

CII CYBERPEACE

Informe Mensual

Junio 2023

CONSUBANCO



www.cyberpeace.tech

	Informe mensual junio 2023	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

SGSI-DOC-SOC-06 INFORME MENSUAL JUNIO 2023

Elaborado por:	Carrizosa Ceron Vilmerth Daniel						
Aprobado por:	Iván Hernández						
Fecha:	05/07/2023						
Objetivo del informe:	Dar a conocer la información relevante sobre los hallazgos en materia de seguridad obtenidos en este periodo de operación.						
Contexto:	Informe emitido como parte de las alertas de seguridad mostrados en el SOC.						
Alcance:	INICIO			FIN			
	01	06	2023		30	06	2023

Contenido

Contenido.....2

Confidencialidad3

Aviso de Restricción3

Introducción.....4

Sentinel – Ambiente SPEI5

Accesos Fallidos6

Sentinel – Forcepoint.....7

Sentinel – VPN.....8

Sentinel – Trafico de red11

Sentinel – Antispam14

Sentinel – Windows.....16

Sentinel – Reputación Diaria.....17

Sentinel – DLP.....18

Recomendaciones.....20

	Informe mensual junio 2023	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Confidencialidad

Para efectos de este documento, el término “Material Confidencial” significa toda información, escrita, gráfica o contenida en cualquier medio tangible o intangible que Cyberpeace entregue a **ConSuBanco (CSB)** para la prestación de los Servicios y la identifique como confidencial.

El término Material Confidencial no incluye aquella información que (I) está disponible al público en general, (II) se puso a disposición de Cyberpeace sin el carácter de confidencial antes de lo aquí establecido, o (III) se puso a disposición de Cyberpeace, sin el carácter de confidencial, por otra fuente sin obligación de confidencialidad.

Para mantener la confidencialidad de este material, FDFLA conviene en: (I) no usar el Material Confidencial, excepto para la prestación de los Servicios; (II) no revelar, -excepto por orden de una autoridad judicial o administrativa- el Material Confidencial a cualquier persona excepto a sus directores, empleados, asesores y representantes (conjuntamente los “Representantes”) que necesiten conocer la información; dichos Representantes se obligan a mantenerla como confidencial, y (III) no usar el Material Confidencial para fines propios y de terceras partes.

Aviso de Restricción

Restricciones de uso, divulgación del contenido

La información contenida en este reporte de servicio o cotización constituye un secreto industrial por lo que está clasificado como confidencial. Es revelada al cliente con la restricción de que no será usada o divulgada, sin el permiso de Cyberpeace, para otros propósitos que no sean su evaluación; obligándose a proteger la Información Confidencial recibida, usando un razonable grado de cuidado, pero no menor al grado de cuidado utilizado para proteger su información o material similar. Esta restricción no limita al derecho del cliente para usar o divulgar esta información si se obtuvo de otra fuente sin obligación de confidencialidad.

	Informe mensual junio 2023	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Introducción

El presente informe se encarga de documentar y reportar la actividad sospechosa o potencialmente crítica que se registró tanto en la plataforma **Sentinel – Azure**.

Al final de este reporte se anexan recomendaciones por parte de Cyberpeace que se espera sean atendidas para poder robustecer la infraestructura de **CSB** tanto en la red empresarial como en la plataforma en la nube. Realizando estas recomendaciones se ayuda a mitigar las vulnerabilidades que pudiese presentarse en los equipos o en la red de **CSB**.

Algunas de estas recomendaciones deberán realizarse periódicamente en los equipos que los usuarios utilizan por lo cual se solicita el apoyo de los administradores para alentar a los usuarios a que las realicen.

Sentinel – Ambiente SPEI

A continuación, se presenta el top 5 de las conexiones exitosas de usuarios realizadas durante este mes en el ambiente SPEI. Como podemos visualizar, durante este mes no se presentaron conexiones por parte de los usuarios.

Ambiente SPEI Ambiente INDEVAL DIRECTORIO ACTIVO FORCEPOINT VPN TRAFICO DE RED



Periodo

6/1/2023 12:00 AM - 6/30/2023 11:59 PM

Usuario: <unset> ▾

Hostname: <unset> ▾

IP: <unset> ▾

Evento: <unset> ▾

Conexiones de Usuarios

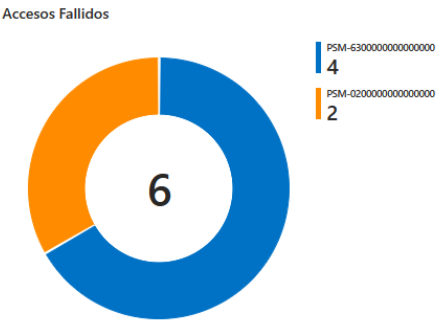


The query returned no results.

Ilustración 1. Top 5 de las conexiones exitosas de usuarios en SPEI.

