



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

February 23, 2026



Organo Judicial 02/23/2026

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde "DICIEMBRE 2025" 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.

RISK

Actual Risk

n/a

El nivel de riesgo actual se mantiene constante con el mes anterior, situándose dentro de un rango bajo. Esto refleja la continuidad en el control de la actividad de amenazas sobre los activos monitoreados y sugiere que las medidas de seguridad implementadas continúan siendo efectivas. Sin embargo, resulta esencial mantener una supervisión constante para preservar este nivel y anticipar posibles cambios en el entorno.

Accepted Risk

n/a

El cliente no ha definido formalmente su nivel de Tolerancia al Riesgo durante la configuración del servicio. Por lo tanto, el análisis se realiza en función del Riesgo Real identificado y las mejores prácticas de ciberseguridad.

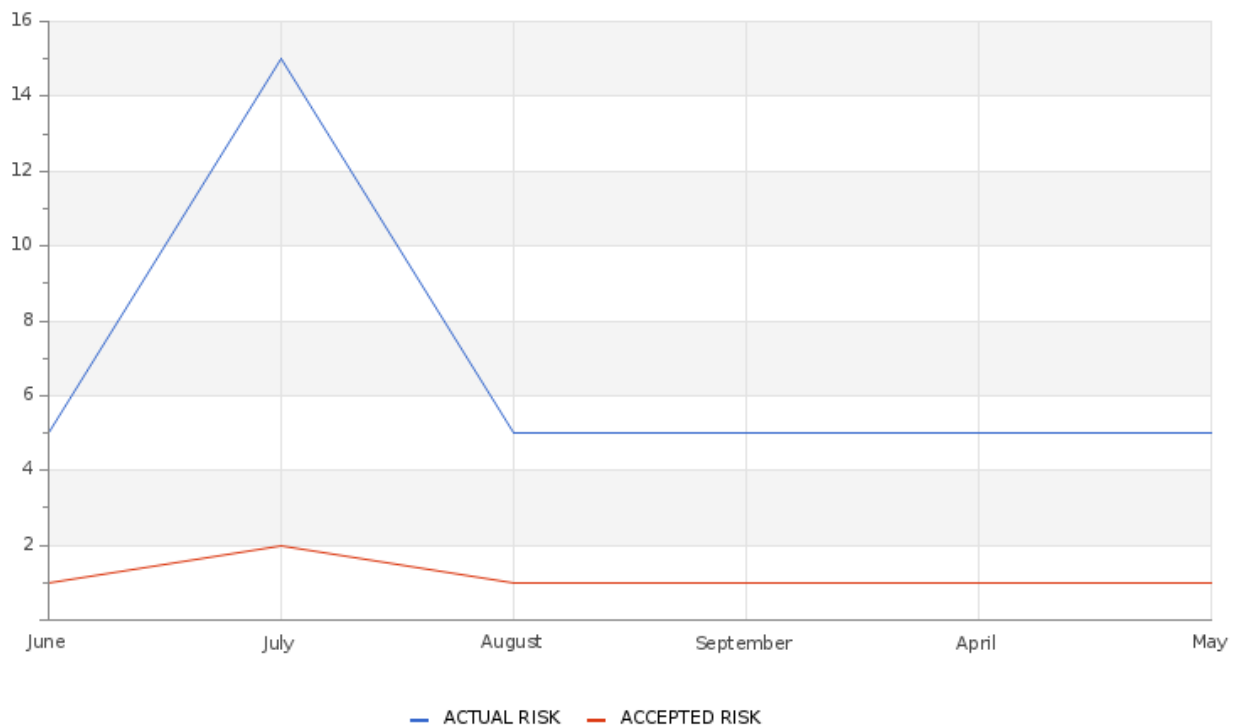
Confidence

Low

La confiabilidad de la evaluación sigue siendo limitada debido a la insuficiencia y falta de consistencia de los datos disponibles. Se sugiere reforzar los procesos de recopilación y correlación de información para incrementar la precisión del análisis y proporcionar un soporte más sólido a la toma de decisiones en materia de seguridad.



