



CII CYBERPEACE

INFORME DE EVENTOS

EXITUS



www.cyberpeace.tech

	Informe de eventos	Versión:	01	
		Clasificación:	Reservado	
		Etiqueta:	TLP: Amber	

SGSI-DOC-SOC-06 EXITUS-INFORME MENSUAL							
Elaborado por:	Juan MARTÍNEZ GUTIÉRREZ						
Aprobado por:	Ivan HERNÁNDEZ CORTES						
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

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

Contenido

Contenido	2
Confidencialidad	3
Aviso de Restricción	4
Introducción.....	5
Actividades realizadas durante el Periodo	5
Evidencia	6
Azure Máquinas Virtuales	6
Alertas de seguridad en Azure	6
Sentinel – Windows	8
Sentinel – MS SQL SERVER	8
Sentinel – Hyper-V	10
Sentinel – Fortigate	11
Interfaces de RED con mayor actividad.....	12
Interfaz Vlan_WIFI.....	12
Interfaz port5.....	13
Interfaz Management.....	14
Interfaz Vlan root	15
Interfaz port7	16
Interfaz ssl.root.....	17
Interfaz port8.....	18
Interfaz Cybolt-RedIT	19
Fortigate-FW-INCLOUDDC_II	20
Mapa de conexiones	21
RECOMENDACIONES	22
Acuse de recibido.....	23

	Informe mensual	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 Exitus Credit 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.

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

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	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Introducción

El presente informe se encarga de documentar y reportar toda actividad sospechosa o potencialmente crítica que se registró tanto en la plataforma de Microsoft Azure, así como del equipo perimetral Fortigate.

Se anexan recomendaciones por parte de Cyberpeace que se espera sean atendidas para poder robustecer la infraestructura de Exitus Credit 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 Exitus Credit.

Actividades realizadas durante el Periodo

- Monitoreo de la infraestructura Azure haciendo inteligencia de amenazas, alertamientos y recomendaciones de seguridad de acuerdo con la visibilidad que se tiene.
- Monitoreo del equipo Firewall Fortigate para observar el comportamiento de la red y de los usuarios que se conectan a la red.
- Investigación de las direcciones IP que son consultadas con mayor frecuencia para la verificación de la existencia de un malware en un host dentro de la red interna

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

Evidencia

Azure Máquinas Virtuales

Se cuenta con 1 máquina virtual que está conectada con la consola de Azure Security Center.

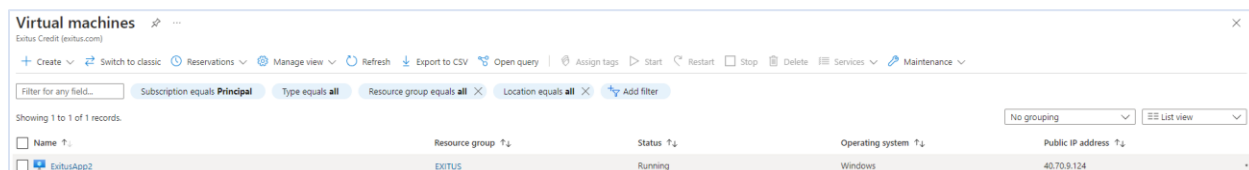


Imagen 1. Máquinas virtuales conectadas con Azure Security Center.

Como se puede visualizar en la siguiente imagen, los permisos para la lectura de recomendaciones de seguridad son limitados. De la misma manera, se muestra que durante este periodo no ha habido incidentes de seguridad relacionados con el sistema y dado a esto, no se realiza recomendación alguna.

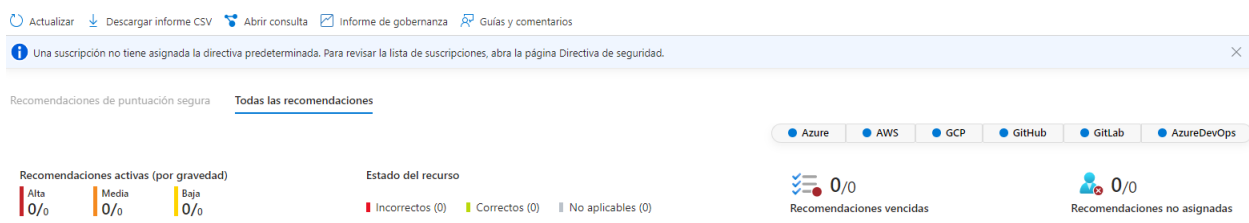





Imagen 2. Recomendaciones de Azure Security Center para los recursos.


Alertas de seguridad en Azure


A continuación, en la siguiente imagen, se muestra que no se cuenta con alguna alertas seguridad o incidencias relacionados con los recursos de Azure.

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

 0
Alertas abiertas

 0
Alertas activas

 0
Alertas en curso

 0
Recursos afectados

Abrir alertas por gravedad

Suscripción == All

Estado == Activo, En curso

Gravedad == Baja, Media, Alta

Add filter

Sin agrupar

Gravedad

Nombre de alerta


Recurso afectado

Grupo de recursos

Hora de inicio de la activid...

Tácticas de MITRE ATT&CK®

Estado



No se ha encontrado ninguna alerta.

Imagen 3. Alertas de seguridad en Azure.

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


Sentinel – Windows

En la sección correspondiente a Sentinel Windows, no se cuentan con registros de Log In fallidos.

Windows

Parametro de tiempo: 1/6/2023 0:00 - 30/6/2023 23:59

Top 5 de Logins Fallidos

 Por el momento no hay accesos fallidos

Logins Fallidos


 Por el momento no hay accesos fallidos

Imagen 5. Eventos en Windows

Sentinel – MS SQL SERVER

A continuación, se presentan top de las direcciones IP con más intentos de inicio de sesión en el Servidor SQL durante el periodo de junio. Los hosts con mayor actividad son: 189.201.147.17 y 201.150.38.154.

