INFORME EJECUTIVO DE SEGURIDAD CIBERNÉTICA DE OPERACIONES E INTELIGENCIA

Metrobank S.A.

Noviembre, 2018

CONFIDENCIAL

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com

Tabla de contenido

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Sobre este informe

El propósito de este documento es reportar el "estado" de seguridad de su organización. Debe ser destacado que GLESEC basa el análisis de la información en los servicios contratados. La información generada por estos servicios es luego agregada, correlacionada y analizada. Mientras más completo sea el grupo de servicios contratados, más precisos y completos serán los resultados.

Este Informe se organiza en tres partes; La primera es el Resumen Ejecutivo con recomendaciones (como sean necesarias o aplicables), la segunda es la Sección de Inteligencia, con más información detallada, tableros de análisis y la última es la Sección Operacional, con el estado de los servicios y contra-medidas bajo contrato, tickets por cambios de mantenimiento e incidentes reportados y actividad consultada en el mes.

Nosotros en GLESEC creemos que la seguridad de la información es un proceso dinámico y holístico que requiere investigación sobre la marcha y seguimiento y debe ser manejado con las herramientas, sistemas y procesos correctos, así como personal capacitado y dedicación. El proceso es dinámico debido al constante descubrimiento de nuevas vulnerabilidades y exploits, la proliferación de herramientas de hacking que hacen muy fácil para principiantes con mínimo conocimiento causar daño. El incremento en malware, phishing, amenazas internas, espionaje, crimen organizado, robo de propiedad intelectual y hacktivismo son la causa de exposición de la seguridad de la información y son impulsados más comúnmente por una ganancia económica. Los servicios subcontratados de GLESEC, basados en el portafolio de su plataforma propietaria TIP™ proveen la respuesta ideal para lo expuesto anteriormente.

Confidencialidad

GLESEC considera la confidencialidad de la información de los clientes como un secreto comercial. La información bajo este contexto se clasifica como:

- Nombre e información de contacto del cliente
- Arquitectura del sistema, configuración, métodos de acceso y control de acceso
- Contenido de seguridad

Todo lo mencionado arriba es resguardado de manera segura de la misma forma como GLESEC resguarda su propia información confidencial.

Alcance de este informe

Tabla Servicios contratados con GLESEC
Esta tabla enlista los servicios e inteligencia de GLESEC TIP™ que están contratados actualmente y la correspondiente fecha de expiración de los mismos.

Type	Service	Contracted?	Service Expiration
Threat Mitigation	MSS-APS	YES	06/01/2019
Threat Mitigation	MSS-APS-SSL		
Threat Mitigation	MSS-APS-PS		
Threat Mitigation	MSS-APFW	YES	06/01/2019
Vulnerability Testing	MSS-VME	YES	06/01/2019
Vulnerability Testing	MSS-VMI		
Compliance	MSS-EPS		
Threat Mitigation	MSS-SIEM		
Risk assessment	MSS-BAS		
Threat Mitigation	MSS-EDR		
Threat Mitigation	MSS-UTM		
Threat Mitigation	MSS-INT		
Access Control	MSS-TAS		

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Resumen Ejecutivo

Este informe corresponde al periodo de Noviembre, 2018

La siguiente tabla describe las categorías principales que GLESEC ha identificado reportar en el estado-de-seguridad de sus clientes-miembros. Las categorías en la tabla de abajo son basadas en una metodología de manejo de riesgo. Esto es un aspecto principal y fundacional de GLESEC.

RIESGO

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance. The NIST Cyber-Security Framework

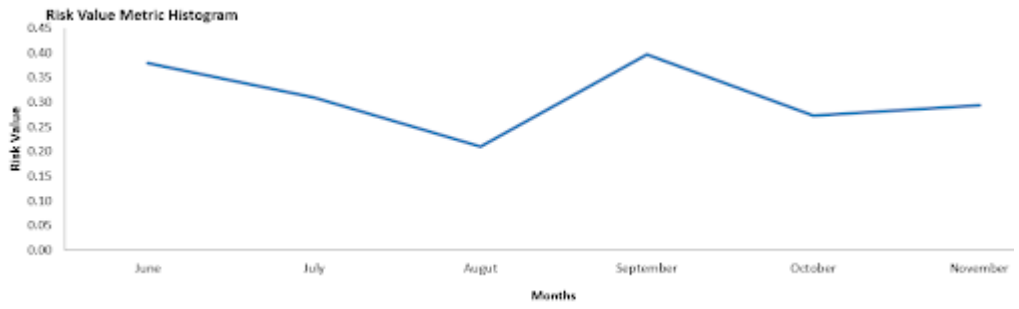
Una de las columnas fundacionales de GLESEC es basar todas sus actividades en lograr la determinación y mitigación de riesgo. Lo que cualquier organización debería querer conocer es cuál es su nivel de Riesgo, en este caso en particular enfocado en seguridad cibernética. Riesgo en Seguridad tiene un impacto directo en el negocio y, como tal, es de suma importancia para los Directivos y la Administración de la compañía.

Nosotros en GLESEC medimos RIESGO a través de varias perspectivas y utilizando varios de los servicios de la plataforma TIP™. El MSS-VM o Servicio de Seguridad Administrado para Manejo de Vulnerabilidades nos proporciona una vista, cuán débiles son los sistemas de la organización. El MSS-BAS nos proporciona una visión de cuán débiles son las defensas de la organización a las últimas amenazas. El MSS-APS, MSS-SIEM, MSS-UTM, MSS-EDR, MSS-EPS nos proporciona información de ataque tanto interna como externa, DDOS, Malware, ransomware y otra información vectorial de ataque, así como también brinda servicios de nivel de protección. El MSS-EPS también nos proporciona información de nivel de RIESGO por incumplimiento de los requisitos y / o regulaciones internas o externas. En general, unas variedades de servicios nos proporcionan diferentes puntos de vista y juntos tenemos la vista más completa de la postura de seguridad de nuestros clientes.

Determinamos que la condición de riesgo para Metrobank S.A. para el mes de agosto es crítica. Esto se puede ver en el indicador de seguridad como se indica a continuación.

Indicador de Riesgo	**Servicio**	**Condición**	**Comentarios**
Métrica de Valor de riesgo	MSS-VME	**CRITICO**	Se reporta 2 vulnerabilidades críticas y 6 altas. Cualquiera de estas puede causar un impacto negativo a Metrobank S.A.

El siguiente histograma de VALOR RIESGO representa los cambios en la métrica de valor de riesgo basada en la vulnerabilidad en los últimos seis meses.



Para el mes de noviembre el aumento en su nivel de riesgo está relacionado a un incremento significativo en las vulnerabilidades de severidad crítica y alta. El host critico 190.34.183.139 presenta una vulnerabilidad en HTTP.sys esto podría permitir

la ejecución remota de código (3042553) (uncredentialed check) en los puertos 80 y 443.

VULNERABILIDADES

El servicio MSS-VM (E / I) de GLESEC se utiliza para realizar dos pruebas semanales a sistemas externos y / o internos (según las opciones del servicio contratado). De las dos pruebas que se realizan semanalmente, una es probar el descubrimiento de los activos en la red y el otro para detectar vulnerabilidades. Las pruebas externas se realizan desde la plataforma en la nube de GLESEC y la interna se realiza con el dispositivo de seguridad múltiple de GLESEC (GMSA).

Las vulnerabilidades son debilidades que, de ser explotadas, pueden comprometer la organización y, como tales, son un componente de RIESGO para la organización. Si hay vulnerabilidades y también amenazas, existe el RIESGO de que la organización puede verse afectada. Las vulnerabilidades informadas por GLESEC deben considerarse todas importantes y abordarse según la prioridad (crítica, alta, media y baja). Un proceso efectivo es trabajar con la información proporcionada por GLESEC y el equipo de consultoría GLESEC para abordar las recomendaciones proporcionadas de manera sistemática y continua. El progreso puede ser determinado por las pruebas semanales.

Para este período, Metrobank S.A, el número total de vulnerabilidades ha aumentado a 64 en comparación con el mes anterior. El número total de vulnerabilidades se clasifica de la siguiente manera: 2 para el riesgo crítico, 6 para el riesgo alto, 34 para el riesgo medio y 22 para el riesgo bajo. Es necesario seguir las recomendaciones para reducir la cantidad de vulnerabilidades actuales.

Entre las categorías con mayor número de vulnerabilidades, podemos mencionar: General con 36 esto representa 56%, Misc. con 16 esto representa el 25% y la detección de servicio con 8 esto representa 12.5%. Dentro de estas categorías, las 3 vulnerabilidades más frecuentes son: certificado SSL no puede ser de confianza (20%), certificados SSL firmados con algoritmos de hashing débiles (17%), y Suite de cifrado SSL anónimas soportado (12.5%). Para obtener más detalles sobre estas y otras vulnerabilidades mencionadas, consulte nuestro informe técnico mensual en la sección sobre vulnerabilidades por severidad.

Los 4 puertos más vulnerables para este período son: 443 (HTTPS), 22 (SSH), 25 (SMTP) y 80 (HTTP). La mayoría de los hosts tienen una vulnerabilidad en el puerto 443. Los hosts 190.34.183.131 y 190.34.183.139 aún presentan la vulnerabilidad crítica del tipo MS15-034: Una vulnerabilidad en HTTP.sys podría permitir la

ejecución remota de código (3042553) (uncredentialed check) en los puertos 80 y 443.

Los hosts más vulnerables para este período son: 190.34.183.142, 190.34.183.139, 190.34.183.152, 190.34.183.149, 190.34.183.90 y 190.34.183.91. La mayoría de estos hosts se presentaron como vulnerables en el mes anterior. Los hosts 190.34.183.142, 190.34.183.139, 190.34.183.149, 190.34.183.152 y 190.34.183.154 tienen una vulnerabilidad de alto riesgo que pertenece a la categoría de detección de protocolo de las versiones 2 y 3 de SSL.

Métrica de Valor de Riesgo

GLESEC utiliza una métrica para proveer una manera de cuantificar las vulnerabilidades basadas en riesgo de la organización. Esta métrica mide el valor relativo de las vulnerabilidades y también el registro de cambio a través del tiempo.

Es importante mencionar que esta métrica considera media de las vulnerabilidades clasificadas como “critical”, “high”, “médium” y “low”, dándoles un peso de 100%, 75%, 50% y 10% respectivamente.

Esto toma en consideración todas las vulnerabilidades, pero es importante destacar que estos valores (100%, 75%, 50% y 10%) son arbitrariamente escogidos por nosotros, por lo cual pueden cambiar con el tiempo como resultado de mejor comprensión de los riesgos involucrados. Podemos usar esta métrica para evaluar el progreso en el tiempo y comparar uno con el otro utilizando un conjunto de cantidad común.

El siguiente rango 190.34.183.0/24 de red externa de Metrobank S.A. fue escaneado en búsqueda de vulnerabilidades.

La siguiente tabla indica la métrica de vulnerabilidades externas.

Total IP's Scanned	IP's Vulnerable
15	11

Risk Distribution				
Critical	High	Medium	Low	Total
2	6	34	22	64

According to the metrics:

RV= 0.294479167

The following values are to clarify RV:
RV=1 Points to every IP address in the infrastructure that are susceptible to attacks
RV=0 Points to no IP address in the infrastructure aret susceptible to attacks
RV=0.1 Point to 1/10 IP address in the infrastructure that are susceptible to attacks

Lista de vulnerabilidades externas según su condición:

Vulnerable Hosts	Critical	High	Medium	Low
190.34.183.81	0	0	0	2
190.34.183.90	0	0	4	1
190.34.183.91	0	0	4	1
190.34.183.132	0	0	4	1
190.34.183.142	0	2	7	3
190.34.183.148	0	0	2	0
190.34.183.149	0	1	4	2
190.34.183.152	0	1	3	4
190.34.183.154	0	1	3	4
190.34.183.131	1	0	0	0
190.34.183.139	1	1	3	4

La siguiente tabla provee de una comparación entre las vulnerabilidades externas persistentes del mes actual con el mes previo.

host-ip	Previous Month	Current Month
190.34.183.131	1	1
190.34.183.132	5	5
190.34.183.139	6	9
190.34.183.142	12	12
190.34.183.148	2	2
190.34.183.149	7	7
190.34.183.152	8	8
190.34.183.154	8	8
190.34.183.81	2	2
190.34.183.90	5	5
190.34.183.91	5	5

Por favor revisar Recomendaciones para más detalles. Esto puede ser visto en el PORTAL de MIEMBROS de GLESEC (GMP).

Categorías de Vulnerabilidades

La siguiente tabla indica las categorías que nosotros usamos para vulnerabilidades como una manera de proveer contexto a las mismas y facilitar la priorización de cómo manejar la remediación.

Preliminary Analysis	Firewalls	Network Devices
SMB/NetBIOS	SSH Servers	Malformed Packets
Simple Network Services	Mail Servers	Proxy Servers
Policy Checks	SQL Servers	Wireless AP
Web Servers	FTP Servers	Webmail Servers
RPC Services	Server Side Scripts	NFS Services
Backdoors	SNMP Services	Printers
Encryption and Authentication	DNS Servers	

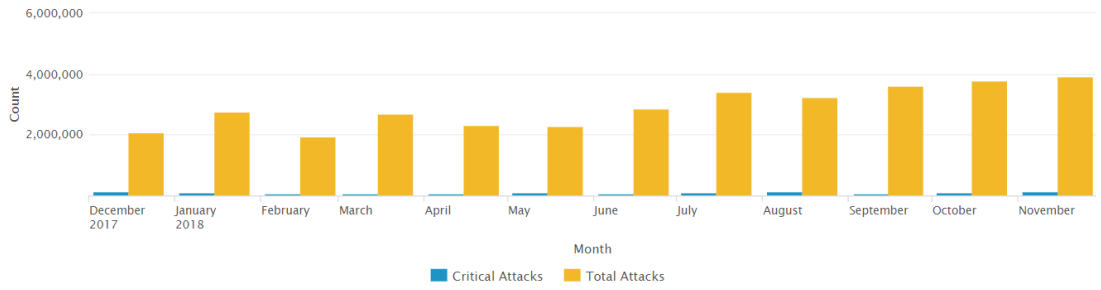
Basado en lo anterior, la siguiente tabla muestra una matriz del total de vulnerabilidades externas por categoría.

