TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

March 09, 2024

Organo Judicial 03/09/2024

TLP AMBER CISO
EXECUTIVE REPORT

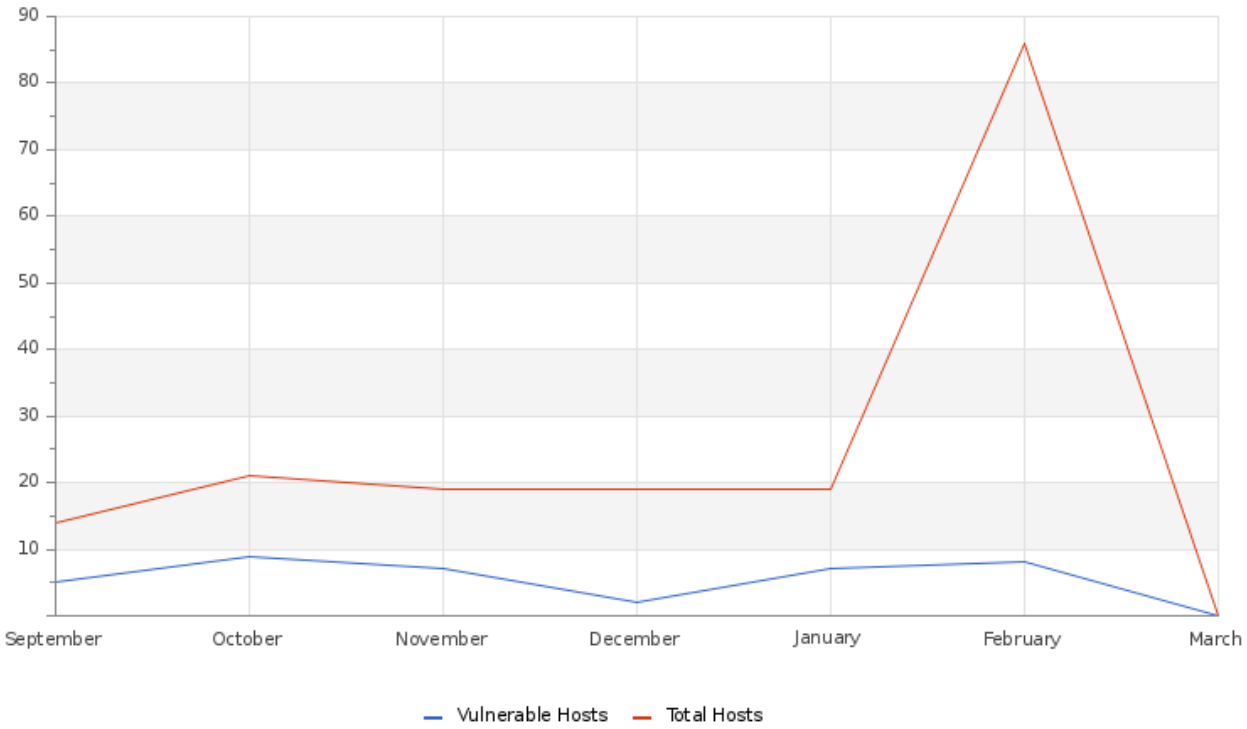
Este informe corresponde a "Febrero" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades,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



Como se observa en la grafica, durante el mes se produjo un aumento significativo en la cantidad total de hosts, esto debido a nuevos hosts han sido descubiertos. Por otro lado, la cantidad de host con vulnerabilidades se mantiene. La mayor parte de estas vulnerabilidades corresponden al uso de protocolos en desuso y actualizaciones no realizadas.

