



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

BLADEX

July 26, 2023



BLADEx 07/26/2023

TLP AMBER CISO EXECUTIVE REPORT

Este informe corresponde al mes de junio 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.

RISK

Actual Risk

n/a

Accepted Risk

n/a

Confidence**Low**

Accepted & Actual Risk

Actualmente Bladex no cumple con los requisitos necesarios para calcular el riesgo.

Table of Comparison of Actual and Acceptable Risk From Current to Previous Month

	Current Month	Previous Month
Actual Risk		
Accepted Risk	0	0

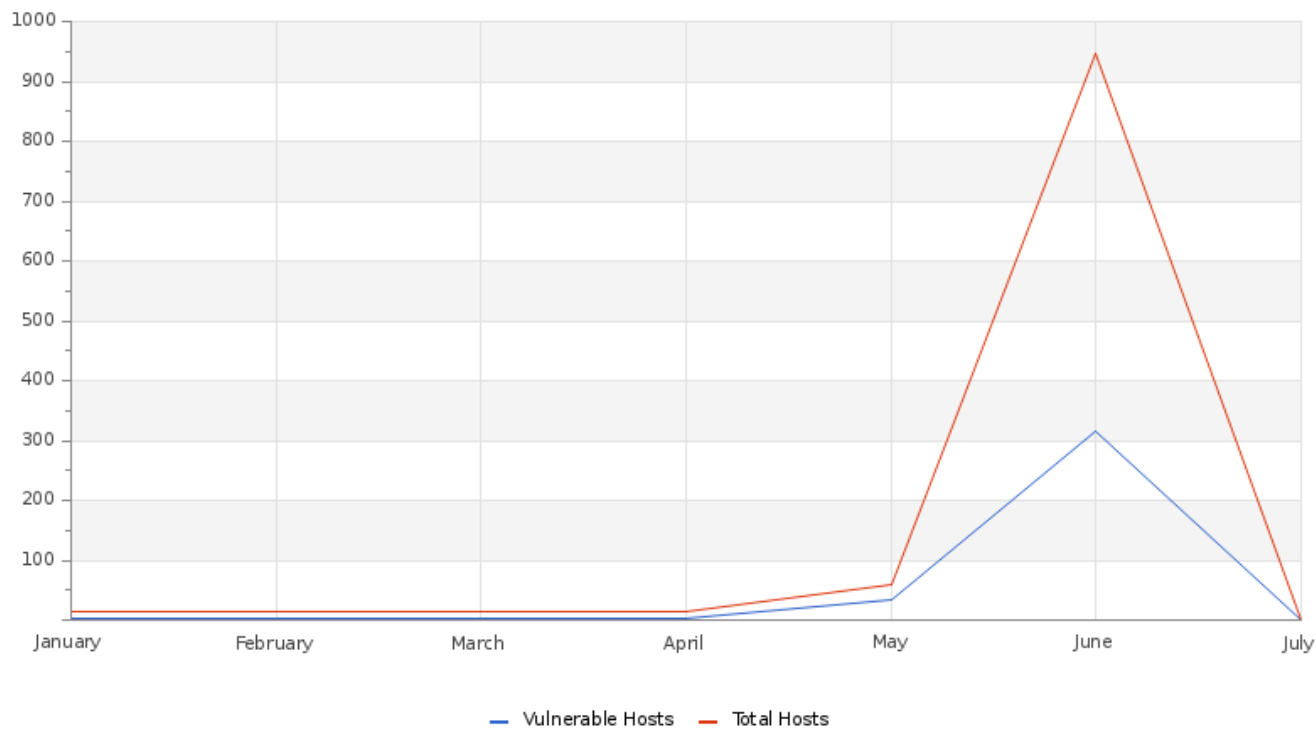
Actualmente Bladex no cumple con los requisitos necesarios para calcular el riesgo.

VULNERABILITY



BLADEX 07/26/2023

Hosts & Vulnerable Hosts In Last 6 Months



El pico registrado durante este mes se debe a la activación del servicio MSS-VM para el escaneo de vulnerabilidades internas. Por ello también se registra un incremento en los hosts que son vulnerables.



BLADEX 07/26/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	898	62
Hosts Discovered	811	16
Vulnerable Hosts	311	4
Critical Vulnerabilities Count	131	0
High Vulnerabilities Count	412	0
Medium Vulnerabilities Count	1414	12
Low Vulnerabilities Count	274	4
Phishing Score	0	0
Email Gateway Score	6	7
Web Application Firewall Score	0	0
Web Gateway Score	16	14
Endpoint Score	33	34
Hopper Score	17	17
DLP Score	100	100

En la siguiente tabla se muestra la comparación entre en mes anterior y el actual, donde se puede observar un incremento significativo en la cantidad de host. Además podemos observar la severidad de las vulnerabilidades que se han descubierto en los hosts y las últimas puntuaciones obtenidas producto de las simulaciones realizadas.

Vulnerability Metric**6**

Se han realizado recomendaciones para abordar y mitigar las diferentes vulnerabilidades que se han identificado en sus sistemas internos y externos. La documentación de las vulnerabilidades se encuentran en la plataforma skywatch.

THREATS**Total and Critical Attacks Successfully Blocked by Security Layer and Department**

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
0	0	43	0

Durante el mes nuestro servicio de MSS-DLP registro un total de 43 acciones realizadas por usuarios dentro de la empresa. Estas acciones fueron reportadas y pueden ser visualizarlas en nuestra plataforma de Skywatch.

BLADEX 07/26/2023

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Abnormal activity in the file system(s)	127
BAS Immediate Threat	29
Change in High or Critical Vulnerabilities	56
Change in Systems Performance	1
Change in Baseline Systems Discovered	1
BAS Web Security	6

Durante el mes se abrieron casos de actividades anormales detectadas por nuestro servicio MSS-DLP, también se documentaron casos del servicio MSS-BAS, se recomienda realizar una revisión de estos casos y aplicar las mitigaciones correspondiente, ya que la mayor parte de estos corresponden a casos de amenazas inmediatas cuyo objetivo es determinar al resiliencia de su sistemas ante las amenazas emergentes. Para mas 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.**





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.