Organo Judicial 02/23/2026

Accepted & Actual Risk**Riesgo Actual (5%)**

Durante el periodo analizado, el nivel de riesgo actual se mantuvo estable en comparación con el mes anterior. El valor del 5% se encuentra dentro de un rango bajo, indicando que la exposición a incidentes potenciales sigue controlada y que las medidas de seguridad implementadas continúan siendo efectivas. No obstante, es esencial mantener una vigilancia constante y una capacidad de respuesta adecuada para prevenir posibles incrementos futuros.

Riesgo Tolerado (1%)

El riesgo tolerado se mantuvo en 1%, reflejando una gestión conservadora y consistente del riesgo residual. Este comportamiento demuestra la correcta aplicación de controles preventivos y la priorización de acciones de mitigación frente a posibles exposiciones, manteniendo el nivel de riesgo dentro de parámetros aceptables.

Table of Comparison of Actual and Acceptable Risk From Current to Previous Month

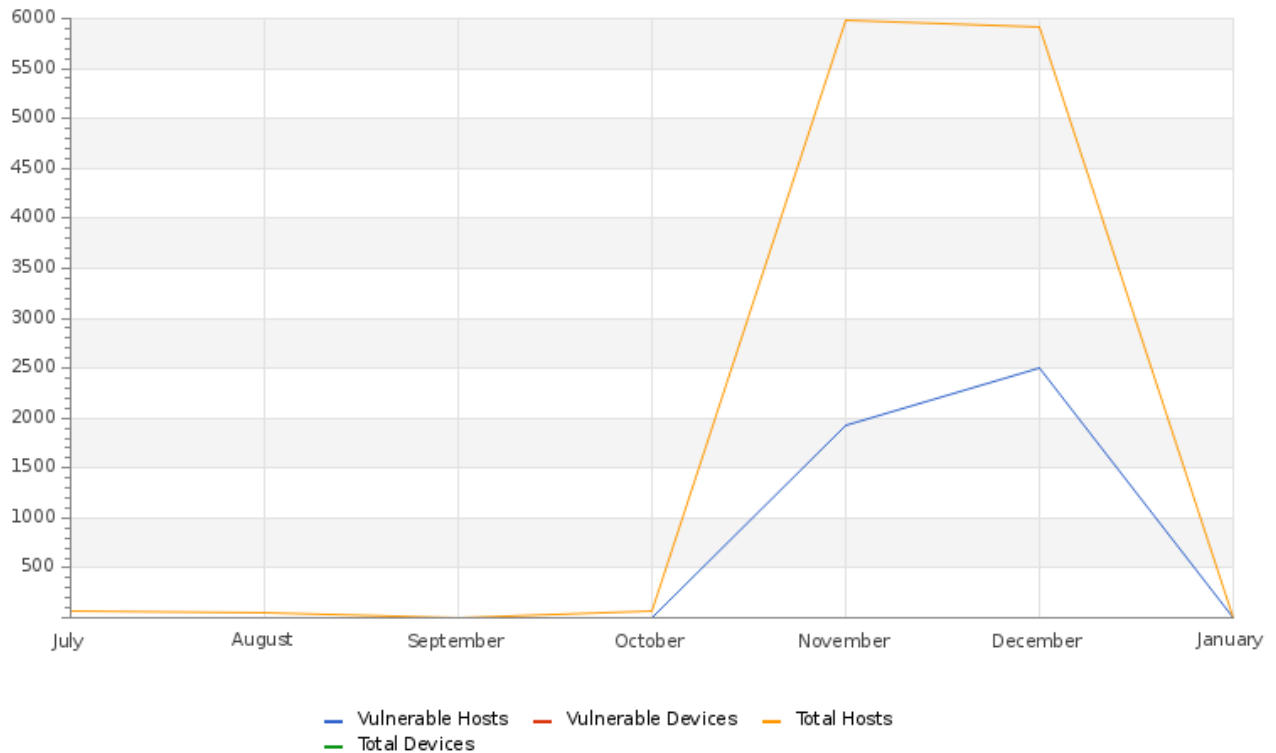
	Current Month	Previous Month
Actual Risk	5	5
Accepted Risk	0	0



Organo Judicial 02/23/2026

VULNERABILITY

Hosts & Vulnerable Hosts In Last 6 Months



En diciembre, el total de hosts activos se mantuvo estable en 5,526, sin variaciones en la infraestructura respecto al mes anterior. Sin embargo, el número de hosts vulnerables presentó cambios, asociados principalmente a la cantidad de equipos registrados en el período.

