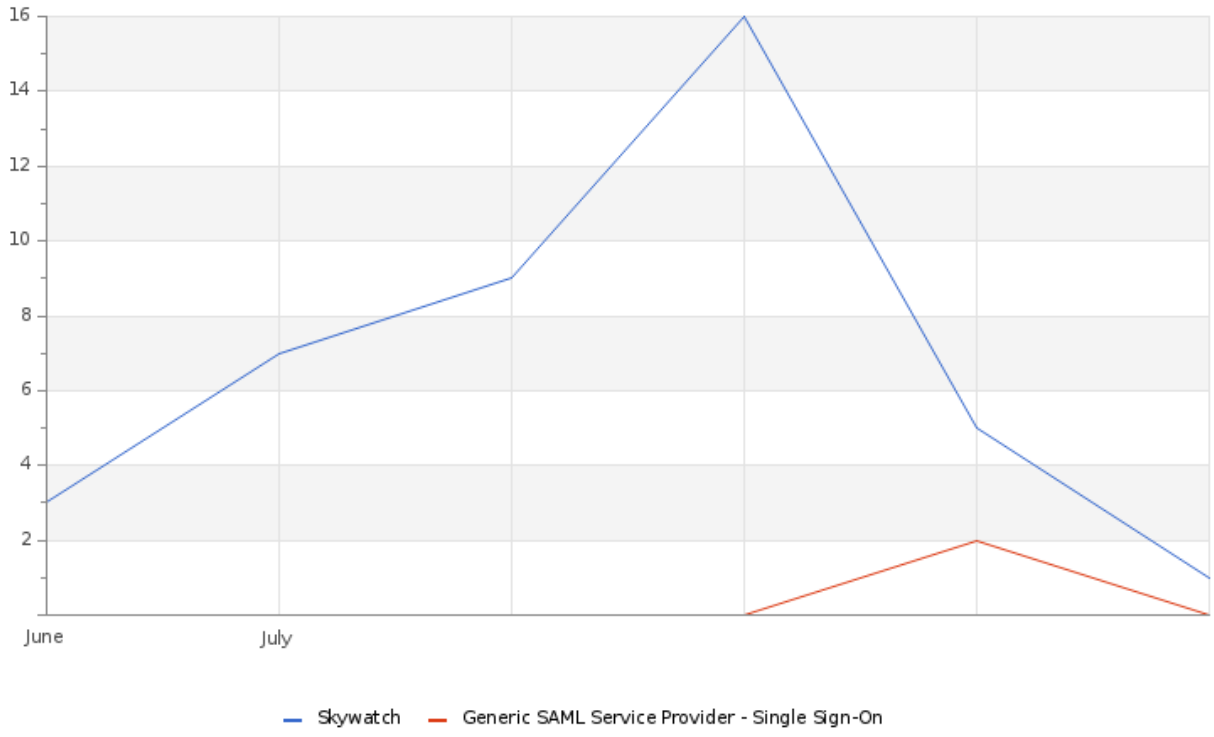
6

Se han identificado y recomendando acciones para abordar y mitigar las vulnerabilidades presentes a nivel externo. Estas vulnerabilidades han sido documentadas y pueden ser visualizadas en el apartado C&RU de SKYWATCH

THREATS

Organo Judicial 08/18/2023

Total Number of Successful MFA authentications per application

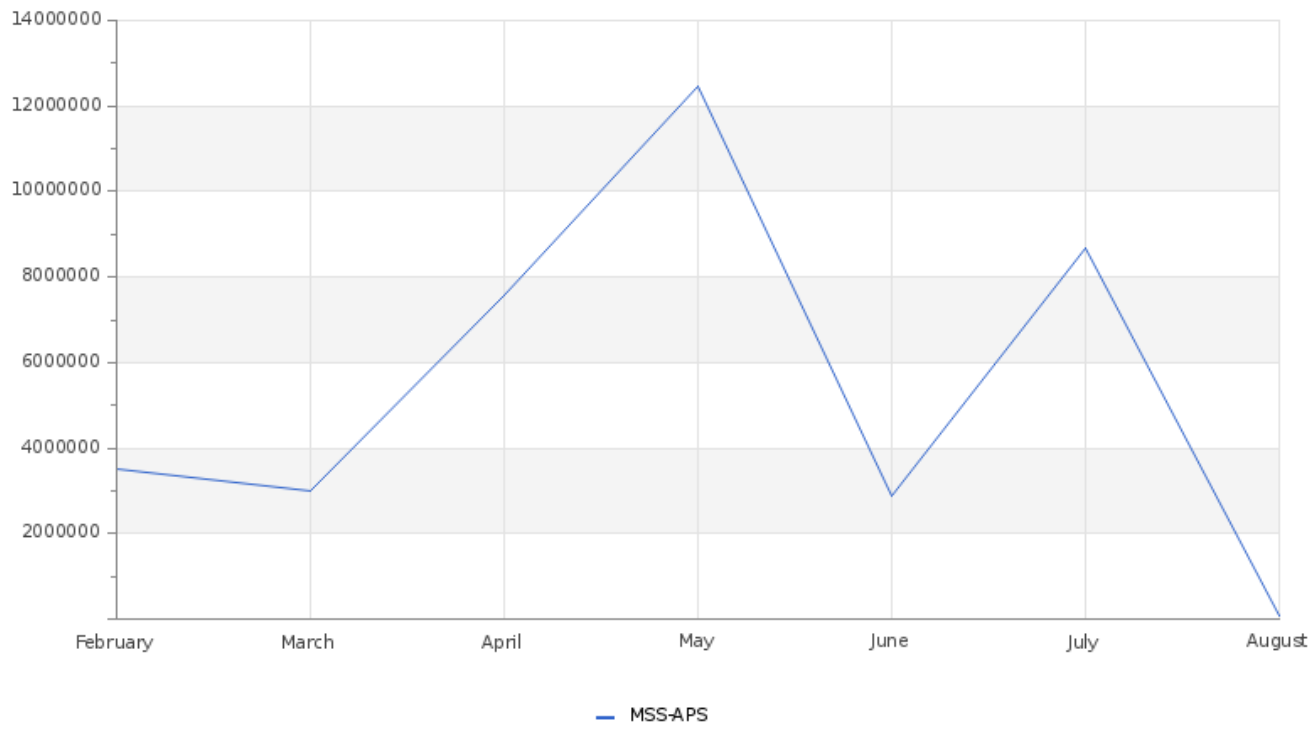


La gráfica muestra una actividad constante por parte de los usuarios en la plataforma SKYWATCH.

