TLP:AMBER

CISO EXECUTIVE REPORT

BLADEX

September 21, 2023

BLADEX 09/21/2023

TLP AMBER CISO
EXECUTIVE REPORT

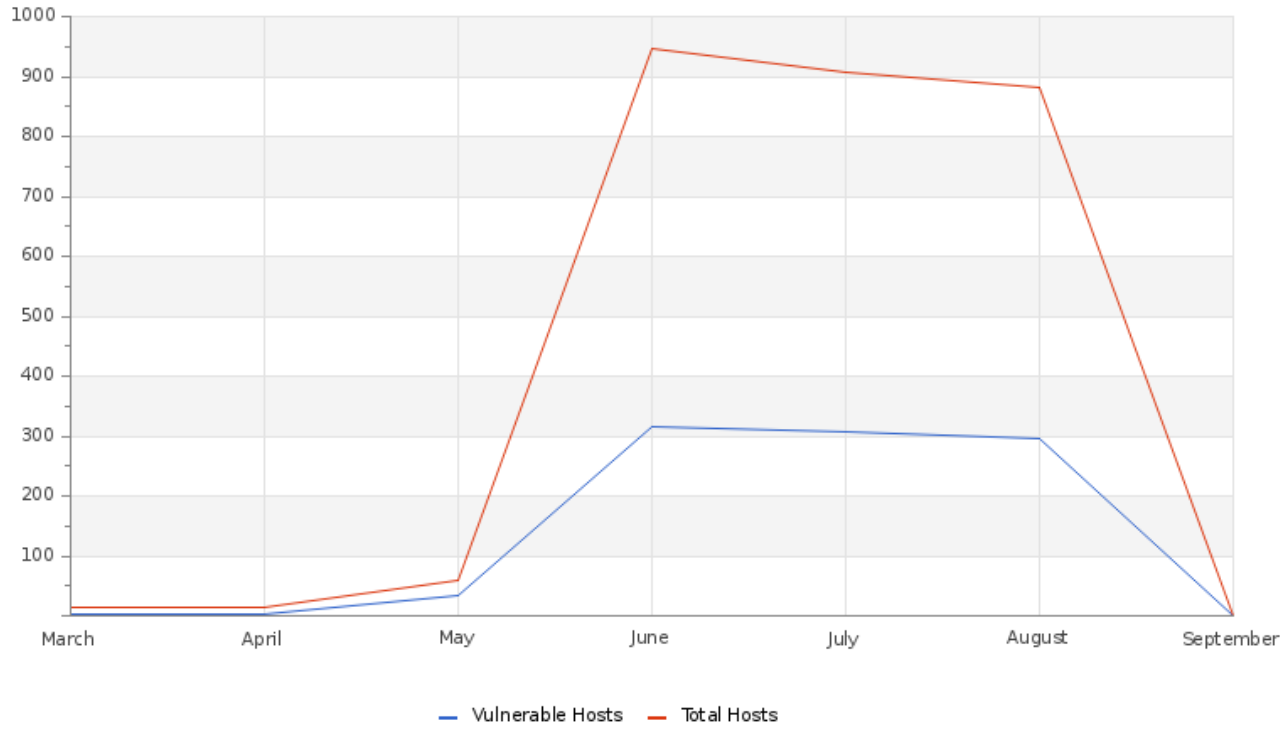
Este informe corresponde Agosto y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, 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 de vulnerabilidades en los sistemas a lo largo de los últimos meses; estas vulnerabilidades mayormente están relacionadas a desactualizaciones de sus diversos software. Todas las vulnerabilidades que han sido identificadas por nuestro SOC, han sido documentadas indicando el tipo de vulnerabilidades y la remediación, podrá visualizarla en nuestra plataforma Skywatch en el apartado de casos (C&RU).

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

BLADEX 09/21/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	898	898
Hosts Discovered	761	769
Vulnerable Hosts	293	285
Critical Vulnerabilities Count	133	124
High Vulnerabilities Count	413	380
Medium Vulnerabilities Count	1346	1282
Low Vulnerabilities Count	258	259
Phishing Score	0	0
Email Gateway Score	6	6
Web Application Firewall Score	0	0
Web Gateway Score	18	17
Endpoint Score	36	36
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 ésta ha ido en aumento debido a vulnerabilidades de secuencia por desactualizaciones, se recomienda actualizar a las versiones más recientes para disminuir esta alza. Para el servicio MSS-BAS podemos observar un incremento en el vector Web Gateway, recomendamos revisar la documentación suministrada en la plataforma Skywatch sobre estos servicios para robustecer su seguridad frente a nuevas amenazas.