Category	Critical	High	Medium	Low	Total
General	0	0	28	8	36
Misc.	0	1	5	10	16
Service detection	0	5	0	3	8
Windows	2	0	1	0	3
Web Servers	0	0	0	1	1

AMENAZAS

GLESEC utiliza sus MSS-APS, MSS-EPS, MSS-SIEM, MSS-EDR y MSS-UTM para determinar actividad de inteligencia de amenazas.

Las Amenazas tal como fueron reportadas por MSS-APS, MSS-EPS, MSS-SIEM, MSS-EDR, MSS-UTM para este mes son ataques de reconocimiento principalmente (escaneos de puertos).



Este mes ha habido un aumento en actividad de ataques con respecto al mes anterior de un 3 aproximadamente y un aumento en ataques críticos con relación al mes anterior de alrededor de un 9%.

La mayoría de los ataques duraron menos de un minuto y seguidamente de 1 a cinco minutos, estos tienen como objetivo puertos múltiples.

La mayoría de los ataques parecen ser de reconocimiento (escaneo). Alrededor de un 94% de los ataques de este mes fueron provenientes de escaneos, los cuales pueden ser considerados reconocimiento y es lo que precede ataques más sofisticados.

Las fuentes de los ataques provienen de los siguientes países: Federación Rusa (26.4%), Panamá (22.2%), Ucrania (18.8%) y Estados Unidos (10.4%).
Los tipos de ataques que estos países más frecuentes son: TCP Scan y TCP Scan (Horizontal).

Basándonos en la información recolectada por las contramedidas de seguridad durante este periodo, 3,874,244 ataques hacia Metrobank S.A.; 87,586 de los cuales fueron considerados “críticos”, todos fueron detenidos por las contramedidas de seguridad administradas por GLESEC.

Metrobank S.A. recibe un promedio de 2,906,483 ataques totales y 87,870 ataques críticos mensualmente. Esto equivale a un promedio de 96,348 ataques totales diarios y 2,913 ataques críticos diarios.

La correlación de información entre los servicios MSS-APS/MSS-APFW y MSS-VME,donde se correlaciona hosts que presentan vulnerabilidades y los ataques que reciben estos sistemas corresponden a sistemas críticos de Metrobank S.A. ; Entre una de las principales sistemas esta la aplicación web metrobank que recibe ataques HTTP page flood attack y presenta 8 vulnerabilidades. Los detalles

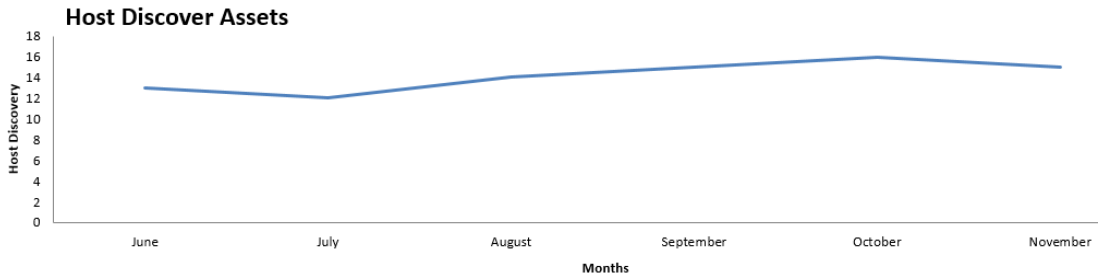
adicionales están detallados en el reporte técnico mensual en la pag.16.

ACTIVOS

El MSS-VM(E/I), MSS-EPS realiza una prueba semanal. El MSS-VM(E/I) identifica activos dentro de la red mientras que el MSS-EPS identifica aplicaciones. Dependiendo de los servicios contratados, es la lista que se puede proporcionar de los activos del sistema o aplicativos.

Nosotros creemos que no se puede proteger lo que no se conoce y conocer los activos (sistemas y aplicaciones) es fundamental para tener una práctica sólida de ciberseguridad. Por lo tanto, lo alentamos a que verifique la información que proporcionamos y nos avise si algo es sospechoso o no lo es. Podemos trabajar con su organización para crear una línea base que pueda ser usada para identificar desviaciones. Por favor contacte nuestro GOC para asistencia en este punto.

El siguiente histograma muestra el total de sistemas descubiertos en el perímetro de su organización en los últimos seis meses.



Saber qué hay en su red es extremadamente importante. Nuestro equipo de monitoreo del GOC ha estado monitoreando todos estos resultados de descubrimiento de host y no ha encontrado nada inusual, como muestra el histograma. Todos los host descubiertos pertenecen al rango de direcciones de Metrobank S.A.

CUMPLIMIENTO

El MSS-EPS o Servicio de Seguridad para manejo de dispositivos finales es un Servicio de Cumplimento y Remediación. Por cumplimento nosotros entendemos la prueba, monitoreo y alerta de las desviaciones de los parámetros de todos los “hosts” y “servers” en la organización de las líneas base establecidas. Estas líneas base se pueden crear para soportar requisitos externos específicos o directrices internas de mejores prácticas. El MSS-EPS puede monitorear desviaciones a estas líneas base y también “hacer cumplir” las mismas.

Los servicios que nos proporcionan información para esta sección no han sido contratados.

VALIDACION DE SEGURIDAD CIBERNETICA

Validación de Seguridad implica la validación de la seguridad completa al hacer pruebas con ataques simulados. Esto es impulsado con el Managed Breach Attack Simulation Service (MSS-BAS). El MSS-BAS es una colección de exploits avanzados de pre-explotación, post-explotación y servicios de prueba de conciencia. Las pruebas se realizan sobre objetivos reales, pero con ataques simulados; es por esto, que estos proveen resultados concluyentes (no falsos positivos). Los distintos vectores de ataque prueban la organización. Los diferentes vectores de ataque prueban las configuraciones, las contramedidas, las implementaciones y la capacidad de la organización para responder de manera continua, produciendo inteligencia y recomendaciones valiosas.

Los servicios que nos proporcionan información para esta sección no han sido contratados.

ACCESO CONFIABLE

El nuevo modelo de TI trae consigo una mayor superficie de ataque, compuesta por empleados que usan sus propios dispositivos para el trabajo, mientras trabajan de forma remota. La proliferación de aplicaciones en la nube para casi todas las necesidades comerciales también ha contribuido a una mayor complejidad técnica. Hoy en día, los atacantes pueden exponer muchas vulnerabilidades diferentes en múltiples vectores, en un solo ataque. La seguridad tradicional está diseñada para abordar ataques aislados y en silos, lo que hace que estas soluciones sean ineficaces contra las amenazas modernas. Estas nuevas amenazas se centran en obtener acceso remoto a sus aplicaciones y datos, ya sea con contraseñas robadas o vulnerabilidades conocidas explotadas dirigidas a sus usuarios, sus dispositivos desactualizados, aplicaciones en la nube y software de acceso remoto.

Los servicios que nos proporcionan información para esta sección no han sido contratados.

Recomendaciones

GLESEC recomienda que Metrobank S.A. aborde los siguientes problemas
Los detalles de las vulnerabilidades por host se presentan en nuestro informe técnico en la sección del Servicio de Vulnerabilidad Gestionada (MSS-VM).

- Recomendamos aplicar actualizaciones de seguridad a sus servidores.

- Desactivar SSL 2.0 y 3.0. Utilice TLS 1.2 (con conjuntos de cifrado aprobados) o superior en su lugar. Muchas de las vulnerabilidades presentes en los dispositivos escaneados corresponden al uso de los protocolos SSL, SSL se ha convertido en un protocolo obsoleto y tiene muchas vulnerabilidades bien documentadas, como Bar Mitzvah. La práctica recomendada es implementar la versión 1.2 de TLS, que es la implementación más segura hasta la fecha.

- Desactive el cifrado del modo CBC y active el cifrado del modo CTR o GCM.

- Reemplace el certificado en la cadena con la clave RSA de menos de 2048 bits de longitud con una clave más larga y vuelva a emitir los certificados firmados por el certificado anterior. Esta es una de las vulnerabilidades más frecuentes.

- Existen vulnerabilidades que afectan el protocolo SSH. Estas vulnerabilidades generalmente se pueden resolver manteniendo los sistemas con las últimas versiones de software y aplicando los últimos parches. En algunos casos, los dispositivos no pueden actualizarse a la última versión, se recomienda restringir o bloquear el acceso de SSH desde la red externa.

Sección de Inteligencia por Módulo de Servicio.

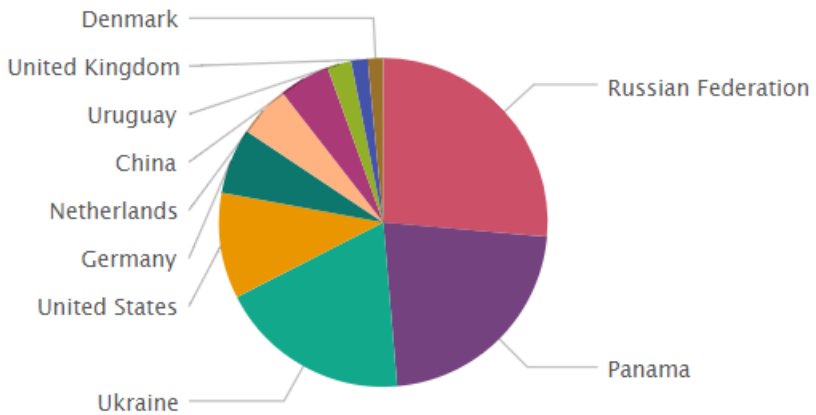
SECCION DE INTELIGENCIA PARA SERVICIO DE SEGURIDAD ADMINISTRADO DE PROTECCION DE ATAQUES (MSS-APS)

El MSS-APS es un servicio completo de protección administrada contra ataques que brinda protección contra: ataques de intrusión dirigidos o automáticos, ataques DDOS, ataques internos y externos, ataques a nivel de red, ataques encriptados, ataques a servicios basados en la nube, ataques que pueden consumir el ancho de banda de los proveedores de servicios de Internet a su organización. El servicio responde a Riesgo de falta de disponibilidad para sistemas críticos debido a un ataque DDOS, Riesgo de fuga de datos debido a un intruso, Riesgo de pérdida de fondos debido a un intruso, Riesgo de contaminación de la imagen corporativa a través de una desfiguración de sitios públicos de la organización.

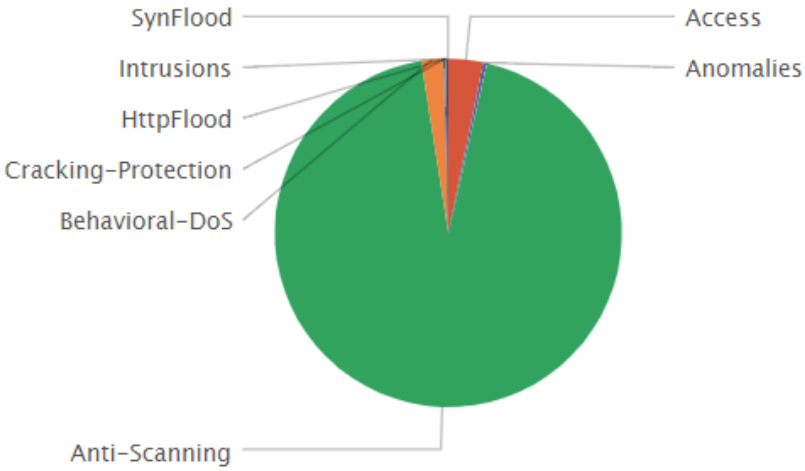
El propósito de esta sección es resaltar la información recopilada de los servicios bajo contrato así como fuentes externas tales como honeypots, fuentes maliciosas conocidas, bases de datos de vulnerabilidades, relaciones con los equipos CERT y CSIRT que posee GLESEC, junto con otras amenazas.

Los siguientes gráficos son tableros generados por la plataforma TIP™ GLESEC. Estos tableros son representativos de métricas para este servicio.

La distribución de fuentes de ataques se puede ver en el siguiente gráfico.

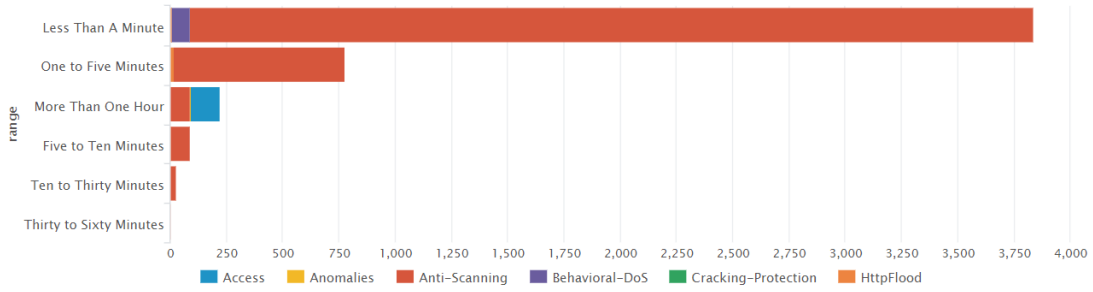


La distribución de ataques por tipo puede verse en el siguiente diagrama.



Duración

Duración de ataques para categorías específicas en el periodo de este informe es ilustrado abajo



Ancho de banda

La siguiente tabla representa el tráfico descartado por categoría.

Category	Gbps	Mbps
Behavioral-DoS	54.21	55512.83
Access	4.41	4519.67
Anti-Scanning	3.26	3338.05
Anomalies	0.50	516.07
Intrusions	0.11	111.54
Cracking-Protection	0.01	7.94
SynFlood	0.00	0.78
HttpFlood	0.00	0.00
Total Bandwidth in Gbps/Mbps	62.50	64006.88

*Favor ver la información de ancho de banda y gráfico: Bandwidth by Blocked Threat Category by Hour of Day and Graph, Top Attacks Blocked by Bandwidth and Graph Y Attack Categories Blocked by Bandwidth disponibles en la sección de inteligencia de este informe.