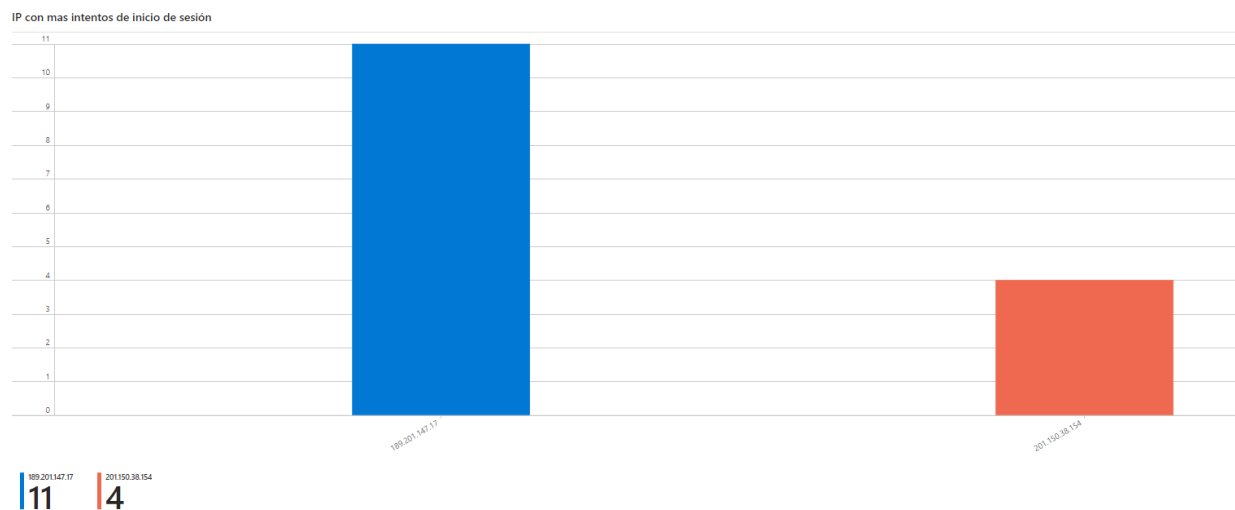


Imagen 4. IPs con más intentos de inicio de sesión.

Cuentas de usuario con mas intentos de inicio de sesión

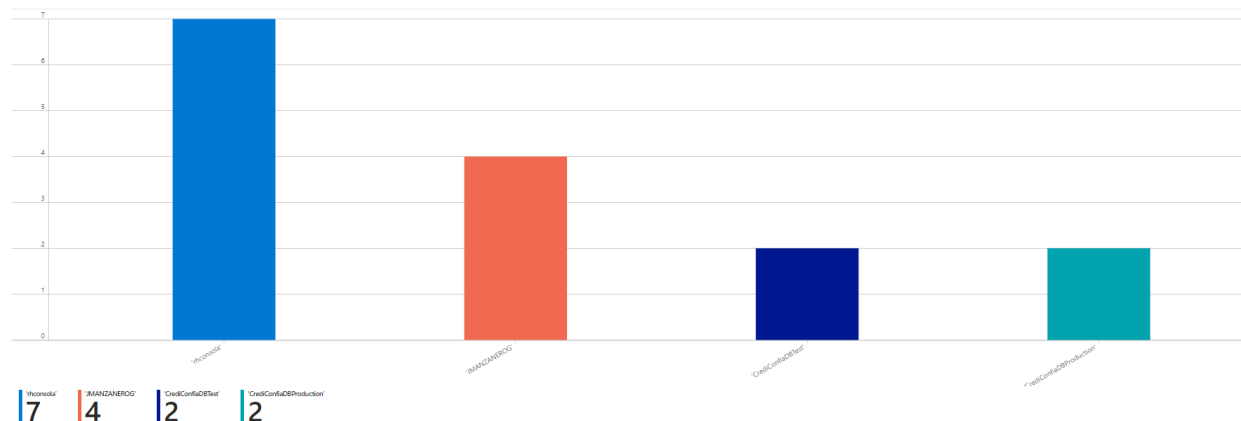


Imagen 7. Cuentas de usuario con más intentos de inicio de sesión.

En la siguiente imagen podemos observar a los usuarios que han tenido mayores inicios de sesión fallidos durante el mes de junio.

Top de Inicio de sesión fallidos

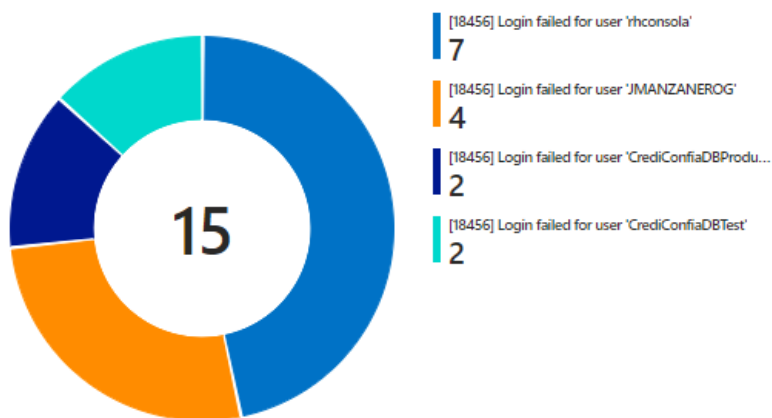
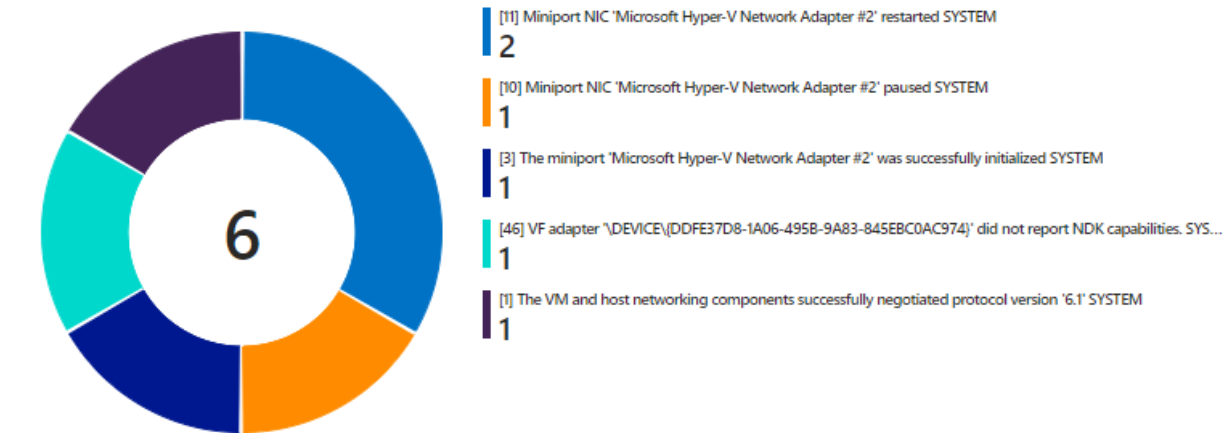


imagen 8. Top 5 inicios de sesión fallidos en el Servidor SQL.

Sentinel – Hyper-V

A continuación, se muestran los eventos que más se presentaron en el host Hyper-V-Netvsc durante el periodo de junio. Aquí se muestran los eventos de red que se suscitaron durante el periodo mencionado.

