TLP:AMBER

CISO EXECUTIVE REPORT

TROPIGAS

July 04, 2026

TROPIGAS 07/04/2026

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde "FEBRERO 2026" 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

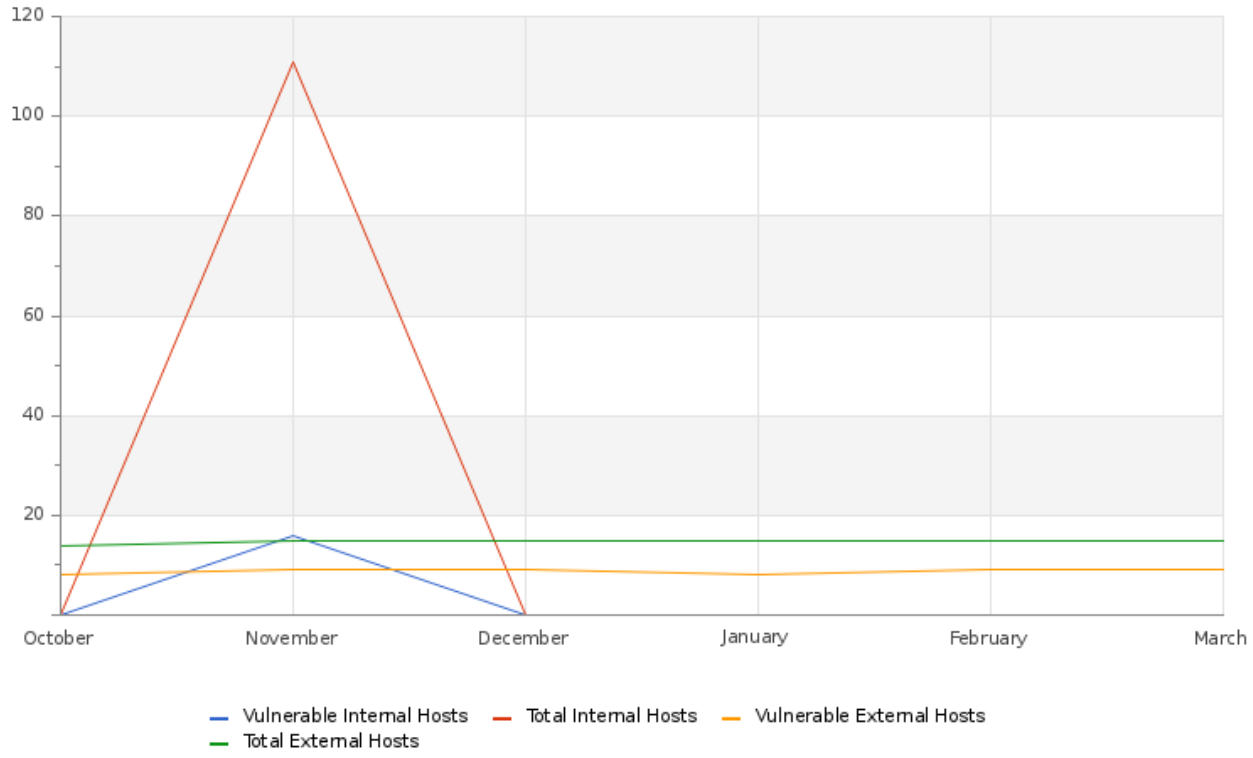
El propósito de este documento es informar sobre el estado" de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

VULNERABILITY

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

TROPIGAS 07/04/2026

Hosts & Vulnerable Hosts In Last 6 Months



Durante el mes de febrero, el número total de hosts externos se ha mantenido estable en 15 a lo largo de los últimos tres meses. En contraste, la cantidad de hosts con vulnerabilidades ha presentado un leve incremento, pasando de 8 a 9. Este comportamiento indica que, aunque la infraestructura se mantiene constante, existe una ligera variación en el nivel de exposición que debe ser atendida. Aun así, las medidas de seguridad implementadas continúan mostrando efectividad en la contención de riesgos. Se recomienda mantener un monitoreo continuo y reforzar las prácticas de gestión de vulnerabilidades, con el fin de identificar oportunamente posibles debilidades y reducir el impacto de riesgos potenciales en el entorno.