Accesos Fallidos

En el transcurso de este mes, ocurrieron 6 accesos fallidos, los cuales corresponden al usuario sqlserveraccount.



Accesos Fallidos

EventTime	↑↓	Source_IP	↑↓	User	↑↓	Source_HostName	↑↓	Evento	↑↓	HostName	↑↓	IP_Destino
6/16/2023, 2:13:19 PM		192.168.201.181		PSM-6300000000000000				Acceso Fallido		csbsamsql32.consupago.com		10.129.212.7
6/16/2023, 2:13:18 PM		192.168.201.181		PSM-6300000000000000				Acceso Fallido		csbsamsql32.consupago.com		10.129.212.7
6/14/2023, 6:54:24 PM		192.168.201.181		PSM-0200000000000000				Acceso Fallido		csbsamsql32.consupago.com		10.129.212.7
6/14/2023, 6:54:23 PM		192.168.201.181		PSM-0200000000000000				Acceso Fallido		csbsamsql32.consupago.com		10.129.212.7
6/14/2023, 6:53:33 PM		192.168.201.181		PSM-6300000000000000				Acceso Fallido		csbsamsql32.consupago.com		10.129.212.7
6/14/2023, 6:53:31 PM		192.168.201.181		PSM-6300000000000000				Acceso Fallido		csbsamsql32.consupago.com		10.129.212.7

Ilustración 2. Accesos fallidos en SPEI.

Así mismo, en este mes, por parte de los servidores SPEI no hubo conexiones realizadas.

Servidores SPEI con mas conexiones


 The query returned no results.

Ilustración 3. Servidores SPEI con más conexiones.

Sentinel – Forcepoint

A continuación, se muestra que durante este periodo el apartado de Url´s bloqueadas las cuales presentan un total e 5M de conexiones teniendo como principal origen play.google.com.

Parametro de Tiempo
6/1/2023 12:00 AM - 6/30/2023 11:59 PM

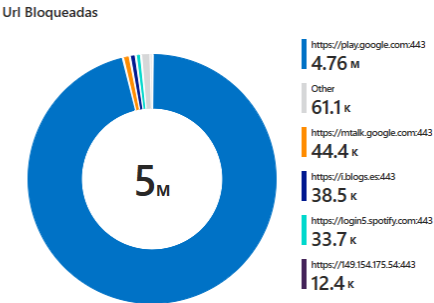


Ilustración 4. Url Bloqueadas.

A continuación, de igual manera como se observa en la siguiente imagen durante este mes se observan datos en el apartado de usuarios con bloqueos web más frecuentes. Encabezada por el usuario Bertin Abel Martinez Plata.

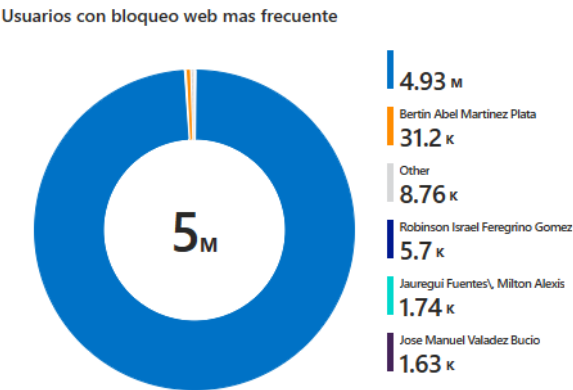


Ilustración 5. Usuarios con bloqueo web más frecuente.

Además, se incluye la captura de los usuarios con acceso más frecuente, lista encabezada por el usuario MonitTI.

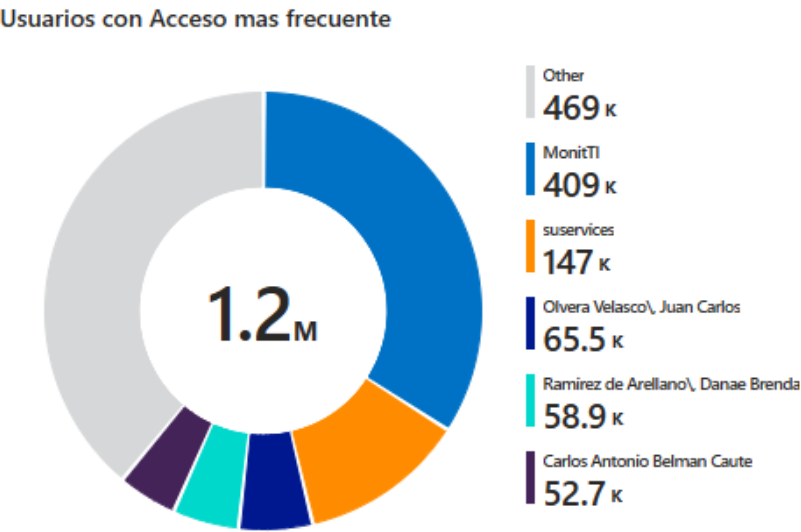


Ilustración 6. Usuarios con Acceso más frecuente.

