
TLP:AMBER

# CISO EXECUTIVE REPORT

BLADEX

January 31, 2024

BLADEX 01/31/2024

# TLP AMBER CISO
## EXECUTIVE REPORT

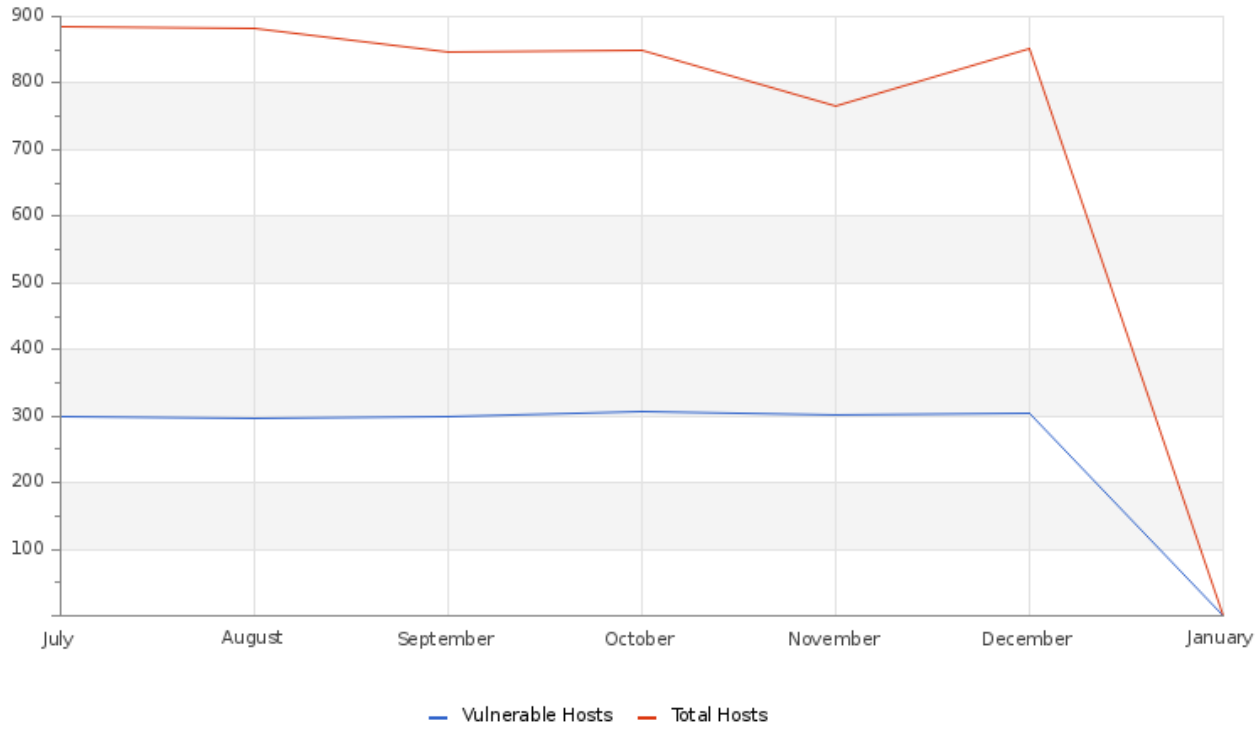
Este informe corresponde "Diciembre " y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, 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

### Hosts & Vulnerable Hosts In Last 6 Months




En la grafica muestra un ligero aumento en la cantidad de host descubiertos en comparación al mes anterior, también muestra la persistencia de vulnerabilidades en los sistemas. La mayor parte de estas vulnerabilidades corresponden a dispositivos que mantiene versiones desactualizadas de aplicaciones. Cada una de las vulnerabilidades identificadas por el GOC, han sido documentadas indicando el tipo de vulnerabilidad y su respectiva remediación, puede acceder a esta información a través de nuestra plataforma de Skywatch.


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

### Total Vulnerability Counts In Current & Previous Month

| | Current Month | Previous Month |
|---|---|---|
| Hosts Baselined | 898 | 898 |
| Hosts Discovered | 481 | 731 |
| Vulnerable Hosts | 122 | 293 |
| Critical Vulnerabilities Count | 39 | 130 |
| High Vulnerabilities Count | 173 | 388 |
| Medium Vulnerabilities Count | 598 | 1319 |
| Low Vulnerabilities Count | 88 | 259 |
| Phishing Score | 0 | 0 |
| Email Gateway Score | 6 | 7 |
| Web Application Firewall Score | 34 | 0 |
| Web Gateway Score | 20 | 20 |
| Endpoint Score | 34 | 35 |
| Hopper Score | 17 | 17 |
| DLP Score | 100 | 100 |

La tabla muestra una comparación de los resultados obtenidos en los últimos 2 meses. Se pueden observar ligeras reducciones en cuanto a los host vulnerables y las vulnerabilidades presentes en estos. En cuanto a las puntuaciones obtenidas para el servicio MSS-BAS, no se observan variaciones significativas en los puntajes con respecto al mes anterior. Recomendamos revisar la documentación proporcionada a través de nuestra plataforma de Skywatch, con los resultados obtenidos para estos servicio y aplicar las mitigaciones correspondientes con el fin de robustecer su seguridad.

