REPORTE DE OPERACIONES E INTELIGENCIA EJECUTIVO DE CIBERSEGURIDAD

Copa Airlines

Noviembre 2018

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

Info@glesec.com
www.glesec.com

Tabla de Contenidos

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 contramedidas 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.

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

Alcance de este informe

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

Type	Service	Contracted?	Service Expiration
Threat Mitigation	MSS-APS		
Threat Mitigation	MSS-APS-SSL		
Threat Mitigation	MSS-APS-PS		
Threat Mitigation	MSS-APFW		
Vulnerability Testing	MSS-VME	YES	11/01/2019
Vulnerability Testing	MSS-VMI		
Compliance	MSS-EPS		
Threat Mitigation	MSS-SIEM		
Risk assessment	MSS-BAS		
Threat Mitigation	MSS-EIR		
Threat Mitigation	MSS-UTM		
Threat Mitigation	MSS-INT		
Access Control	MSS-TAS	YES	11/01/2019

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

Resumen Ejecutivo

Este informe corresponde al periodo 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.

RISK

La Gestión de riesgo es el proceso continuo de identificar, evaluar y responder al riesgo. Para gestionar el riesgo, las organizaciones deben entender la probabilidad que un evento ocurra y el impacto resultante. Con esta información, las organizaciones pueden determinar el nivel aceptable de riesgo para la prestación de servicios y pueden expresar esto como su tolerancia al riesgo. El marco de referencia para Ciberseguridad del NIST.

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.

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

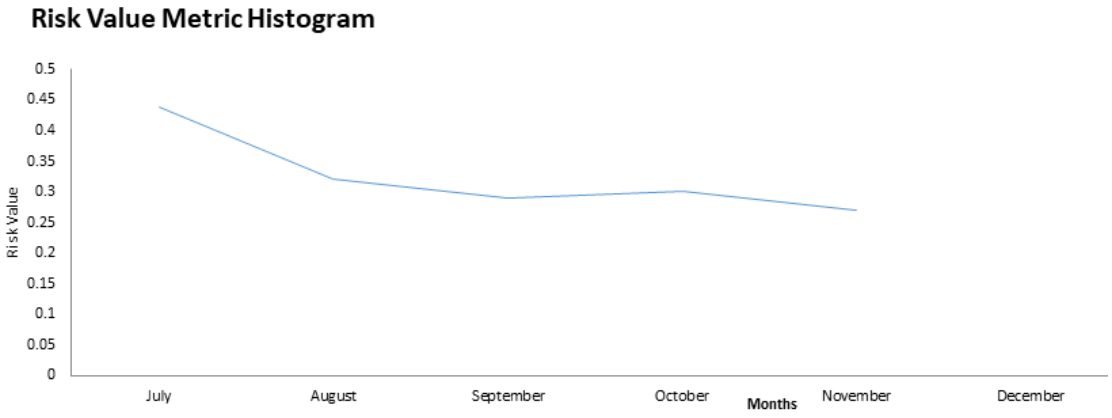
Nosotros en GLESEC medimos RIESGO a través de varias perspectivas y utilizando varios de los servicios de la plataforma TIP™. El MSS-VM o Servicio de Seguridad Administrado para Manejo de Vulnerabilidades nos proporciona una vista, cuán débiles son los sistemas de la organización. El MSS-BAS nos proporciona 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 proporcionan 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, una variedad de servicios nos proporcionan diferentes puntos de vista y juntos tenemos la vista más completa de la postura de seguridad de nuestros clientes.

La condición de riesgo para Copa Airlines para el mes de noviembre es crítica. Esto se puede ver en los indicadores de seguridad descritos a continuación.

Indicador de Riesgo	**Servicio**	**Condición**	**Comentarios**
Métrica de Valor de riesgo	MSS-VME	**CRITICAL**	3 vulnerabilidades de severidad Critica y 9 vulnerabilidades de severidad alta fueron encontradas en este periodo. Cualquiera de éstas, al ser explotadas, podrían causar un impacto negativo severo a sus sistemas y servicios.

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

El histograma de MÉTRICA DE VALOR DE RIESGO que se muestra a continuación representa los cambios en la métrica de valor de riesgo basada en vulnerabilidades en los últimos seis meses.



Durante este periodo del mes como muestra el histograma se presenta una disminución de su nivel de riesgo, esto se debe a la disminución de hosts analizados y la disminución de sistemas vulnerables de 33 en el mes de octubre a 28 durante el mes de noviembre.

Para GLESEC, es importante saber si estos servidores deberían estar 100% operativos durante todo el día o si experimentan tiempo de inactividad en horas específicas.