Sentinel – VPN

A continuación, se muestra la actividad de conexiones VPN que se manifestaron en el periodo reportado. Como se puede apreciar, México domina el primer lugar realizando 9,781 conexiones mediante VPN, seguido de Colombia con 117, Estados Unidos 56, Argentina 35 y Panamá 12.

Actividad de conexiones VPN

*Ilustración 7. Actividad de conexiones VPN.*

En la siguiente ilustración, podemos ver el Top 5 usuarios con más conexiones desde México durante este mes, siendo con más frecuencia el usuario aramme, seguido por amorales, amillan, pmorett y fcornejo.

Top de Usuario con mas Conexiones desde México

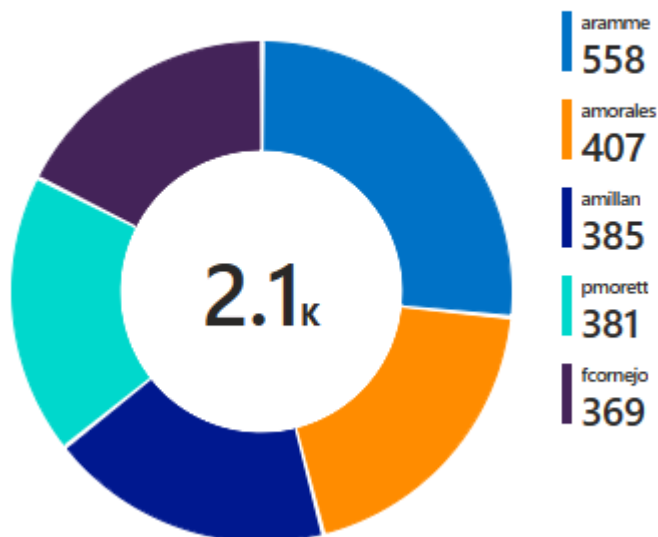


Ilustración 8. Top de Usuario con más Conexiones desde México.

En la siguiente imagen se visualiza el top de inicios de sesión por usuario desde el extranjero que se realizaron durante este mes, siendo el usuario exbhgarcia el que más veces inició sesión desde el exterior, seguido de Other, exjflorez, raguirre y excandres.

Top de inicios de sesión por usuario desde el extranjero

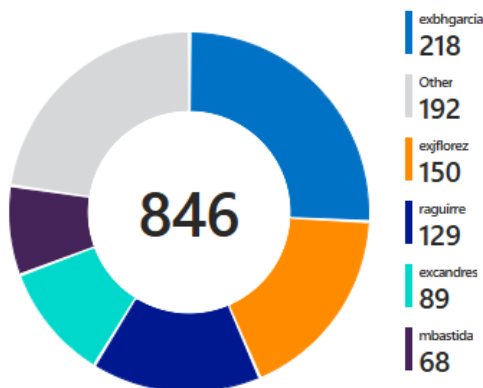


Ilustración 9. Top de inicios de sesión por usuario desde el extranjero

Sentinel – Trafico de red

A continuación, se puede apreciar el total de tráfico aceptado durante este mes, el cual fue de 12,595 Terabytes.

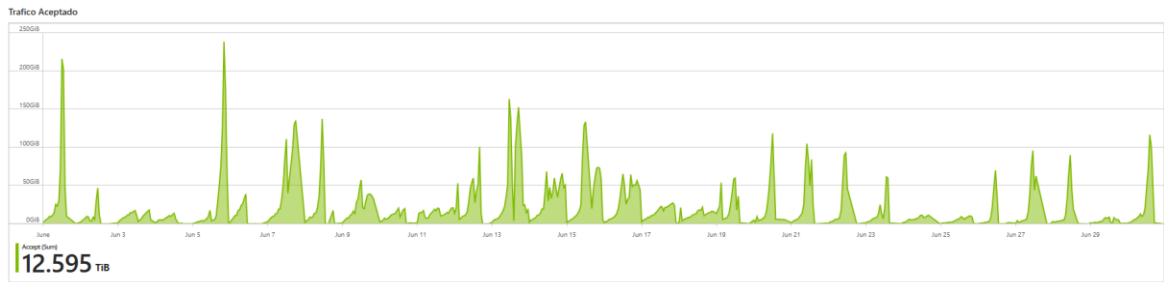


Ilustración 10. Trafico aceptado.

En la siguiente ilustración, se puede visualizar el top 5 de conexiones de origen aceptadas desglosado por direcciones IP durante este mes, las cuales son 192.168.201.113, 10.128.1.21, 192.168.201.210, 192.168.201.211 y 192.168.201.138.

