TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

October 18, 2023

Organo Judicial 10/18/2023

TLP AMBER CISO

EXECUTIVE REPORT

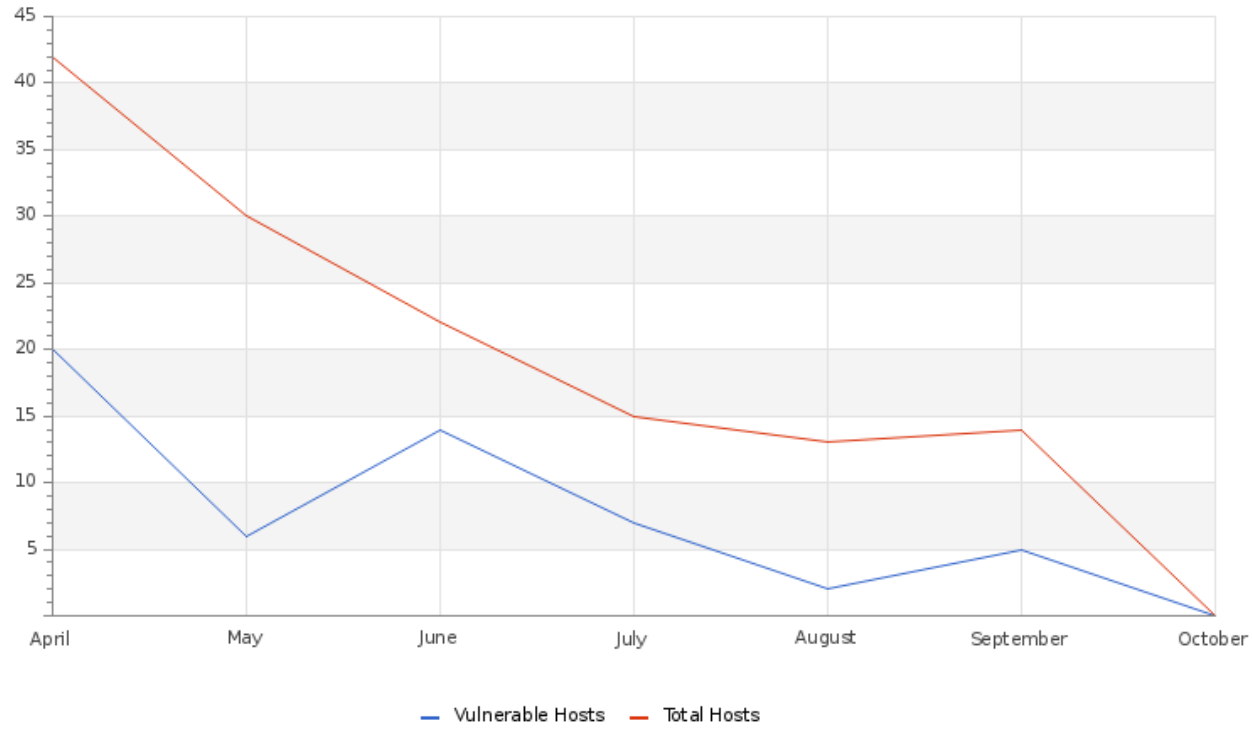
Este informe corresponde "Septiembre" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, 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 grafica se observa un leve incremento tanto en el descubrimiento de los host, como en los que son vulnerables. Las vulnerabilidad descubiertas en los hosts indican que algunos de estos utilizan protocolos que actualmente se consideran obsoletos. Por lo que recomendamos actualizar a versiones mas recientes de estos protocolos, con el fin de mejorar la seguridad de la organización.

