



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

CISO EXECUTIVE REPORT

TROPIGAS
June 02, 2026



TROIPIGAS 06/02/2026

TLP AMBER CISO EXECUTIVE REPORT

Este informe corresponde "MARZO 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

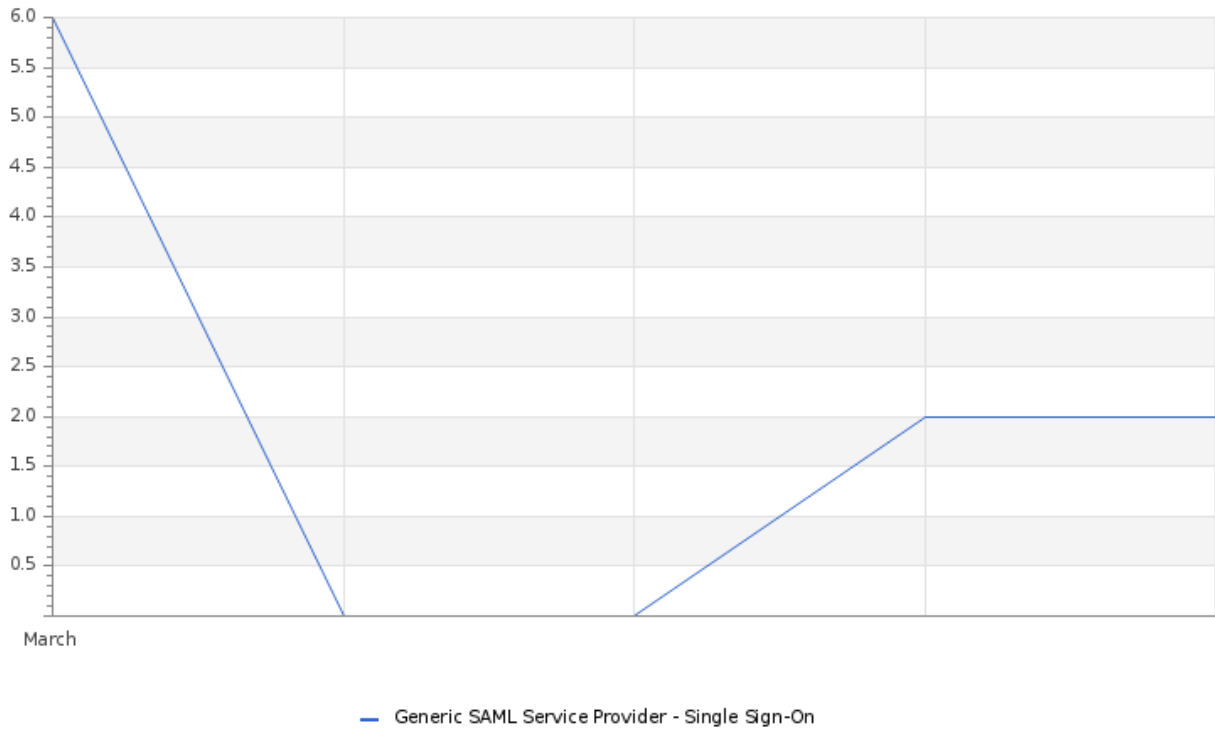
El propósito de este documento es informar sobre el estado de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

VULNERABILITY

THREATS

TROPIGAS 06/02/2026

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 marzo, se registraron 5 accesos exitosos y 2 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.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Device Outages	3	0
Critical Device Outages	0	0

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		8687	2026-03-02 00:09:50	2026-04-01 05:34:22