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
dest	201.226.254.231	1
Current	1	

TROPIGAS 07/04/2026

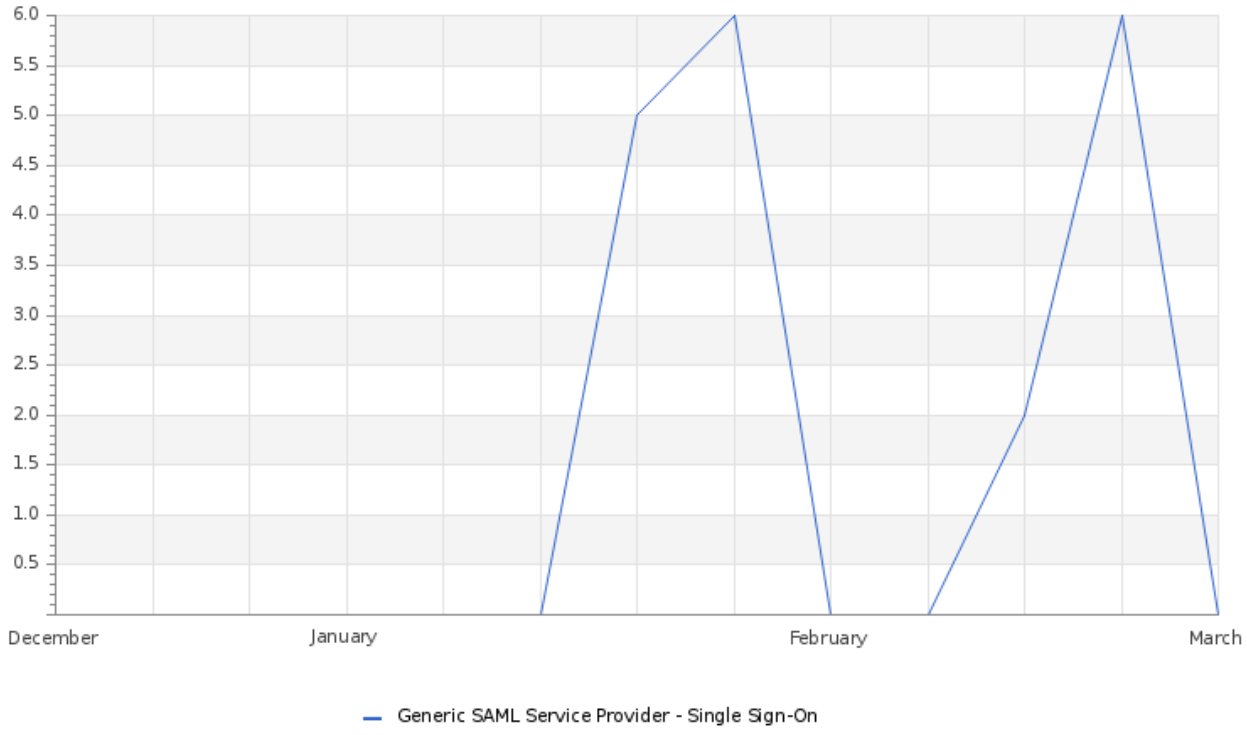
Vulnerability Metric

5

El análisis de los 15 hosts registrados en la organización durante el mes evaluado muestra una variación controlada en el número de activos vulnerables, con un incremento de 8 a 9 equipos afectados. En total, se identificaron 16 vulnerabilidades de severidad media y 9 de nivel bajo, lo que sitúa la métrica general de vulnerabilidades en un 5%. Este resultado refleja un nivel de exposición relativamente bajo y gestionable; sin embargo, evidencia la necesidad de mantener y fortalecer las prácticas de gestión de vulnerabilidades. Se recomienda continuar priorizando la remediación de hallazgos de mayor impacto, así como sostener un monitoreo constante que permita reducir progresivamente la superficie de riesgo y asegurar la protección de la infraestructura tecnológica.