Eventos por Hyper-V



EventTime	↑↓	HostName	↑↓	Evento	↑↓
18/6/2023, 2:12:36		Microsoft-Windows-Hyper-V-Netvsc		[11] Miniport NIC 'Microsoft Hyper-V Network Adapter #...	
18/6/2023, 2:12:36		Microsoft-Windows-Hyper-V-Netvsc		[10] Miniport NIC 'Microsoft Hyper-V Network Adapter #...	
18/6/2023, 2:12:25		Microsoft-Windows-Hyper-V-Netvsc		[46] VF adapter '\DEVICE\{DDFE37D8-1A06-495B-9A83-8...	
18/6/2023, 2:12:25		Microsoft-Windows-Hyper-V-Netvsc		[11] Miniport NIC 'Microsoft Hyper-V Network Adapter #...	
18/6/2023, 2:12:25		Microsoft-Windows-Hyper-V-Netvsc		[3] The miniport 'Microsoft Hyper-V Network Adapter #2'...	
18/6/2023, 2:12:24		Microsoft-Windows-Hyper-V-Netvsc		[1] The VM and host networking components successfully...	

Imagen 9. Eventos notificados de Hyper-V durante el mes de junio.

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

Sentinel – Fortigate

En este apartado, se muestran las actividades de las interfaces. Durante el mes de junio se puede observar que la interfaz Vlan_WIFI es la interfaz con más actividad.

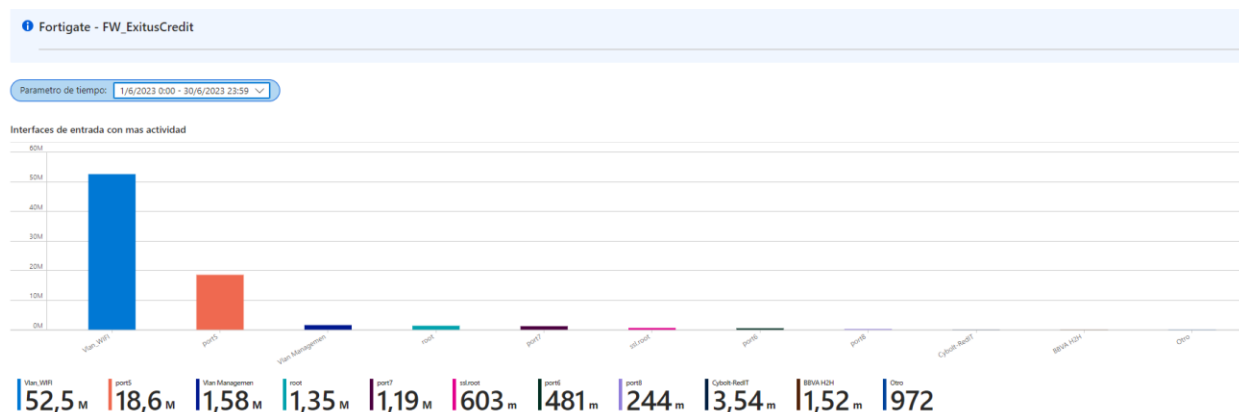


Imagen 10. Número de conexiones de las interfaces durante este último mes.

De igual forma, en seguida, se presentan los protocolos más utilizados durante el mes de junio, siendo el HTTPS (Protocolo que se usa para navegar en los sitios web de forma segura) el primer lugar, en segundo lugar, DNS, y SNMP, siendo los más relevantes.

Protocolos mas utilizados

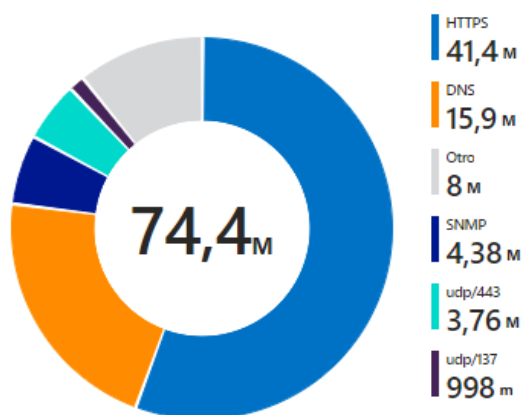


Imagen 11. Top 5 protocolos más usados por las interfaces.

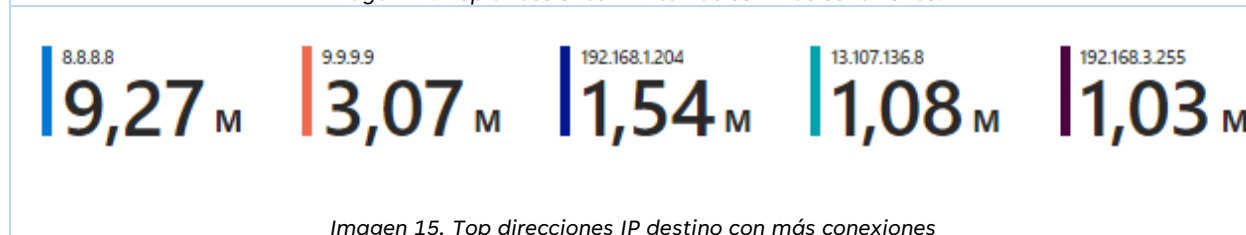
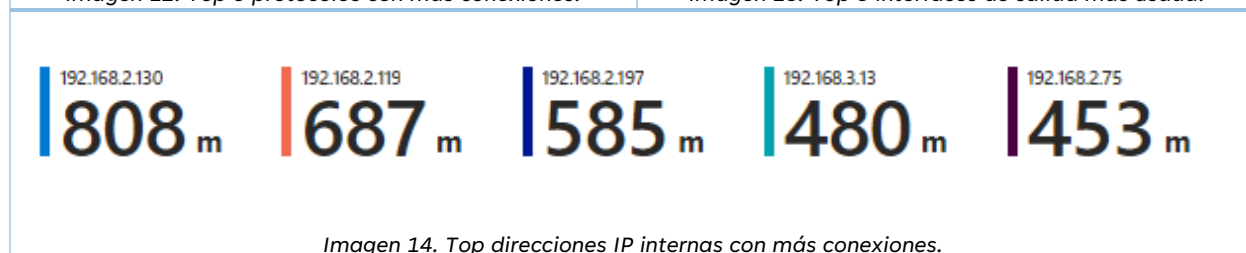
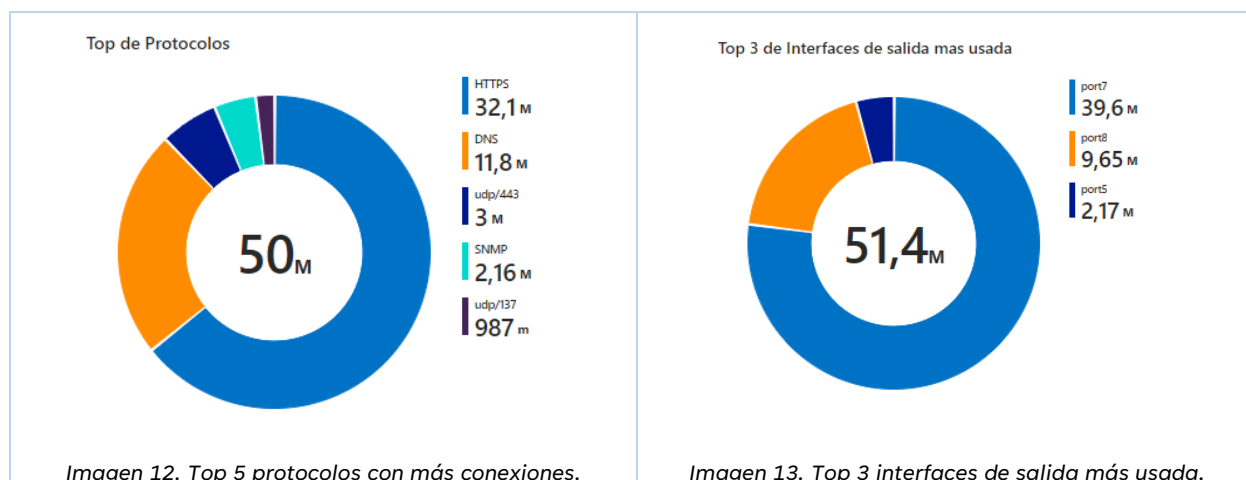
	Informe mensual	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Interfaces de RED con mayor actividad