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 una prueba de 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.

El número total de vulnerabilidades presentadas en Copa Airlines para el mes de noviembre es 102, esto muestra un decremento leve comparado al mes anterior (103) debido a esto se puede decir que las vulnerabilidades no se han mitigado de manera efectiva. Estas vulnerabilidades están clasificadas de acuerdo con las siguientes severidades: 3 críticas, 9 altas, 70 medias y 20 bajas.

Las vulnerabilidades críticas reportadas el mes anterior fueron descubiertas en dispositivos a los cuales no se pudo alcanzar durante este periodo. Estas fueron: MS15-034: Vulnerabilidad en HTTP.sys Puede permitir ejecución remota de código (3042553) (uncredentialed check) en los equipos 200.46.240.230, 2000.46.240.161 y 200.46.240.24 y Versión sin soporte detectada, Microsoft IIS 6.0 en el equipo 200.46.240.139. Detalles adicionales de la severidad de estas vulnerabilidades están incluidas en nuestro reporte técnico mensual.

Los 5 equipos más vulnerables para este periodo son:

200.46.240.161 con 11 vulnerabilidades, 201.218.212.9 con 11 vulnerabilidades, 201.218.212.10 con 10 vulnerabilidades, 200.46.240.166 con 7 vulnerabilidades, 200.46.240.82 con 6 vulnerabilidades

Las categorías de vulnerabilidad más frecuente son:

General

- Suites de cifrado de fortaleza media soportada, con un total de 17 sistemas afectados.
- Vulnerabilidad de desglose de información por implementación de inicialización del vector en el protocolo SSL/TLS (BEAST) con 16 sistemas afectados.
- Suites de cifrado RC4 soportados, con un total de 10 sistemas afectados

Misceláneo

- Modo 6 de escaneo en el protocolo de tiempo de red (NTP) con un total de 4 sistemas afectados.
- Vulnerable a SSL DROWN con un total de 4 sistemas afectados

Detección de Servicios

- SSL versión 2 y/o SSL versión 3 habilitados, con un total de 8 sistemas afectados.

Los puertos 443 (HTTPS), 8080 (Alt. HTTPS), 8443 (Alt. HTTPS) y 80 (HTTP) son considerados los más vulnerables para este periodo debido a que se encontraron muchas vulnerabilidades relacionadas a los servicios que escuchan en dichos puertos, estas vulnerabilidades están clasificadas como riesgo medio.

La gran mayoría de sus sistemas tienen vulnerabilidades relacionadas a servicios que utilizan el protocolo de capa de transporte TCP para comunicarse a excepción del equipo 201.218.212.9, que presenta una vulnerabilidad a través del protocolo UDP de tipo Internet Key Exchange (IKE) Modo Agresivo con Llave previamente compartida, de severidad media.

Métrica de Valor de Riesgo

GLESEC utiliza una métrica para proveer una manera de cuantificar las vulnerabilidades basada 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 “críticas”, “alto”, “medio” y “bajo”, 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 comprender mejor 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.

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

La siguiente tabla indica la métrica de vulnerabilidades externas.

Total IP's Scanned	IP's Vulnerable
47	28

Risk Distribution				
Critical	High	Medium	Low	Total
3	9	70	20	102

According to the metrics:

RV= 0.273049645

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

Listado externo de vulnerabilidades por condición:

host-ip	Crcitial	High	Low	Medium	Total
200.46.240.161	1	2	1	7	11
201.218.212.9	0	1	2	8	11
201.218.212.10	0	1	2	7	10
200.46.240.166	0	1	1	5	7
200.46.240.82	0	1	2	3	6
200.46.240.179	0	1	1	4	6
200.46.240.230	1	0	0	5	6
200.46.240.30	0	1	2	2	5
200.46.240.195	0	1	1	3	5
200.46.240.24	1	0	0	3	4
200.46.240.137	0	0	0	4	4
200.46.240.136	0	0	1	2	3
201.218.212.35	0	0	0	3	3
201.218.212.36	0	0	1	2	3
201.218.212.122	0	0	3	0	3
52.86.152.128	0	0	1	1	2
201.218.212.149	0	0	1	1	2
201.218.212.175	0	0	0	2	2
52.3.92.27	0	0	0	1	1
52.72.43.239	0	0	0	1	1
200.46.240.1	0	0	0	1	1
200.46.240.2	0	0	0	1	1
200.46.240.33	0	0	1	0	1
200.46.240.90	0	0	0	1	1
200.46.240.253	0	0	0	1	1
200.46.240.254	0	0	0	1	1
200.46.241.161	0	0	0	1	1

