TLP:AMBER

CISO EXECUTIVE REPORT

BLADEX

October 17, 2023

BLADEX 10/17/2023

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde "Septiembre" 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

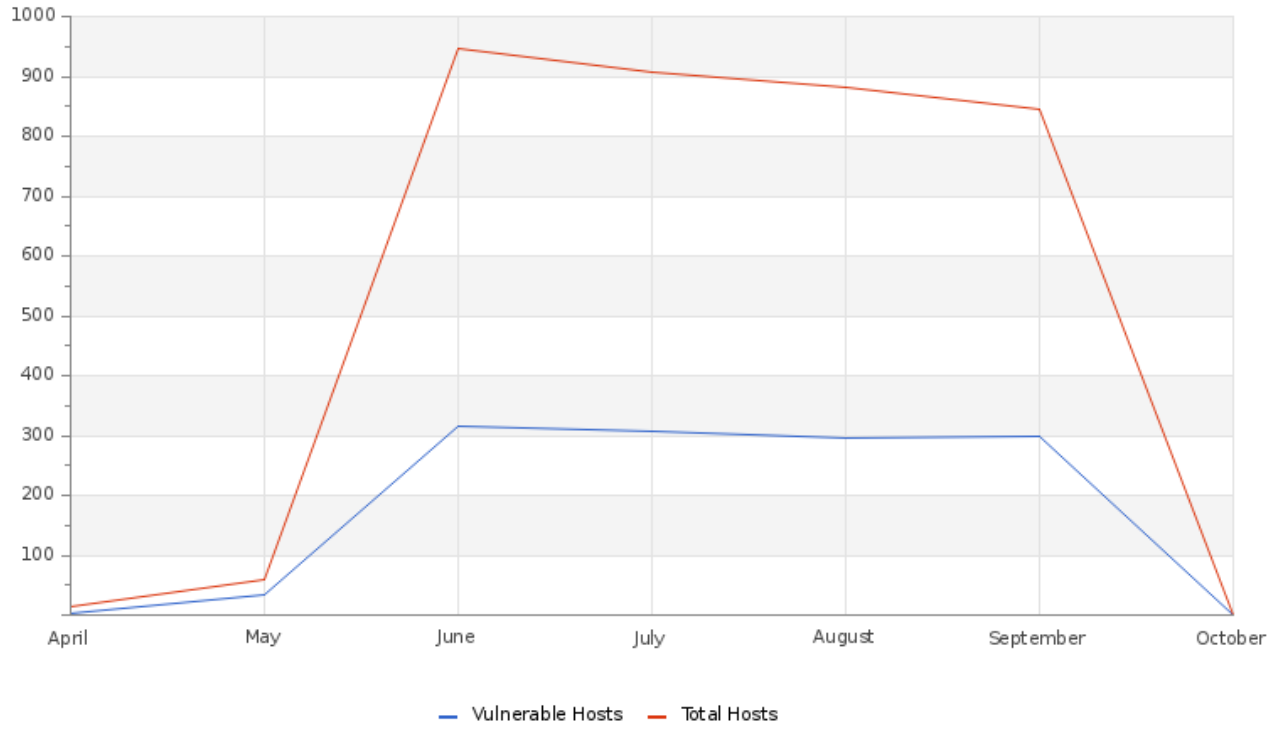
El propósito de este documento es informar sobre el estado de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

VULNERABILITY

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

BLADEX 10/17/2023

Hosts & Vulnerable Hosts In Last 6 Months



La gráfica refleja la persistencia de vulnerabilidades en los sistemas a lo largo de los últimos meses; Los casos mayormente están relacionados a dispositivos que mantienen versiones inferiores a las más recientes y esto provoca vulnerabilidad en los dispositivos porque no se logra corregir aquellos inconvenientes que surgen en las versiones anteriores y que se mitigan con las nuevas. 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 10/17/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	898	898
Hosts Discovered	742	774
Vulnerable Hosts	296	293
Critical Vulnerabilities Count	121	116
High Vulnerabilities Count	405	395
Medium Vulnerabilities Count	1354	1320
Low Vulnerabilities Count	259	257
Phishing Score	0	0
Email Gateway Score	7	6
Web Application Firewall Score	0	0
Web Gateway Score	18	18
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; para el caso del servicio MSS-VM/VME podemos observar el aumento de vulnerabilidades en las diversas severidades donde 5 host han pasado a estado “critical”, 10 host a estado “high”, 34 host a estado “medium” y 2 host han aumentado en el estado “low”. Para el servicio MSS-BAS, los valores en comparación con el mes previo se han mantenido. Recomendamos revisar la documentación suministrada en la plataforma Skywatch sobre estos servicios para robustecer su seguridad frente a nuevas amenazas.