Interfaz Vlan_WIFI

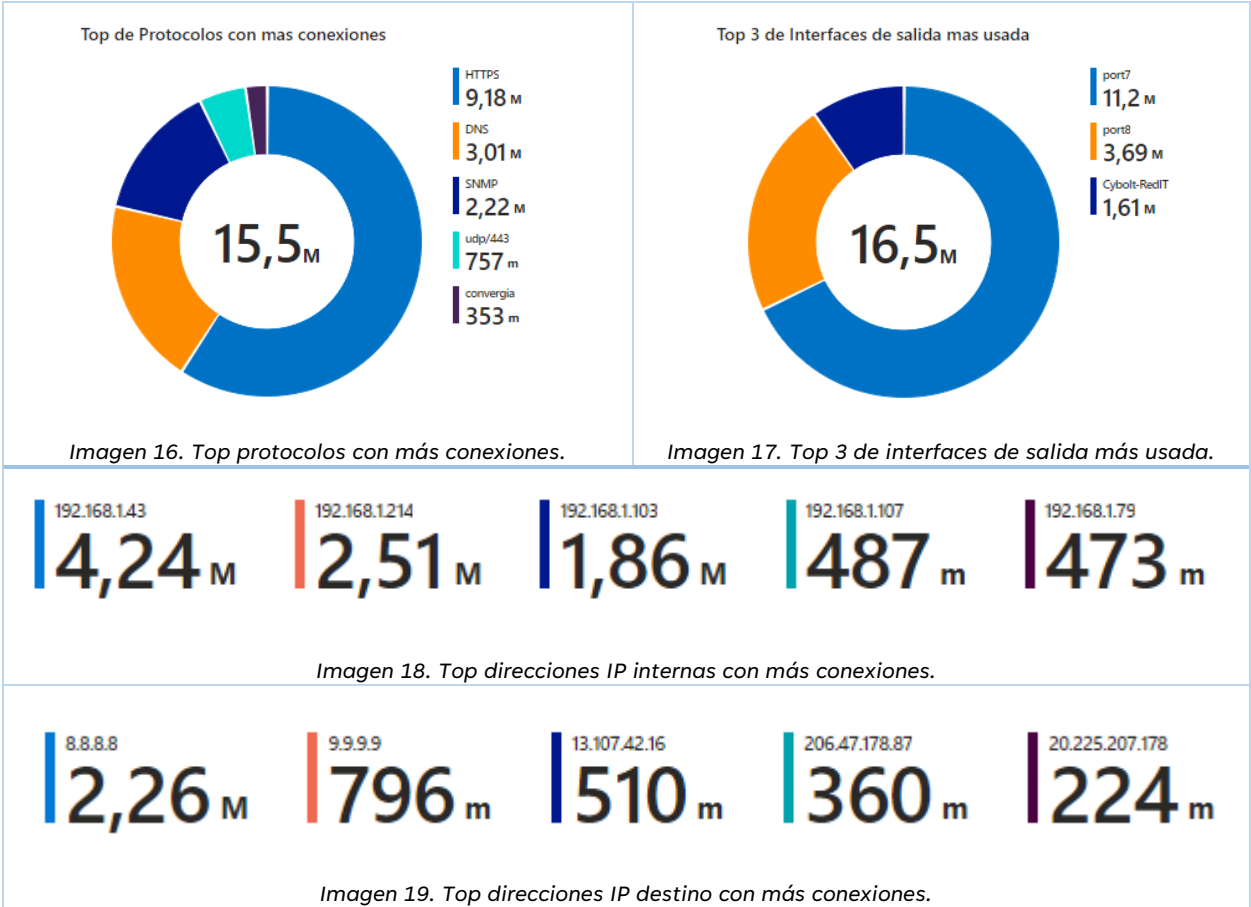
A continuación, se presentan los protocolos con más actividad durante el mes de junio, junto con las interfaces de salida más usadas y las direcciones IP de destino con más eventos.

Los protocolos más utilizados, corresponden a HTTPS (permite establecer una conexión segura entre el servidor y el cliente), DNS (traduce los nombres de dominio en direcciones IP), 443, SNMP (diseñado para supervisar la infraestructura de red y proporciona a los administradores visibilidad centrada en el dispositivo) siendo los más relevantes.