Este comportamiento sugiere que las medidas de seguridad implementadas continúan siendo efectivas para gestionar los riesgos identificados, aun cuando el volumen de activos administrados no ha cambiado. No obstante, es fundamental mantener una supervisión continua y una gestión proactiva de la seguridad, para asegurar que la estabilidad de la infraestructura no oculte riesgos potenciales ni genere una falsa sensación de seguridad.

Organo Judicial 02/23/2026

Total Vulnerability Counts In Current & Previous Month

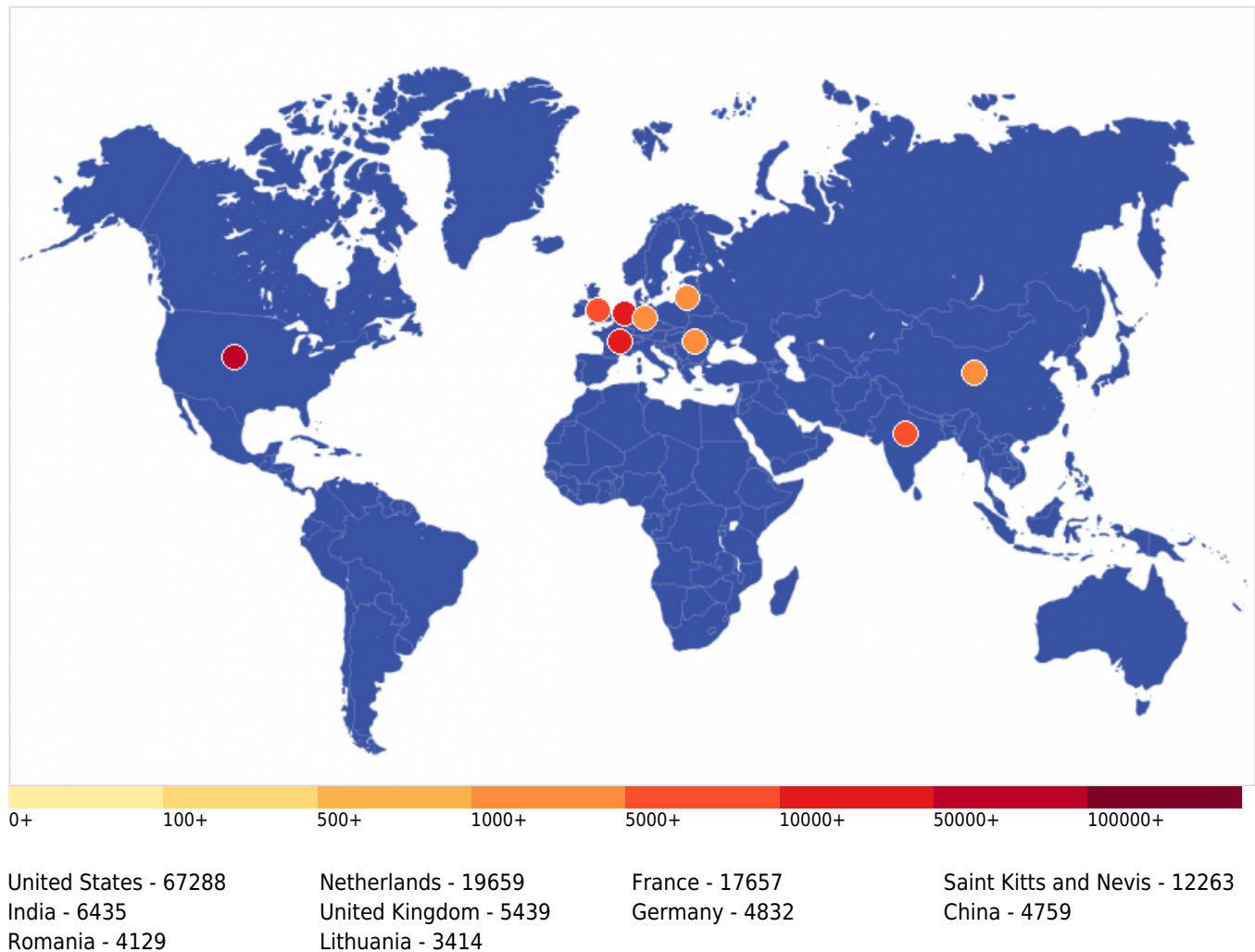
	Current Month	Previous Month
Hosts Baselined	5526	5526
Hosts Discovered	403	2869
Vulnerable Hosts	343	1375
Baseline Devices	0	0
Vulnerable Devices	0	0
Critical Vulnerabilities Count	144	187
High Vulnerabilities Count	1375	1724
Medium Vulnerabilities Count	648	903
Low Vulnerabilities Count	395	1418
Phishing Score	0	0
Email Gateway Score	1	0
Web Application Firewall Score	0	0
Web Gateway Score	57	56
Endpoint Score	4	3
Hopper Score	0	0
DLP Score	0	0

