TLP:AMBER

CISO EXECUTIVE REPORT

BLADEX

August 20, 2023

BLADEX 08/20/2023

TLP AMBER CISO
EXECUTIVE REPORT

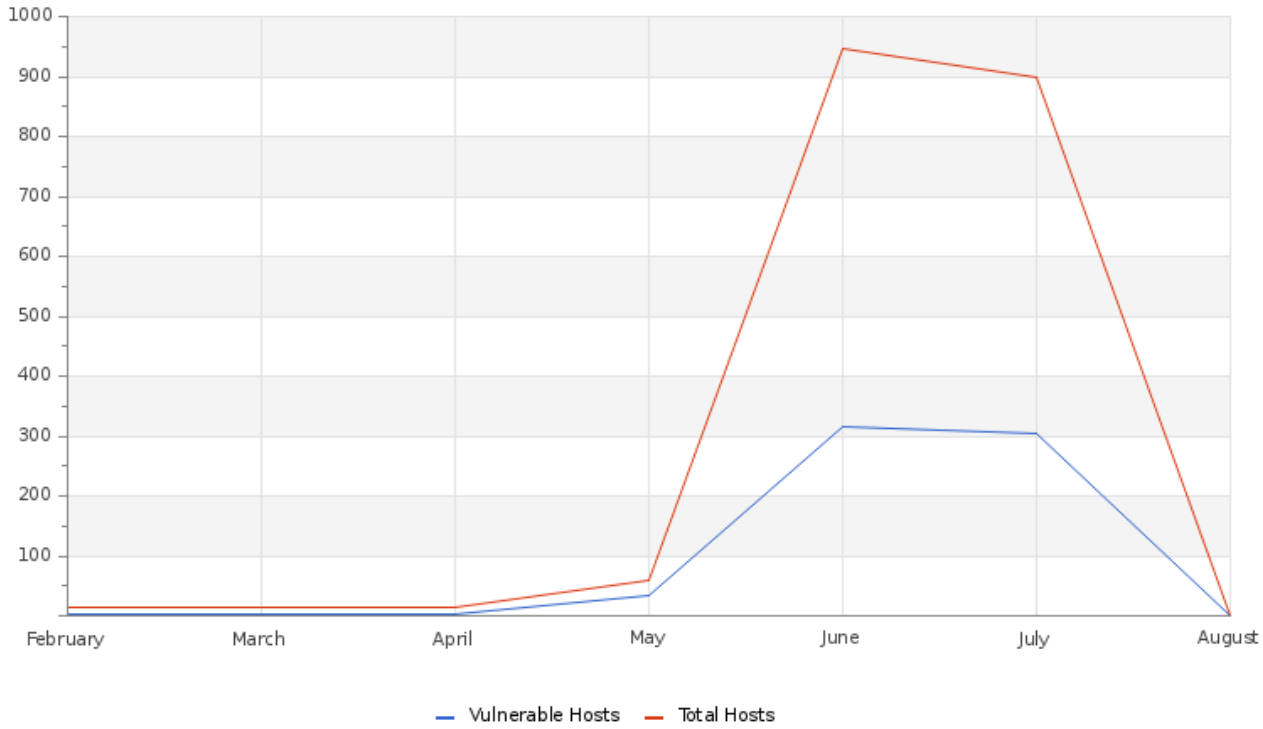
Este informe corresponde julio y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, 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 muestra que los sistemas mantienen vulnerabilidades durante los últimos meses; estás vulnerabilidades mayormente se tratan de software que presentan desactualizaciones las cuales requieren atención. Todas las vulnerabilidades identificadas se encuentran documentadas en nuestra plataforma Skywatch en el apartado de casos (C&RU).

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

BLADEX 08/20/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	898	898
Hosts Discovered	720	803
Vulnerable Hosts	7	311
Critical Vulnerabilities Count	0	131
High Vulnerabilities Count	1	412
Medium Vulnerabilities Count	20	1414
Low Vulnerabilities Count	6	274
Phishing Score	0	0
Email Gateway Score	6	6
Web Application Firewall Score	0	0
Web Gateway Score	17	16
Endpoint Score	36	33
Hopper Score	17	17
DLP Score	100	100

En la tabla podemos observar la comparación entre el mes anterior y el mes actual, donde se muestra la severidad de las vulnerabilidades que se han descubierto en los hosts y las últimas puntuaciones obtenidas las cuales reflejan un decremento en comparación con el mes previo. Para el servicio MSS-BAS podemos observar un incremento en los vectores Web Gateway y Endpoint(EDR), recomendamos revisar la documentación suministrada en la plataforma Skywatch sobre estos servicios para robustecer su seguridad frente a nuevas amenazas.