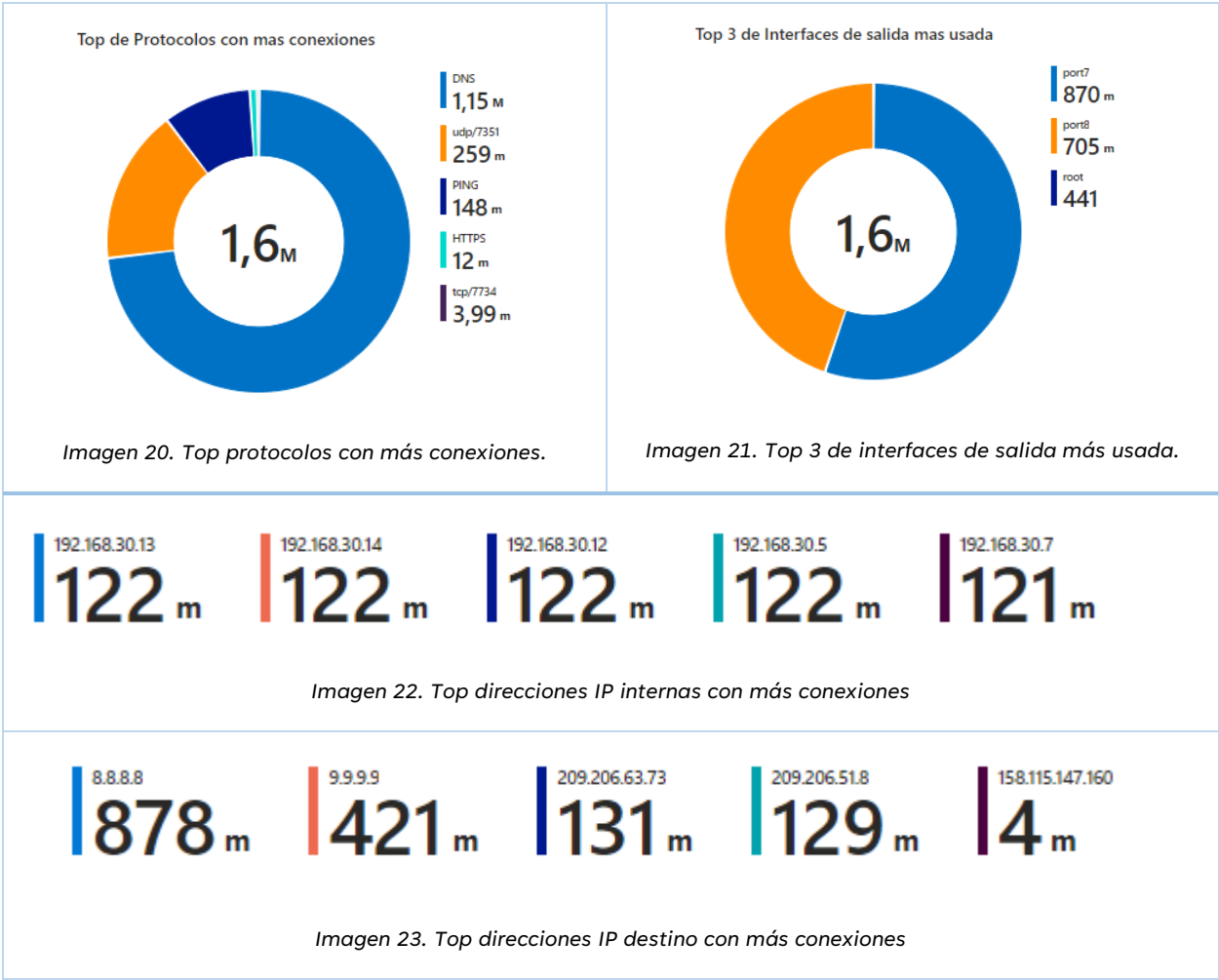
Interfaz port5

A continuación, se presentan los protocolos e interfaces con más frecuencia en el mes de junio, junto con las interfaces de salida más usadas y las direcciones IP de destino con más conexiones.



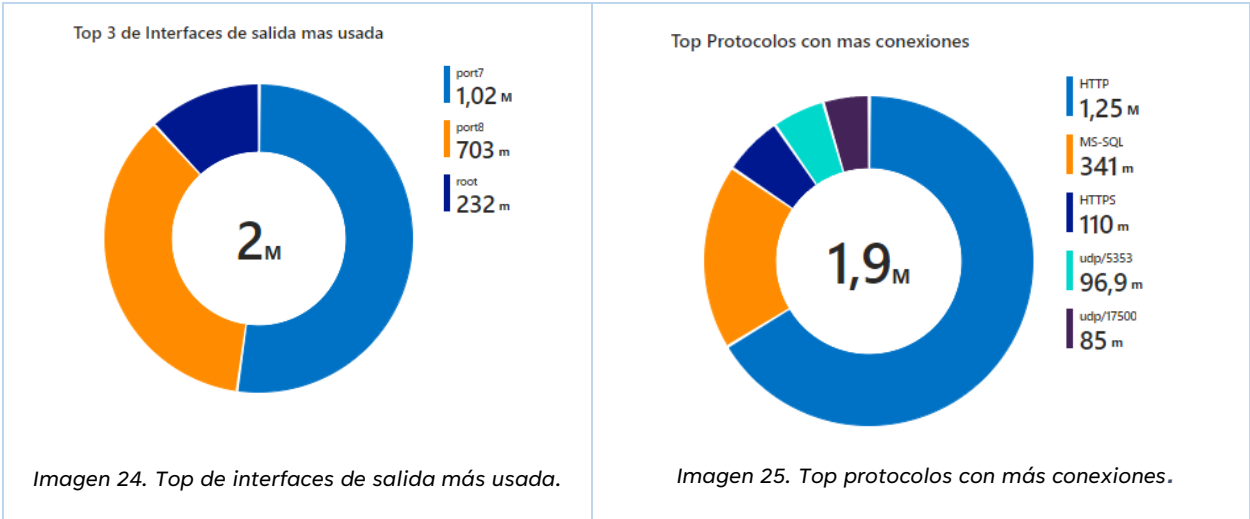
Interfaz Management

En el apartado corresponde a la interfaz Management, se muestran los protocolos más frecuentes durante el mes de junio, junto con las interfaces de salida más usadas y las direcciones IP de destino con más conexiones.