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

Organo Judicial 10/18/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	39	38
Hosts Discovered	11	12
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	53	54
Endpoint Score	5	5
Hopper Score	0	0
DLP Score	0	0

Las comparaciones de los resultados que se obtuvieron durante el mes actual respecto al anterior, destaca el puntaje que se obtuvo del vector Web Gateway, recomendamos realizar una revisión de las extensiones de archivos que no estén en uso y proceder con el bloqueo de estas. Los resultados obtenidos de las evaluaciones del servicio MSS-BAS, se encuentran documentadas en la plataforma SKYWATCH.

Vulnerability Metric

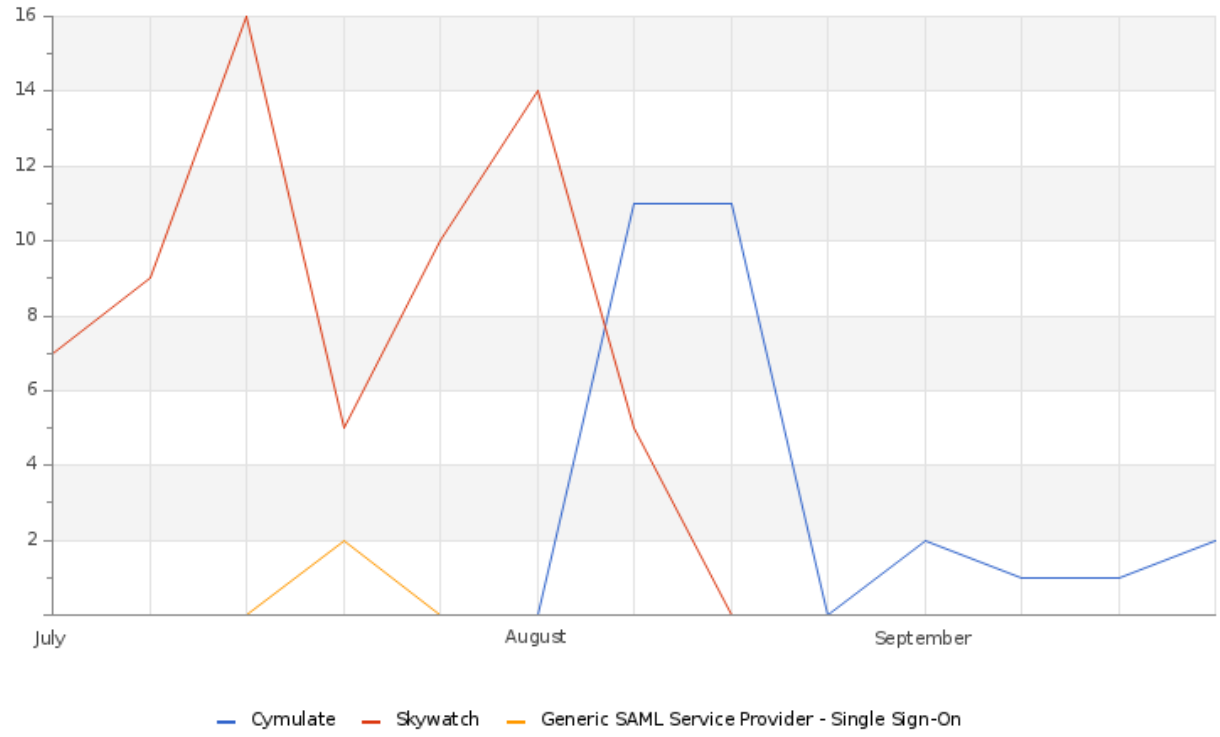
3

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 10/18/2023

Total Number of Successful MFA authentications per application

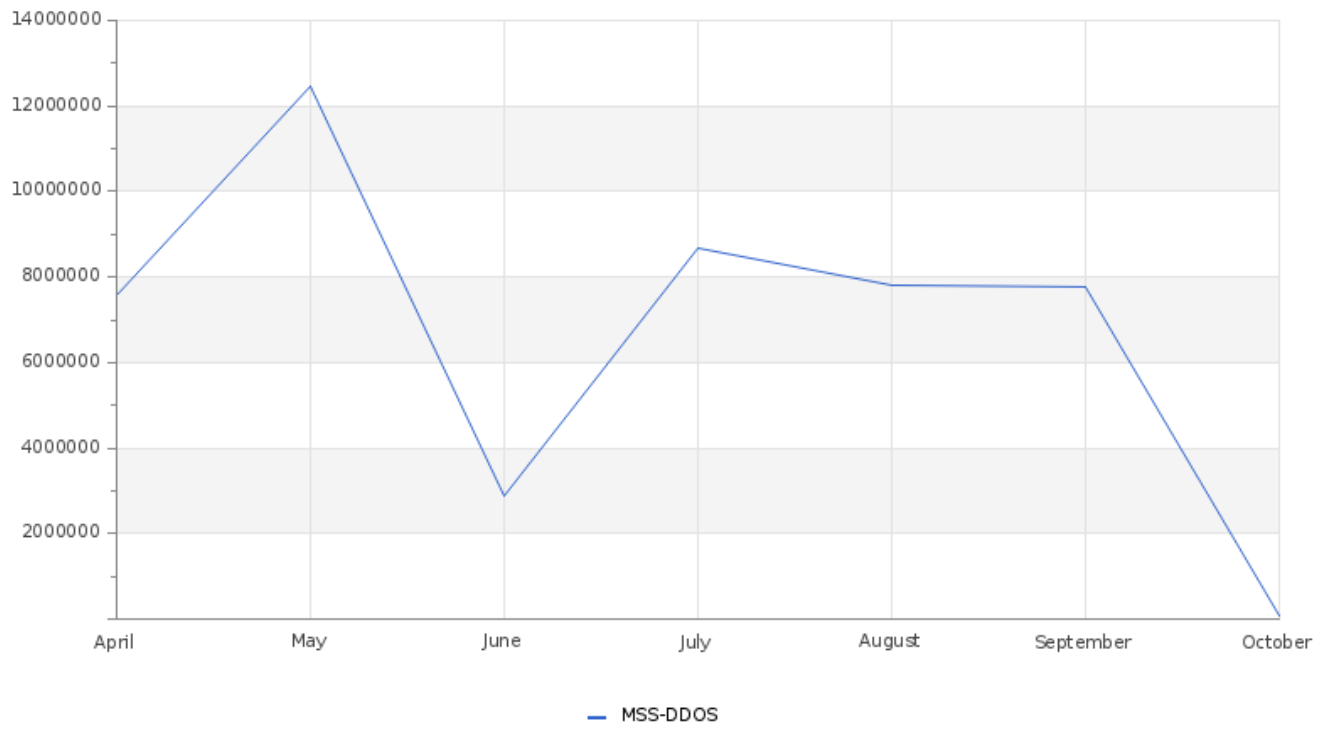


La grafica muestra la actividad por parte de los usuarios, que durante el mes realizaron múltiples ingresos a las plataformas de Skywatch y Cymulate.