Vulnerability Metric

9

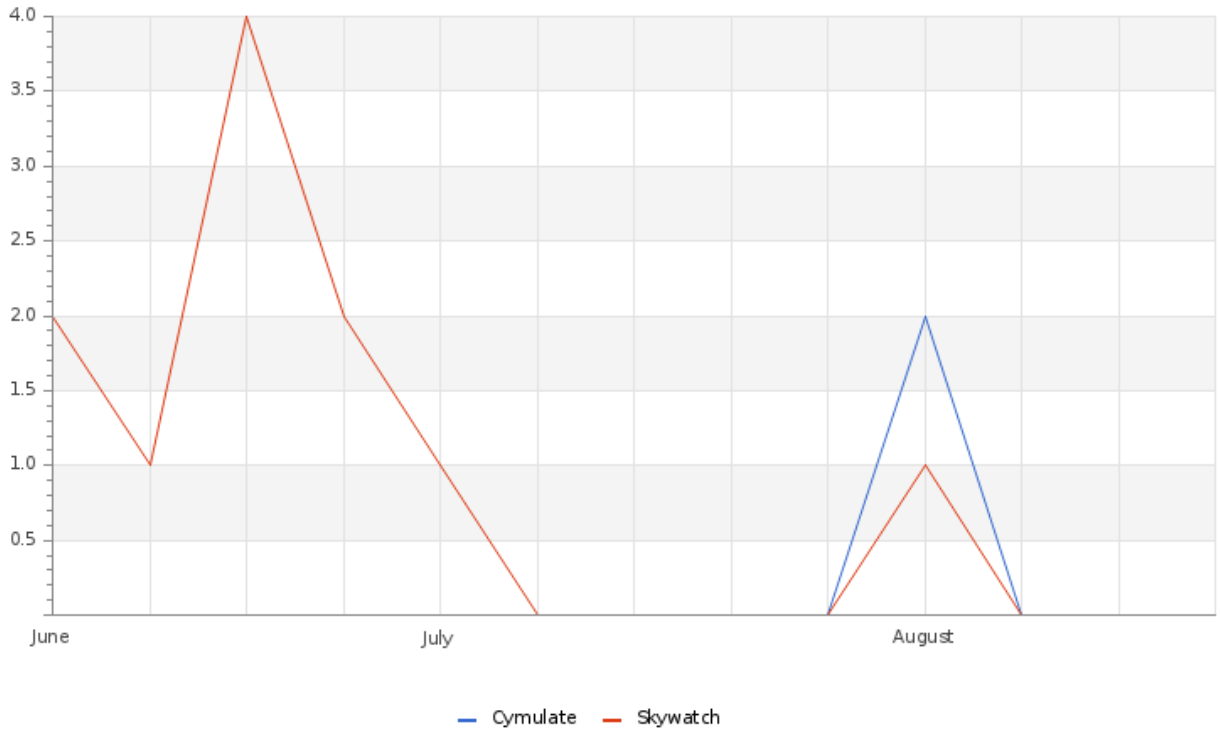
Se han realizado recomendaciones para abordar y mitigar las diferentes vulnerabilidades que se han identificado en sus sistemas internos y externos. La documentación de las vulnerabilidades se encuentra en la plataforma Skywatch en el apartado de casos.

THREATS

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

BLADEX 09/21/2023

Total Number of Successful MFA authentications per application



En la gráfica podemos observar que hubo actividad por parte de los usuarios en la plataforma Skywatch en comparación con el mes previo, esto se debe a configuraciones en la cuenta con SSO. La nueva barra reflejada en la gráfica se debe a la implementación de acceso de los usuarios a Cymulate y la actividad que han registrado en la plataforma. 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 Down Devices	3	5
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	39	0

Durante el transcurso del mes, el servicio MSS-DLP ha recibido alertas sobre AccessDenied y DeletePath, las mismas han sido documentadas por nuestro SOC y notificadas al área correspondiente de Bladex para su verificación.

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

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	40
Abnormal activity in the file system(s)	90
Change in High or Critical Vulnerabilities	4
BAS Endpoint Security	3
BAS Web Security	3
Non Baselined Discovered System	16

Para el servicio MSS-BAS se realizaron documentaciones detalladas que le permiten conocer el estado de la seguridad de su empresa; relacionado a los servicios de MSS-BAS-IMTHREAT, se crearon reportes de incidentes donde detallan la correlación entre diversos casos generados por este servicio, la información detallada la puede encontrar en Skywatch-Report-Incident Report; 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.**

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