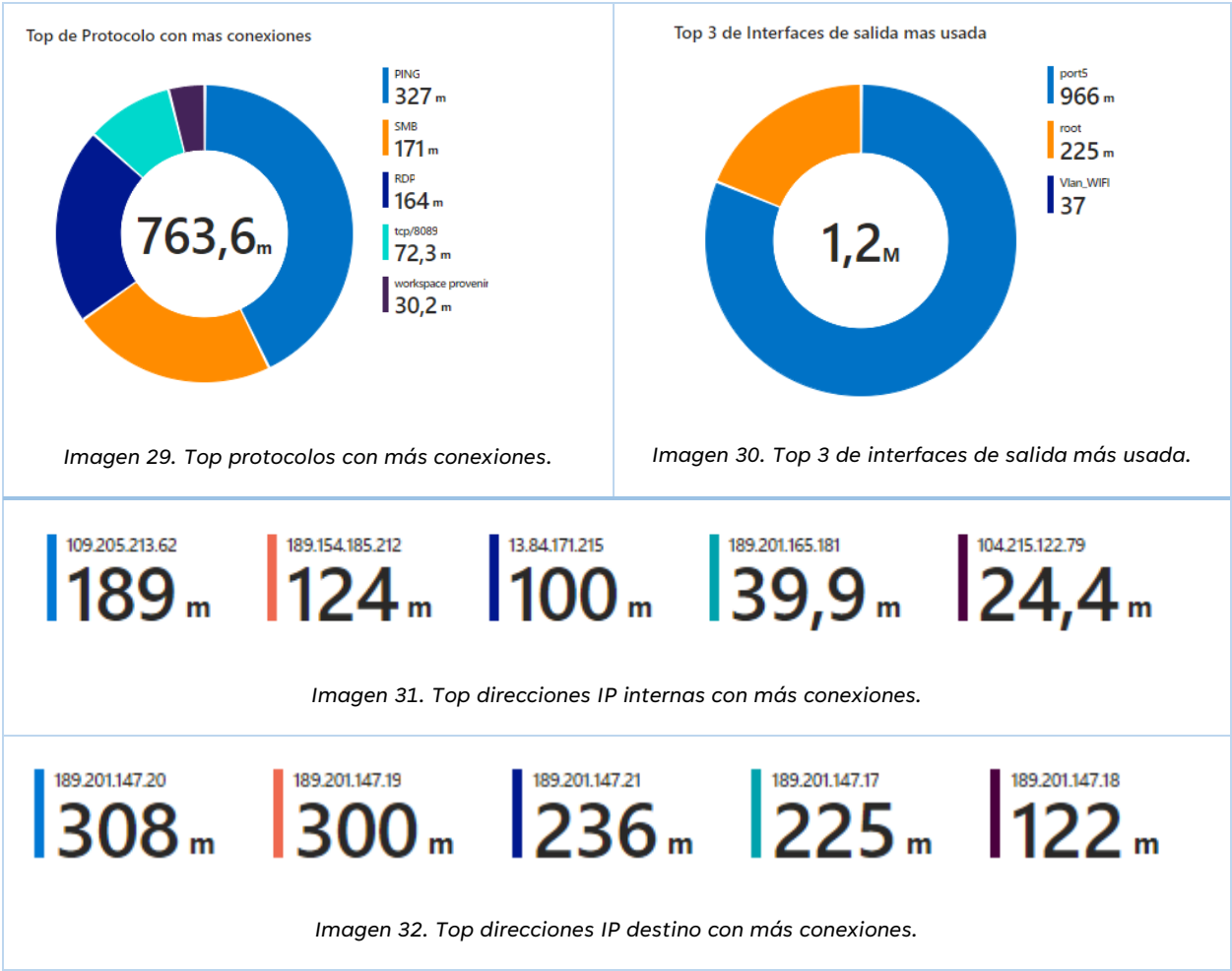
Interfaz Vlan root

Posteriormente, se exponen los protocolos e interfaces que con más recurrencia se estuvieron presentando en el mes de junio, junto con las interfaces de salida más usadas y las direcciones IP de destino con más conexiones.



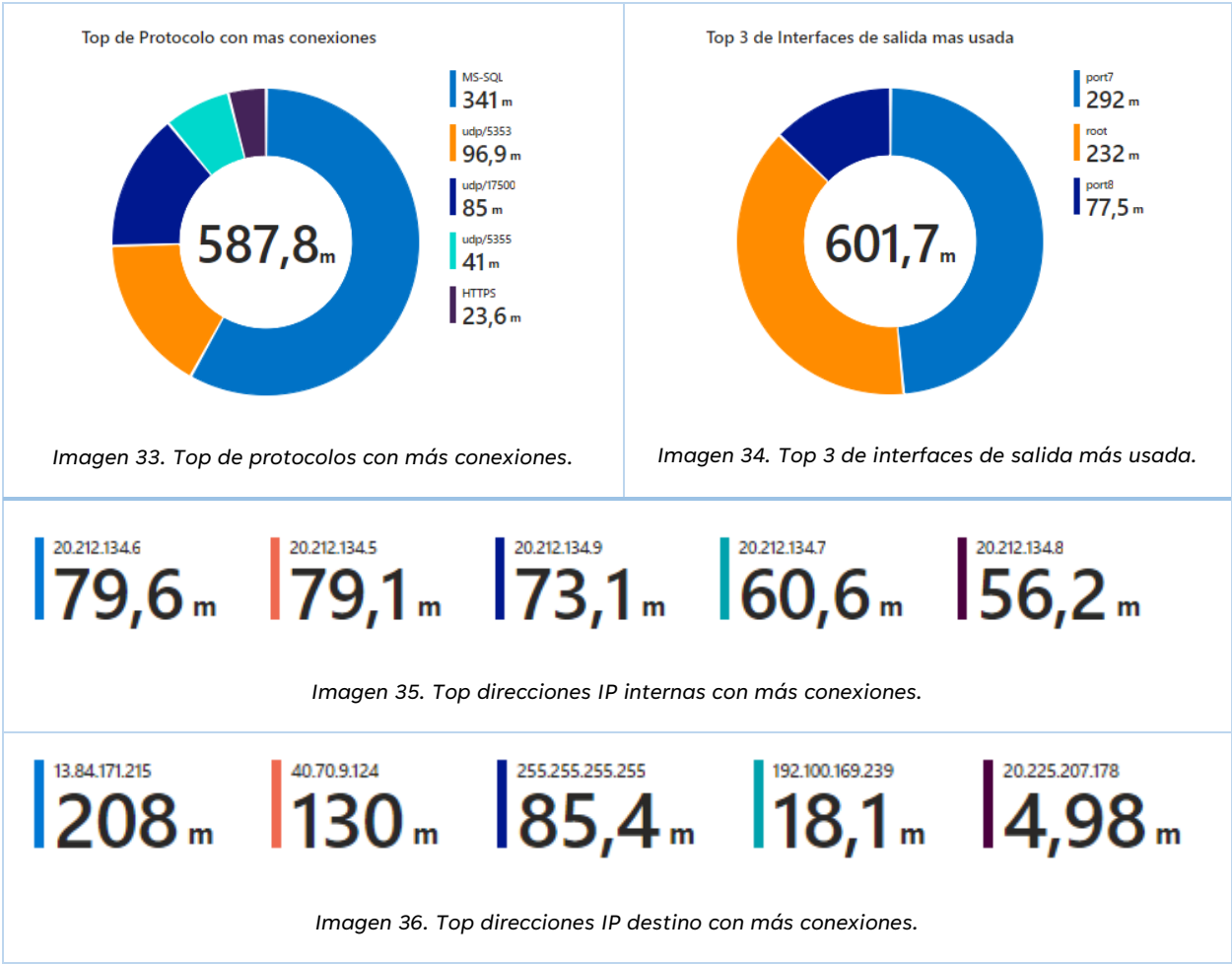
Interfaz port7

En seguida se presentan los protocolos más relevantes durante en el periodo del mes de junio correspondiente a la interfaz port7, junto con las interfaces de salida más usadas y las direcciones IP de destino con más conexiones.