Vulnerability Metric**9**

Durante el mes de diciembre, se detectaron 144 host de estado crítico, 1375 host de vulnerabilidad alta, 648 de vulnerabilidad media y 395 de vulnerabilidad baja, lo que nos indica que la métrica de vulnerabilidad de la organización es 9%.

THREATS**Critical Attacks Per Country In Past Week**

Organo Judicial 02/23/2026



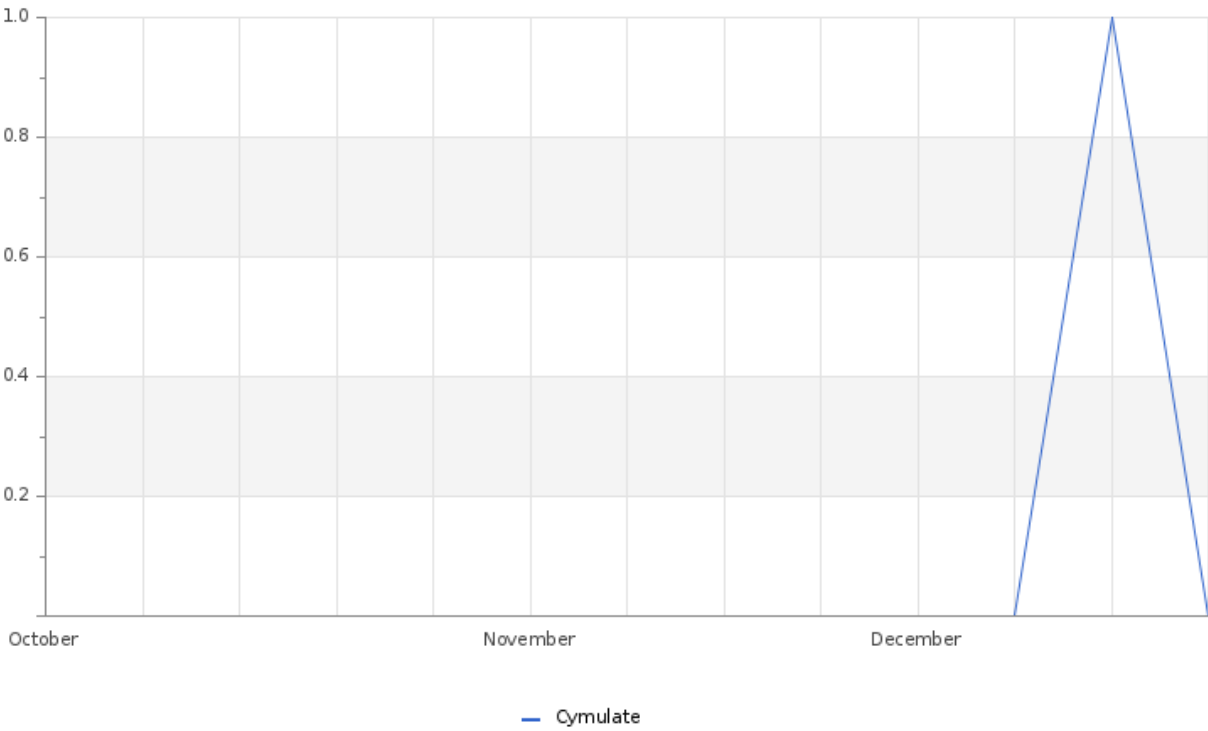
La gráfica del período analizado evidencia una concentración significativa de ciberataques provenientes principalmente de América del Norte y Europa Occidental, con presencia adicional en Asia. Estados Unidos se mantiene como la principal fuente, con 67,288 intentos registrados, seguido por Países Bajos (19,659), Francia (17,657) y Saint Kitts and Nevis (12,263). En un segundo nivel se ubican India (6,435), Reino Unido (5,439), China (4,759), Alemania (4,832), Rumania (4,129) y Lituania (3,414).