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

Organo Judicial 08/18/2023

Total Attacks Successfully Blocked Per Service

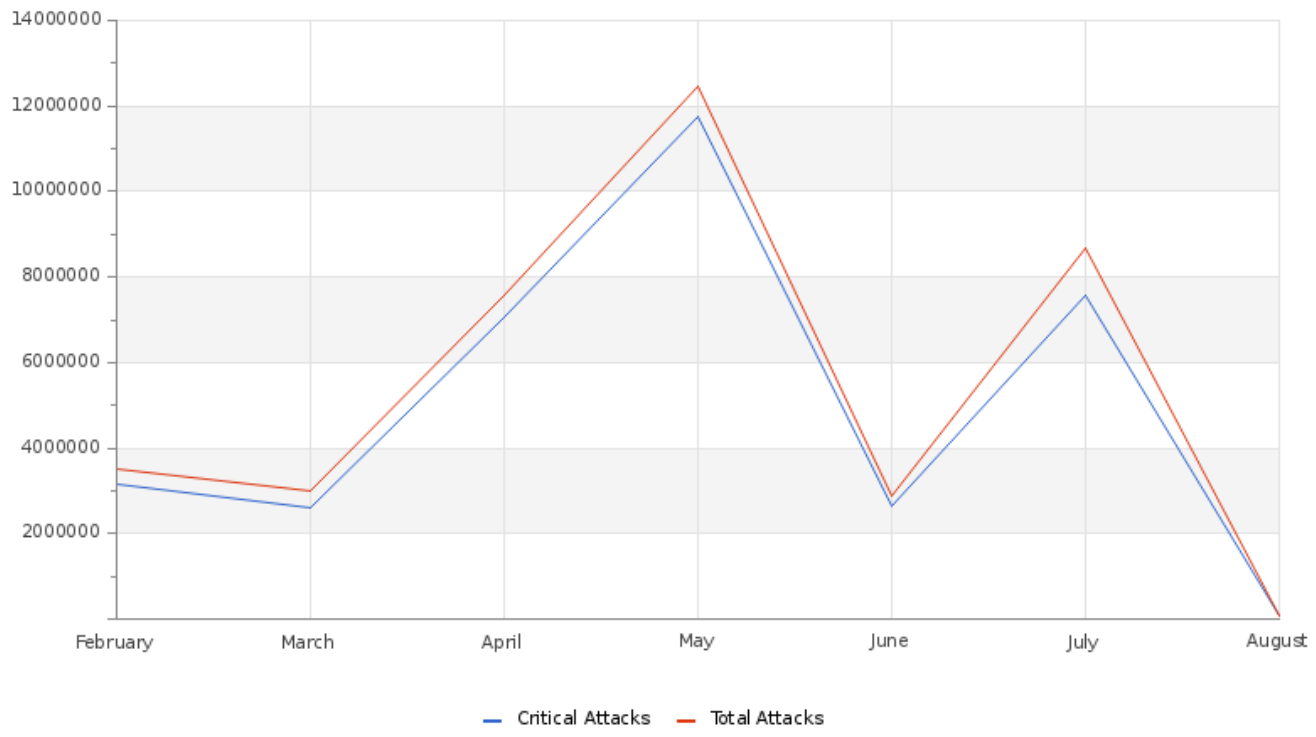


Durante el mes se registraron un total de 8,666,093 ataques totales, hemos estado monitoreando estas actividades y se han abierto casos de los ataques de persistencias realizados a sus dispositivos. Estos ataques suelen provenir de IP's maliciosas y Botnets.

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

Organo Judicial 08/18/2023

Attacks Successfully Blocked by Severity



La cantidad de ataques críticos fue de 7,563,589, la mayoría de estos clasificados como Ertfeed, éste se centra en una inteligencia única en tiempo real que puede proporcionar protección preventiva contra amenazas emergentes específicas de DDoS, incluido IoT en evolución botnets y nuevos vectores de ataque DNS.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Down Devices	2	4
Critical Down Devices	0	0

La pagina principal de Organo judicial, estuvo restringida exteriormente y debido a e esto se generaron alertas. Solo estaba accesible en Panamá.

Histogram of Total and Critical Device Outages

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

Organo Judicial 08/18/2023

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Baseline Systems Discovered	2
BAS Immediate Threat	47
BAS Web Security	8
Change in Critical Perimeter Attacks	1
Change in Systems Availability	1
Change in Systems Performance	3
Change in Vulnerable Systems	1

Durante el mes se han reportado aquellas vulnerabilidades que aún persisten en sus sistemas, se han abierto casos de ataques realizados a sus dispositivos, así como la documentación de los resultados de las diferentes pruebas realizadas por el servicio MSS-BAS, se recomienda revisar y aplicar las soluciones correspondientes, sobre todo a las relacionadas con amenazas inmediatas, que buscan probar la resiliencia de su entorno a las amenazas recientes. 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