### Vulnerability Metric

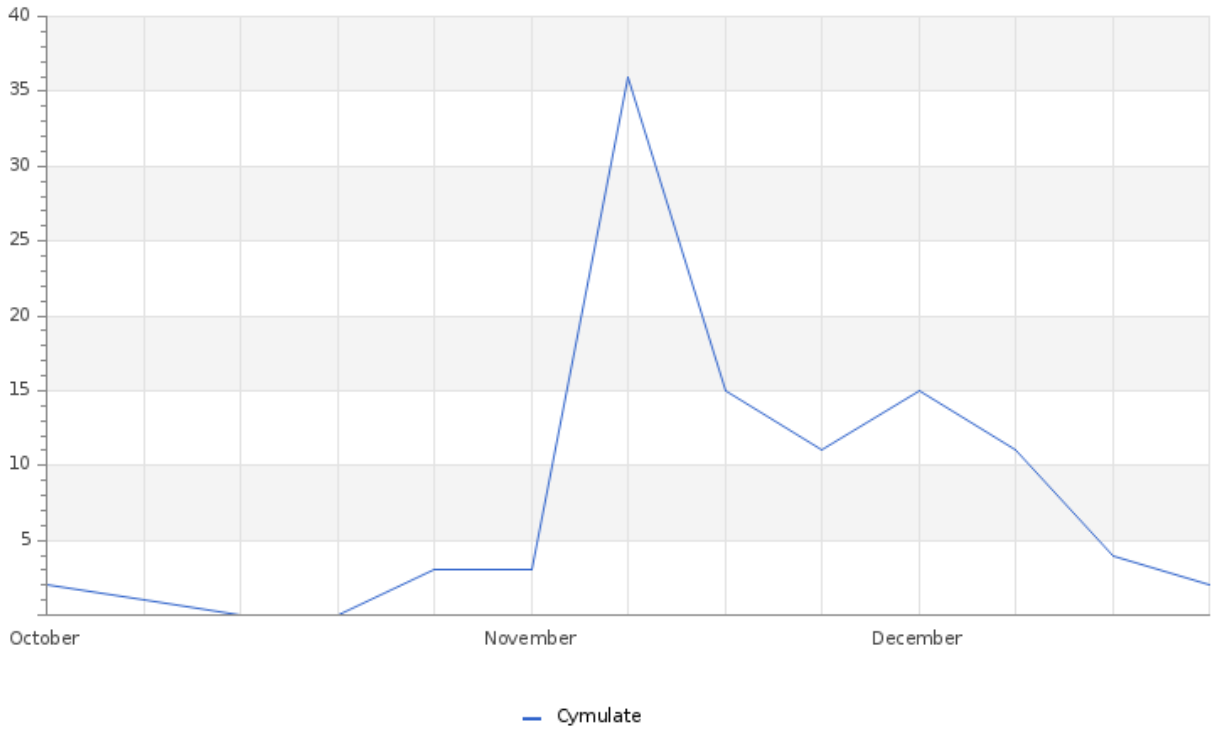
**9**

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 01/31/2024

## Total Number of Successful MFA authentications per application




La grafica muestra la actividad del cliente en las diferentes plataformas durante el mes.
En Skywatch podrá encontrar documentación sobre los casos, incidentes, reportes, etc., que les brindan información útil para 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 Device Outages | 5 | 1 |
| Critical Device Outages | 0 | 0 |

Durante el mes se reportaron alertas relacionadas con el rendimiento de los dispositivos, además de alertas de perdidas de conexiones momentáneas las cuales se pueden producir debido a problemas de congestión en la red.


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

BLADEX 01/31/2024

### Total and Critical Attacks Successfully Blocked by Security Layer and Department

| MSS-UTM | MSS-DDOS | MSS-DLP | MSS-EDR |
|---|---|---|---|
| 0 | 0 | 0 | 0 |

Durante el mes se ha estado trabajando en la migración del servicio MSS-DLP, por lo que no se generaron alertas para este servicio.

# OPERATIONAL

### Notable Events Active For The Last Month

| Notable Event Type | How Many # |
|---|---|
| Abnormal activity in the file system(s) | 16 |
| BAS Immediate Threat | 60 |
| BAS Endpoint Security | 8 |
| BAS Web Security | 14 |
| BAS WAF | 6 |
| Change in High or Critical Vulnerabilities | 17 |

Durante el mes se documentaron múltiples casos relacionados con el servicios MSS-BAS, en estos casos se encuentran adjuntos los IoC's de aquellas muestras usadas en las evaluaciones que lograron evadir sus medidas de seguridad. También se documentaron nuevas vulnerabilidades descubiertas por el el servicio MSS-VME y se actualizaron aquellas que persisten en sus sistemas. Se recomienda realizar una revisión de estos casos y aplicar las mitigaciones correspondientes. 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.**


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


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