THREATS

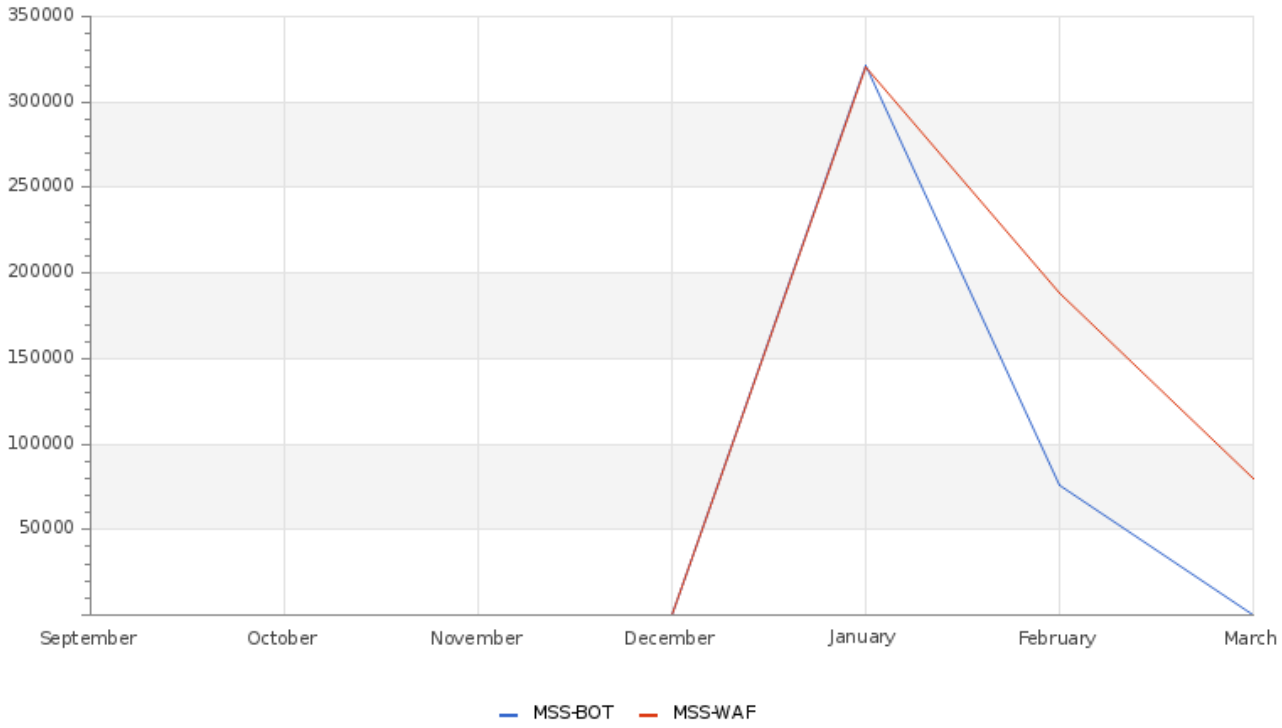
Total Number of Successful MFA authentications per application



La gráfica permite visualizar la actividad del cliente en las diferentes plataformas a las que tiene acceso. Durante el mes de noviembre, se registraron 6 accesos exitosos y 4 intentos denegados en la aplicación "Generic SAML Service Provider Single Sign-On", reflejando el nivel de interacción del usuario y la efectividad de los controles de acceso implementados.

