Scitum

CIBERSEGURIDAD

Reporte Ejecutivo

Dashboard

Diciembre 2025

JULIO®

Sección 1. Reporte Ejecutivo.

El periodo del presente reporte comprende desde el **1 al 31 de Diciembre de 2025**, cuyo alcance abarca la entrega del resumen ejecutivo con el contexto de los resultados del monitoreo de seguridad.

En la presente información se incluye nuestra política de intercambio de información **TLP (Traffic Light Protocol)** con la cual puede ser consultada directamente en el siguiente sitio:

- https://www.scitum.com.mx/ScitumCsirt/TLP

Visión general

Durante el periodo correspondiente al mes de diciembre, no se identificaron eventos relevantes para reportar. Las operaciones se mantuvieron dentro de los parámetros habituales.

- Adición de 497 Indicadores de Compromiso (IOC) —hashes, direcciones IP y dominios— a las reglas de detección de Cortex XDR, mismos que fueron obtenidos del Ciber-Ecosistema de SCILabs, con el objetivo de fortalecer la detección de amenazas avanzadas en los activos de GRUPO JULIO.

Tendencia de eventos de seguridad

A continuación, se presenta una gráfica con las alertas de seguridad identificadas en la herramienta de monitoreo a lo largo del servicio.

Ilustración 1. Tendencia de actividad sospecha

Disponibilidad de Cortex XDR

Durante el presente periodo se observa que la disponibilidad de Cortex XDR fue del 100%. Es importante mencionar que se considera la tecnología en la región “Estados Unidos – Américas”

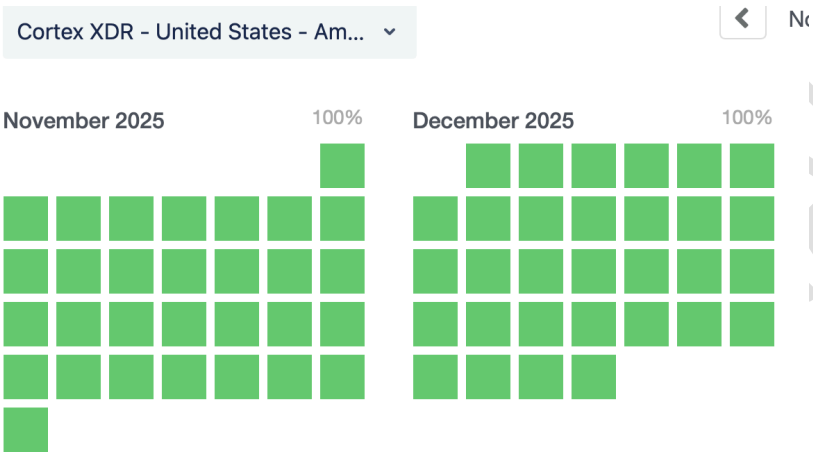
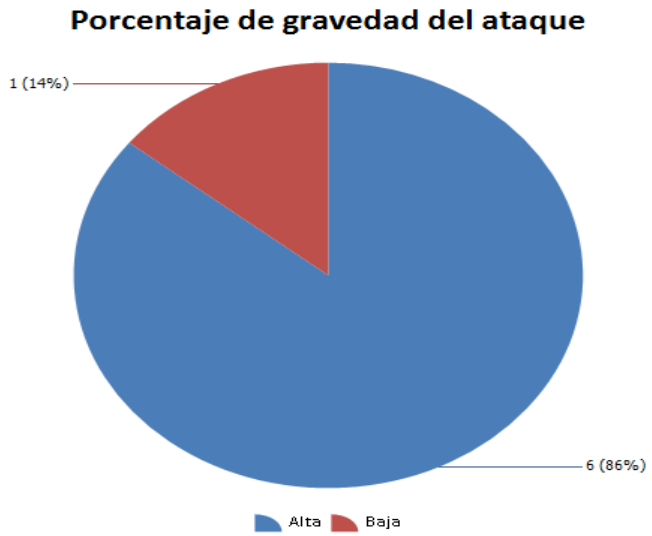


Ilustración 2. Disponibilidad de la herramienta

Administración FW SDWAN (SOC)

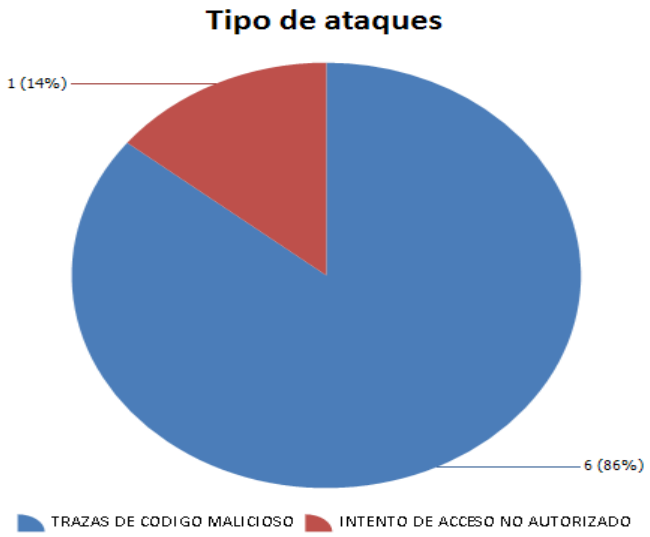
1. Severidad de ataques.

