TLP:AMBER

CISO EXECUTIVE REPORT

BLADEX

June 24, 2024

BLADEX 06/24/2024

TLP AMBER CISO
EXECUTIVE REPORT

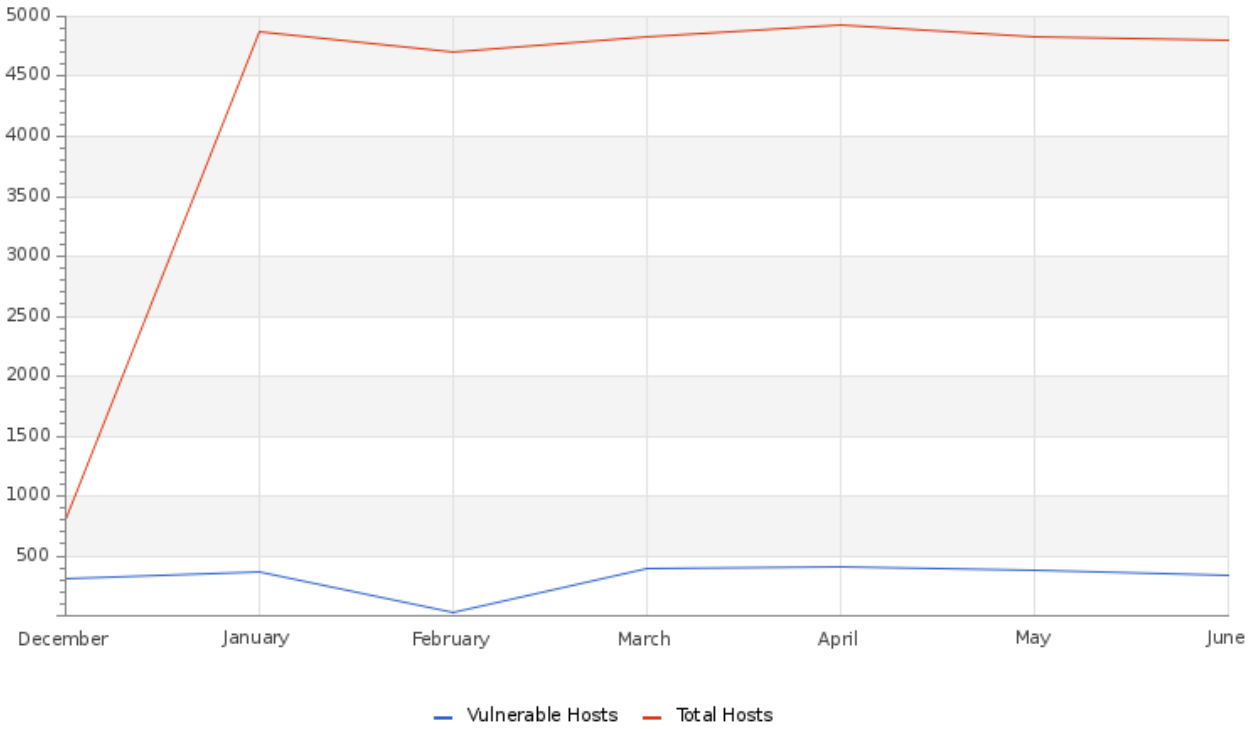
Este informe corresponde a "Mayo 2024" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, 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 leves cambios en los 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 06/24/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	925	925
Hosts Discovered	726	4411
Vulnerable Hosts	327	366
Critical Vulnerabilities Count	100	123
High Vulnerabilities Count	517	491
Medium Vulnerabilities Count	1899	1836
Low Vulnerabilities Count	203	239
Email Gateway Score	6	5
Web Gateway Score	19	18
Endpoint Score	25	24

La tabla presenta una comparación de vulnerabilidad de los últimos dos meses. En el último mes se observa una leve disminución 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 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