Actividad de puertos

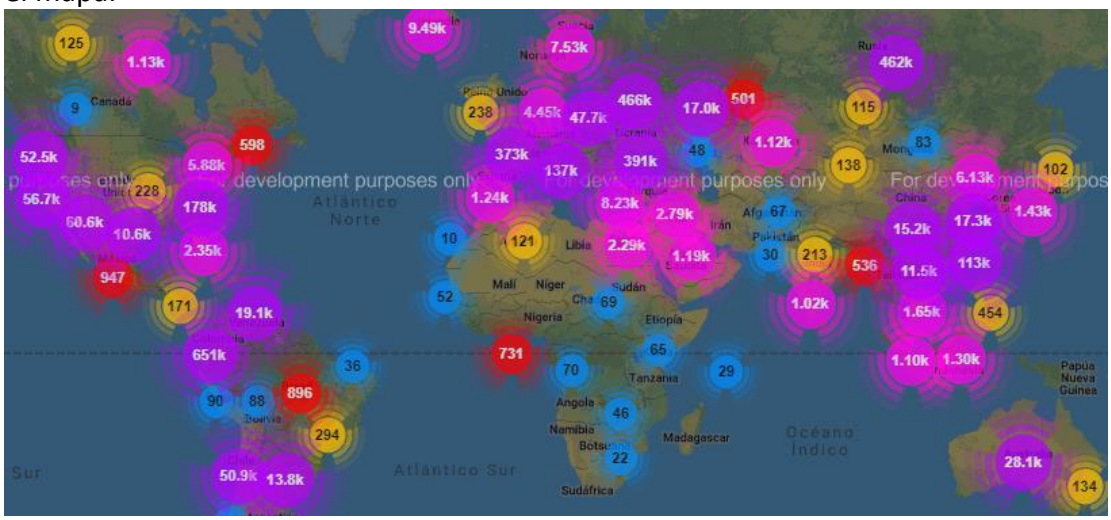
Las capacidades avanzadas de detección y prevención de intrusiones ofrecidas por DefensePro IPS NBA, DoS y Reputación de Servicio proporcionan la máxima protección para los elementos de red, hosts y aplicaciones. Está compuesto por diferentes funciones de protección a nivel de aplicación para evitar intentos de intrusión como gusanos, caballos de Troya y ataques de bala única, lo que facilita la limpieza completa y de alta velocidad de todas las intrusiones maliciosas.

El DefensePro asistió en prevenir ataques dirigidos a nivel de servidor y red; los cuales fueron dirigidos a números de puertos bien conocidos como se ve en el siguiente diagrama.

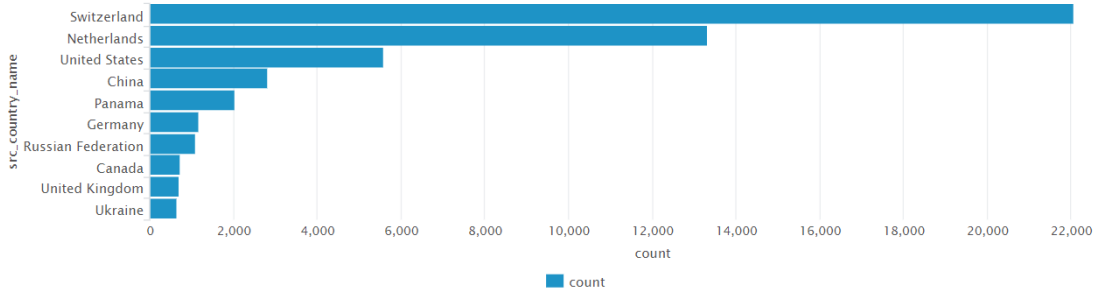
La información sobre números de puertos que se utilizan son basados en el Servicio de Nombres IANA y Registro de Numero de Puertos de Protocolos de Transporte y fuentes adicionales son usadas para ilustrar la relación a vectores de ataque comúnmente explotados.

La gran mayoría de los ataques hacia Metrobank S.A. son geográficamente originarios de los siguientes países como se muestra en el diagrama. Algunos resultados no incluyen información de localización que puedan ser desplegados en

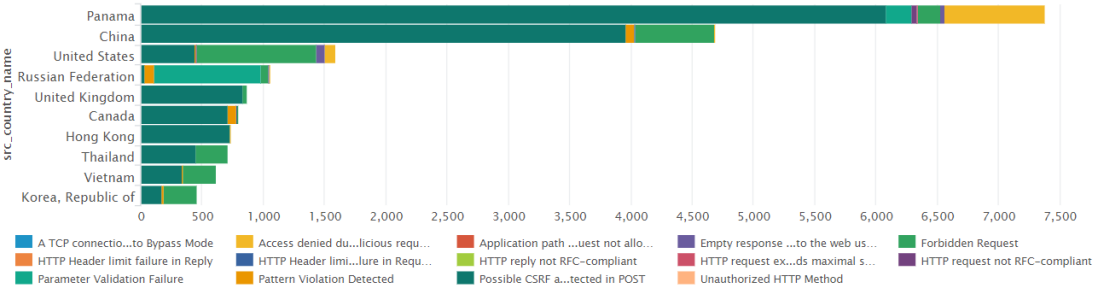
el mapa.



Graph: Top 10 Attacking Countries Blocked
Este reporte provee la cuenta de los ataques totales bloqueados por país.

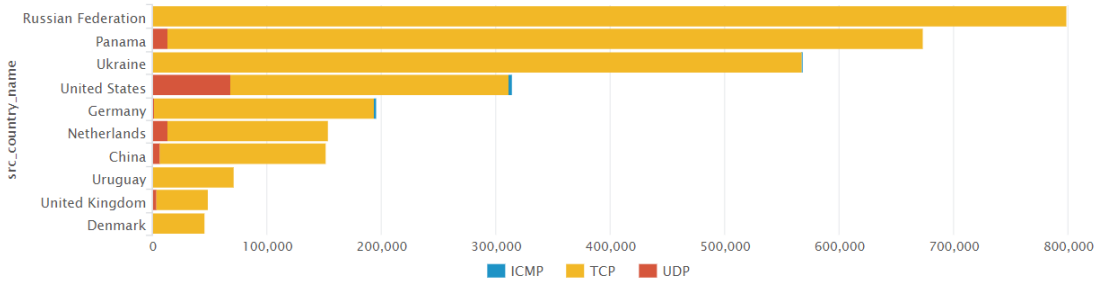


Graph: Top 10 Attacking Countries Blocked by Attack Type
Este gráfico provee la cuenta del total de tipos de ataques bloqueados por país

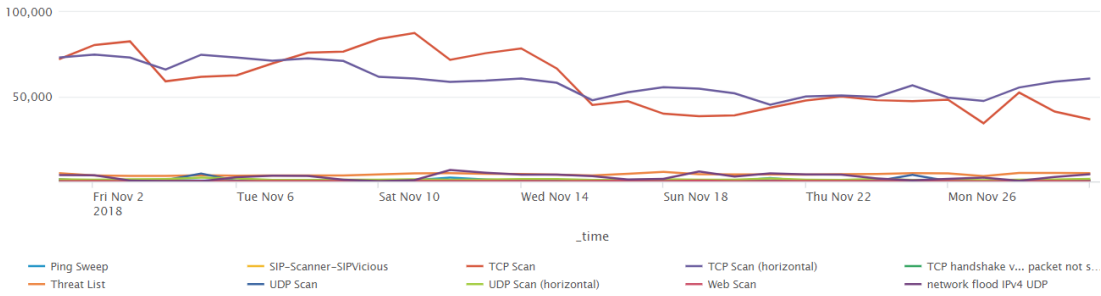


Graph: Top 10 Attacking Countries Blocked by Protocol
Esta gráfica muestra la cuenta de ataques descartados por protocolo y por país

origen.

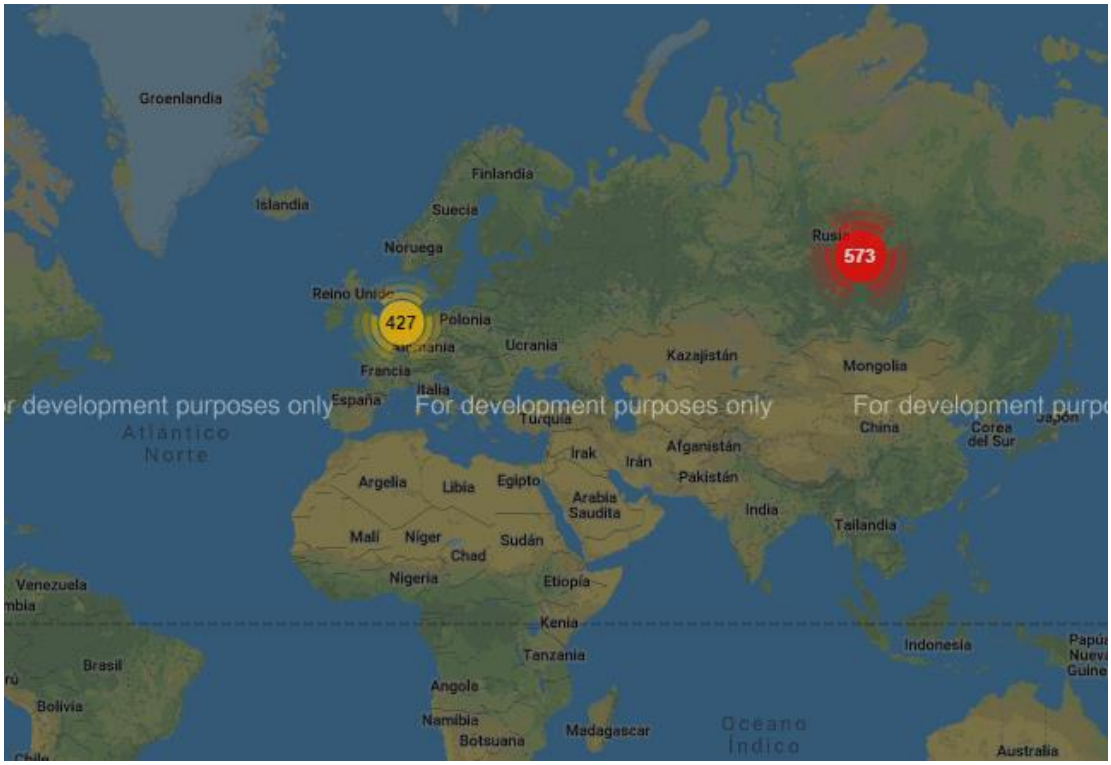


Graph: Attacks Types Blocked by Week
Esta gráfica muestra la cuenta de ataques bloqueados a la semanalmente

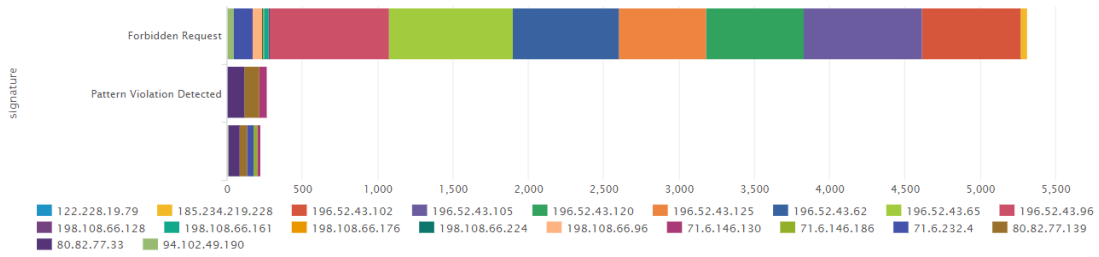


INFORMACION SOBRE INTELIGENCIA DE AMENAZAS DE GLESEC
La parte de información de Threat Intelligence de GLESEC de la plataforma TIPTM es responsable de compilar datos de muchas fuentes, incluidos honeypots, fuentes maliciosas conocidas, bases de datos de vulnerabilidades, relaciones con equipos de CERT y CSIRT, entre otros, en los sistemas BigData de GLESEC para indexación, correlación, análisis e incidentes.

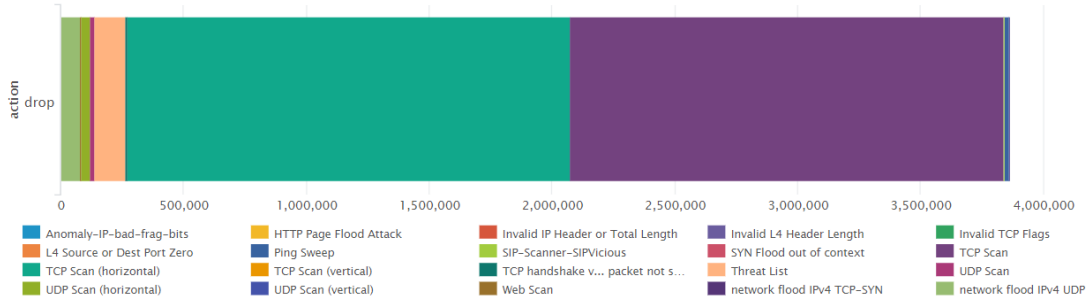
Los datos de inteligencia de amenazas de GLESEC se correlacionan con la información relacionada con los servicios de GLESEC contratados por Metrobank S.A. El resultado de esto es que **31,508** ataques a Metrobank S.A. han sido detectados por esta correlación como se puede ver en la siguiente imagen. Algunos resultados no incluyen información de ubicación que permita el trazado del mapa.



Graph: Known Threat Sources by Threat Type
Esta gráfica muestra las 20 IPs origen de amenazas conocidas con su respectivo tipo de amenaza.



Graph: Attacks Denied
Esta gráfica provee de la cantidad total de ataques denegados junto con la regla de seguridad de red correspondiente.