Vulnerability Metric

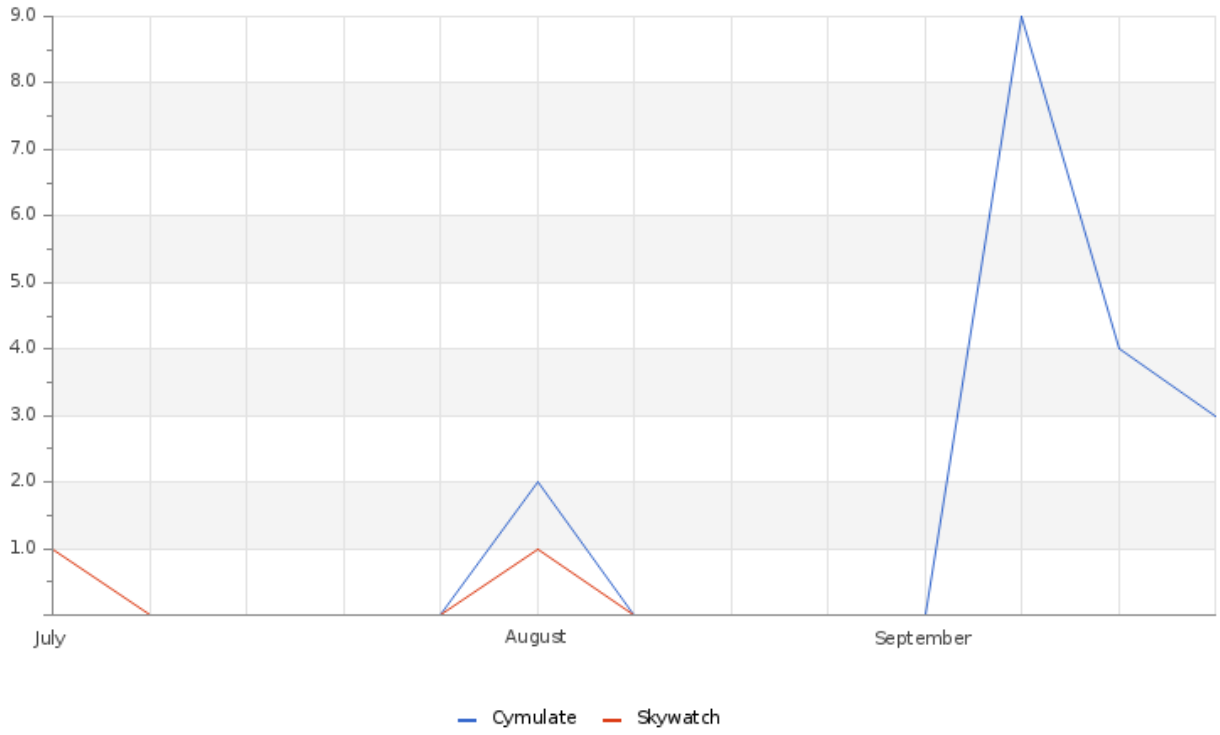
9

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 (C&RU).

THREATS

BLADEX 10/17/2023

Total Number of Successful MFA authentications per application



En la gráfica se puede observar que para este mes ha habido gran actividad por parte del cliente para la plataforma Cymulate. 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	3
Critical Down Devices	0	0

Para el servicio MSS-CSM, durante el mes recibimos alertas relacionadas con el rendimiento del CPU y no hubo sistemas que pasaran a un estado de inactividad.

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
0	0	47	0

En el transcurso del mes, nuestro SOC ha recibido diversas alertas relacionadas con el servicio MSS-DLP, estas alertas consisten en AccessDenied y DeletePath, las mismas han sido documentadas y notificadas al cliente. Recomendamos verificar que los usuarios que acceden a el servidor protegido por el servicio MSS-DLP son autorizados.

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Abnormal activity in the file system(s)	72
BAS Immediate Threat	31
BAS Endpoint Security	6
BAS Web Security	8
Non Baselined Discovered System	32
Change in High or Critical Vulnerabilities	3

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 eludido al 50% sus contramedidas de seguridad. 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