La severidad de las actividades sospechosas notificadas es categorizada por la herramienta de monitoreo.



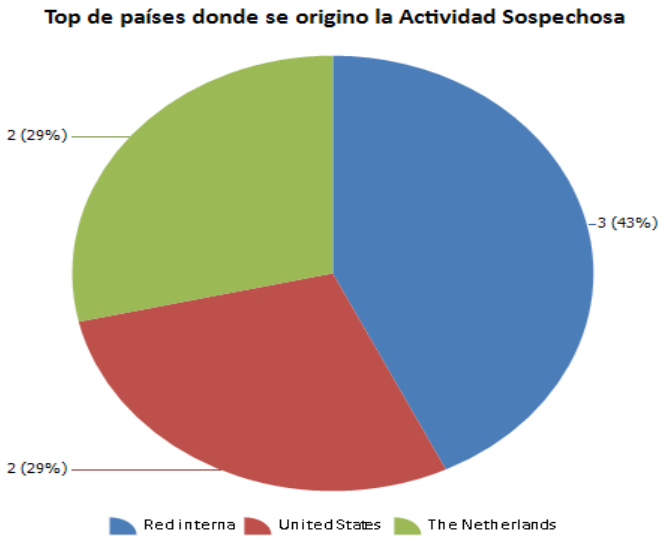
2. Categorización de ataques.

El tipo de ataque se refiere a una categorización asignada según el patrón de ataque reportado.

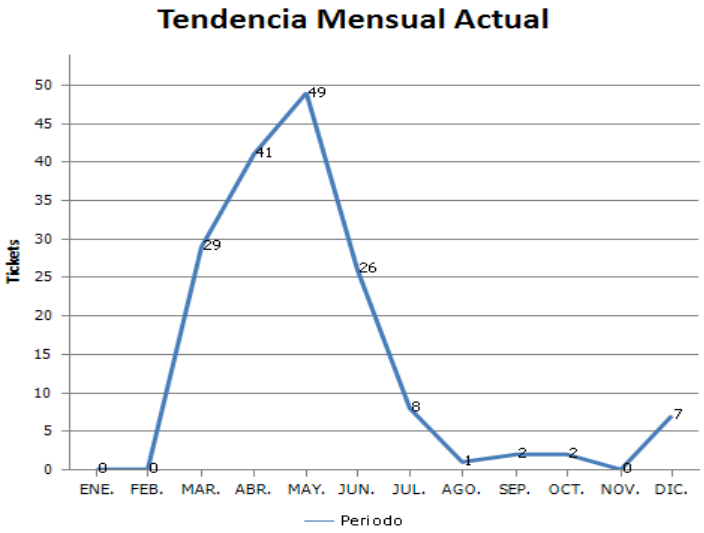


3. Origen de actividad sospechosa.

4. Top de países que generaron actividad sospechosa hacia el cliente.



5. Tendencia de actividad sospechosa.



Servicio Tráfico Seguro

Eventos presentados a partir del aprovisionamiento en la herramienta

- **GRUJU-S-CLP-GL-PKF001**

Cliente	Sitio	Referencia	Tamaño de enlace
GRUPO JULIO S.A. DE C.V.	Corporativo Tlalpan Principal	C20-2409-0049	300 Mbps
	Corporativo Tlalpan Respaldo	5543179755	300 Mbps

- **GRUJU-S-CLP-GL-PKF002**

Cliente	Sitio	Referencia	Tamaño de enlace
GRUPO JULIO S.A. DE C.V.	CEDIS_IZTAPALAPA_FINSA	C00-2409-0057	100 Mbps

Durante el mes de **diciembre**, se presentó **01** evento para el MO **GRUJU-S-CLP-GL-PKF001**, dentro del servicio de Tráfico Seguro (Clean Pipes).

1. Severidad de ataques.

La severidad de las actividades sospechosas notificadas es categorizada por la herramienta de monitoreo.

2. Categorización de ataques.

El tipo de ataque se refiere a una categorización asignada según el patrón de ataque reportado.

3. Origen de actividad sospechosa.

4. Top de países que generaron actividad sospechosa hacia el cliente.