



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

BLADEX

March 13, 2024



BLADEx 03/13/2024

TLP AMBER CISO EXECUTIVE REPORT

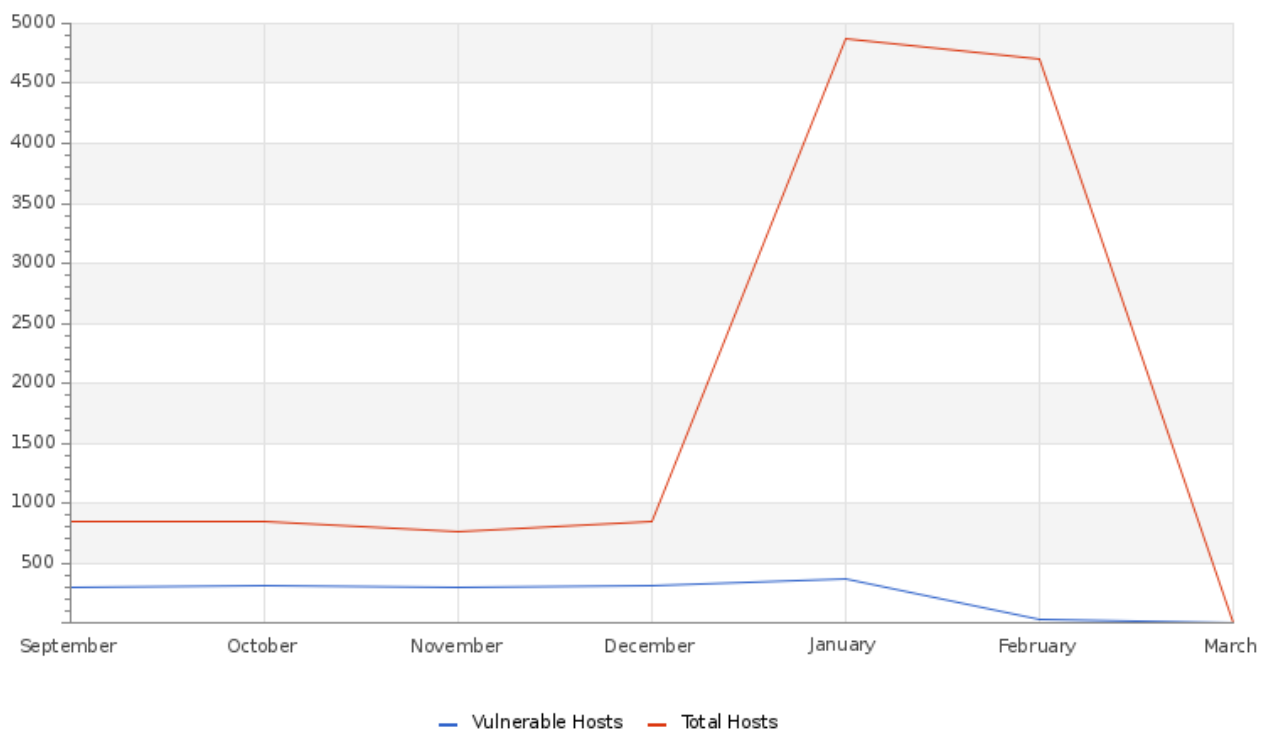
Este informe corresponde "EDIT MONTH" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades,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



La gráfica refleja la persistencia en el aumento de Total Hosts y la disminución en las vulnerabilidades que estos tienen. Nuestro equipo en conjunto con el cliente se encuentra trabajando para corregir cualquier inconveniente presentado. Para más información puede acceder a nuestra plataforma para clientes <https://skywatch.glesec.com> en la sección C&RU donde detallamos este evento y las actualizaciones que se han realizado a partir del mismo.



BLADEx 03/13/2024

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	898	898
Hosts Discovered	4646	4667
Vulnerable Hosts	0	20
Critical Vulnerabilities Count	0	0
High Vulnerabilities Count	0	10
Medium Vulnerabilities Count	0	56
Low Vulnerabilities Count	0	12
Phishing Score	0	0
Email Gateway Score	6	6
Web Application Firewall Score	34	35
Web Gateway Score	21	21
Endpoint Score	25	34
Hopper Score	17	17
DLP Score	100	100

En la tabla podemos observar una comparación de vulnerabilidad correspondiente a los dos últimos meses, para el último mes podemos observar una gran disminución en cuanto a los host vulnerables y las vulnerabilidades presentes en estos, nuestro equipo ha trabajado en conjunto con el cliente para verificar los cambios observados en el Total Hosts y Vulnerable Hosts. Para el servicio MSS-BAS podemos observar que sus valores se mantienen sin variaciones significativas a lo largo del mes, recomendamos revisar la documentación suministrada en la plataforma Skywatch sobre estos servicios para robustecer su seguridad frente a nuevas amenazas.