La siguiente tabla provee una comparativa de las vulnerabilidades externas persistentes del mes actual con respecto al mes pasado.

host-ip	Previous Month	Current Month
200.46.240.1	3	1
200.46.240.136	3	3
200.46.240.137	4	4
200.46.240.161	7	11
200.46.240.166		7
200.46.240.179	6	6
200.46.240.195	9	5
200.46.240.2	1	1
200.46.240.228	6	
200.46.240.230	4	6
200.46.240.24	4	4
200.46.240.253	1	1
200.46.240.254	1	1
200.46.240.30	5	5
200.46.240.33	1	1
200.46.240.82	6	6
200.46.240.90	1	1
200.46.241.161	1	1
201.218.212.10	10	10
201.218.212.122	4	3
201.218.212.149	3	2
201.218.212.175	2	2
201.218.212.35	2	3
201.218.212.36	3	3
201.218.212.72	4	
201.218.212.76	3	
201.218.212.9	11	11
52.3.92.27	1	1
52.72.43.239	1	1
52.86.152.128	2	2

Por favor referirse a las recomendaciones para más detalles. Estas pueden ser vistas en el GLESEC MEMBER PORTAL (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	50	12	62
Misc.	0	0	8	5	13
Service detection	0	8	0	0	8
Web Servers	0	0	8	0	8
FTP	0	0	1	3	4
Windows	3	0	1	0	4
CGI abuses	0	1	2	0	3

AMENAZAS

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

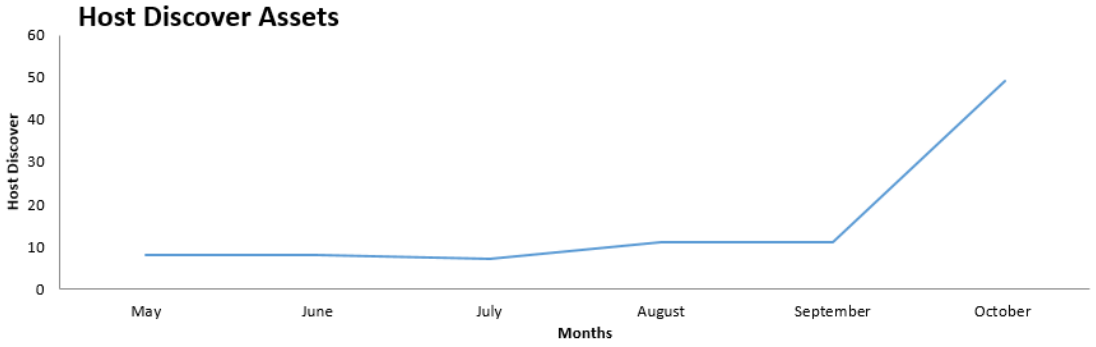
Los servicios que nos proporcionan información para esta sección no han sido contratados.

ACTIVOS

Creemos que no podemos proteger lo que no sabemos y conocer los activos (sistemas y aplicaciones) es fundamental para tener una buena práctica de seguridad cibernética. Por lo tanto, le recomendamos que verifique la información que proporcionamos y que nos haga saber si algo es sospechoso o simplemente no está bien. Podemos trabajar con su organización para crear una línea base que se pueda usar para identificar desviaciones. Por favor, póngase en contacto con nuestro GOC para obtener ayuda en este tema.

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.

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



Para Copa Airlines durante el periodo del mes, el número total de sistemas descubiertos disminuyó de 47 con respecto a los 49 sistemas alcanzados en el mes de octubre. Con el rango de direcciones proporcionados por Copa Airlines se encontró que 28 hosts son vulnerables, comparado con los 33 hosts vulnerables del mes anterior; Este decremento se debe a que no se logró alcanzar todos los hosts de los cuales algunos de ellos presentaban vulnerabilidades como 201.218.212.76 y 200.46.240.139.

CUMPLIMIENTO

El MSS-EPS o Managed End Point Security Service es un servicio de cumplimiento y remediación. Por cumplimiento entendemos el monitoreo, pruebas y alertas de las desviaciones de los parámetros de todos los "equipos" y "servidores" en la organización con respecto a las líneas base establecidas. Estas líneas base puede ser creadas para soportar requisitos específicos externos o guías internas sobre las mejores prácticas. El MSS-EPS puede vigilar las desviaciones de estas líneas base y también puede "forzar" el cumplimiento de estas.