La distribución geográfica muestra un patrón marcado hacia países con alta infraestructura tecnológica y nodos relevantes de conectividad global, lo que sugiere el posible uso de servicios alojados, redes comprometidas o infraestructuras intermedias como vectores de origen. Asimismo, se observa diversidad regional, incorporando fuentes tanto de Europa del Este como de Asia.

Este comportamiento confirma la naturaleza global y distribuida de las amenazas, así como la necesidad de mantener estrategias de monitoreo continuo con enfoque regional diferenciado. La visualización permite identificar focos prioritarios y ajustar controles de seguridad, reglas de filtrado y capacidades de respuesta ante incidentes, en un entorno de riesgo dinámico y en constante evolución.

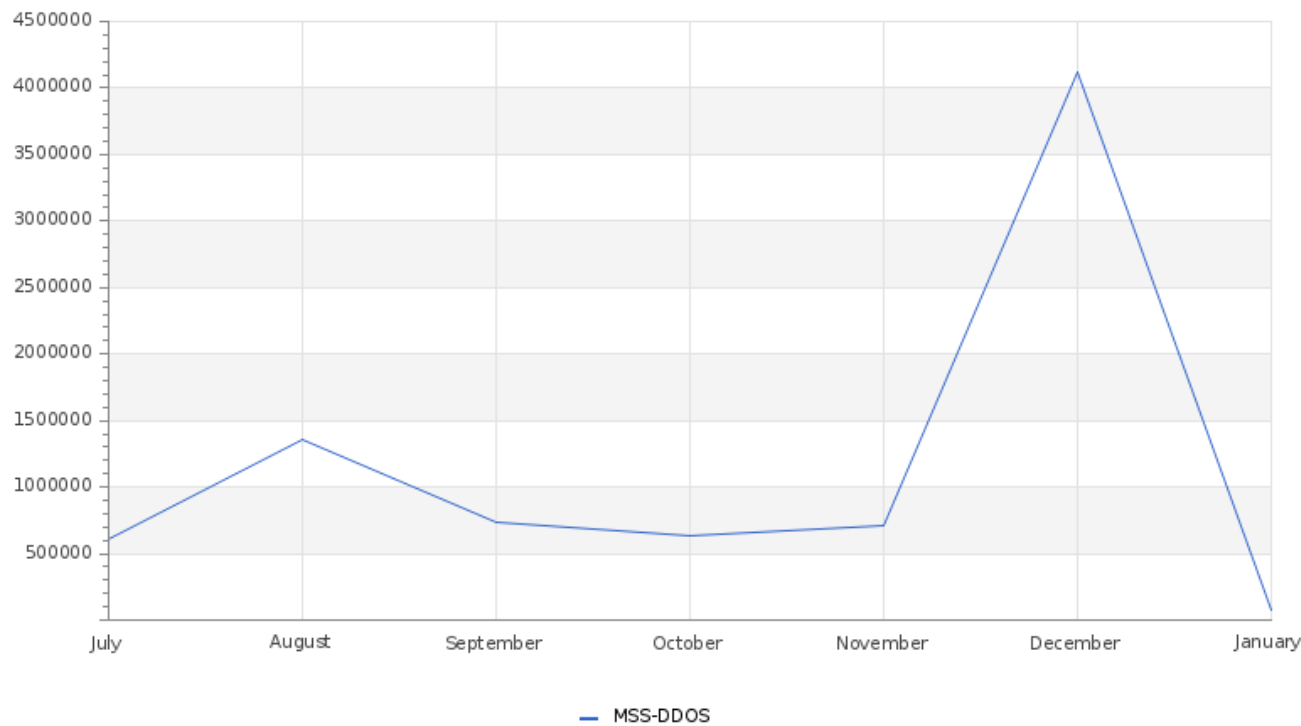
Organo Judicial 02/23/2026

Total Number of Successful MFA authentications per application