Top de Conexiones Origen Aceptadas

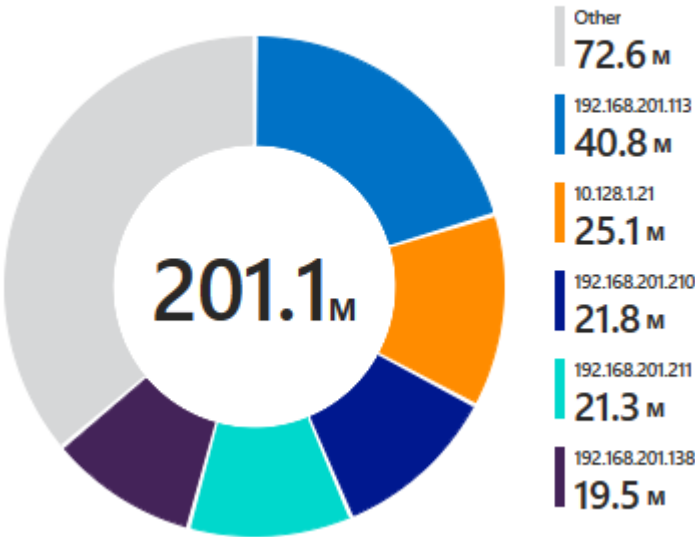


Ilustración 11. Top de conexiones de origen aceptadas desglosado por IP

Sentinel – Tráfico de red rechazada

Como se puede apreciar, las actividades de tráfico rechazado en la red durante este mes, fue de un total 2,867 Gigabytes.

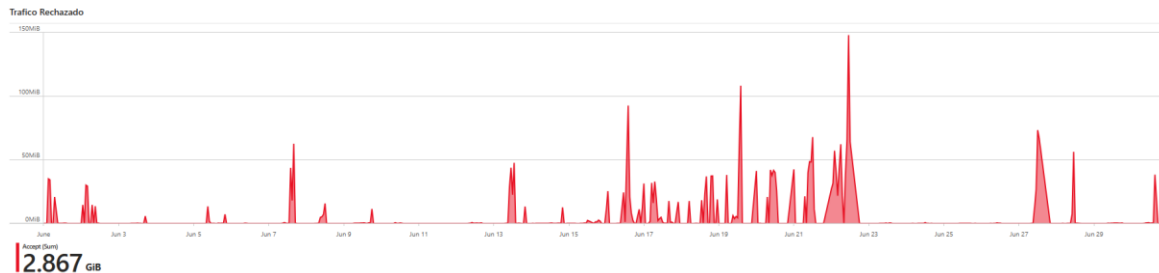


Ilustración 12. Trafico rechazado en la red.

En la siguiente imagen, se puede observar el top de conexiones de origen rechazadas desglosadas por dirección IP durante este mes por posible configuración del Firewall o posiblemente sean sitios bloqueados, las direcciones son: 35.247.51.220, 192.168.201.113, 201.163.187.116, 192.168.195.2 y la 0.0.0.0.

Top de Conexiones Rechazadas por origen

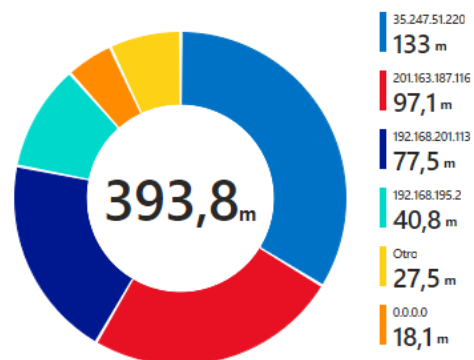


Ilustración 13. Top de conexiones de origen rechazadas desglosadas por IP.

En la siguiente imagen, se puede observar el Top 5 de IP con más tráfico de subida durante este mes, siendo con más frecuencia la dirección IP 10.128.1.21, 192.168.201.166, 192.168.201.208, 192.168.67.21 y por último tenemos a la dirección IP 10.129.214.14.

Top 5 de ip con mas Tráfico de subida

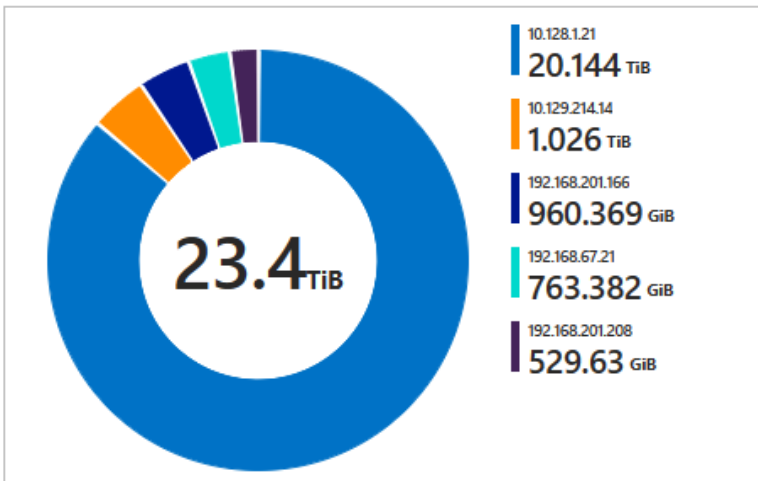


Ilustración 14. Top 5 de ip con más Trafico de subida.