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

VALIDACIÓN DE CIBER SEGURIDAD

La validación de seguridad conlleva validar la totalidad de la seguridad a través de pruebas con ataques simulados. Estas pruebas se realizan con el Servicio Managed Breach Attack Simulation (MSS-BAS). El MSS-BAS es una colección avanzada de servicios de prueba que abarca pruebas pre-explotación, post-explotación y de percepción. Las pruebas se realizan sobre objetivos reales, utilizando ataques simulados, por lo tanto, proveen resultados concluyentes (sin falsos positivos). Los diferentes vectores de ataques prueban las de las contramedidas de la organización en diferentes factores como: configuraciones, implementaciones y habilidad de

responder en forma continua produciendo recomendaciones e inteligencia valiosas a la organización.
Los servicios que nos proporcionan información para esta sección no han sido contratados.

ACCESO CONFIABLE

El nuevo modelo de TI viene con una superficie de ataque mayor, conformada por los empleados que utilizan sus dispositivos personales para el trabajo, mientras laboran de forma remota. La proliferación de aplicaciones en la nube para casi cualquier necesidad de negocio también ha contribuido al incremento de complejidad técnica. Hoy día, los atacantes pueden exponer diferentes vulnerabilidades en múltiples vectores en un solo ataque. La seguridad tradicional está diseñada para lidiar con ataques aislados o separados, haciendo estas soluciones poco efectivas contra las amenazas modernas. Estas nuevas amenazas se centran en obtener acceso remoto a sus aplicaciones y datos, ya sea con credenciales robadas o explotando vulnerabilidades conocidas dirigidas a sus usuarios, sus dispositivos desactualizados, aplicaciones en la nube y software de acceso remoto.

Durante este periodo del mes Copa Airlines tuvo una tasa de acceso exitoso de 92.6%. Se registraron 573 autenticaciones denegadas: 471 autenticaciones denegadas por accidente debido a error del usuario, 38 autenticaciones denegadas voluntariamente por los usuarios en las que el usuario tomo acción para denegarlas en la notificación de Duo o Duo Mobile,59 autenticaciones bloqueadas por políticas o reglas del sistema.

El número total de usuarios para el mes de noviembre fue de 486.

El 80.94 % de los usuarios que utilizan la aplicación Duo, se autentifican con el método “Passcode”, se recomienda utilizar el método de autentificación “Duo Push” el cual sólo representa un 2.38% de las autenticaciones exitosas de este periodo.

El país donde mayormente se reciben autentificaciones es Colombia con un 37.9 %, seguido de Panamá con 25.5% y Estados Unidos con 17.8%.

Sistemas Operativos de Dispositivos Móviles con vulnerabilidades (127 endpoints desactualizados):

- ✓ 8 IOS
- ✓ 119 Android

Endoints con Navegadores Desactualizados (29 endpoints desactualizados):

- ✓ 1 navegadores Firefox
- ✓ 1 internet Explorer
- ✓ 24 chrome
- ✓ 3 edge

Endpoints con complementos desactualizados (21 puntos finales desactualizados):

- ✓ 21 actualización de flash player

Tener sistemas operativos y/o aplicaciones desactualizadas; es decir, con actualizaciones del fabricante no aplicados al *endpoint* que resuelven vulnerabilidades de *Zero-Day* conocidos con lleva a un riesgo de seguridad crítico ya que deja al *endpoint* sin las protecciones necesarias para repeler o mitigar este ataque, exponiéndolo y a la red de Copa Airlines (en la mayoría de los casos) a ataques que pueden con llevar una disrupción temporal, total de parte o todo el sistema.
Se recomienda que se tomen las medidas necesarias e inmediatas para solventar esta situación.

Nuestro Servicios Profesionales en GLESEC (y haciendo uso de la hora de consultoría contratada por Uds.) puede ayudarlos a abordar y remediar estas situaciones.

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

Recomendaciones

GLESEC recomienda a Copa Airlines abordar lo siguiente:

1. Tomar acciones inmediatas siguiendo las recomendaciones detalladas en este reporte.

2. Los certificados inválidos deben ser corregidos para que puedan ser confiables, aún más cuando el servicio es expuesto a internet. Sistemas afectados: 201.218.212.10 y 201.218.212.9.

3. Las cadenas de certificado SSL que contienen llaves RSA con menos de 2048 bits deben ser corregidos. Sistemas afectados: 201.218.212.10 y 201.218.212.9.

4. Para la vulnerabilidad de "Browsable Web Directories" utilizar restricciones de acceso o deshabilitar la indexación para cualquier usuario que pueda hacerlo. Asegurarse que estos directorios navegables no filtren información confidencial o den acceso a recursos confidenciales.