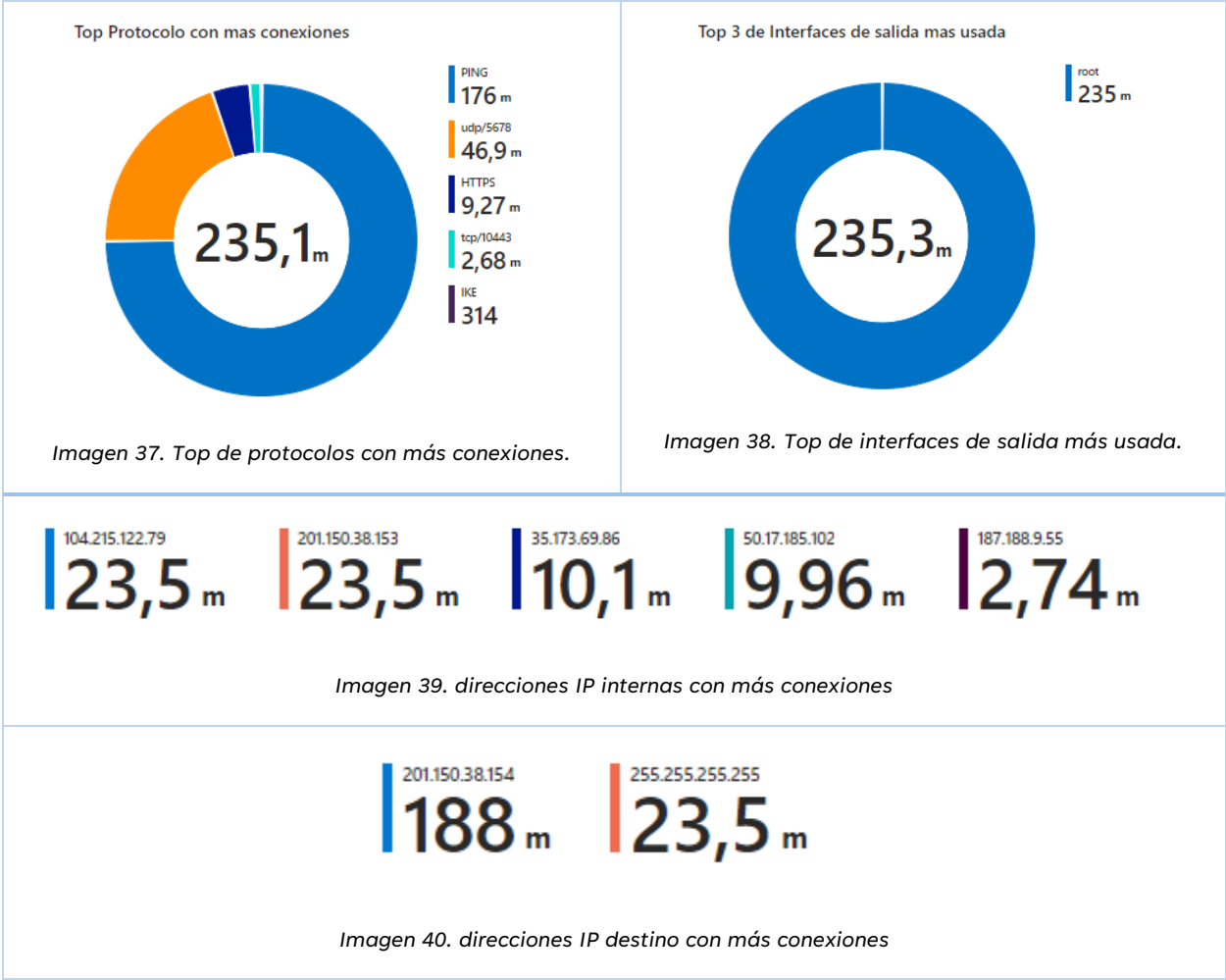
Interfaz ssl.root

En la interfaz ssl.root se dan a conocer los protocolos más recurrentes que se suscitaron en el mes de junio, junto con las interfaces de salida más usadas y las direcciones IP de destino con más conexiones.



Interfaz port8

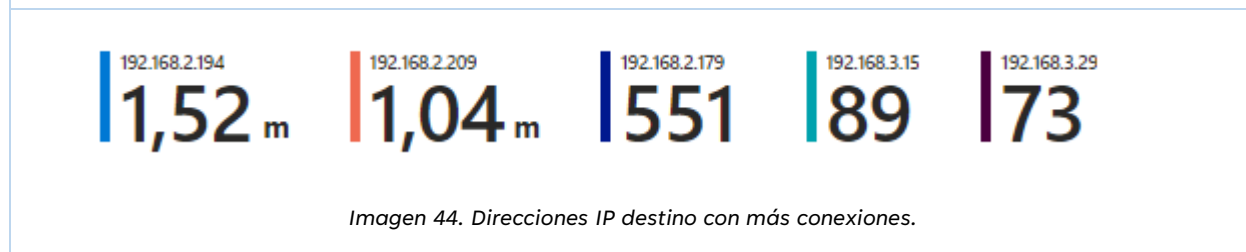
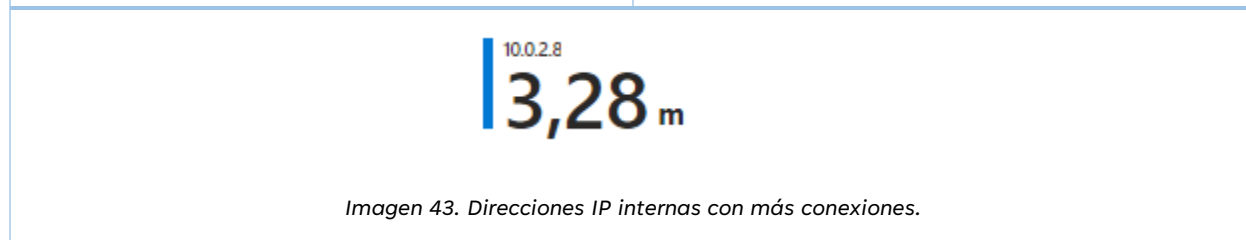
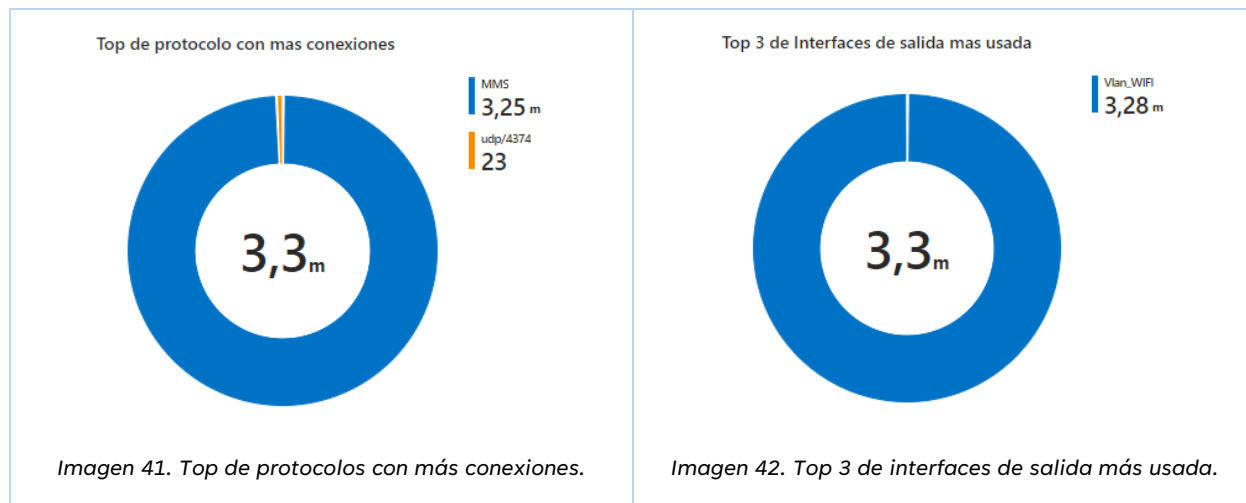
A continuación, se exhiben los protocolos que más presentes estuvieron en el mes de junio, junto con las interfaces de salida más usadas y las direcciones IP de destino con más conexiones. Los protocolos más relevantes son: PING (utilidad de diagnóstico en redes) y puerto 5678 (Conexión del agente de replicación remota).