En la siguiente imagen, se puede percibir el Top 5 de IP con más tráfico de bajada durante el periodo del mes de marzo, siendo con más recurrencia la dirección IP 10.128.1.21, 192.168.201.32, 10.129.214.14, 192.168.67.54 y la dirección IP 10.129.212.7.

Top 5 de ip con mas trafico de bajada

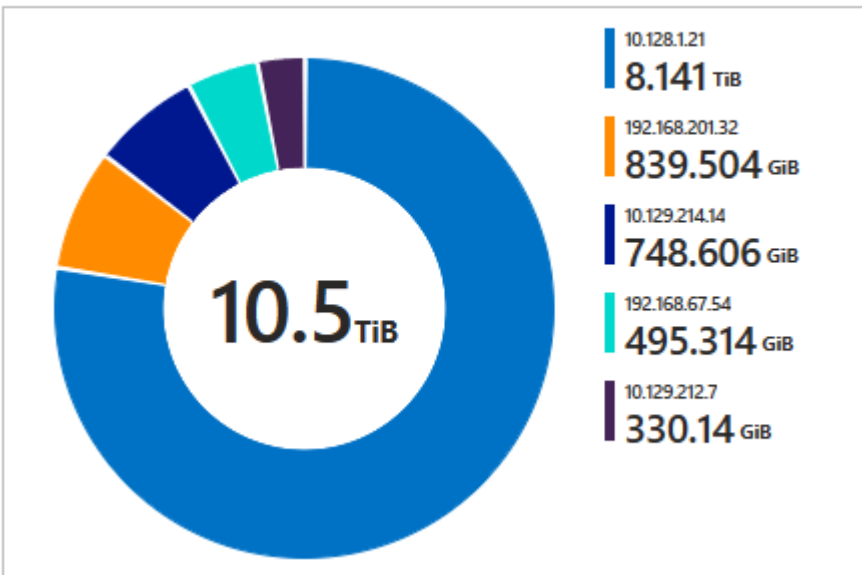


Ilustración 15. Top 5 de IP con más tráfico de bajada.

Sentinel – Antispam

A continuación, se muestra la cantidad de correos movidos a cuarentena durante este mes. Se puede observar que fueron 1067 puestos en cuarentena.

Periodo de tiempo
6/1/2023 12:00 AM - 6/30/2023 11:59 PM
Total de correos Movidos a cuarentena
Total↑↓
1067

Ilustración 16. Total, de correos movidos a cuarentena.

En la ilustración siguiente, se muestra el top 5 a destinatarios más frecuentes que reciben spam en este mes, el correo con mayor actividad fue, bpm@consupago.com, egrajalesg@consubanco.com, comunica@consubanco.com, y comunicadoscomercial@consubanco.com siendo los más relevantes.

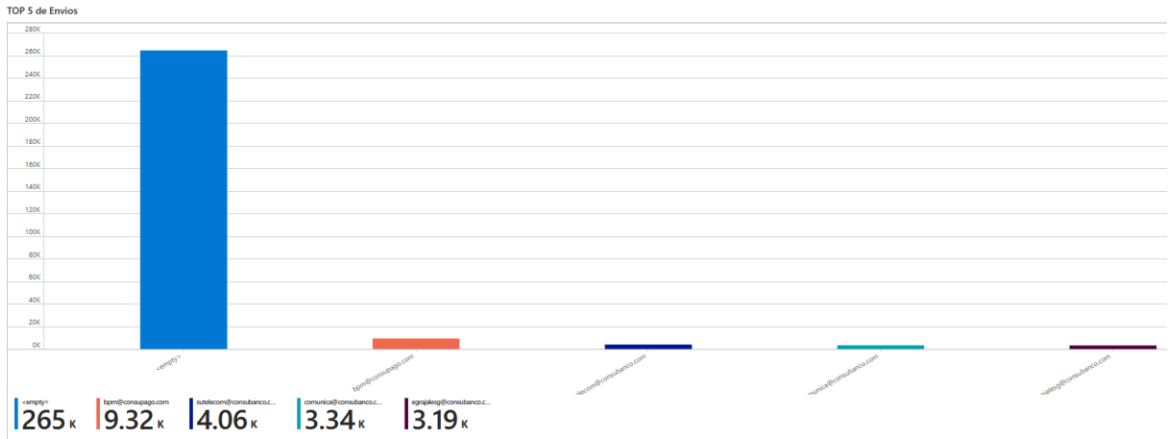


Ilustración 17. Top 5 de envíos de correos

En la siguiente Ilustración, se puede observar los correos más frecuentes movidos a cuarentena en este mes, por motivos de spam, siendo con más frecuencia el correo:

noreply@sending.enlazadot.com, bounce-166610704@bounce.getresponse-mail.com, bounce-107812903@bounce.getresponse-mail.com, postmaster@sendpulse.email, emblue3prd_user2@emark9.embluejet.com y postmaster@sendpulse.email siendo los más sobresalientes. De igual forma se sugiere bloquearlos e ingresarlos a una lista negra para llevar un control de estos.