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

Organo Judicial 10/18/2023

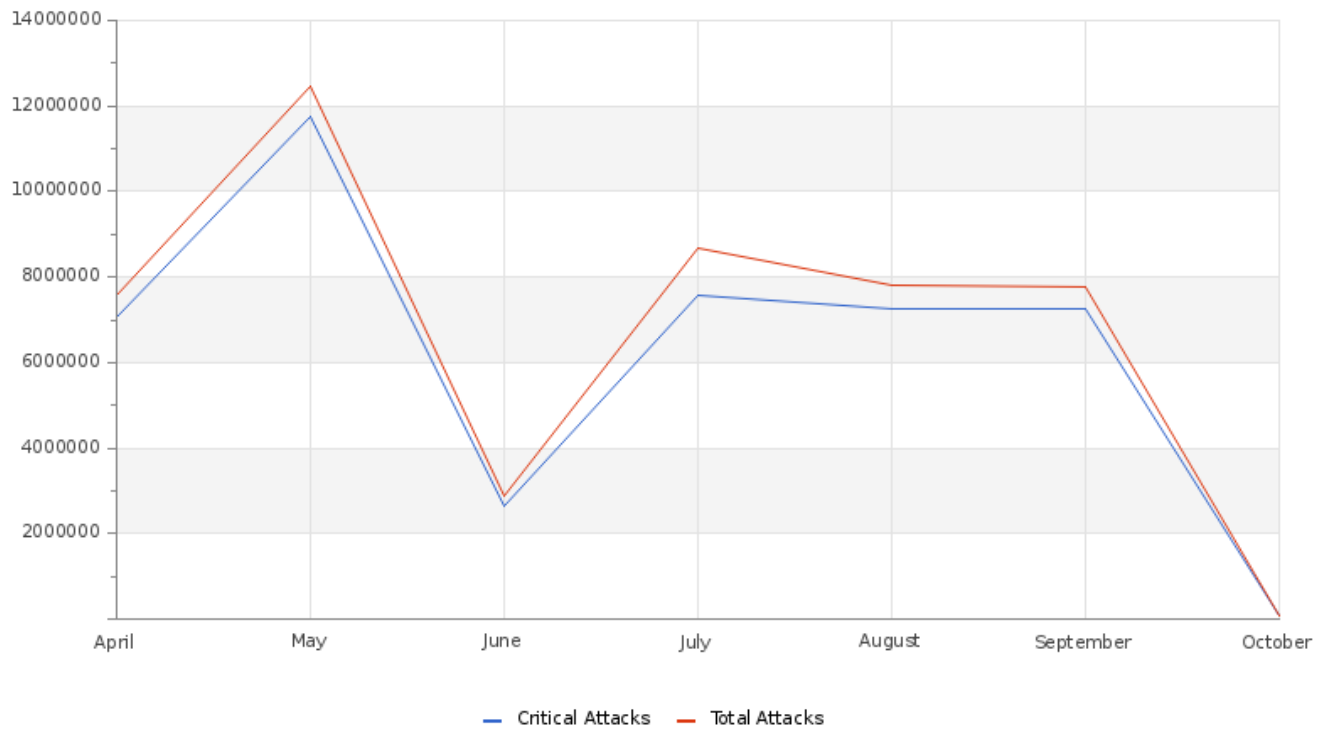
Total Attacks Successfully Blocked Per Service



Durante el mes se registraron un total de 7,766,228 ataques. Se reportaron IP's las cuales realizaban ataques persistente contra direcciones de la organización. La mayor parte de estos ataques suelen provenir de IP’s maliciosas y Botnets.

Organo Judicial 10/18/2023

Attacks Successfully Blocked by Severity



La cantidad de ataques críticos registrados durante el mes fue de 7,246,380, la mayoría de estos clasificados como ataques ErtFeed y GeoFeed. Tanto ErtFeed como GeoFeed son configuraciones adicionales que permiten robustecer la seguridad.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Down Devices	6	0
Critical Down Devices	0	0

Durante el mes no se registraron caídas, ni problemas de rendimiento en los sistemas, todos los dispositivos permanecieron en estado UP.

Histogram of Total and Critical Device Outages

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

Organo Judicial 10/18/2023

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Immediate Threat System Vulnerable and Remediation by Patch Management	19
Change in Critical Perimeter Attacks	5
BAS Immediate Threat	48
BAS Web Security	4
Change in Systems Performance	3
Non Baselined Discovered System	25

Durante el mes fueron documentados casos de las pruebas realizadas por el servicio MSS-BAS, alertas del servicio MSS-DDoS de ataques de persistencia . Además, se actualizaron los casos de aquellas vulnerabilidades que todavía persisten en los sistemas. Recomendamos realizar una revisión minuciosa de los casos y aplicar las recomendaciones y remediaciones 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