5. Las suites de cifrado SSL con fortaleza media no se deben permitir para conexiones SSL. Para corregir esta vulnerabilidad se debe habilitar TLS 1.2 o superior y deshabilitar todas las versiones previas, que son vulnerables.

6. Se recomienda utilizar el método de autentificación "Duo Push" en lugar del método "PASSCODE" para el Servicio TAS el cual sólo representa un 2.38% de las autenticaciones exitosas de este periodo.

7. Los equipos con IP 201.218.212.9, 200.46.240.90 y 200.46.240.2 presentan una vulnerabilidad en el protocolo IKE (Internet Key Exchange) en modo agresivo con llave pre-compartida. Acciones por tomar:

    - Deshabilitar el modo agresivo si el dispositivo es compatible con dicha opción.
    - No utilizar llaves pre-compartidas para la autenticación si es posible.
    - Si el uso de una llave pre-compartida es inevitable, utilizar llaves Fuertes.

En nuestro reporte técnico mensual encontrará más información acerca de los equipos afectados con las vulnerabilidades mencionadas.

Sección de Inteligencia por módulo de servicio.

Managed Vulnerability Service (MSS-VM) Intelligence Section

El Managed Vulnerability Service (MSS-VM) permite a las organizaciones minimizar los riesgos de las vulnerabilidades mediante la rápida detección de debilidades, midiendo el riesgo potencial y la exposición, generar alertas, proveer información de remediación necesaria para mitigar estos riesgos de forma regular y facilitando el reporte de desviaciones y el cumplimiento con las regulaciones y mejores prácticas.

El propósito de esta sección es resaltar la Inteligencia recopilada de este y otros servicios contratados, así como también de fuentes externas como "honeypots", fuentes maliciosas conocidas, base de datos de vulnerabilidades, relaciones con los equipos de CERT y CSIRT que GLESEC posee, en conjunto con otras fuentes de amenazas.

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

Es importante establecer un programa de gestión de vulnerabilidades como parte de la estrategia de seguridad de la información debido a que poco después que las vulnerabilidades son descubiertas y reportadas por investigadores de seguridad o proveedores, los atacantes desarrollan código para explotar las vulnerabilidades y lanzan ataques con este código contra destinos de interés. Cualquier demora significativa en encontrar o reparar software con vulnerabilidades peligrosas provee amplias oportunidades para que ataques persistentes logren pasar las defensas, obteniendo control sobre las máquinas vulnerables y obteniendo acceso sobre la información sensible contenida en los mismo. Las organizaciones que no realizan escaneos en busca de vulnerabilidades y no corrigen las fallas descubiertas de forma proactiva enfrentan una mayor probabilidad de tener sus sistemas comprometidos

Muchas de las vulnerabilidades proveerán información CVE. El CVE (Common Vulnerabilities and Exposures) es una lista de riesgos de seguridad y vulnerabilidades patrocinados por el US-CERT y mantenido por la Corporación MITRE. La misión del CVE es proveer nombres estándares para todos los riesgos de seguridad conocidos públicamente, así como también definiciones estándares para términos de seguridad. El CVE puede ser buscado en línea en la dirección http://nvd.nist.gov/

<u>Puntuación de Vulnerabilidad</u>
La puntuación de vulnerabilidad está determinada por su factor de riesgo; crítico, alto, medio o bajo, así como también su valor en el Common Vulnerability Scoring

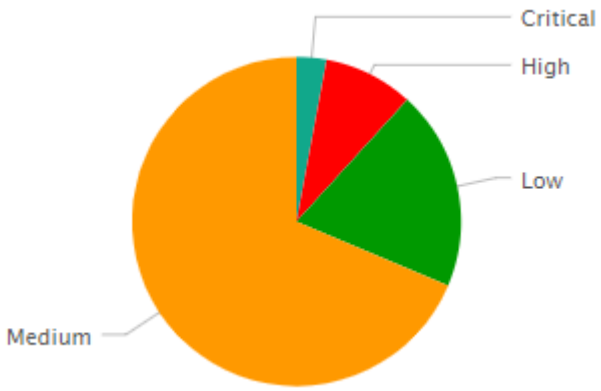
System (CVSS). La "puntuación base" representa el riesgo innato de alguna característica de cada vulnerabilidad. El CVSS es un sistema de puntuación de vulnerabilidades designado para proveer un método estandarizado y abierto para calificar las vulnerabilidades de TI. CVSS ayuda a las organizaciones priorizar y coordinar una respuesta conjunta para resolver estas vulnerabilidades, comunicando las propiedades base, temporales y circunstanciales de cada vulnerabilidad. Adicional a los valores números, el CVSS provee clasificaciones de Alto, Medio y Bajo, pero estos rangos cualitativos están relacionados a los valores numéricos CVSS.