TLP AMBER CISO EXECUTIVE REPORT

TROPIGAS 06/02/2026

Device	Sensor	Group	Status	Criticality	Events	First_Seen	Last_Seen
Gateway: 10.100.40.1	SSL Certificate Sensor (Port 443)	Network Infrastructure	Warning		8687	2026-03-02 00:09:49	2026-04-01 05:34:15
192.168.12.20	SSL Certificate Sensor (Port 443)	Linux / macOS / Unix	Warning		8687	2026-03-02 00:09:49	2026-04-01 05:34:02
201.226.254.228	SSL Certificate Sensor (Port 443)	WEB SERVER	Warning		1626	2026-03-26 18:09:01	2026-04-01 09:37:55
Probe Device	System Health	MSS-CSME-Tropigas	Warning		43	2026-03-02 13:13:09	2026-03-30 10:43:06
DNS: 8.8.8.8	Ping v2	Network Infrastructure	Down		2	2026-03-19 18:09:38	2026-03-19 22:36:42
DNS: Glesec AD1	Ping v2	Network Infrastructure	Down		2	2026-03-17 10:54:12	2026-03-18 21:25:12
201.226.254.228	SSL Security Check (Port 443)	WEB SERVER	Down		1	2026-03-15 19:34:05	2026-03-15 19:34:05
201.226.254.228	HTTP v2	WEB SERVER	Warning		1	2026-03-13 18:29:06	2026-03-13 18:29:06

El análisis correspondiente al período evaluado evidencia una concentración significativa de alertas relacionadas con la validación de certificados SSL/TLS y la disponibilidad de servicios críticos dentro de la infraestructura monitoreada. Los activos 192.168.12.22, Gateway 10.100.40.1 y 192.168.12.20 registraron la mayor cantidad de eventos mediante el sensor "SSL Certificate Sensor (Port 443)", todos clasificados con estado Warning y una criticidad acumulada de 8,687 eventos, lo que indica la persistencia de condiciones anómalas asociadas a los servicios HTTPS publicados.

Adicionalmente, el servidor 201.226.254.228, perteneciente al grupo WEB SERVER, presentó 1,626 eventos relacionados con el mismo sensor SSL, así como alertas adicionales detectadas por los sensores HTTP v2 y SSL Security Check (Port 443), evidenciando posibles problemas tanto en la configuración de los servicios web como en la implementación de los mecanismos de seguridad asociados al protocolo HTTPS.

Asimismo, se identificaron eventos con estado Down asociados al sensor Ping v2 sobre los activos DNS: 8.8.8.8 y DNS: Glesec AD1, indicando pérdida de conectividad o indisponibilidad temporal durante el período monitoreado. Aunque el volumen de eventos registrados es reducido, estas alertas pueden representar afectaciones en la resolución de nombres, conectividad de red o disponibilidad de servicios internos críticos, por lo que se recomienda validar la estabilidad de las comunicaciones y descartar interrupciones recurrentes.

En términos de criticidad acumulada, los activos 192.168.12.22, Gateway 10.100.40.1 y 192.168.12.20 representan los elementos con mayor impacto operativo al concentrar la mayor cantidad de eventos detectados. La recurrencia sostenida de estas alertas desde el inicio del período monitoreado sugiere la existencia de condiciones persistentes que requieren revisión y remediación, especialmente si los servicios afectados corresponden a infraestructura productiva, componentes de autenticación, servicios corporativos o recursos expuestos a Internet.

TROPIGAS 06/02/2026

Total and Critical Attacks Successfully Blocked by Security Layer and Department

MSS-UTM	MSS-BOT	MSS-DDOS	MSS-DLP	MSS-EDR	MSS-WAF
0	329,237	0	0	0	214,391

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Web Security	9
Change in Systems Performance	2
Non Baselined Discovered System	194
MSS-DLP - Abnormal activity in the file system(s)	322
Internal user deleted or moved a SoftwareMine	139
Monitoring for open ports	10
MSS-DLP - External File access	180
High Persistency Detection	180
Threat Intelligence Validation	30
Notable Event Alert: Vulnerability exposure from Threat Intelligence	1
TEVR BAS Immediate Threats	1
Change in Systems Availability	1

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.