TROPIGAS 07/04/2026

Total Attacks Successfully Blocked Per Service

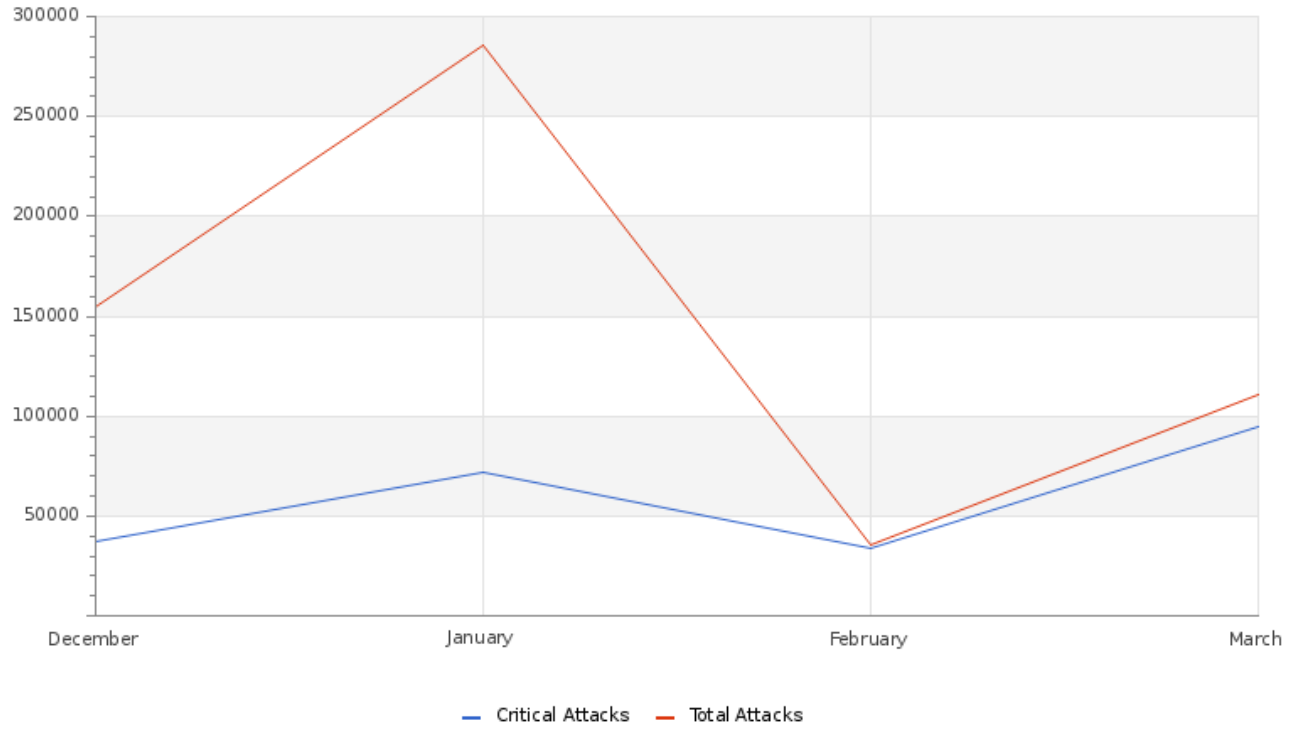


En febrero, el número de ataques bloqueados muestra una tendencia relativamente estable, con fluctuaciones moderadas a lo largo del mes. La actividad de MSS-BOT parece haberse reducido significativamente en comparación con períodos anteriores, lo que indica que el pico de intentos de automatización maliciosa fue temporal y que, desde entonces, ha remitido a niveles más bajos. Por el contrario, MSS-WAF mantiene una presencia más constante, con una ligera tendencia al alza que sugiere intentos continuos de explotar aplicaciones web. Aunque no se observan picos pronunciados durante este mes, la actividad constante refleja un enfoque persistente en los vectores de ataque basados en la web. Febrero representa un periodo de estabilización, en el que los volúmenes de ataques se mantienen controlados pero continuos. Este comportamiento pone de relieve la importancia de mantener una supervisión activa y controles de seguridad por capas para abordar de forma eficaz las amenazas actuales y en constante evolución.

Attacks Successfully Blocked by Severity

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

TROPIGAS 07/04/2026



Durante el mes de febrero se registró una disminución significativa en el volumen de ataques bloqueados, alcanzando un total aproximado de 35,000 eventos, lo que representa una reducción considerable con respecto al pico observado en enero. Este descenso sugiere una disminución temporal de la actividad maliciosa o una variación en los patrones de ataque durante el periodo analizado.