Las vulnerabilidades están catalogadas de esta forma:

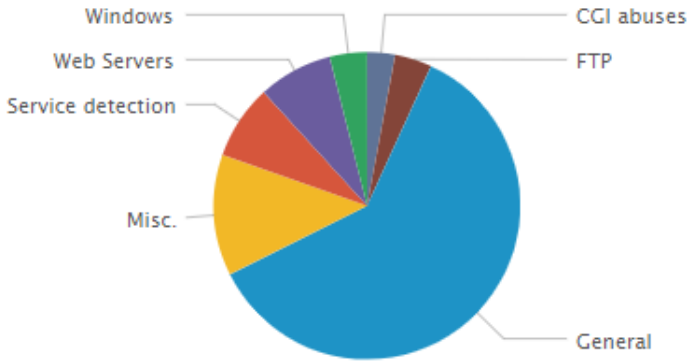
Riesgo bajo si tienen una puntuación CVSS base de 0.0 – 3.9.
Riesgo medio si tienen una puntuación CVSS base de 4.0 – 6.9.
Riesgo alto si tienen una puntuación CVSS base de 7.0 – 10.0.

Información de vulnerabilidades

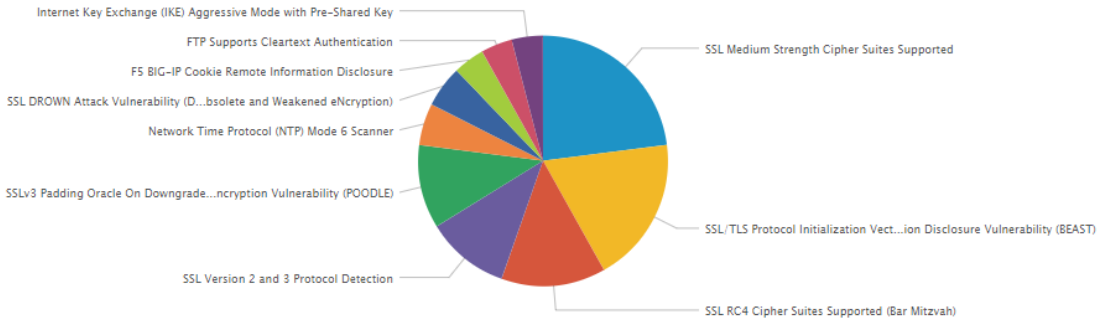
Graph: Risk Distribution
Esta gráfica muestra la distribución de riesgo de las vulnerabilidades descubiertas en el periodo de este reporte.



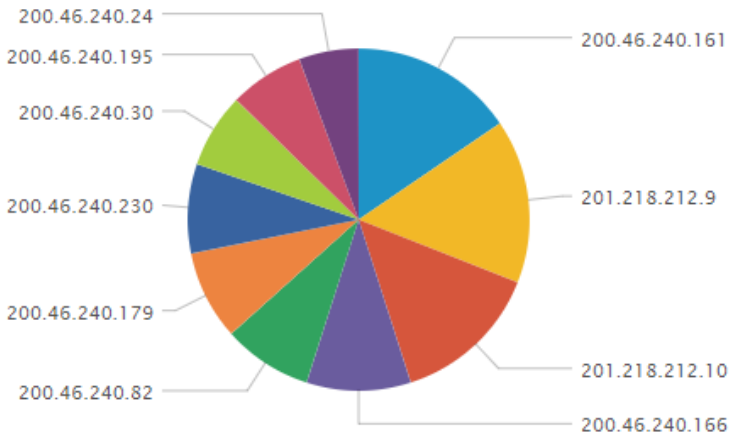
Graph: Most Frequent Vulnerability Category
Esta gráfica muestra la categoría de vulnerabilidad más frecuente descubiertas durante el periodo de este reporte.



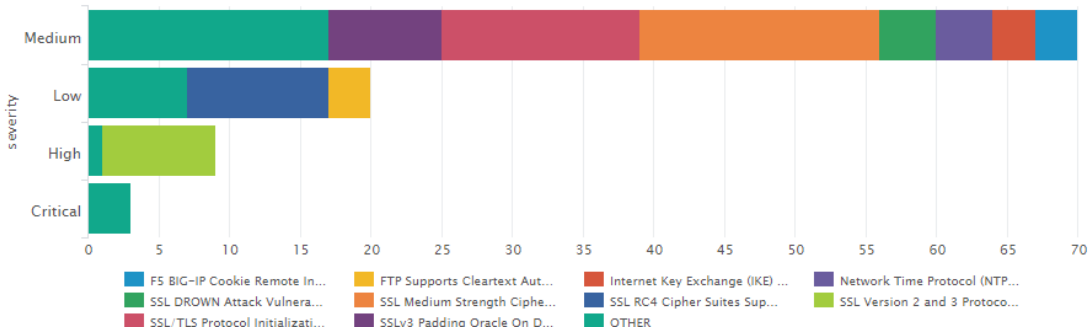
Graph: Most Frequent Vulnerability Name.
Esta gráfica muestra las vulnerabilidades más frecuentes descubiertas durante el periodo de este reporte.