Información de Puertos

Información del puerto: Puerto 80 (http), Puerto 1443 (ms-sql), Puerto 8080 (https-alt), Puerto 3306 (mysql) Comúnmente escaneado para atacar servidores web. Actualmente, la inyección SQL es la forma más común de ataques a sitios web, ya que los formularios web son muy comunes, a menudo no están codificados correctamente y las herramientas de pirateo utilizadas para encontrar debilidades y aprovecharlas están disponibles en línea. Este tipo de ataque es lo suficientemente fácil de lograr que incluso los hackers inexpertos pueden realizarlos. Sin embargo, en manos del pirata informático muy hábil, una debilidad del código web puede revelar el acceso de nivel root de los servidores web y, a partir de ahí, se pueden realizar ataques contra otros servidores en red. Structured Query Language (SQL) es el lenguaje casi universal de las bases de datos que permite el almacenamiento, la manipulación y la recuperación de datos. Las bases de datos que usan SQL incluyen MS SQL Server, MySQL, Oracle, PostgreSQL, MongoDB, Access y Filemaker Pro y estas bases de datos están igualmente sujetas a ataques de inyección SQL.

Los formularios web deben permitir cierto acceso a su base de datos para permitir la entrada de datos y una respuesta, por lo que este tipo de ataque evita los firewalls y las defensas de dispositivos finales. Cualquier formulario web, incluso un simple formulario de inicio de sesión o cuadro de búsqueda, puede proporcionar acceso a sus datos mediante inyección SQL si está codificado incorrectamente.

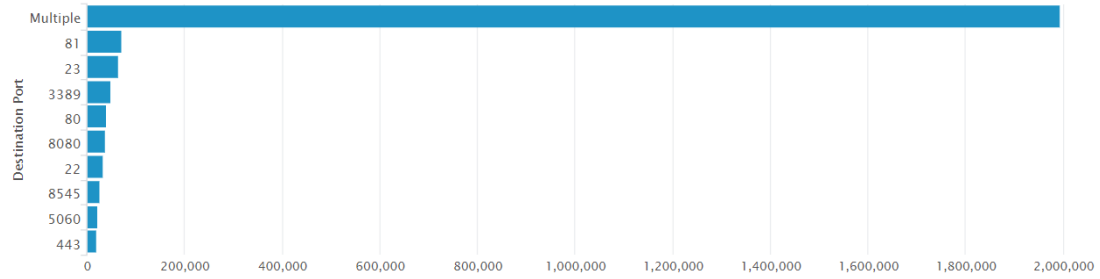
El Top 10 de OWASP enumera A1-Injection como la mayor amenaza y define esta categoría como:

Las fallas de inyección, como SQL, OS e inyección de LDAP ocurren cuando los datos que no son de confianza se envían a un intérprete como parte de un comando o

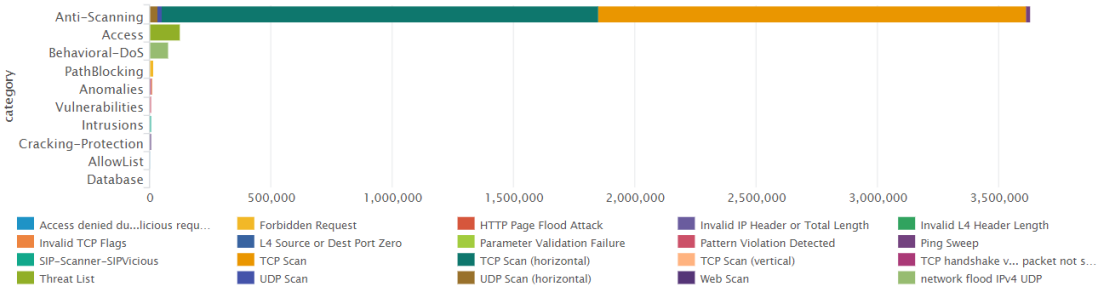
consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a los datos sin la debida autorización.

Un ataque de inyección SQL consiste en la inserción o "inyección" de una consulta SQL a través de los datos de entrada del cliente a la aplicación. Un exploit de inyección SQL exitoso puede leer datos sensibles de la base de datos, modificar datos de base de datos (Insertar / Actualizar / Eliminar), ejecutar operaciones de administración en la base de datos (como apagar el DBMS), recuperar el contenido de un archivo dado presente en el archivo DBMS sistema y, en algunos casos, emitir comandos al sistema operativo. Los ataques de inyección SQL son un tipo de ataque de inyección, en el que los comandos SQL se inyectan en la entrada del plano de datos para efectuar la ejecución de comandos SQL predefinidos.

Graph: Attacks Blocked by Destination Port
Este record provee información sobre número de ataques total que fueron descartados pero que fueron dirigidos a los siguientes puertos y cuantas veces sucedió.

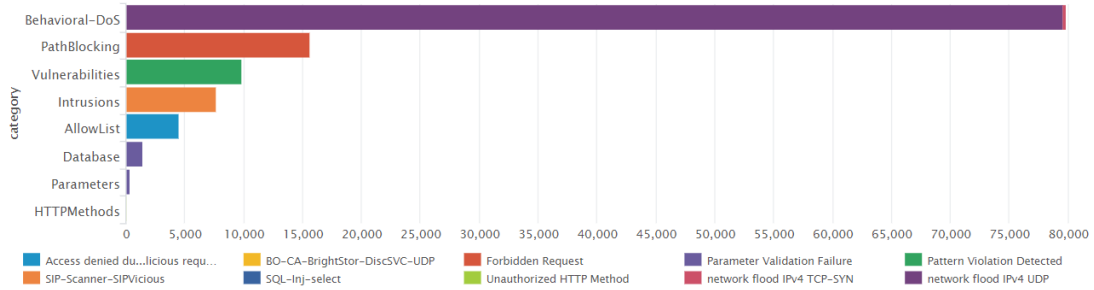


Graph: Attacks Blocked By Threat Category
Esta gráfica lista los ataques bloqueados por categoría de ataque, enlistando los nombres de ataques.



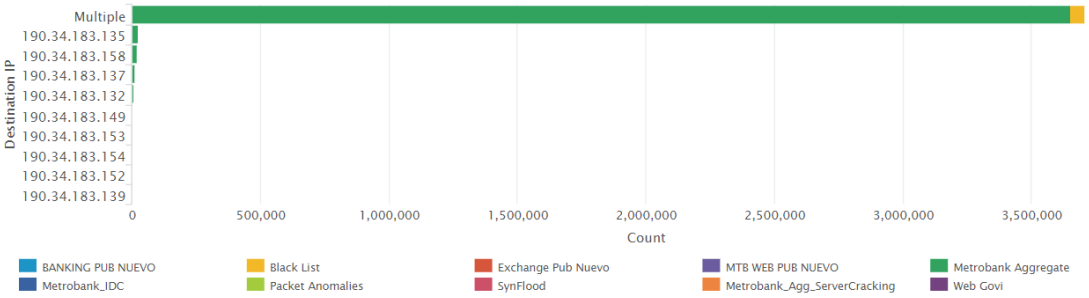
Graph: Critical Attacks Blocked

Esta Gráfica evidencia la información sobre ataques críticos, nombre de ataque y regla de seguridad de red junto con el número de veces que un ataque fue comenzado.



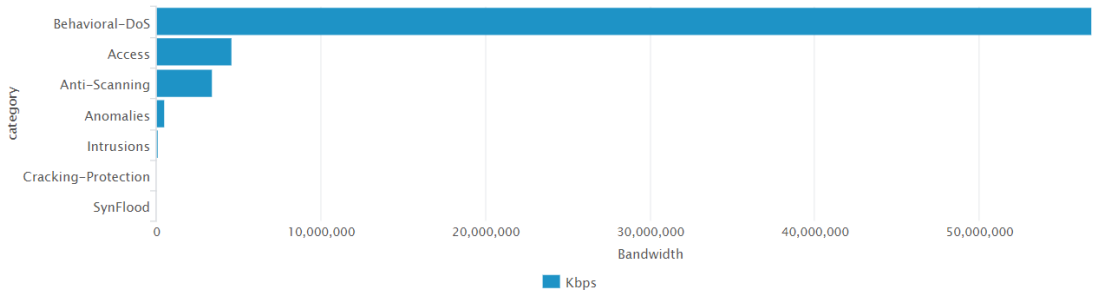
Graph: Top Attacked Destinations Blocked

La siguiente gráfica provee información sobre Ips de sistemas, lo cuales fueron el destino de los ataques y la cantidad de intentos junto con la regla de seguridad de red.

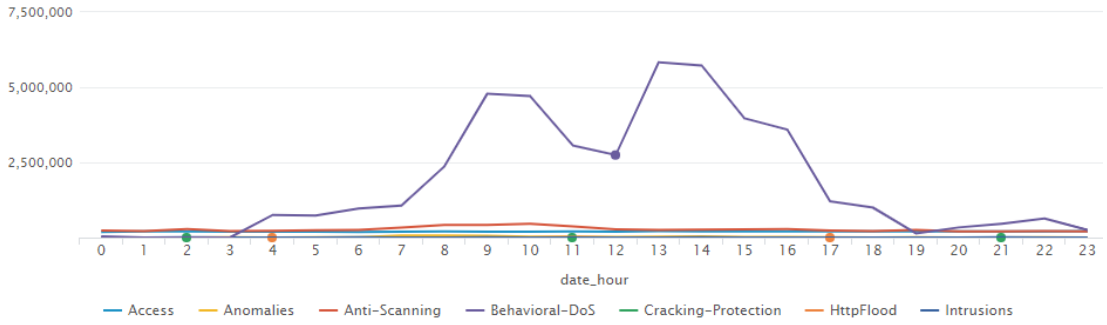


Graph: Attack Categories Blocked by Bandwidth

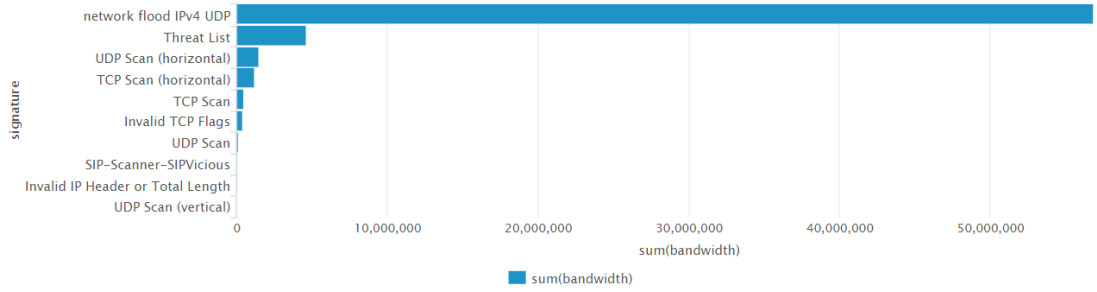
Esta gráfica muestra las categorías de ataques basados en Ancho de Banda de los ataques compartiendo la misma categoría, ancho de banda descartado en Kbps.



Graph: Bandwidth by Blocked Threat Category by Hour of Day
Este gráfico muestra las categorías de amenazas que consumen más ancho de banda en función del ancho de banda de los ataques que comparten la misma categoría de amenaza para cada hora del día.

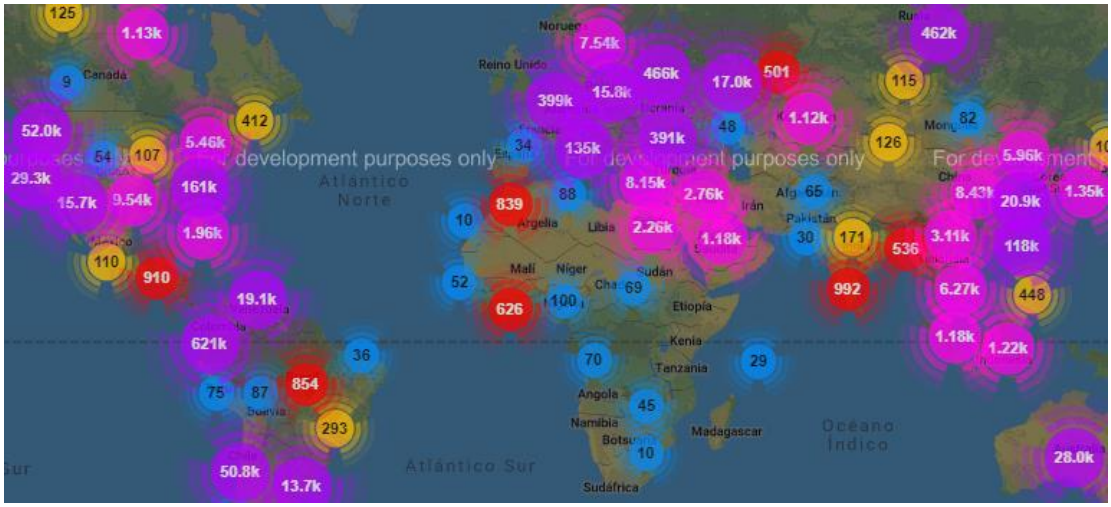


Graph: Top Attacks Blocked by Bandwidth
Esta gráfica muestra la mayoría de los ataques que consumen ancho de banda basados en el BW del ataque que incluye Kbits.



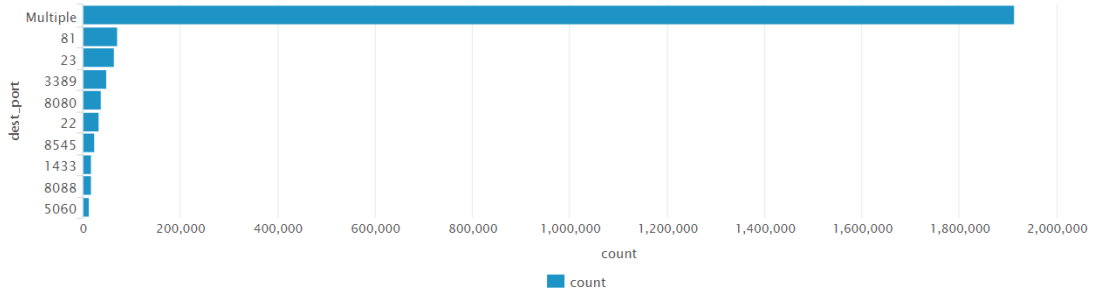
<u>Información de Escaneo</u>
El siguiente mapa despliega la distribución geográfica de **3,530,406** ataques hacia Metrobank S.A desde fuentes de escaneo.