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

Organo Judicial 03/09/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	45	45
Hosts Discovered	82	19
Vulnerable Hosts	0	7
Critical Vulnerabilities Count	0	2
High Vulnerabilities Count	0	2
Medium Vulnerabilities Count	0	13
Low Vulnerabilities Count	0	1
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 una comparación de los resultados obtenidos producto de las evaluaciones y escaneos realizados, en comparación con el mes anterior. Para este mes se puede destacar el aumento significativo en la cantidad de host descubiertos, así como el puntaje obtenido en las evaluaciones del servicio MSS-BAS-WEB. Recomendamos realizar el bloqueo de las extensión que no se utilizan, esto 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

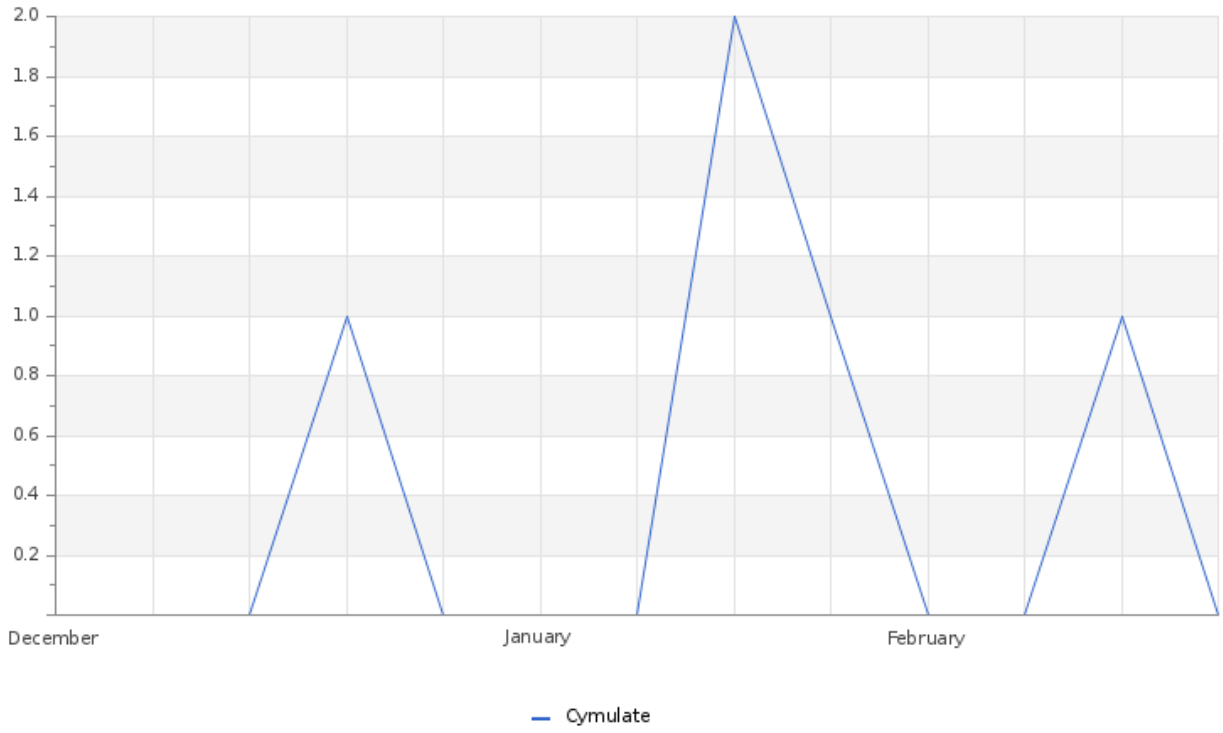
0

Hemos identificado vulnerabilidades que persisten en sus sistemas, por lo que recomendamos 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 03/09/2024