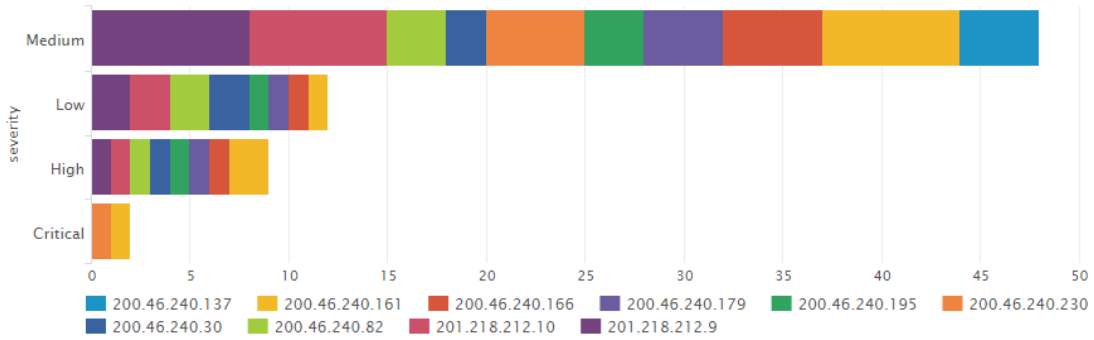
Graph: Most Vulnerable Host
Este gráfico muestra los equipos más vulnerables descubiertos durante el periodo de este reporte.



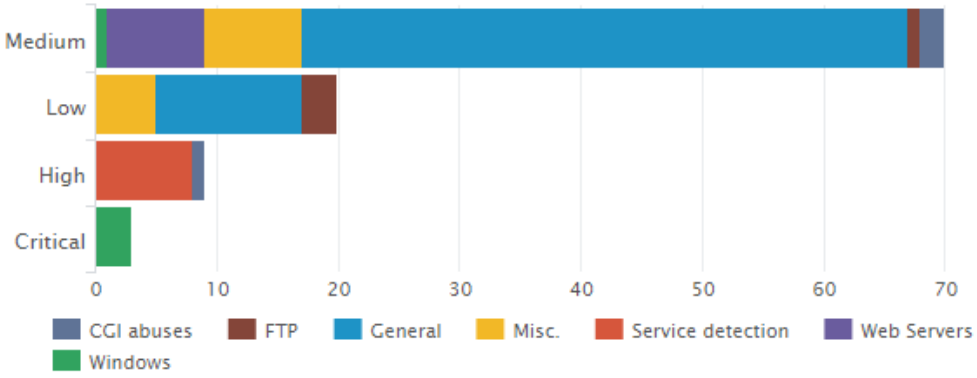
Graph: Vulnerability Risk by Vulnerability Name
Este gráfico ilustra el riesgo de las vulnerabilidades descubiertas y el conteo por nombre de vulnerabilidades durante el periodo de este reporte.



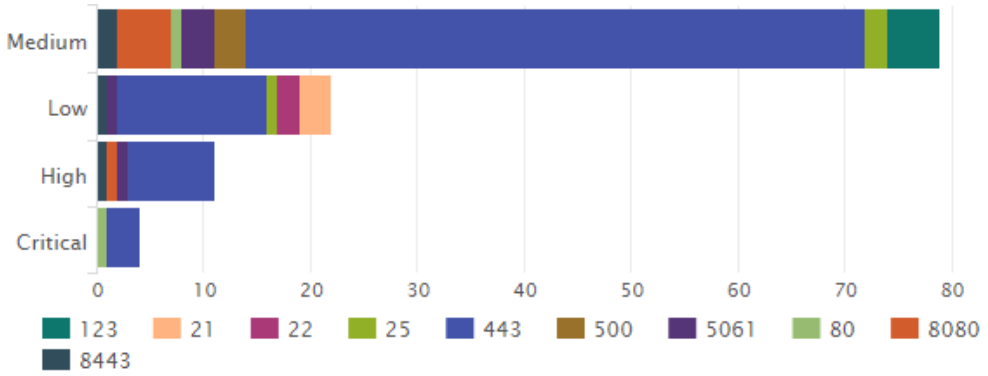
Graph: Vulnerability Risk by Host
Este gráfico ilustra el riesgo de las vulnerabilidades descubiertas y el conteo por categoría durante el periodo de este reporte.