Algunos resultados no incluyen información de locación que permita desplegarlos en el mapa.

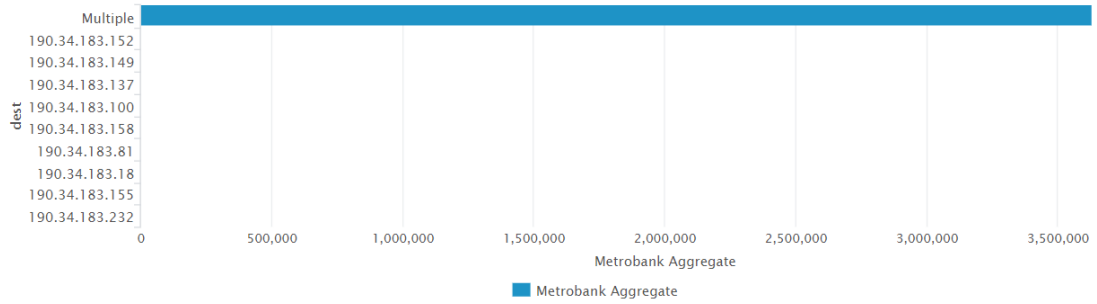


Anti-escaneos muy sofisticados redujeron los intentos de enumeración que, de lo contrario, frustrarían cualquier esfuerzo de modelado de amenazas, algo habitual después de la fase de recopilación de información de un ataque dirigido o planificado.

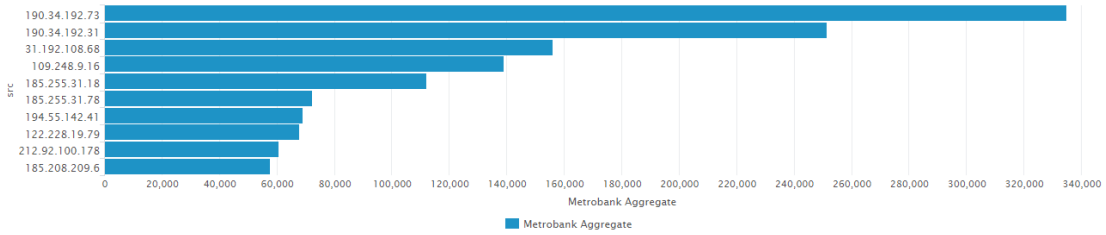
Graph: Top Probed Applications Blocked
Este gráfico muestra una vista histórica de los puertos L4 mas sondeados.



Graph: Top Probed IP Addresses Blocked
Este gráfico muestra una vista histórica de las direcciones IP probadas que se escanearon junto con la regla de seguridad de la red.

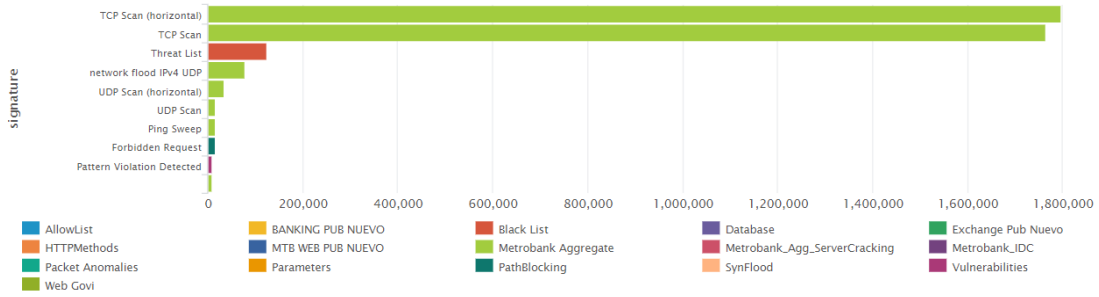


Graph: Top Scanners Blocked (Source IP Addressed)
Este gráfico muestra una vista histórica de las principales direcciones IP de origen que han escaneado las actividades de escaneo red junto con la regla de seguridad de red.

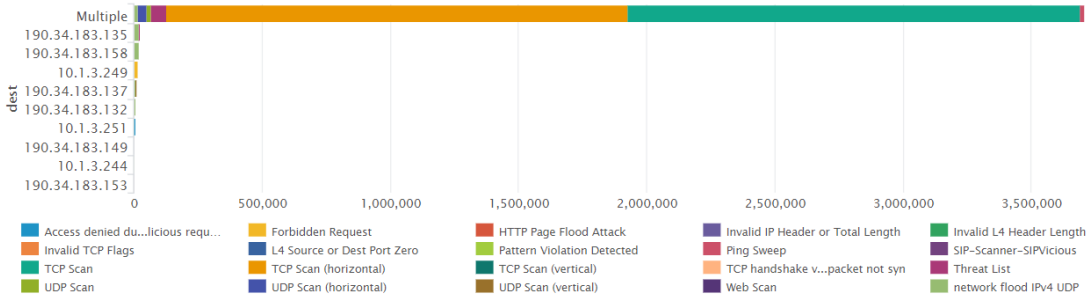


NOTE: Ver Appendix 2 – Top Scanners Blocked (Source IP Addressed)

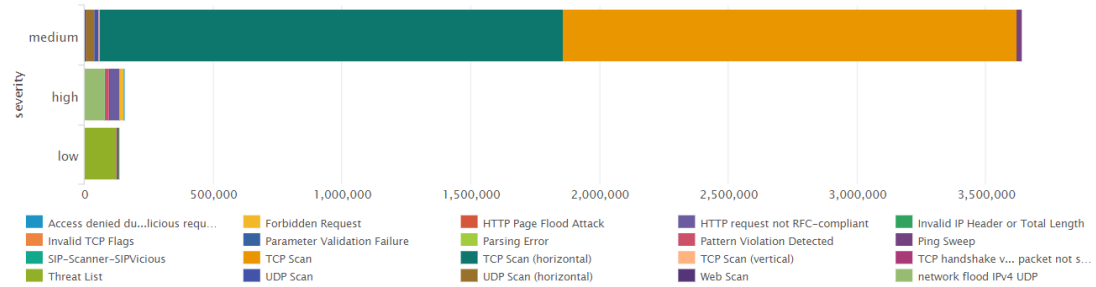
Graph: Top Attacks Blocked
Este informe proporciona información sobre los principales ataques bloqueados, el nombre del ataque, la regla de seguridad de la red y el número total de ataques bloqueados con esta combinación.



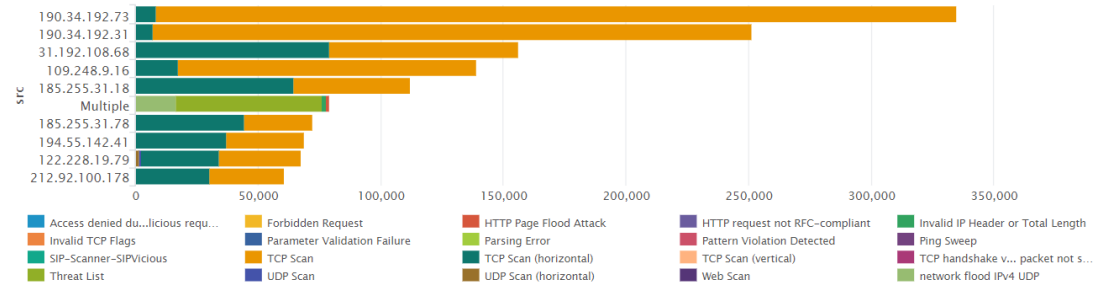
Graph: Top Attacks Blocked by Destination
En este reporte, se muestran el destino en el que se intentó el ataque, el nombre del ataque y el recuento.



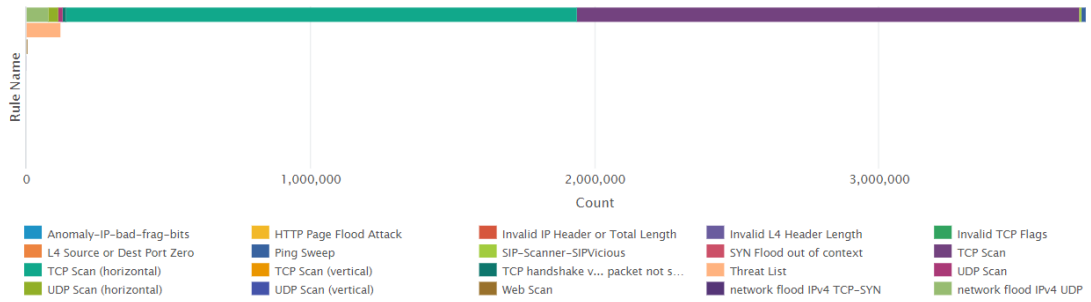
Graph: Top Attacks Blocked By Risk
Este reporte proporciona información sobre los ataques que se bloquearon en DP IPS en función de su riesgo.



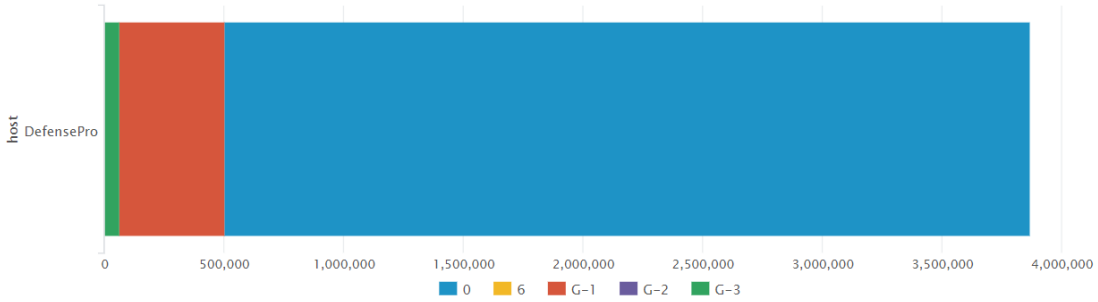
Graph: Top Attacks Blocked by Source
Este reporte proporciona información sobre los principales ataques bloqueados, categorizados por ataques para cada fuente donde se originaron los ataques, junto con el nombre del ataque y la cantidad de ataques que se activaron con esta combinación.



Graph: Attacks Blocked by Network Security Rule
Este informe enumera los ataques por regla de seguridad de la red, el nombre del ataque e IP del sistema protegido del destino.



Graph: Attacks Blocked by Physical Port (per single IPS device)
Esta grafica muestra la cantidad de ataques descartados por Puerto físico.



<u>Bandwidth</u>
El siguiente diagrama muestra el ancho de banda de los ataques del mes.

Category	Gbps	Mbps
Behavioral-DoS	54.21	55512.83
Access	4.41	4519.67
Anti-Scanning	3.26	3338.05
Anomalies	0.50	516.07
Intrusions	0.11	111.54
Cracking-Protection	0.01	7.94
SynFlood	0.00	0.78
HttpFlood	0.00	0.00
Total Bandwidth in Gbps/Mbps	62.50	64006.88

SECCIÓN DE INTELIGENCIA PARA EL SERVICIO DE SEGURIDAD ADMINISTRADO DE VULNERABILIDADES (MSS-VM)

El Servicio Administrado de Vulnerabilidades (MSS-VM) le permite a la organización minimizar el riesgo de vulnerabilidades al descubrir las debilidades rápidamente, midiendo el riesgo potencial y exposición, reportando, brindando información necesaria para mitigar esos riesgos de manera continua y facilitar la presentación de informes y el cumplimiento de las reglamentaciones y las mejores prácticas.

El propósito de esta sección es resaltar la inteligencia recolectada por este y otros servicios contratados, así como también fuentes externas como Honeypots, fuentes maliciosas conocidas, bases de datos vulnerables, relaciones con los equipos CERT y CSIRT que posee GLESEC, junto con otras fuentes de amenazas.

Los siguientes gráficos son tableros generados por la plataforma TIP™ de GLESEC. Estos tableros son representativos de métricas para este servicio.

Es importante establecer un programa de administración de vulnerabilidades como parte de la estrategia de seguridad de la información porque poco después de que los investigadores o proveedores de seguridad descubran y den a conocer nuevas vulnerabilidades, los atacantes diseñan el código de explotación y luego lo lanzan contra objetivos de interés. Cualquier retraso significativo en la búsqueda o reparación de software con vulnerabilidades peligrosas ofrece una amplia oportunidad para que los atacantes persistentes puedan abrirse paso, obtener control sobre las máquinas vulnerables y obtener acceso a los datos confidenciales que contienen. Las organizaciones que no analizan las vulnerabilidades y abordan de forma proactiva las fallas detectadas enfrentan una gran probabilidad de que sus sistemas se vean comprometidos.