Correos mas Frecuentes movidos a Cuarentena

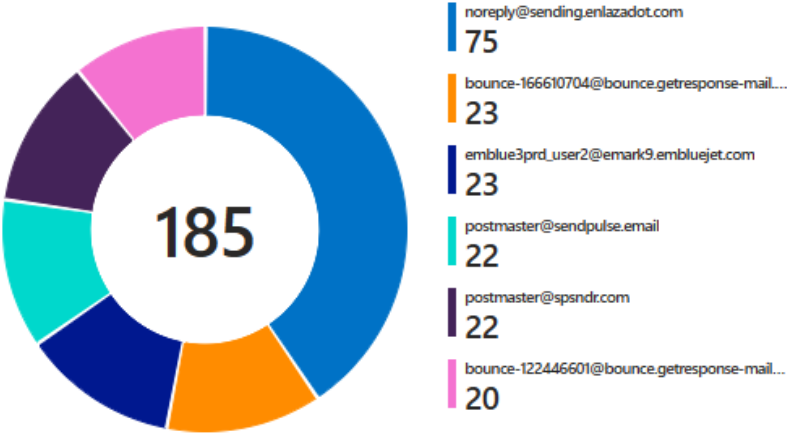


Ilustración 18. Correos más frecuentes movidos a cuarentena

En la próxima gráfica, apreciamos los correos con destinatarios más frecuentes en este mes, siendo con más frecuencia el correo de infosec@consubanco.com, emeza@consupago.com, ralbarran@consubanco.com, rlopez@consupago.com, atencionusuarios@consupago.com y mchavez@consupago.com.

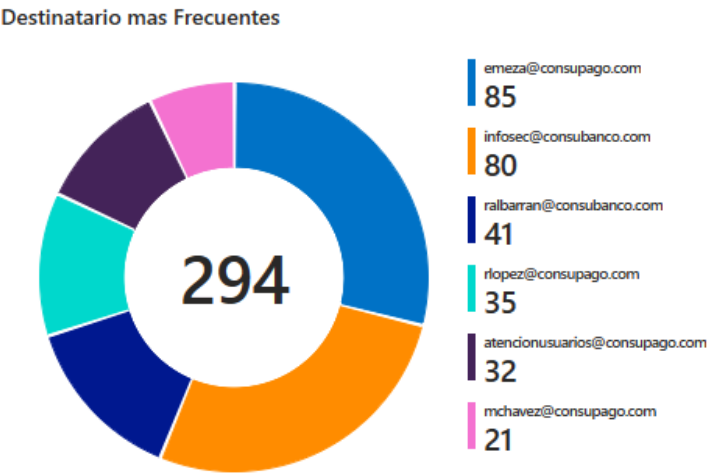


Ilustración 19. Destinatarios de correos más frecuentes

Sentinel – Windows

En seguida, se muestra los accesos fallidos, dominando el primer lugar por el usuario BHERNANDEZ\$, seguido por CSP504GTE1\$, CSB871SUP1\$ y BP0010006587\$.

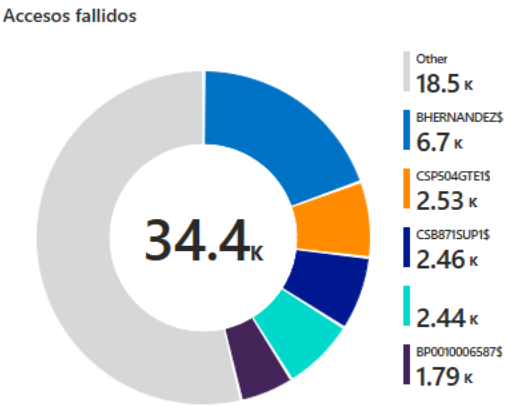


Ilustración 20. Accesos fallidos

En la siguiente ilustración, se puede observar los hosts con accesos fallidos durante el periodo de este mes, siendo con más frecuencia el host cspсадads02.consupago.com, cspсадads01.consupago.com, cspmexads01.consupago.com, CSPMEXADS02.consupago.com y cspjalads02.consupago.com.

