



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

BLADEX
March 13, 2026



BLADEX 03/13/2026

TLP AMBER BOARDROOM EXECUTIVE REPORT

Este informe corresponde "EDIT MONTH" 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.

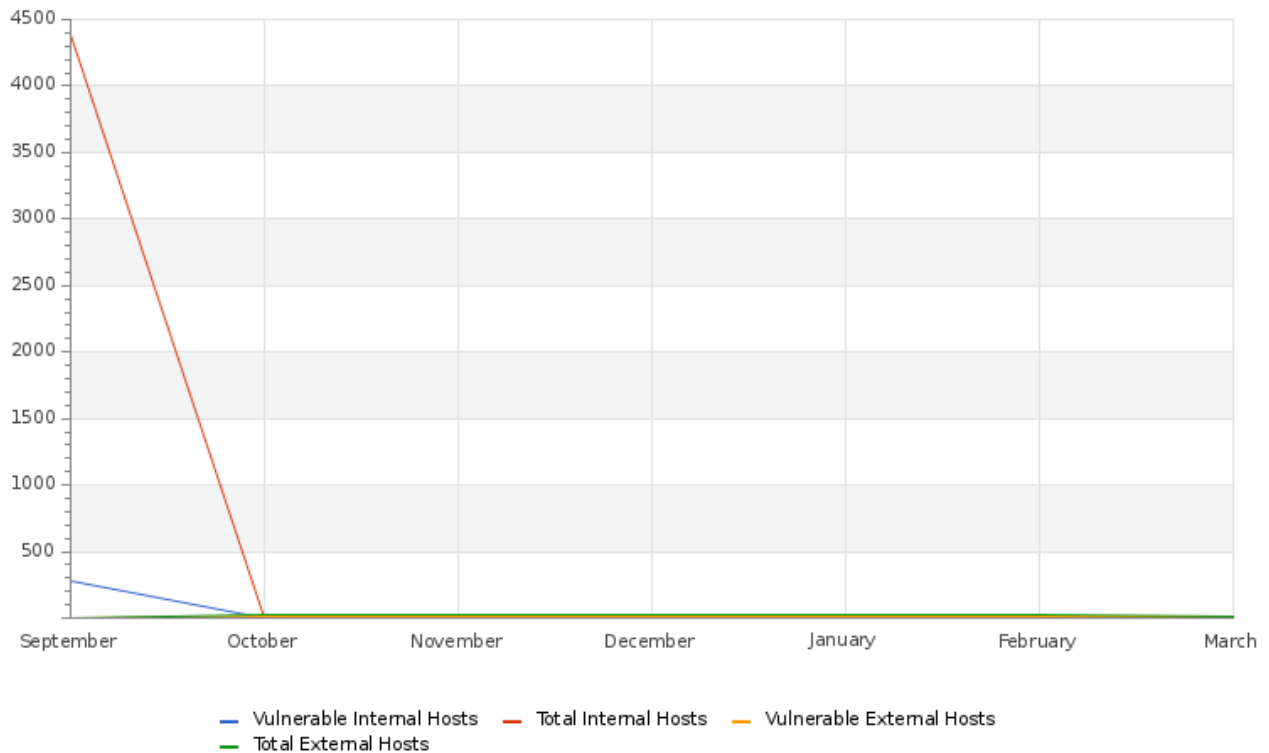
SOBRE ESTE INFORME

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.



BLADEX 03/13/2026

Hosts & Vulnerable Hosts In Last 6 Months



Durante el mes de febrero se identificaron 18 hosts externos, lo que representa una variación leve en comparación con meses anteriores, donde el promedio se mantenía alrededor de 17 hosts externos, alcanzando incluso 19 hosts durante los meses de octubre y noviembre.

Esta variación refleja un comportamiento relativamente estable en la cantidad de activos externos detectados y evaluados durante el período analizado manteniéndose dentro de un rango similar al observado en meses previos.

En términos generales, los resultados muestran que la superficie de exposición externa se mantiene consistente, sin cambios significativos en la cantidad de activos visibles desde el exterior. No obstante, se continúa con el monitoreo periódico de estos activos con el fin de identificar oportunamente cualquier incremento o reducción relevante en la infraestructura expuesta.

Total Attacks Successfully Blocked

0

El análisis de los eventos de seguridad registrados durante el mes de febrero evidencia que no se identificaron ataques que hayan requerido ser bloqueados por los controles de seguridad implementados. Este comportamiento sugiere que durante el período evaluado no se detectaron intentos de explotación dirigidos a la infraestructura monitoreada.

BLADEX 03/13/2026

Critical Attacks Successfully Blocked

0

El análisis de los eventos de seguridad clasificados como críticos durante el mes de febrero evidencia que no se registraron ataques de severidad crítica que hayan requerido acciones de bloqueo.

Vulnerability Metric

2

El análisis del Vulnerability Metric registrado en la organización durante el mes de febrero presenta una ponderación de 2, lo que corresponde a un nivel de riesgo bajo dentro del entorno evaluado. Este resultado se encuentra asociado a la identificación de 11 hosts vulnerables durante el período analizado.

En comparación con enero donde se registraron 12 hosts vulnerables, se observa una ligera disminución en la cantidad de activos con vulnerabilidades detectadas. Este comportamiento refleja una leve mejora en la gestión de vulnerabilidades, manteniendo el nivel de riesgo dentro de un rango bajo.

Aun así la presencia de estos hosts vulnerables resalta la importancia de continuar con las acciones de seguimiento y remediación, así como mantener un monitoreo constante del entorno con el objetivo de reducir progresivamente la superficie de exposición y fortalecer la postura de seguridad de la organización.

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

BOARDROOM EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