Vulnerability Metric

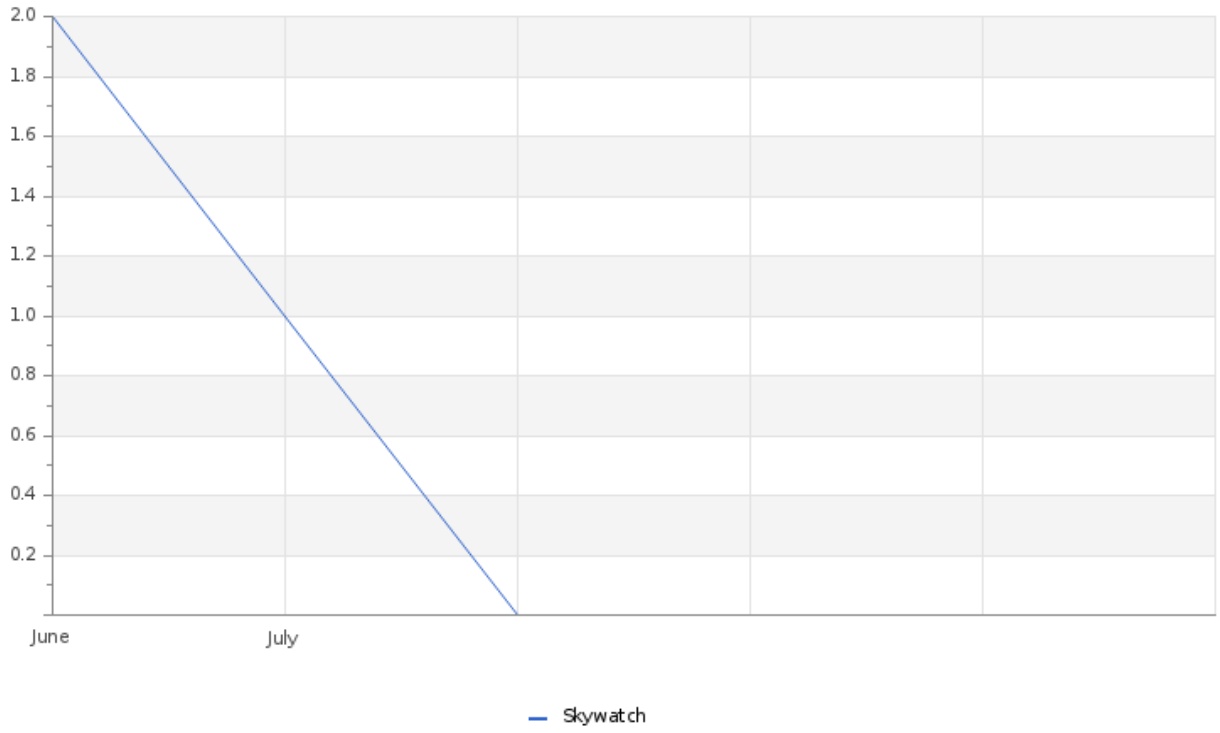
8

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 encuentra en la plataforma Skywatch en el apartado de casos.

THREATS

BLADEX 08/20/2023

Total Number of Successful MFA authentications per application



En la gráfica podemos observar un decremento en la actividad por parte de los usuarios en la plataforma Skywatch en comparación con el mes previo. En la plataforma 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 Down Devices	6	2
Critical Down Devices	0	0

Recibimos alerta relacionadas al rendimiento del CPU, no hubo sistemas en estado Down.

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
0	0	29	0

El servicio MSS-DLP continuamente recibe alertas sobre AccessDenied y DeletePath, los cuales han sido documentados por nuestro SOC y notificado al área correspondiente de Bladex para su verificación.

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

BLADEX 08/20/2023

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Baseline Systems Discovered	1
BAS Web Security	8
Abnormal activity in the file system(s)	113
Change in High or Critical Vulnerabilities	12
BAS Immediate Threat	39
BAS Endpoint Security	1

En el transcurso del mes se presentaron casos de actividad que deben ser verificados los cuales fueron detectados por nuestro servicio MSS-DLP y documentado por nuestro SOC, de igual forma para el servicio MSS-BAS se realizaron documentaciones detalladas que le permiten conocer el estado de la seguridad de empresa; El servicio MSS-VME cuenta con su documentación correspondiente donde le brindamos la descripción de las vulnerabilidades presentes y las remediaciones que puede implementar. 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.**

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