



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

BLADEX

November 21, 2023



BLADEX 11/21/2023

TLP AMBER CISO EXECUTIVE REPORT

Este informe corresponde "Octubre" 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.

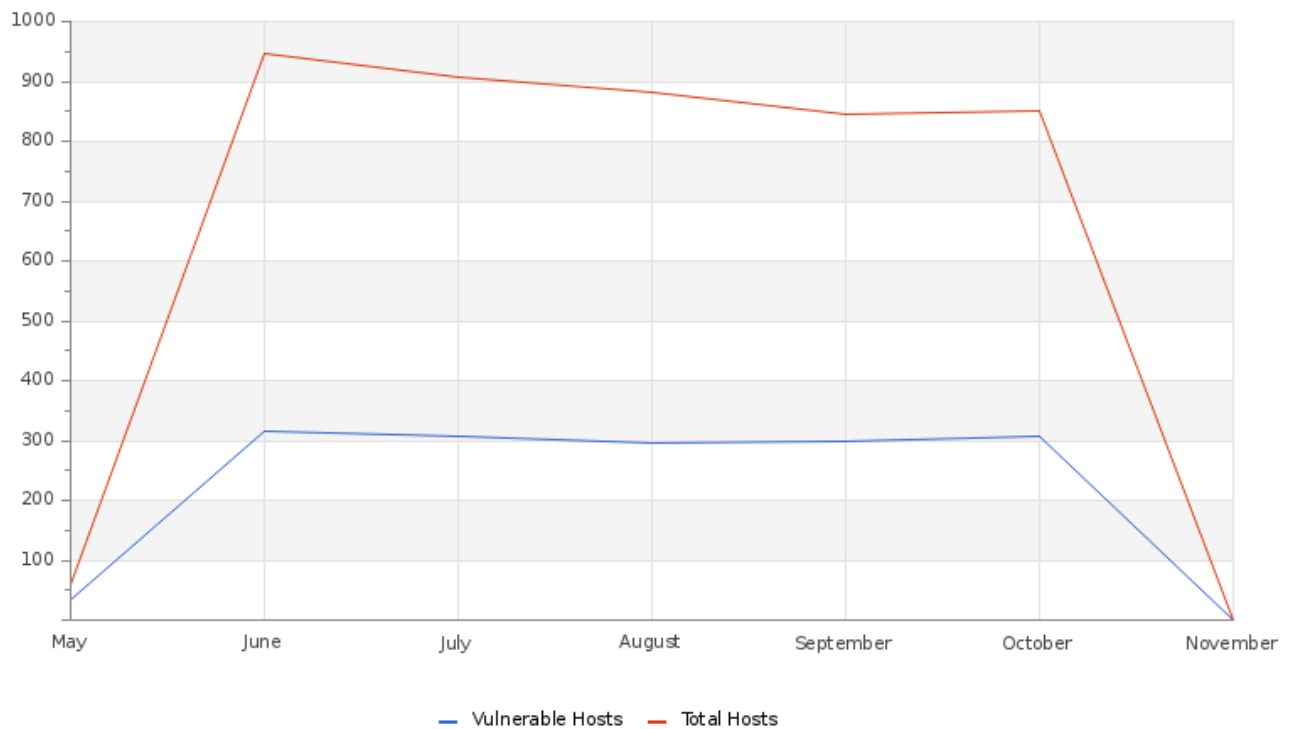
SOBRE ESTE INFORME

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



BLADEX 11/21/2023

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).