Host con mas accesos Fallidos

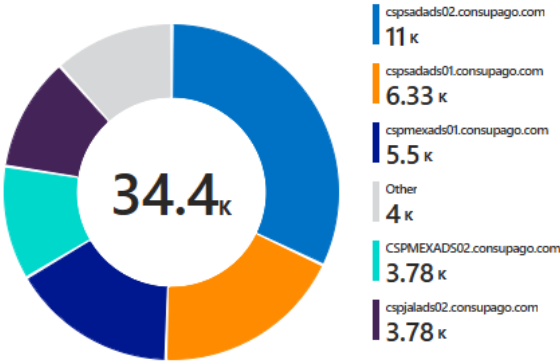


Ilustración 22. Host con más accesos fallidos

Sentinel – Reputación Diaria

A continuación, se observa las conexiones maliciosas bloqueadas por país correspondientes al periodo de este mes, siendo con mayor frecuencia Mexico, seguido por Estados Unidos, en tercer lugar, encontramos a Países Bajos, en cuarto sitio observamos a Canadá, seguido de Reino Unido, Venezuela, después se encuentra a china, Francia y singapur siendo las más destacadas.

Conexiones Maliciosas Bloqueadas

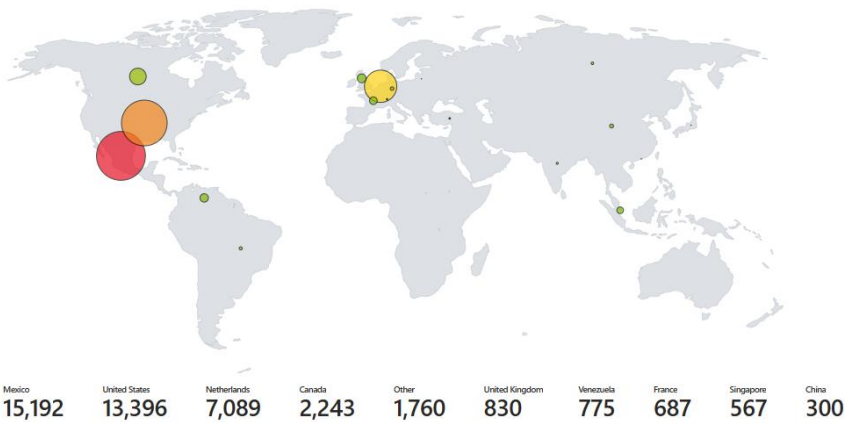


Ilustración 23. Conexiones maliciosas bloqueadas

En la siguiente ilustración se muestra los países con conexiones aceptadas en este mes, siendo con más recurrencia Estados Unidos, México, Países Bajos, Corea del Sur, Bélgica, China y Luxemburgo como los más relevantes.

Conexiones Aceptadas

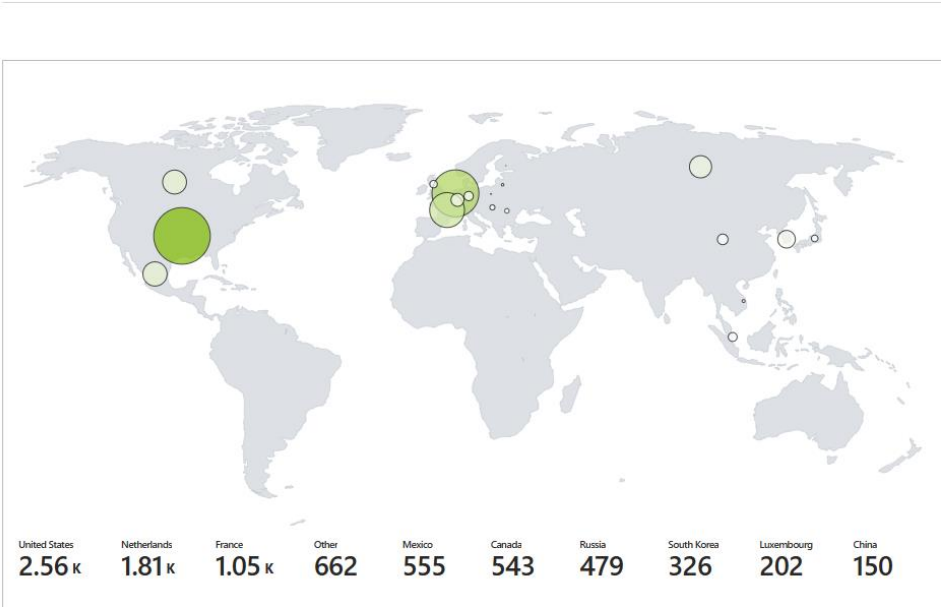


Ilustración 24. Países con conexiones aceptadas

Sentinel – DLP

A continuación, se muestran los archivos que han tenido más movimiento en este mes, los cuales pertenecen a la categoría de Attachment principalmente.