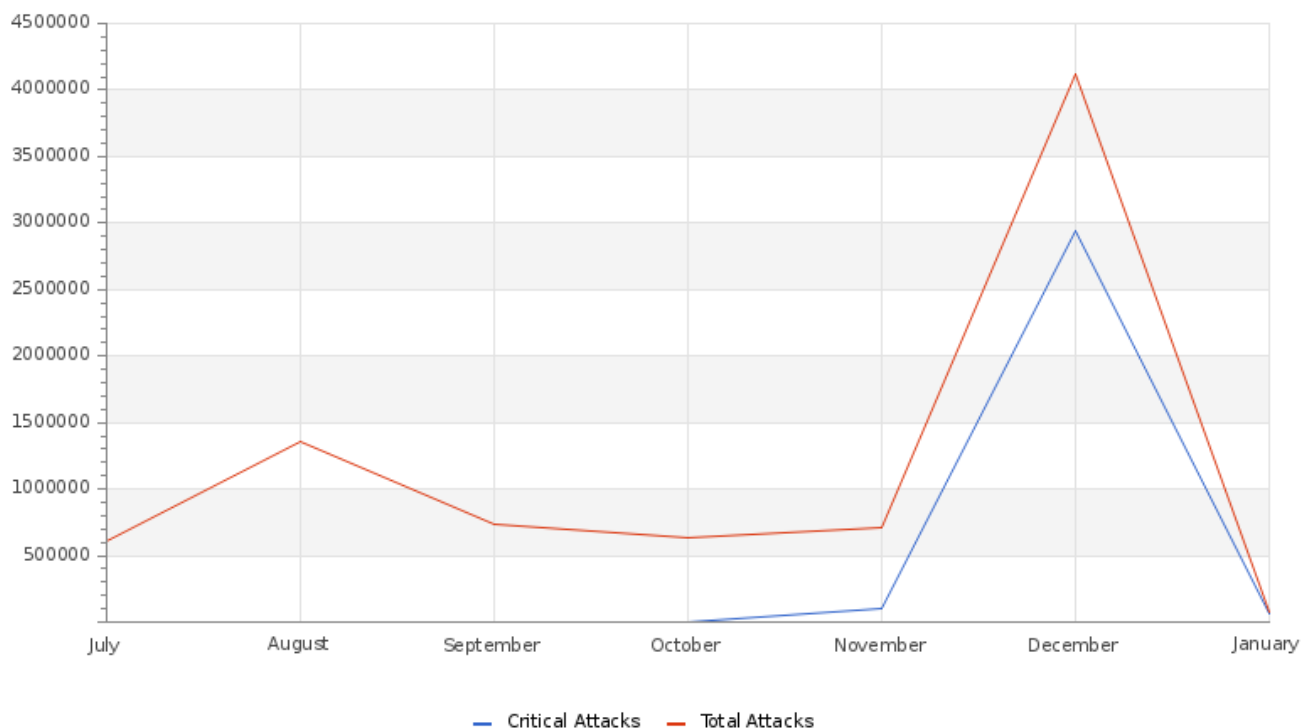


Organo Judicial 02/23/2026

Total Attacks Successfully Blocked Per Service



Organo Judicial 02/23/2026

Attacks Successfully Blocked by Severity**System Availability and Performance in current & previous month**

	Current Month	Previous Month
Total Device Outages	2	14
Critical Device Outages	0	0

Histogram of Total and Critical Device Outages**Total and Critical Attacks Successfully Blocked by Security Layer and Department**

MSS-UTM	MSS-DDOS	MSS-DLP	MSS-EDR
0	172,969	0	33



Organo Judicial 02/23/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Critical Perimeter Attacks	15
BAS Immediate Threat	5
Change in Systems Performance	26
Notable Event Alert: Vulnerability exposure from Threat Intelligence	1
Change in High or Critical Vulnerabilities	79
Change in Systems Availability	12
High Persistency Detection	9

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.