En cuanto a la severidad, los Critical Attacks se situaron alrededor de 33,000 eventos, representando una proporción muy elevada del total de ataques bloqueados. Este comportamiento indica que, aunque el volumen general de eventos disminuyó, la mayoría de las amenazas detectadas correspondieron a ataques de alta criticidad, evidenciando que los intentos de compromiso continuaron dirigidos a objetivos de alto impacto.

La reducción observada respecto al mes anterior podría estar relacionada con cambios en las campañas de los actores de amenaza, una mayor efectividad de los mecanismos de prevención y mitigación implementados o variaciones en la superficie de exposición de los activos protegidos. Sin embargo, la alta concentración de ataques críticos demuestra que el riesgo operativo se mantuvo elevado, por lo que una disminución en el volumen de eventos no debe interpretarse como una reducción proporcional en el nivel de amenaza.

Se recomienda mantener un monitoreo continuo de los eventos de seguridad, reforzar las capacidades de detección y respuesta ante incidentes, validar periódicamente la efectividad de los controles implementados y continuar con la revisión de la superficie de ataque para identificar oportunamente posibles vectores de compromiso y contener amenazas de alta severidad.

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

TROPIGAS 07/04/2026

Histogram of Total and Critical Device Outages

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
192.168.12.22	SSL Certificate Sensor (Port 443)	Clients	Warning		8785	2026-02-10 00:04:50	2026-03-12 14:00:06
Gateway: 10.100.40.1	SSL Certificate Sensor (Port 443)	Network Infrastructure	Warning		8785	2026-02-10 00:04:50	2026-03-12 13:59:59
192.168.12.20	SSL Certificate Sensor (Port 443)	Linux / macOS / Unix	Warning		8180	2026-02-10 00:04:50	2026-03-12 13:59:46
Probe Device	System Health	MSS-CSME-Tropigas	Warning		16	2026-03-02 13:13:09	2026-03-11 22:05:02

El análisis correspondiente al período evaluado evidencia la generación sostenida de alertas asociadas al monitoreo de certificados SSL/TLS sobre servicios expuestos mediante el puerto 443 en activos críticos de la infraestructura. Los dispositivos 192.168.12.22, Gateway: 10.100.40.1 y 192.168.12.20 registraron eventos a través del sensor “SSL Certificate Sensor (Port 443)”, todos clasificados bajo estado Warning, indicando anomalías relacionadas con la gestión criptográfica de los servicios HTTPS publicados.

Las alertas detectadas pueden estar asociadas a certificados expirados o próximos a su vencimiento, inconsistencias en la cadena de confianza (CA), algoritmos criptográficos obsoletos, errores en la validación del Common Name (CN) o Subject Alternative Name (SAN), así como configuraciones TLS inseguras o incompletas. Este tipo de condición puede impactar directamente la disponibilidad, integridad y confiabilidad de las comunicaciones cifradas, además de incrementar la superficie de exposición frente a ataques de interceptación, degradación criptográfica o pérdida de confianza por parte de clientes y servicios consumidores.

En términos de criticidad acumulada, el activo 192.168.12.22 presentó el mayor volumen de eventos con un total de 8,785 registros desde el 10 de febrero de 2026, seguido por el host 192.168.12.20 con 8,180 eventos. Asimismo, el Gateway 10.100.40.1 reflejó igualmente 8,785 eventos asociados a componentes de infraestructura de red, lo que podría representar un riesgo operativo significativo en caso de que los certificados afectados pertenezcan a servicios productivos, plataformas corporativas o recursos accesibles externamente.

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	396,660	0	0	0	30,451

El análisis correspondiente al período evaluado evidencia que la capa MSS-BOT se consolidó como el principal mecanismo de defensa frente a actividades automatizadas y tráfico malicioso, registrando un total de 396,660 ataques bloqueados exitosamente. Este volumen representa la mayor concentración de eventos detectados dentro de las capas de seguridad monitoreadas, lo que sugiere una alta actividad relacionada con bots automatizados, intentos de scraping, reconocimiento, abuso de aplicaciones web o campañas automatizadas dirigidas contra los servicios expuestos.