BLADEX 11/21/2023

Total Vulnerability Counts In Current & Previous Month

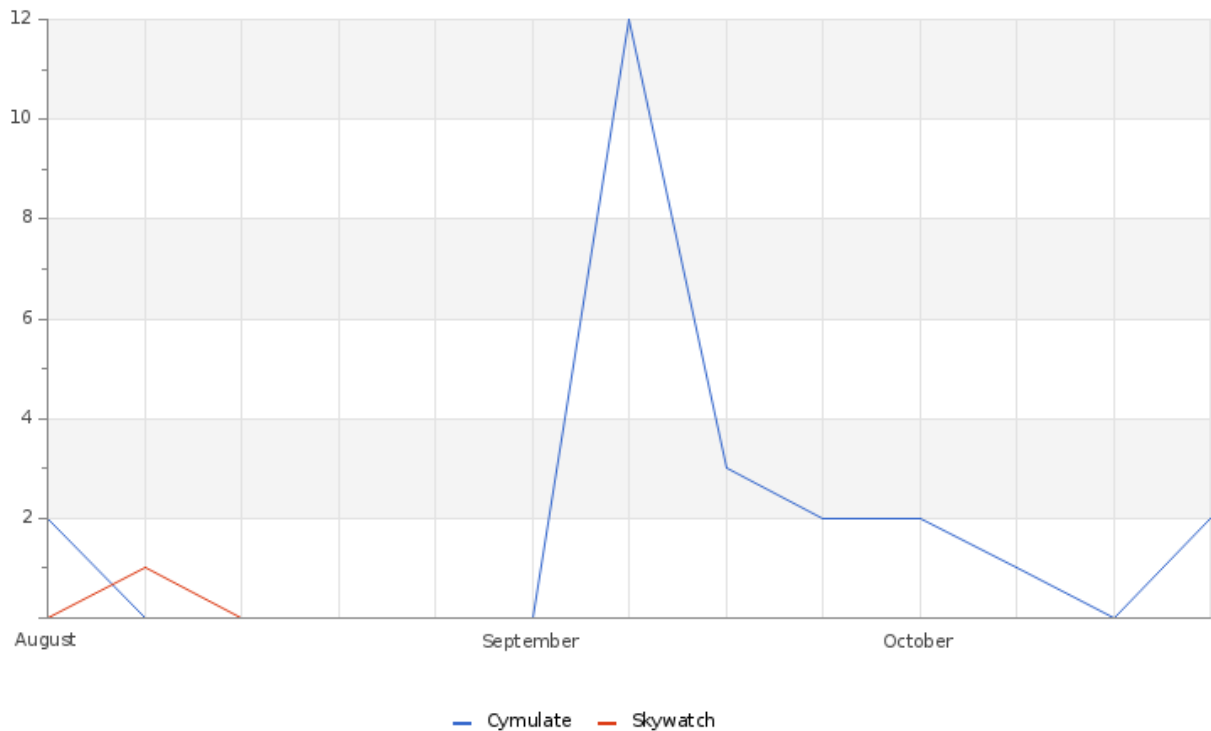
	Current Month	Previous Month
Hosts Baselined	898	898
Hosts Discovered	32	742
Vulnerable Hosts	19	296
Critical Vulnerabilities Count	5	121
High Vulnerabilities Count	17	405
Medium Vulnerabilities Count	114	1354
Low Vulnerabilities Count	9	259
Phishing Score	0	0
Email Gateway Score	7	7
Web Application Firewall Score	0	0
Web Gateway Score	20	18
Endpoint Score	36	36
Hopper Score	17	17
DLP Score	100	100

Vulnerability Metric**10**

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 11/21/2023

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. Durante el mes de octubre se observó actividad en las plataformas Skywatch con un total de 11 accesos exitosos y 6 correspondientes a 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. 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 Down Devices	4	1
Critical Down Devices	0	0

Nuestro servicio MSS-CSM durante el mes reportó alertas relacionadas al rendimiento del CPU, adicional a esto, no hubo sistemas que pasaran a un estado de inactividad.



BLADEX 11/21/2023

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
0	0	41	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 al 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)	88
BAS Immediate Threat	63
Change in High or Critical Vulnerabilities	9
BAS Endpoint Security	7
BAS Web Security	12
Change in Baseline Systems Discovered	68

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. 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.

Los cambios en el sistema reflejados en la tabla se deben a la actualización correspondiente al apartado de impacto para los servidores notificados.

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.