Total Number of Successful MFA authentications per application

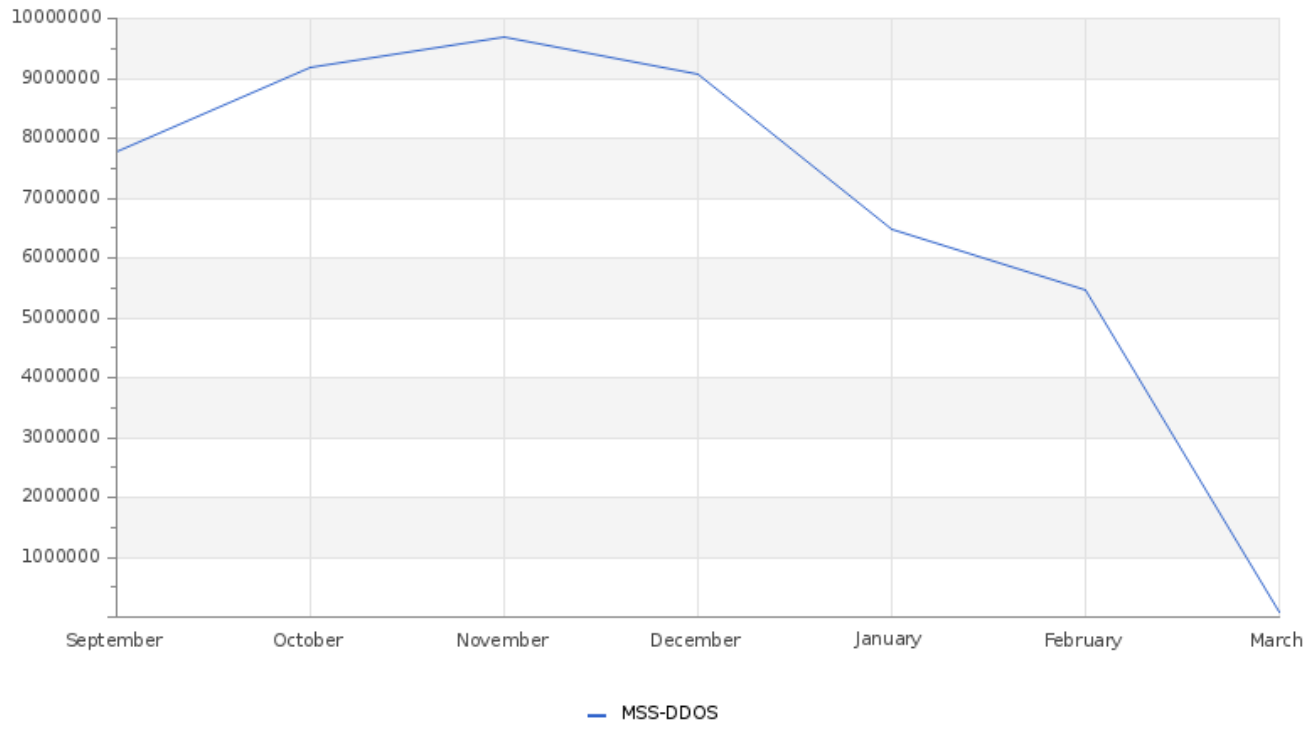


La grafica muestra la actividad de los usuarios durante el mes en las diferentes plataformas. Se puede observar una reducción en el numero de ingresos a la plataforma de Cymulate durante el mes.