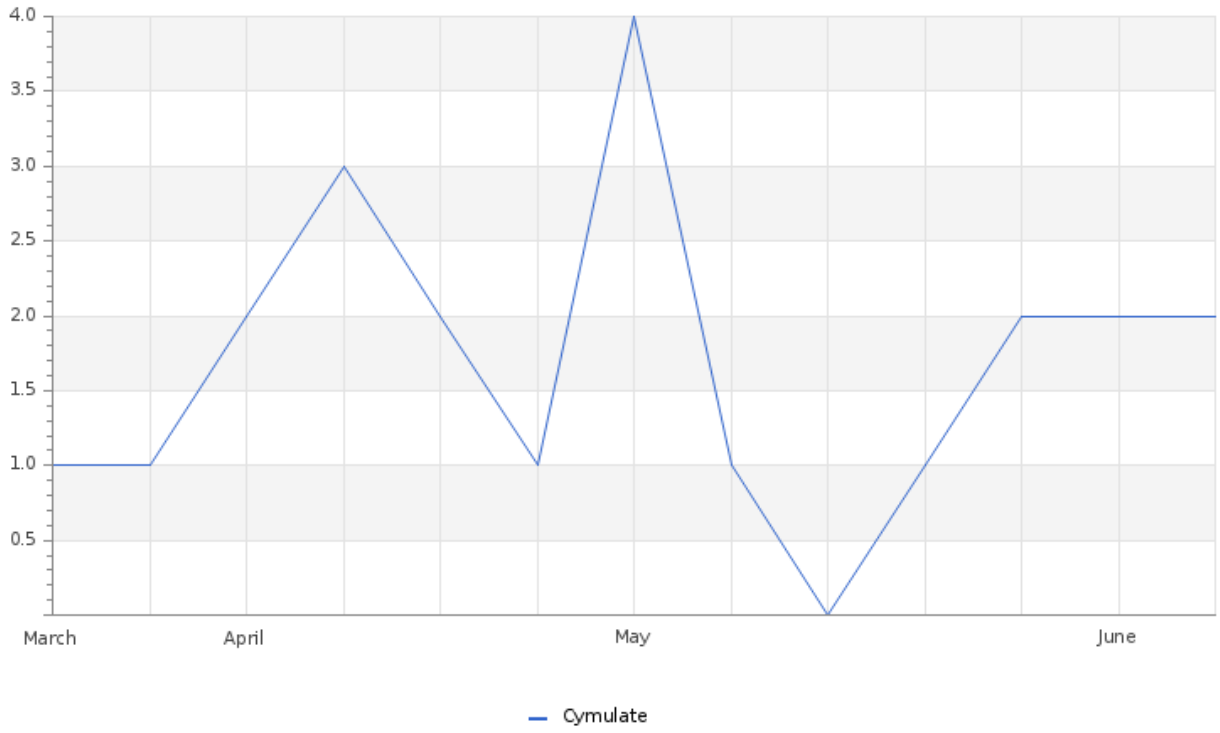
0

Se mantienen casos abiertos del servicio MSS-VM donde se han realizado recomendaciones para abordar y mitigar las diferentes vulnerabilidades que se han identificado en sus sistemas internos y externos previamente. La documentación de las vulnerabilidades se encuentra en la plataforma Skywatch en el apartado de casos (C&RU).

THREATS

BLADEX 06/24/2024

Total Number of Successful MFA authentications per application



La gráfica nos permite visualizar la actividad que ha mantenido el cliente en las diferentes plataformas a las que tiene acceso. La gráfica refleja actividad en nuestra plataforma Cymulate, esta plataforma brinda información relacionada a nuestro servicio MSS-BAS; nos permite validar los controles de ciberseguridad y proporciona evaluaciones continuas las cuales les detallamos en los diversos casos relacionados a este servicio. En Skywatch puede encontrar documentación detallada sobre los casos, incidentes, reportes, etc., que les brindan información útil que permite robustecer la seguridad de su empresa.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	5	2
Critical Device Outages	0	0

Nuestro servicio MSS-CSM durante el mes reportó alertas relacionadas al rendimiento del CPU y alertas de pérdidas de conexiones las cuales se pueden producir debido a problemas de congestión en la red. Nuestro equipo realizó la documentación correspondiente y se envió un correo electrónico notificando el evento.

Histogram of Total and Critical Device Outages

BLADEX 06/24/2024

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	30
BAS Endpoint Security	4
BAS Web Security	4
BAS WAF	4
Change in High or Critical Vulnerabilities	8
Change in Systems Performance	1

Para el servicio MSS-BAS se realizaron documentaciones detalladas que le permiten conocer el estado de la seguridad de su empresa; se han abierto casos que se deben tomar en cuenta ya que estos han logrado eludir un porcentaje mayor al 50% sus contramedidas de seguridad. Para el servicio MSS-VME, se recomienda realizar una revisión de los casos que hemos documentado y aplicar las mitigaciones correspondientes para salvaguardar la seguridad de su empresa. Para más información puede acceder a nuestra plataforma para clientes 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.**

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