TLP:AMBER

CISO EXECUTIVE REPORT

BLADEX

June 17, 2024

BLADEX 06/17/2024

TLP AMBER CISO
EXECUTIVE REPORT

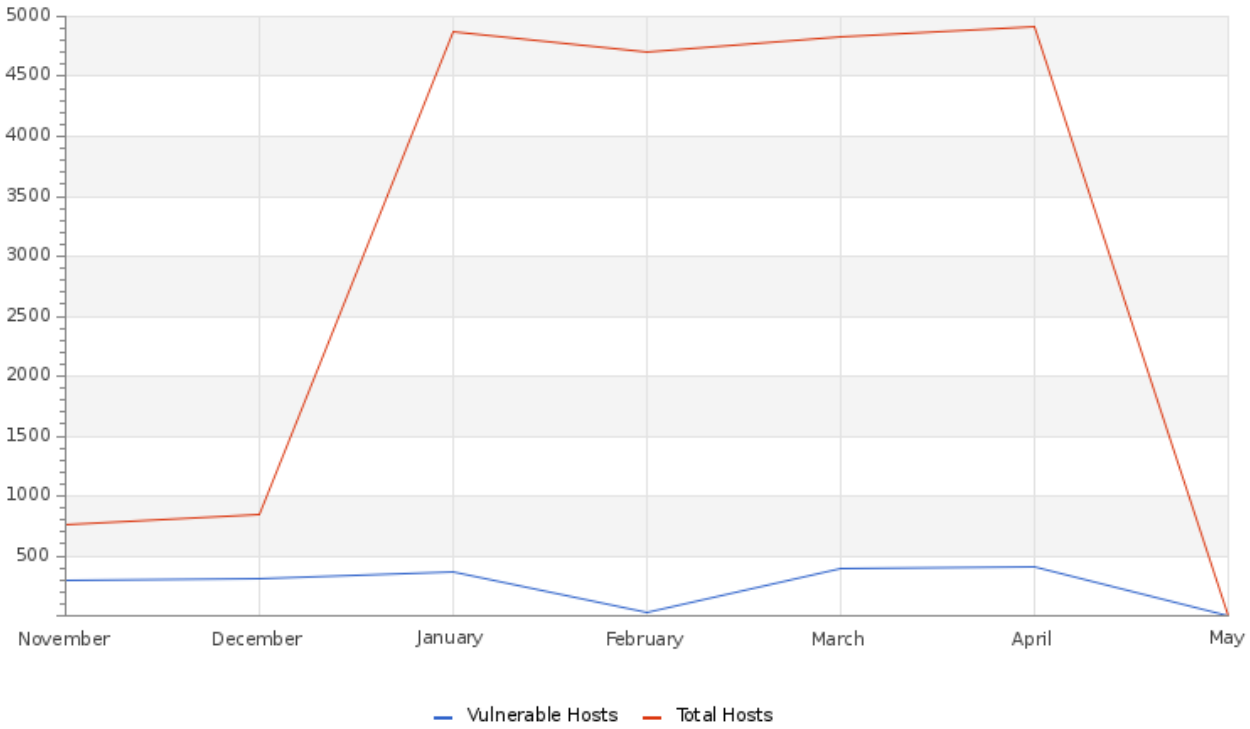
Este informe corresponde "Abril 2024" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, Amenazas, Activos, Cumplimiento, Validación de Ciberseguridad y Acceso.

SOBRE ESTE INFORME

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 indica un aumento constante en el número de hosts totales y hosts vulnerables. Estamos trabajando junto con el cliente para resolver cualquier problema identificado. Para más detalles, visite nuestra plataforma de clientes en [Skywatch Glesec] (https://skywatch.glesec.com), en la sección C&RU, donde encontrará información detallada sobre este evento y las actualizaciones realizadas. Si tiene alguna pregunta, no dude en ponerse en contacto con GLESEC GOC o con el equipo de Servicios Profesionales.

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

BLADEX 06/17/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	925	925
Hosts Discovered	4446	4636
Vulnerable Hosts	355	34
Critical Vulnerabilities Count	146	0
High Vulnerabilities Count	570	20
Medium Vulnerabilities Count	2022	87
Low Vulnerabilities Count	332	45

La tabla presenta una comparación de vulnerabilidad de los últimos dos meses. En el último mes se observa un aumento en el número de hosts vulnerables y en la gravedad de estas vulnerabilidades. Nuestro equipo ha trabajado estrechamente con el cliente para verificar los cambios observados en los Hosts totales y los Hosts vulnerables. En el servicio MSS-BAS también se ha producido un ligero aumento de los valores. Recomendamos revisar la documentación disponible en la plataforma Skywatch sobre estos servicios para fortalecer su seguridad ante nuevas amenazas.