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

Organo Judicial 03/09/2024

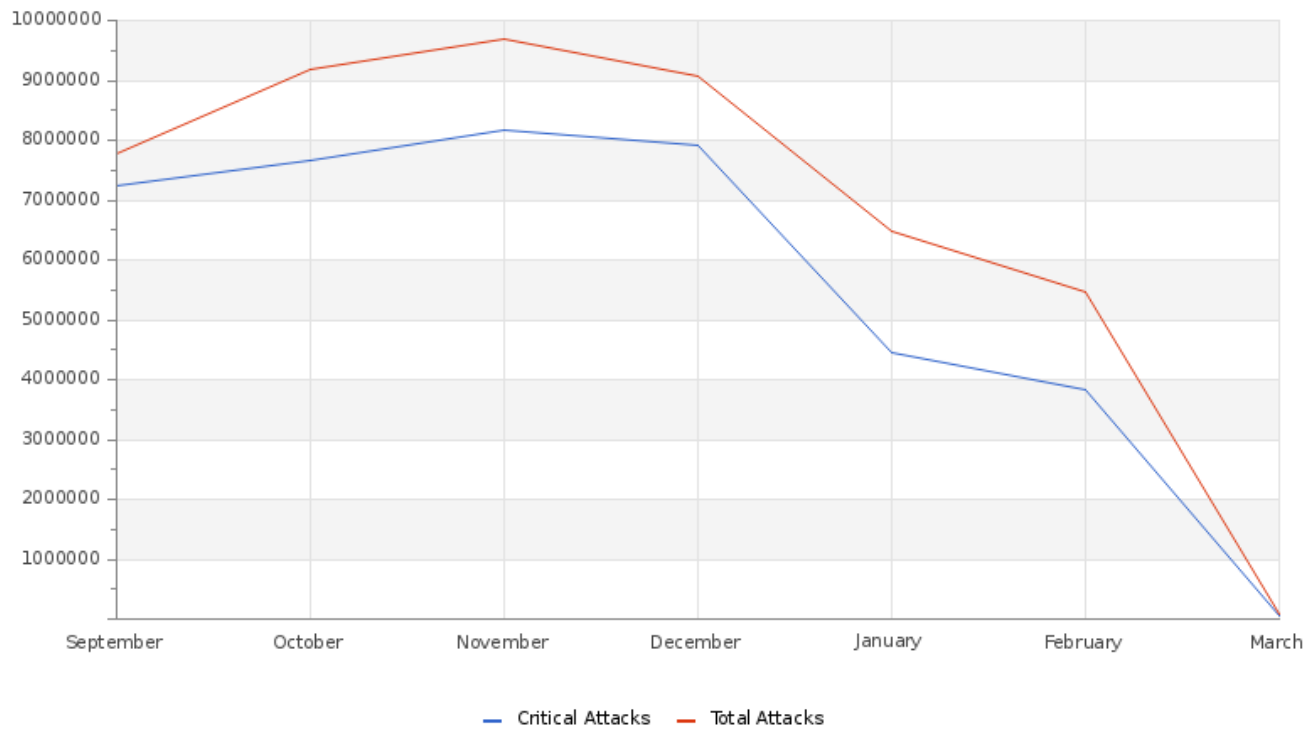
Total Attacks Successfully Blocked Per Service



Durante el mes fueron registrados un total de 5,460,275 ataques, estos fueron realizados contra múltiples sistemas de su organización. Se identificaron varios ataques de persistencia los cuales provenían de IPs catalogados como maliciosas.

Organo Judicial 03/09/2024

Attacks Successfully Blocked by Severity



Un total de 3,835,804 ataques fueron catalogados como críticos, los sistemas lograron bloquear de manera exitosas todos estos ataques. La mayor parte de estos ataques son clasificados como ErtFeed y GeoFeed, estas clasificaciones se deben a que 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	5	1
Critical Device Outages	0	0

Durante el mes se presentaron múltiples caídas en sus sistemas, incluyendo el sitio web https://www.organojudicial.gob.pa/. Estos eventos fueron notificados y documentados respectivamente.

Histogram of Total and Critical Device Outages

Organo Judicial 03/09/2024

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	45
Change in Critical Perimeter Attacks	4
BAS Web Security	14
EDR Alerts	1
Change in High or Critical Vulnerabilities	2
Non Baselined Discovered System	54

Se documentaron múltiples casos para el servicio MSS-BAS, la mayor parte de estos corresponden al servicio MSS-BAS-IMTHREAT. También se documentaron ataques de persistencias provenientes de direcciones IPs con múltiples reportes de actividad maliciosa. Por ultimo, se identificaron vulnerabilidades que persisten en sus sistemas. Recomendamos llevar a cabo 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