Muchas de las vulnerabilidades van a contar con data CVE. CVE (Common Vulnerabilities and Exposures) es una lista de exposiciones a la seguridad de la información y vulnerabilidades patrocinadas por US-CERT y mantenida por la Corporación MITRE. La misión de CVE es de proporcionar nombres estándar para todas las exposiciones a la seguridad de la información conocidas, así como también definiciones estándar para términos sobre seguridad. El CVE puede ser buscado en línea en http://nvd.nist.gov/

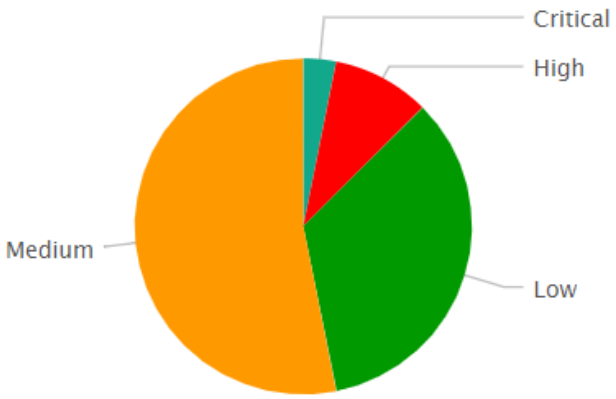
Puntuación de vulnerabilidades

Esta puntuación de vulnerabilidades es determinada por su factor de riesgo: "Critical", "High", "Medium" o "Low", así como también en el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS). La puntuación base del CVSS representa la característica de riesgo innata de cada vulnerabilidad. El CVSS es un sistema de puntuación de vulnerabilidades diseñado para proporcionar un método de evaluación abierto y estandarizado para vulnerabilidades de TI. CVSS ayuda a las organizaciones a priorizar y coordinar una respuesta conjunta a las vulnerabilidades de seguridad al comunicar las características base, temporales y de ambiente para cada vulnerabilidad. Además de puntuaciones numéricas, el CVSS provee una clasificación de seguridad de "High", "Medium" y "Low", pero estas clasificaciones cualitativas están directamente identificadas por la puntuación numérica del CVSS. Las vulnerabilidades están etiquetadas así:

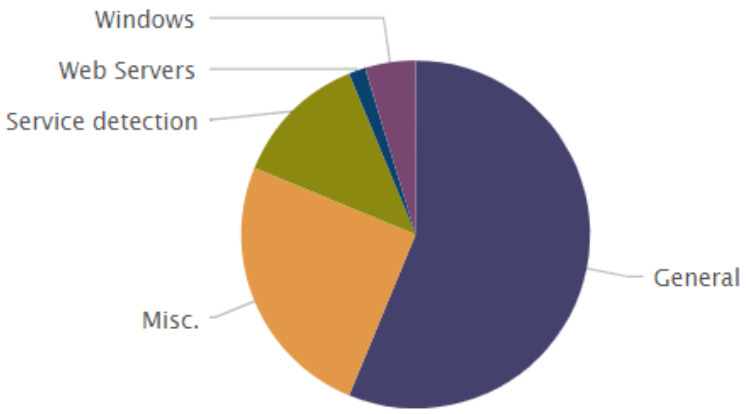
Low risk si estas poseen una puntuación CVSS base de 0.0 – 3.9
Medium risk si estas poseen una puntuación CVSS base de 4.0 – 6.9
High risk si estas poseen una puntuación CVSS base de 7.0 – 10.0

Información de Vulnerabilidades

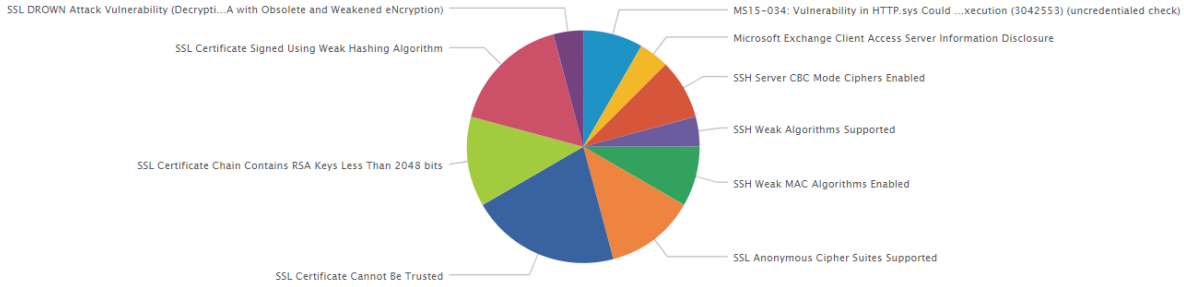
Graph: Risk Distribution
En este gráfico se muestra la distribución del riesgo de las vulnerabilidades descubiertas en este período del informe



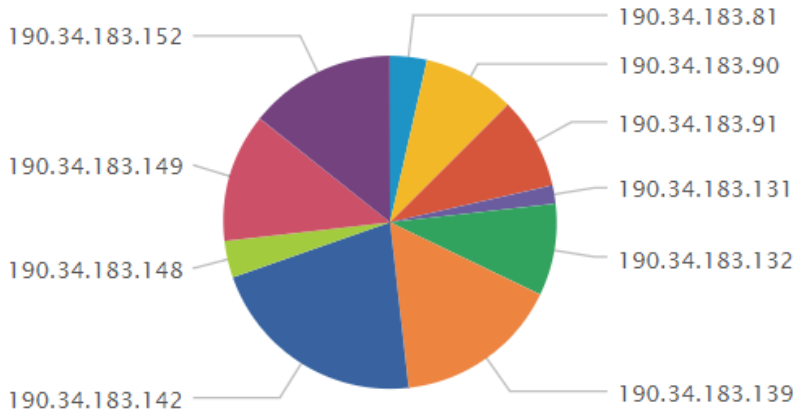
Graph: Most Frequent Vulnerability Category
En la siguiente gráfica se puede observar las vulnerabilidades más ocurrentes por categoría descubiertas en este periodo.



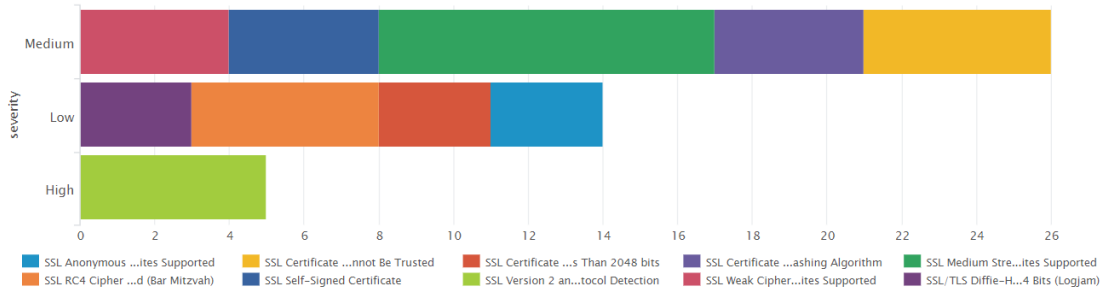
Graph: Most Frequent Vulnerability Name
En la siguiente grafica se muestran las vulnerabilidades más frecuentes descubiertas en este periodo.



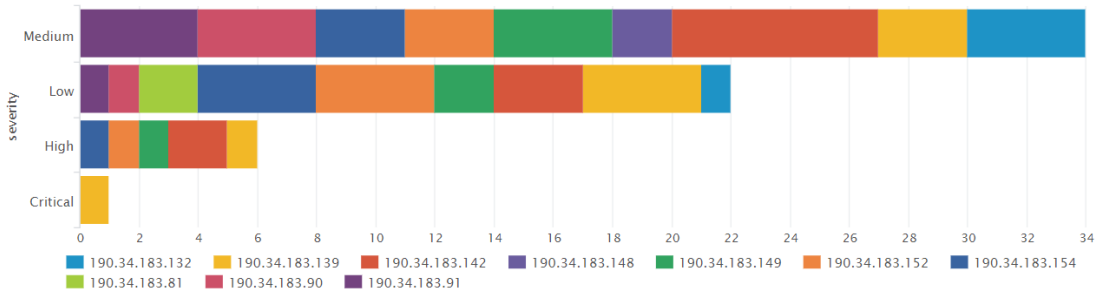
Graph: Most Vulnerable Host
En la siguiente gráfica se pueden identificar los hosts más vulnerables de este periodo.



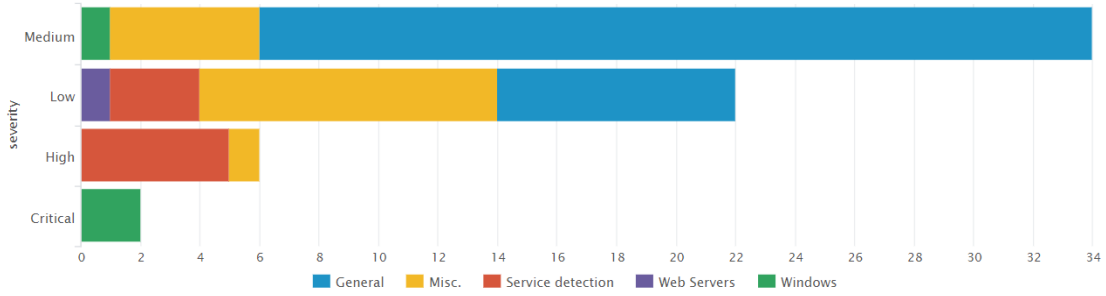
Graph: Vulnerability Risk by Vulnerability Name
En el siguiente diagrama se pueden observar la proporción de ocurrencias de vulnerabilidades clasificadas por nivel de riesgo, encontradas durante este periodo.



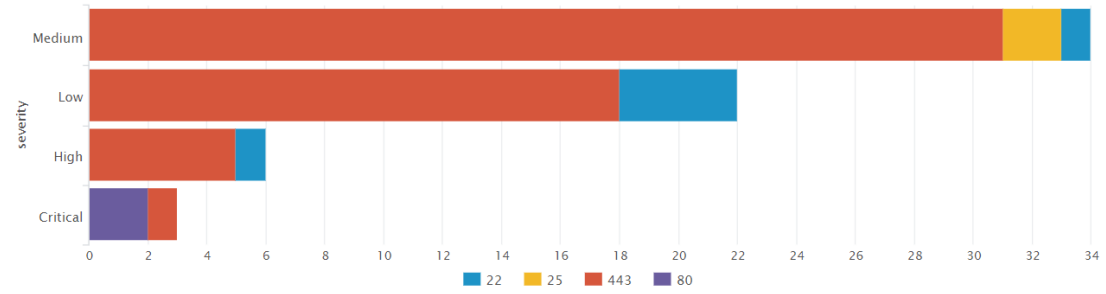
Graph: Vulnerability Risk by Host
En el siguiente diagrama se puede identificar la proporción de ocurrencias de cada host con respecto al nivel de riesgo, encontradas durante este periodo.



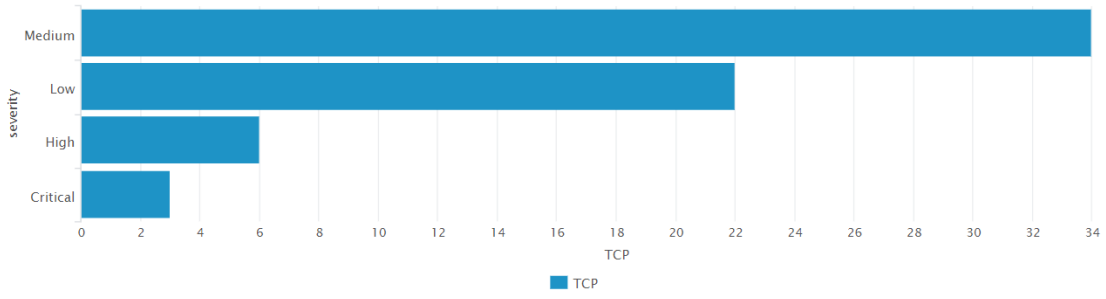
Graph: Vulnerability Risk by Category
Este reporte ilustra el riesgo y cantidad de ocurrencia de vulnerabilidades basado en categorías, encontradas durante este periodo.



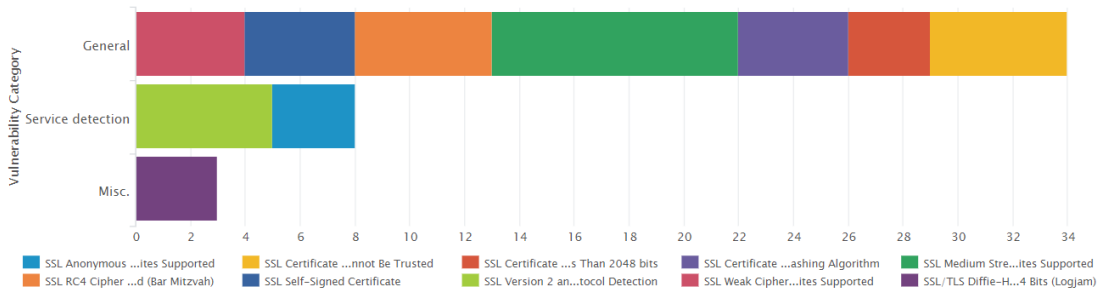
Graph: Vulnerability Risk by Port
Este diagrama ilustra el nivel de riesgo y cantidad de ocurrencia de vulnerabilidades asociadas a puertos específicos, encontradas durante este periodo.



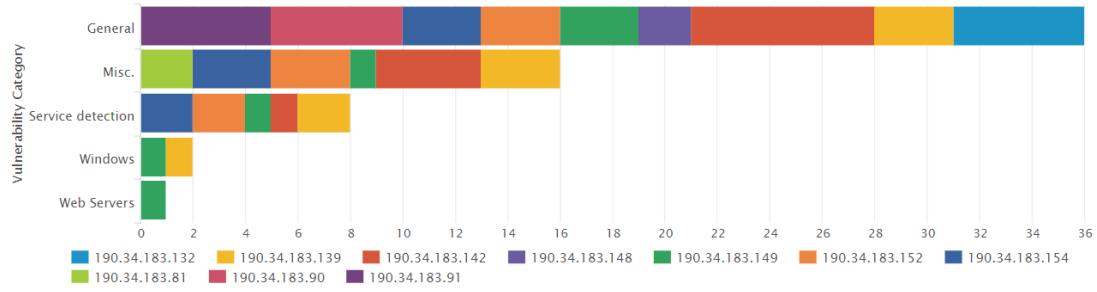
Graph: Vulnerability Risk by Protocol
Este diagrama ilustra el nivel de riesgo y cantidad de ocurrencia de vulnerabilidades asociadas a protocolos específicos, encontradas durante este periodo.