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

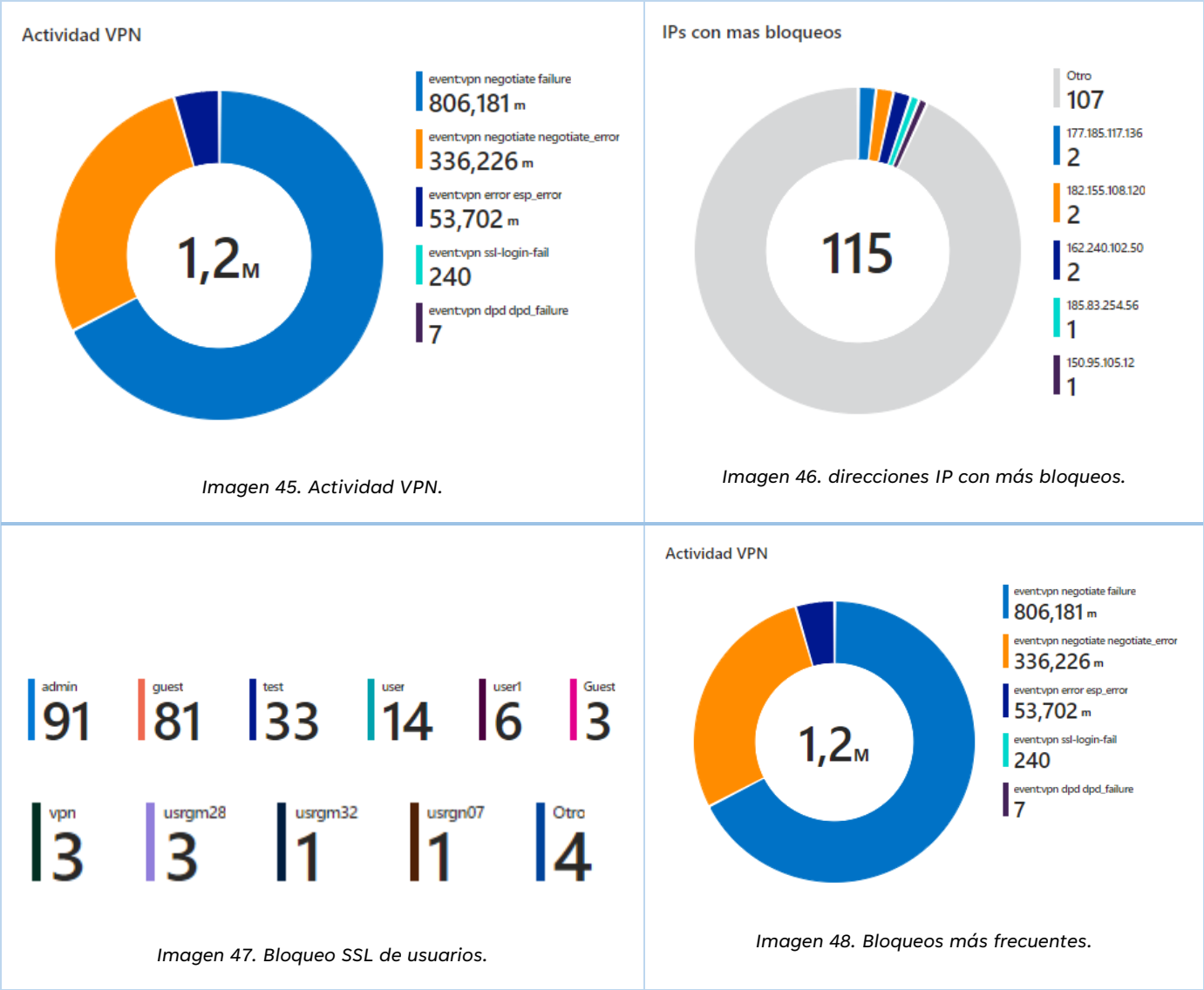
Interfaz Cybolt-RedIT

A continuación, se presentan los protocolos más relevantes en el mes de junio, junto con las interfaces de salida más usadas y las direcciones IP de destino con más conexiones. El protocolo más usado en este mes es MMS (Protocolo estándar de envío de mensajes que incluyen contenido multimedia hacia y redes móviles a través de una red celular).



Fortigate-FW-INCLOUDDC_II

En esta sección se presenta la actividad de la VPN, los bloqueos SSL (protocolo para establecer enlaces en una comunicación), las direcciones IP que fueron bloqueadas durante el periodo del mes de junio y por ultimo los eventos que con mayor frecuencia se presentan, los cuales fueron bloqueados.



Se destaca que el apartado de bloqueo SSL corresponde a inicios de sesión fallidos por parte de los usuarios: admin, guest, test, user, user1, Guest y vpn.

Así mismo, los bloqueos más recurrentes son debido a eventos relacionados a backdoor:

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

Mirai.Botnet, misc:AndroxGh0st.Malware, backdoor:Bladabindi.Botnet, web_server: PHPUnit.Eval-stdin.PHP.Remote.Code.Execution y backdoor: SystemBC.Botnet.

Se recomienda aplicar las actualizaciones o parches de seguridad más recientes del proveedor y utilizar el software antivirus para escanear y limpiar los dispositivos infectados.

Mapa de conexiones

Durante el mes de junio no hubo actividad sospechosa bloqueada durante el periodo reportado.

Parametro de Tiempo

1/6/2023 0:00 - 30/6/2023 23:59

Conexiones Bloqueadas

i
La consulta no devolvió ningún resultado.

i
La consulta no devolvió ningún resultado.

Imagen 49. Mapa de conexiones bloqueadas.

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

RECOMENDACIONES

- Hacer uso de políticas de inicio de sesión de usuarios con privilegios altos.
- 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. Así mismo puede utilizar un administrador de contraseñas que le permitirá mantener sus contraseñas encriptadas de forma segura.
- 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.

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

Acuse de recibido

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

Stephanie Anabel Ramos

SOC Manager - Ivan Hernández Cortés

Observaciones