Asimismo, la capa MSS-WAF reportó el bloqueo de 30,451 ataques, reflejando una actividad constante orientada a la explotación de aplicaciones web y posibles intentos de acceso no autorizado, validación de vulnerabilidades o ejecución de patrones maliciosos sobre los recursos publicados. La correcta actuación de esta capa demuestra la efectividad de las reglas de protección y mitigación implementadas para salvaguardar los entornos web críticos.

TROPIGAS 07/04/2026

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
MSS-DLP - Abnormal activity in the file system(s)	603
BAS Web Security	9
Change in Systems Performance	2
Non Baselined Discovered System	301
Internal user deleted or moved a SoftwareMine	245
Monitoring for open ports	10
MSS-DLP - External File access	292
High Persistency Detection	435
Threat Intelligence Validation	30
Notable Event Alert: Vulnerability exposure from Threat Intelligence	1
TEVR BAS Immediate Threats	1
Change in Systems Availability	2

Durante el período en cuestión, se ha identificado una actividad considerable relacionada con eventos de seguridad, monitoreo operativo y control de activos dentro de la infraestructura tecnológica. El evento con mayor recurrencia correspondió a MSS-DLP - Abnormal activity in the file system(s), con un total de 603 registros, lo que evidencia comportamientos anómalos asociados al acceso, modificación, movimiento o manipulación de archivos dentro de sistemas monitoreados. Esta actividad puede estar relacionada con transferencias no autorizadas, cambios masivos en información sensible, ejecución de procesos inusuales o posibles intentos de exfiltración de datos, lo que representa un riesgo relevante para la integridad y confidencialidad de la información corporativa.

Asimismo, se detectaron 164 eventos de Non Baselined Discovered System, lo que indica la presencia de activos que no cumplen con las configuraciones base definidas o que no han sido correctamente integrados dentro de los procesos de control e inventario corporativo. Este comportamiento constituye una debilidad significativa desde la perspectiva de la gestión de activos, el refuerzo de la seguridad y el cumplimiento de las políticas de seguridad, lo que potencialmente aumenta la superficie de exposición frente a amenazas internas o externas.

En lo que respecta a las actividades asociadas a la persistencia y los accesos externos, se han registrado un total de 119 eventos de MSS-DLP - External File Access y 117 eventos de High Persistency Detection. Estos indicadores podrían estar relacionados con accesos recurrentes a archivos sensibles, mecanismos de persistencia no habituales, ejecución sostenida de procesos o comportamientos potencialmente vinculados a actividades maliciosas avanzadas dentro del entorno monitoreado. La combinación de ambos tipos de eventos subraya la importancia de mantener una supervisión continua sobre los usuarios, los procesos y los sistemas que tienen acceso a información crítica.

Adicionalmente, se identificaron 99 eventos relacionados con Internal user deleted or moved a SoftwareMine, lo que refleja acciones internas de modificación o desplazamiento de recursos monitoreados. Aunque este tipo de actividad puede corresponder a tareas administrativas legítimas, también podría representar riesgos asociados a alteraciones no autorizadas, pérdida de trazabilidad o eliminación accidental de componentes críticos.

Por otro lado, se registraron eventos de menor volumen, pero igualmente relevantes desde el punto de vista de seguridad,

incluyendo 19 eventos de BAS Immediate Threat, 10 eventos de Monitoring for open ports, 9 eventos de BAS Web Security, así como eventos individuales relacionados con exposición de vulnerabilidades provenientes de inteligencia de amenazas, cambios en disponibilidad de sistemas y variaciones en el rendimiento operacional. Aunque su frecuencia fue reducida, este tipo de alertas puede representar indicadores tempranos de exposición, degradación operacional o intentos de explotación sobre servicios tecnológicos.

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