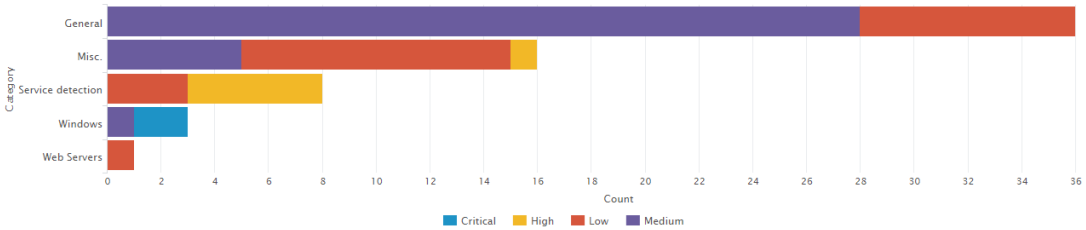
Graph: Vulnerability Category by Vulnerability Name
Este diagrama ilustra el nivel de riesgo y cantidad de ocurrencia de vulnerabilidades asociadas a nombres específicos, encontradas durante este periodo.



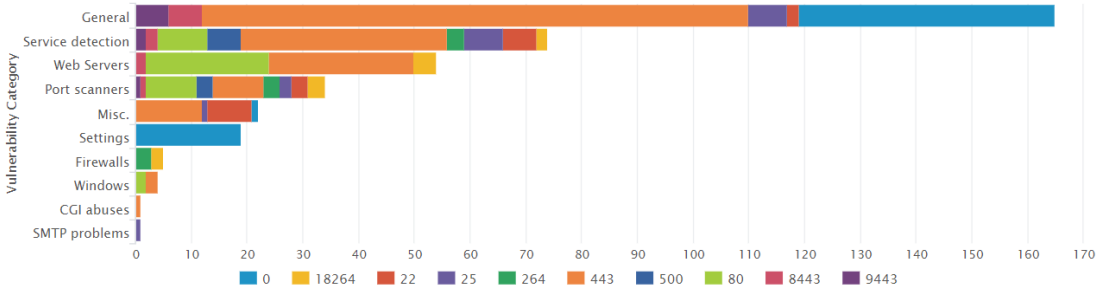
Graph: Vulnerability Category by Host
Este diagrama ilustra las categorías y cantidad de ocurrencia de vulnerabilidades asociadas a hosts específicos, encontradas durante este periodo.



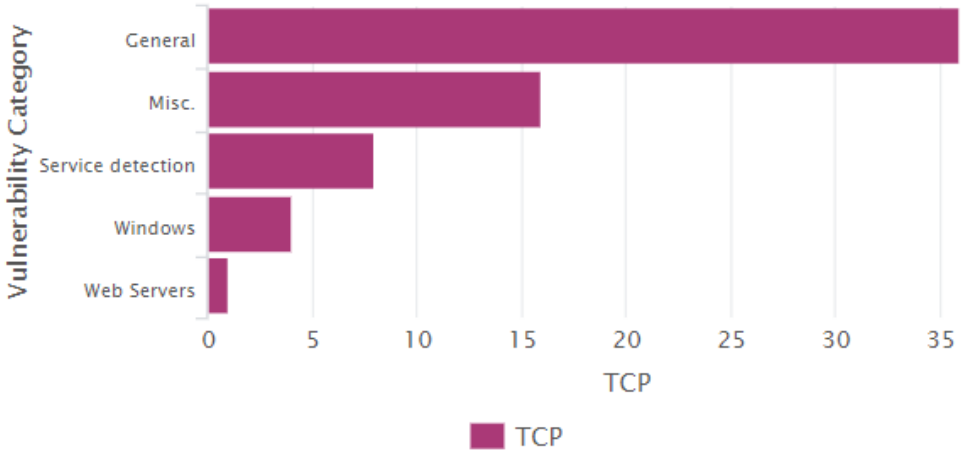
Graph: Vulnerability Category by Risk
Este diagrama ilustra las categorías y cantidad de ocurrencia de vulnerabilidades asociadas a nivel de riesgo, encontradas durante este periodo.



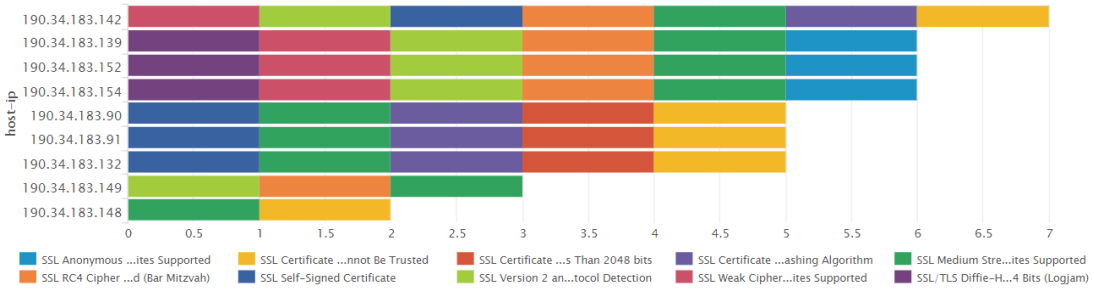
Graph: Vulnerability Category by Port
Este diagrama ilustra las categorías y cantidad de ocurrencia de vulnerabilidades asociadas a puertos específicos, encontradas durante este periodo.



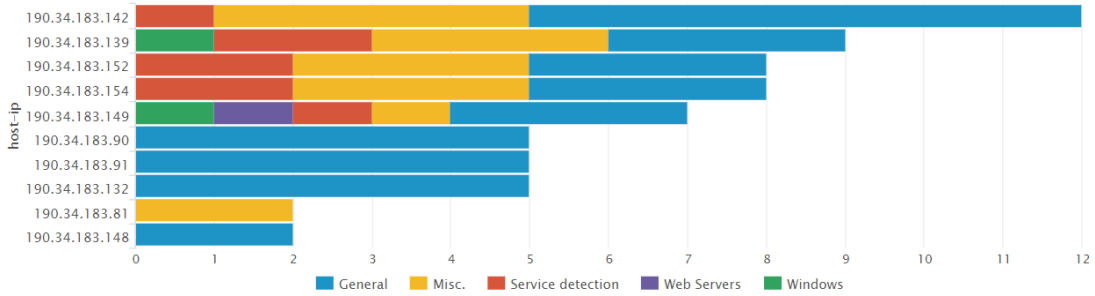
Graph: Vulnerability Category by Protocol
Este diagrama ilustra las categorías y cantidad de ocurrencia de vulnerabilidades asociadas a protocolos específicos, encontradas durante este periodo.



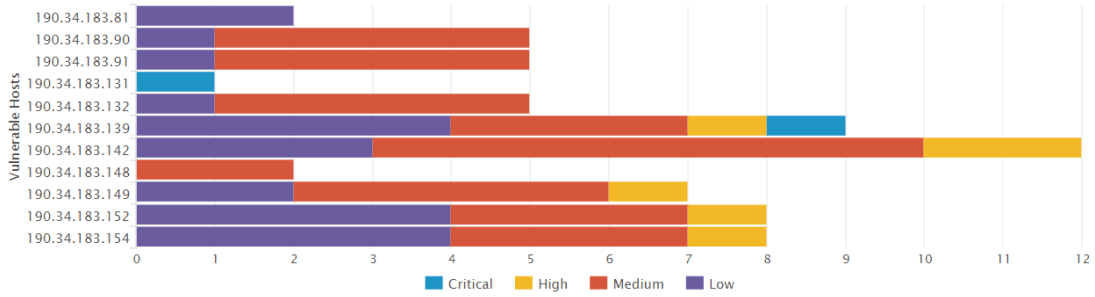
Graph: Host by Vulnerability Name
Este diagrama muestra los nombres y cantidad de ocurrencia de vulnerabilidades asociadas a hosts específicos, encontradas durante este periodo.



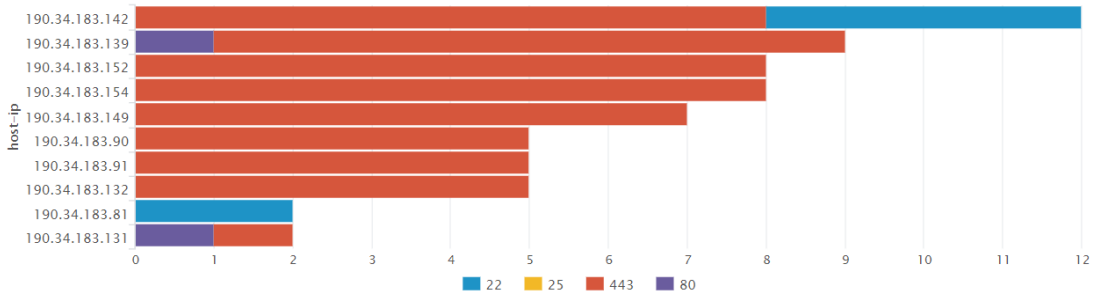
Graph: Host by Vulnerability Category
Este diagrama muestra las categorías y cantidad de ocurrencia de vulnerabilidades asociadas a hosts específicos, encontradas durante este periodo.



Graph: Host by Vulnerability Risk
Este diagrama muestra el riesgo y cantidad de ocurrencia de vulnerabilidades asociadas a hosts específicos, encontradas durante este periodo.



Graph: Host by Port
Este diagrama muestra los puertos vulnerables y cantidad de vulnerabilidades identificadas para cada uno, asociadas a hosts específicos, encontradas durante este periodo.



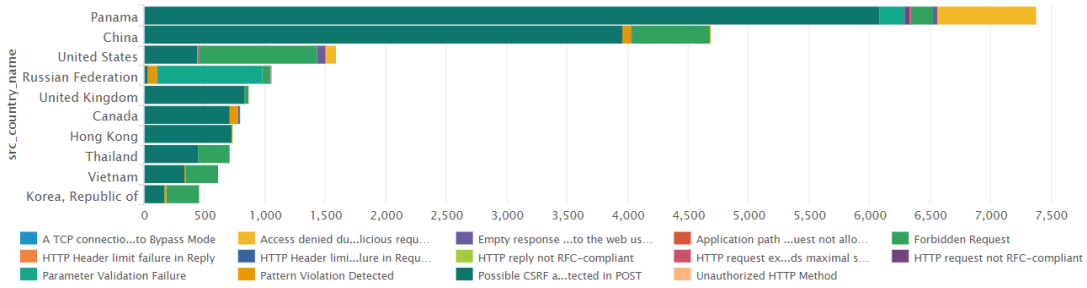
SECCION DE INTELIGENCIA PARA EL SERVICIO DE SEGURIDAD ADMINISTRADO DEL CORTAFUEGO DE APLICACION (MSS-APFW)

El MSS-APFW monitorea y protege contra ataques a nivel de aplicación hacia los servidores de la organización 7x24x365. Este servicio también envía información para su correlación y proceso de inteligencia.

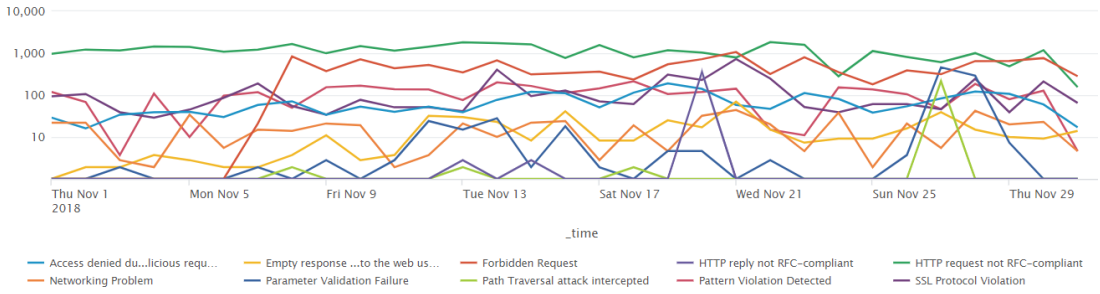
El propósito de esta sección es resaltar la inteligencia recolectada por este y otros servicios contratados, así como también fuentes externas como Honeypots, fuentes maliciosas conocidas, bases de datos vulnerables, relaciones con los equipos CERT y CSIRT que posee GLESEC, junto con otras fuentes de amenazas.

Los siguientes diagramas son tableros generados por la plataforma TIPTM de GLESEC. Estos tableros son representativos de métricas para este servicio.

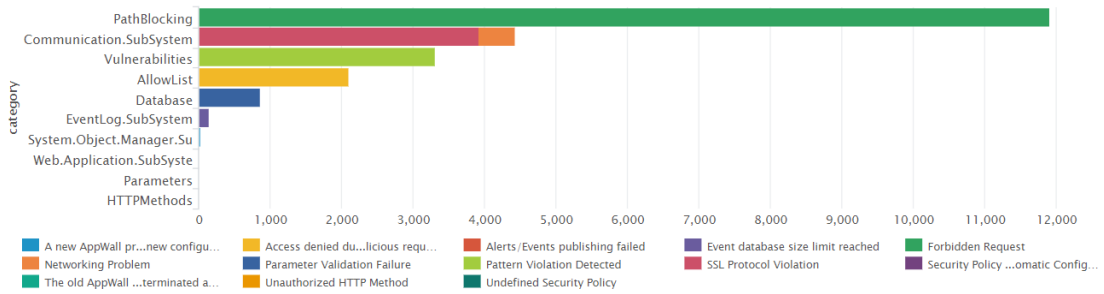
Graph: Top 10 Attacking Countries Blocked by Attack Type – AppWall
Para este periodo no se cuenta con suficientes resultados del AppWall para generar información.



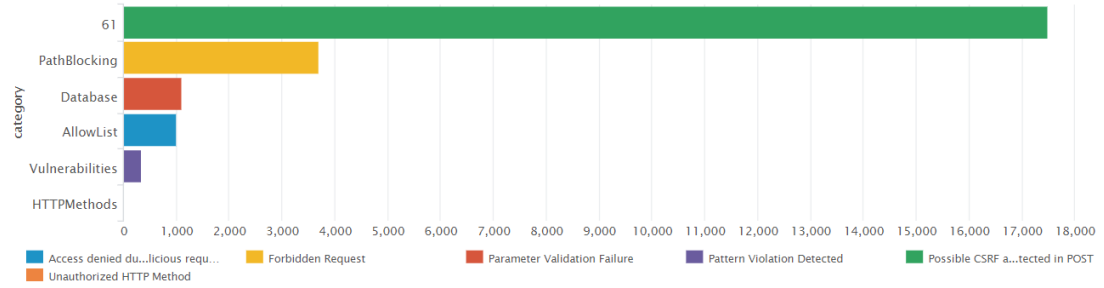
Graph: Attacks Types Blocked by Week – AppWall
Este reporte proporciona la cantidad de ataques bloqueados por semana.
Para este periodo no se cuenta con suficientes resultados del AppWall para generar información.