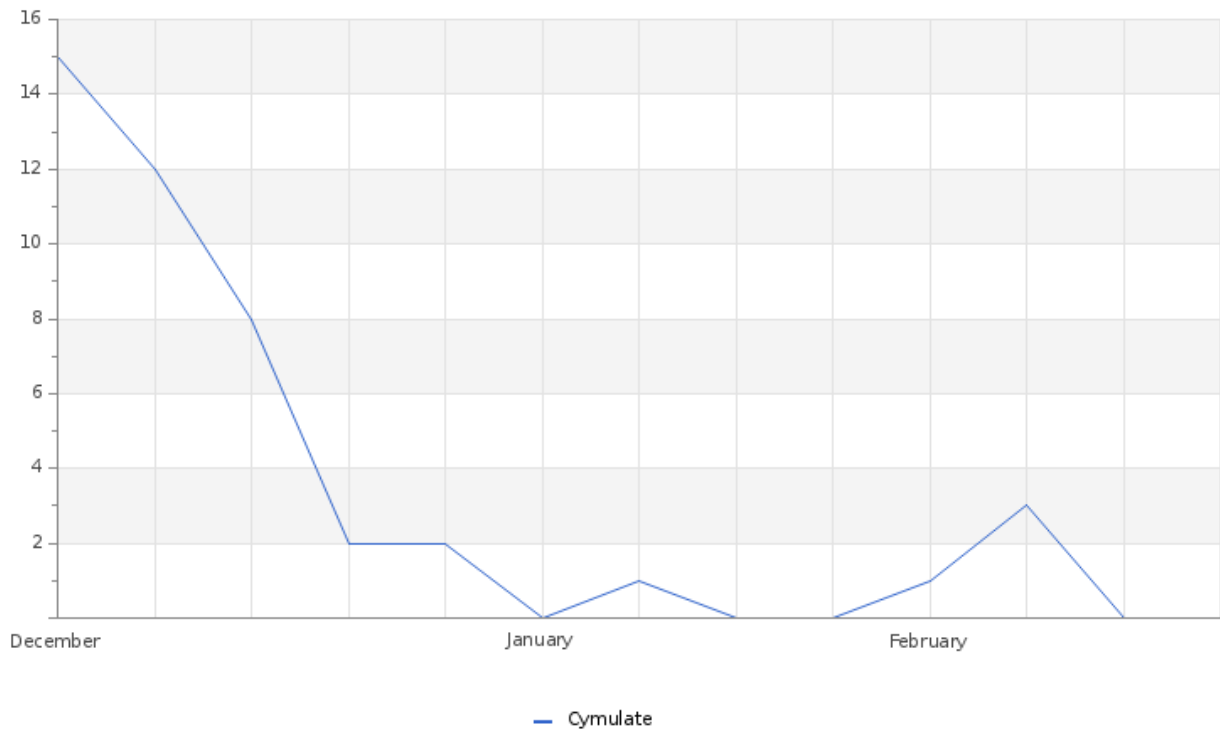
Vulnerability Metric**0**

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 03/13/2024

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. 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. En Cymulate podrá encontrar información relacionada a nuestro servicio MSS-BAS; esta plataforma nos permite validar los controles de ciberseguridad y proporciona evaluaciones continuas las cuales les detallamos en los diversos casos relacionados a este servicio.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	5	1
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.



BLADEX 03/13/2024

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	31
BAS Endpoint Security	1
BAS Web Security	6
BAS WAF	4
Change in Systems Availability	1
Non Baselined Discovered System	29

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 le ha proporcionado información valiosa sobre el aumento significativo de los Total Hosts, seguimos trabajando para solucionar en conjunto este evento.

Se recomienda realizar una revisión de estos casos y aplicar las mitigaciones correspondientes. 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.**





GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