Archivos mas frecuentes

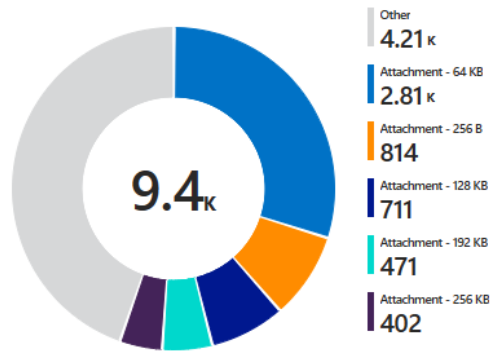


Ilustración 25. Archivos más frecuentes

En la imagen siguiente, se puede ver el top de usuarios a los que más se les ha enviado archivos durante este mes, siendo con más frecuencia el usuario Erika Ivonne Miranda Ramos, MonitTI MonitTI, Hector Esteban Rodriguez, Maria Del Rocio Fonseca Merlos, Gustavo Alejo De Luna, Nancy Yaremi Ruiz Ortega, Sergio Daniel Angel Martinez Davila, Barrientos Cervantes, Andres, Hidalgo Pena, Raymundo Antonio los cuales completan el top.

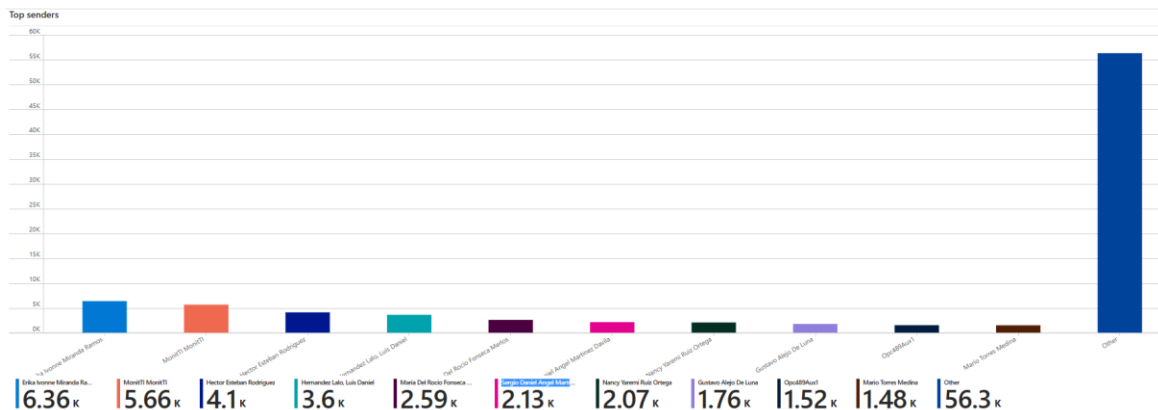


Ilustración 26. Usuarios con más recepción de archivos.

	Informe mensual junio 2023	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Recomendaciones

Se recomienda llevar a cabo las siguientes medidas de seguridad. Adicionalmente, se tomarán los datos recopilados en este análisis para identificar comportamientos anómalos que indiquen vulnerabilidades o incidentes de seguridad.

- Los fallos de autenticación al iniciar sesión los usuarios es importante verificar que estos errores no superen la cantidad media reportada mes con mes, monitorear los inicios de sesión por si hay alguno de forma sospechosa. Ya que los fallos en usuarios son algo normal, sin embargo, en caso contrario si se tiene una alta incidencia podría tratarse de algún tipo de ataque de fuerza bruta.
- Hacer uso de contraseñas robustas para el ingreso a páginas de administración. Las contraseñas deberán tener una longitud de al menos 14 caracteres, entre mayúsculas, minúsculas, números y caracteres especiales.
- Es necesario verificar que la modificación de algún objeto de usuario, así como cuando se realizan cambios en los controladores de dominio, servidores miembros y estaciones de trabajo estos cambios sean legítimos.
- Realizar seguimientos de los cambios para las cuentas temporales, en estaciones de trabajo de usuario para evitar estaciones de trabajo no autorizadas.
- No abrir correos electrónicos de personas o empresas ajenas a esta y que contengan archivos desconocidos.
- Las políticas de DLP están estrechamente ligadas a los usuarios, grupos y listas. Es importante asegurarse de que la herramienta de DLP se integre correctamente con la estructura de directorios de la organización, y utiliza la función que existe en la mayoría de las herramientas de DLP para enlazar a los usuarios con sus direcciones de protocolo de configuración para cliente dinámico (DHCP). Algunas organizaciones son descuidadas con sus directorios, lo cual puede hacer difícil localizar a un usuario infractor (o aplicar políticas a las personas adecuadas).

	Informe mensual junio 2023	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Acuse de recibido

Leído y analizado el presente informe, se firma de conformidad para todos los efectos.

Dpto. TI - Luis Hernández

Depto. TI – Márquez Álvarez Alejandro

SOC Manager - Ivan Hernández Cortés

Observaciones



CII