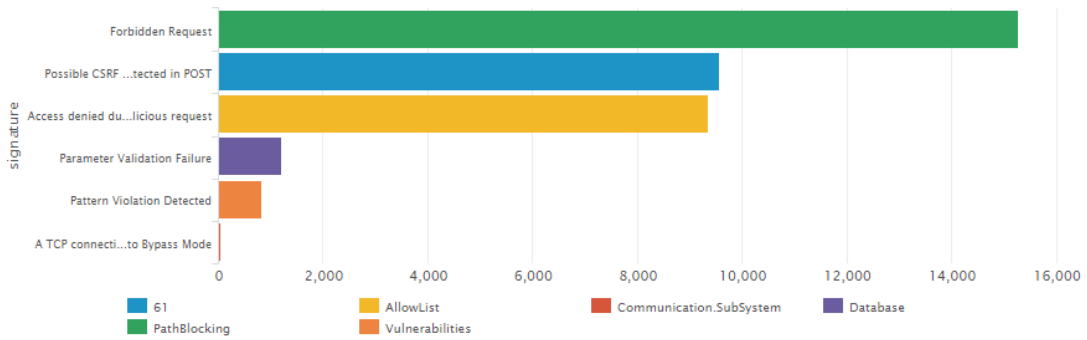
Graph: Attacks Blocked By Threat Category - AppWall
Este reporte lista las categorías de ataques que fueron bloqueados en este periodo por nombre de ataque.



Graph: Critical Attacks Blocked – AppWall
La siguiente gráfica muestra información sobre ataques críticos, nombre de ataques, regula de seguridad de red junto con cantidad de intentos.

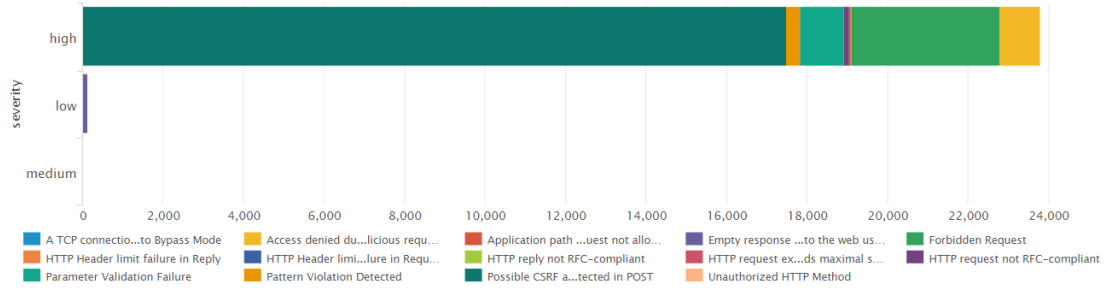


Graph: Top Attacks Blocked – AppWall
Este reporte provee información sobre los ataques bloqueados con más intentos, identificado por nombre de ataque, regla de seguridad de red y el número total de ataques bloqueados con esta combinación.



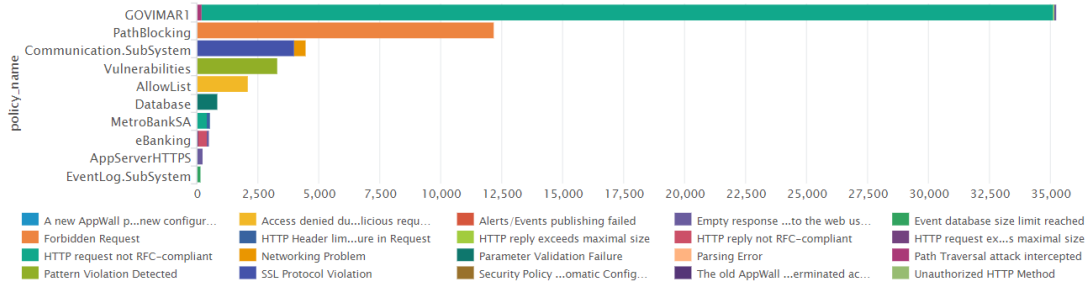
Graph: Top Attacks Blocked By Risk - AppWall

En el siguiente diagrama se muestra información sobre los ataques bloqueados por el APFW organizado por nivel de riesgo.



Graph: Attacks Blocked by Network Security Rule - AppWall

Este reporte lista la cantidad de ataques organizado por regla de seguridad de red, mencionando el nombre de ataque.



Operaciones de Ciberseguridad

El propósito de esta sección es para destacar las actividades realizadas por el Centro de Operaciones Global (GOC) de GLESEC incluyendo: monitoreo de disponibilidad y rendimiento de los servicios contratados, Administración de Cambios, actividades de respuesta a incidentes y actividades de consultoría.

MONITOREO DE DISPONIBILIDAD

Esta sección informa sobre la disponibilidad de las contramedidas contratadas con GLESEC.

El AppWall fue considerado en funcionamiento y disponible el 100% durante el periodo de este informe.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	31d 1h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	31d 1h 0m 0s	100.000%	100.000%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	31d 1h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.888% (99.888%)	0.089% (0.089%)	0.000% (0.000%)	0.022% (0.022%)	0.000%
Average	99.888% (99.888%)	0.089% (0.089%)	0.000% (0.000%)	0.022% (0.022%)	0.000%

El DefensePro fue considerado en funcionamiento y disponible el 100 % durante el periodo de este informe.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	31d 1h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	31d 1h 0m 0s	100.000%	100.000%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	31d 1h 0m 0s	100.000%	100.000%

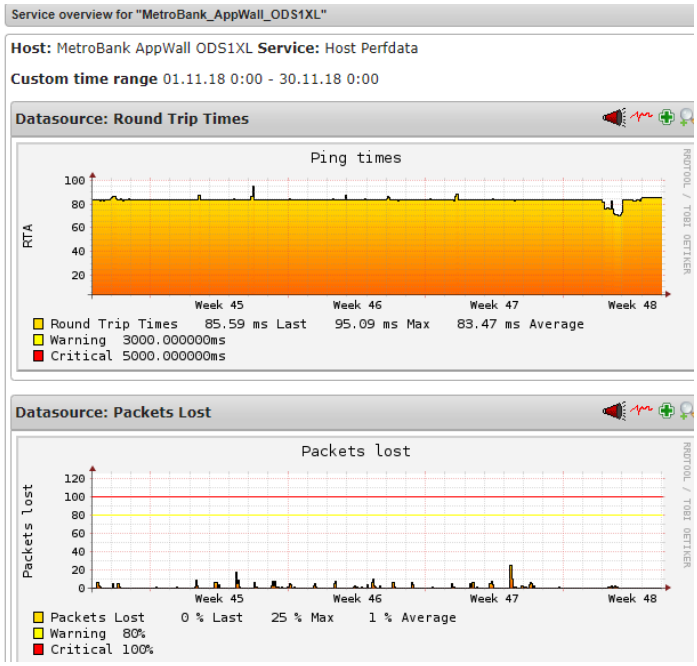
State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.732% (99.732%)	0.235% (0.235%)	0.000% (0.000%)	0.034% (0.034%)	0.000%
Average	99.732% (99.732%)	0.235% (0.235%)	0.000% (0.000%)	0.034% (0.034%)	0.000%

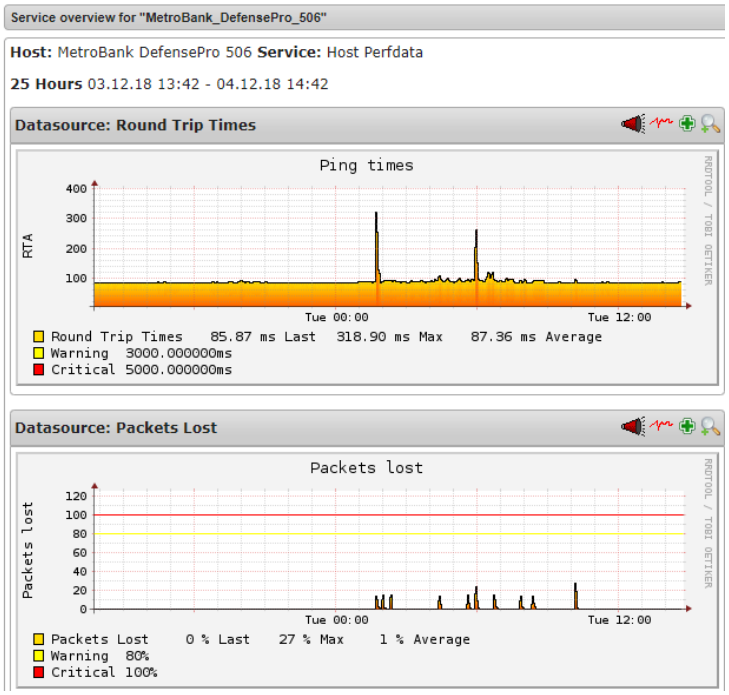
MONITOREO DE RENDIMIENTO Y CONTRAMEDIDAS

En esta sección nosotros monitoreamos y registramos el tiempo de respuesta desde los IDCs de GLESEC hacia las contramedidas bajo administración de GLESEC.

Tiempo de ida y vuelta de ping promedio 83.47 desde el GOC de GLESEC hacia el AppWall de Metrobank S.A. con 0% de pérdida de paquetes promedio.



Metrobank S.A. Rendimiento del DefensePro
Tiempo de ida y vuelta de ping promedio 87.36 desde el GOC de GLESEC hacia el DefensePro de Metrobank S.A. con 0% de perdida de paquetes promedio.



ACTIVIDAD DE SERVICIOS PROFESIONALES

A continuación, describimos el uso del servicio de consultoría de la actividad de servicios profesionales para el mes correspondiente. En esto mostramos el total de horas facturables y no facturables, el retenedor contratado, el total de horas utilizadas en el mes y las horas por encima del retenedor.

Horas de consulta facturables	Horas de consulta no facturables	Horas contratadas de retención	Horas totales utilizadas	Horas por encima del retenedor
0	0	1	0	0

ACTIVIDAD DE TICKETS

En esta sección nosotros registramos todos los tickets de cambios de administración e incidentes para este mes.

Ticket#	Title	Created
2018112310000027	RE: Seguimiento a Sistemas Críticos	2018-11-23 12:20:03
2018112310000018	RE: Seguimiento a Sistemas Críticos	2018-11-23 12:10:09
2018111510000051	Problemas en la aplicación Ebanking - Carga de archivos de fotos via ipad	2018-11-15 12:20:03
2018111410000071	Cambio de la configuración de la protección de la aplicación Ebanking para modo pasivo	2018-11-14 20:10:03
2018111410000062	Problema con la protección de Ebanking	2018-11-14 19:50:04
2018111210000039	RE: Solucion de Aplicacion eBanking	2018-11-12 12:30:03
2018111010000061	Reporte Mensual de Operaciones Octubre 2018	2018-11-10 13:17:00
2018110710000058	RE: MetroBank - Activacion de la Protección para las aplicaciones	2018-11-07 16:00:06

Durante este periodo del mes el GOC ha dado un seguimiento a los sistemas críticos del cliente, respecto a las vulnerabilidades de estos sistemas.
El Departamento de Servicios Profesionales de GLESEC, ha estado en continua comunicación con el cliente debido a los cambios realizados en el dispositivo AppWall que protege sus sitios web.

Definiciones

Una lista más complete está disponible en el portal GMP

Las vulnerabilidades altas (High Vulnerabilities) se definen como pertenecientes a una o más de las siguientes categorías: puertas traseras, acceso completo de lectura / escritura a archivos, ejecución remota de comandos, posibles caballos de Troya o divulgación de información crítica (por ejemplo, contraseñas).

Vulnerabilidades medianas (Medium Vulnerabilities) describe las vulnerabilidades que exponen datos confidenciales, exploración de directorios y transversales, divulgación de controles de seguridad, facilitan el uso no autorizado de servicios o denegación de servicio a un atacante

Vulnerabilidades bajas (Low Vulnerabilities) describe las vulnerabilidades que permiten la recopilación de información preliminar o delicada para un atacante o plantea riesgos que no están completamente relacionados con la seguridad pero que pueden utilizarse en ingeniería social o ataques similares.

Las vulnerabilidades de SMB / NetBIOS podrían permitir la ejecución remota de código en los sistemas afectados. Un atacante que explota con éxito estas vulnerabilidades podría instalar programas; ver, cambiar o eliminar datos; o cree cuentas nuevas con derechos de usuario completos. Las mejores prácticas de Firewall y las configuraciones estándar de firewall predeterminadas pueden ayudar a proteger las redes de los ataques que se originan fuera del perímetro de la empresa. Las mejores prácticas recomiendan que los sistemas que están conectados a Internet tengan una cantidad mínima de puertos expuestos

Las vulnerabilidades de red simples afectan a protocolos como NTP, ICMP y aplicaciones de redes comunes como SharePoint, entre otros. Esto no pretende ser una lista completa.

La autenticación y el cifrado son dos tecnologías entrelazadas que ayudan a asegurar que sus datos permanezcan seguros. Autenticación es el proceso de asegurar que ambos extremos de la conexión sean de hecho "quién" dicen que son. Esto se aplica no solo a la entidad que intenta acceder a un servicio (como un usuario final) sino también a la entidad que presta el servicio (como un servidor de archivos o un sitio web). La encriptación ayuda a asegurar que la información dentro de una sesión no se vea comprometida. Esto incluye no solo leer la información dentro de un flujo de datos, sino también alterarla.

Si bien la autenticación y el cifrado tienen sus propias responsabilidades para asegurar una sesión de comunicación, la máxima protección solo puede lograrse cuando los dos se combinan. Por este motivo, muchos protocolos de seguridad contienen especificaciones de autenticación y cifrado.

USA-ARGENTINA-PANAMA
México-Perú-Brasil- Chile

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com