Vulnerability Metric

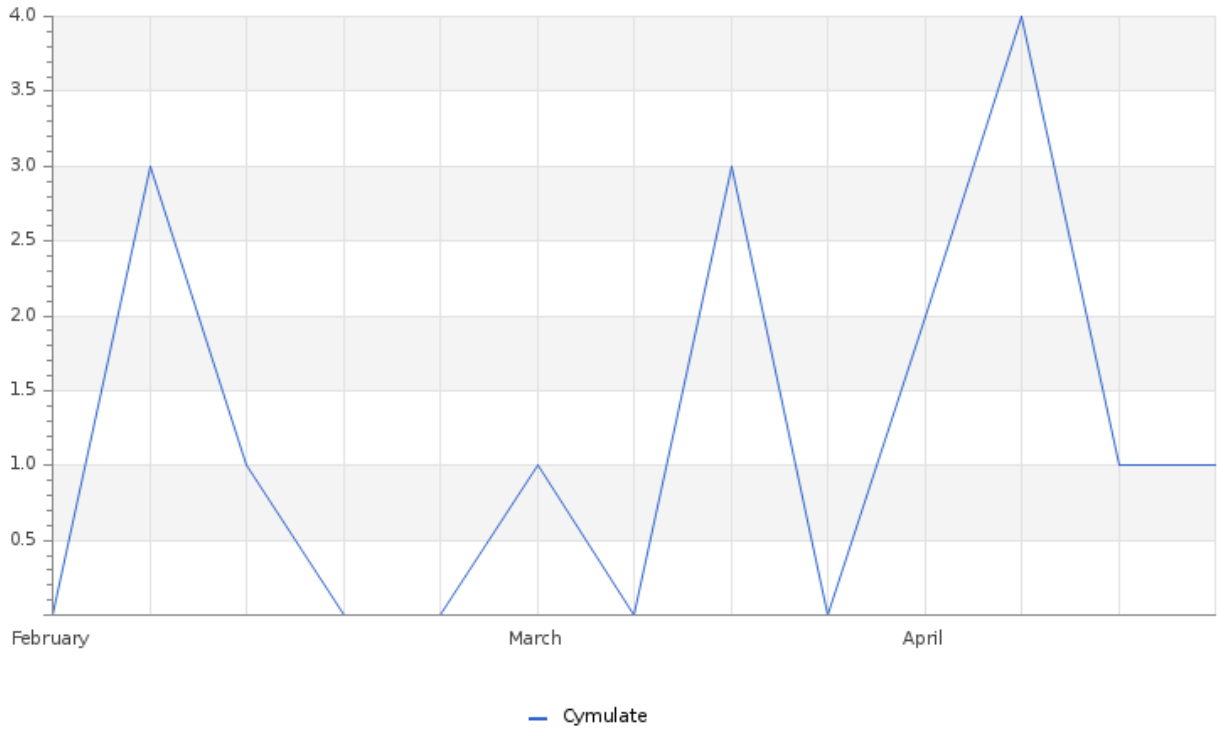
1

Un análisis de 925 hosts según su rango de direcciones reveló que 355 hosts son vulnerables. Estas vulnerabilidades se clasifican por gravedad, como se muestra en la tabla adjunta. Durante este período, registramos 146 vulnerabilidades críticas, 570 de alto riesgo, 2022 de riesgo medio y 332 vulnerabilidades de bajo riesgo. Según estos hallazgos, el índice de vulnerabilidad de su organización se encuentra actualmente en 1%.

THREATS

BLADEX 06/17/2024

Total Number of Successful MFA authentications per application



La gráfica nos permite visualizar la actividad del cliente en las diferentes plataformas a las que tiene acceso. En particular, muestra la actividad en nuestra plataforma Cymulate, que proporciona información relacionada con nuestro servicio MSS-BAS. Esta plataforma nos permite validar controles de ciberseguridad y brinda evaluaciones continuas y detalladas de los distintos casos relacionados con este servicio. En Skywatch podrá encontrar documentación detallada sobre casos, incidentes, informes y otros recursos útiles para fortalecer la seguridad de su empresa.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	4	1
Critical Device Outages	0	0

Durante el mes, nuestro servicio MSS-CSM reportó alertas relacionadas con el rendimiento de la CPU y anomalías en la conexión, las cuales podrían deberse a problemas de congestión de la red. Nuestro equipo documentó estos eventos y se envió un correo electrónico notificando la situación.

Histogram of Total and Critical Device Outages

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

BLADEX 06/17/2024

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
0	0	0	0

Nuestro equipo se encuentra trabajando en la migración del servicio MSS-DLP con el fin de brindarle un mejor servicio, es por esta razón que durante el mes no se generaron alertas para este servicio.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	77
BAS Endpoint Security	9
BAS Web Security	9
BAS WAF	10
Change in High or Critical Vulnerabilities	39
Immediate Threat System Vulnerable and Remediation by Patch Management	2
Change in Systems Performance	1

Para el servicio MSS-BAS se han realizado documentaciones detalladas que le permiten conocer el estado de seguridad de su empresa. Se han abierto casos que conviene tener en cuenta, ya que han logrado burlar más del 50% de sus contramedidas de seguridad.

En cuanto al servicio MSS-VME, seguimos trabajando juntos para atender eventos relacionados con el importante aumento en el número total de hosts. Se recomienda revisar estos casos y aplicar las mitigaciones correspondientes para salvaguardar la seguridad de su empresa.

Para obtener más información, puede acceder a nuestra plataforma de clientes en [Skywatch Glesec](https://skywatch.glesec.com) en la sección C&RU.

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.**

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