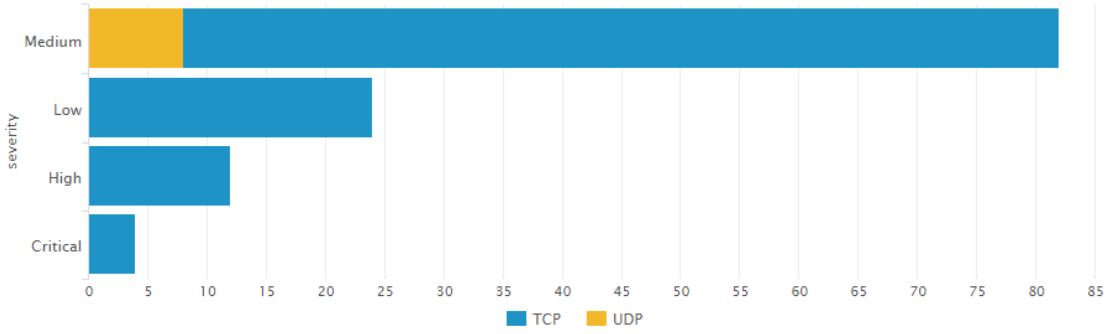
Graph: Vulnerability Risk by Vulnerability Category.
Esta gráfica ilustra el riesgo de las vulnerabilidades descubiertas y su categoría durante el periodo de este reporte.



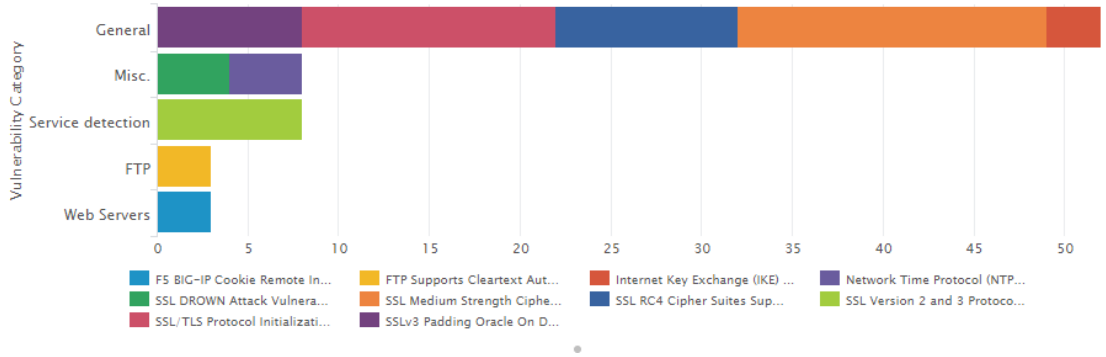
Graph: Vulnerability Risk by Port.
Esta gráfica ilustra el riesgo de las vulnerabilidades descubiertas y el conteo por puerto en el periodo de este reporte.



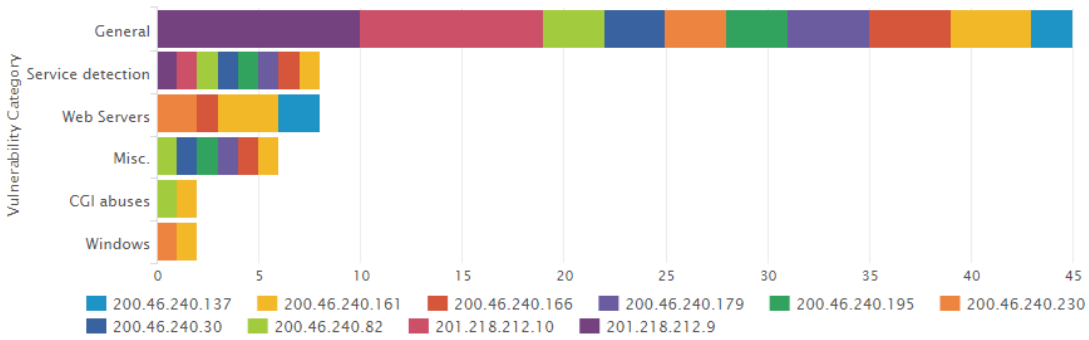
Graph: Vulnerability Risk by Protocol.
Esta gráfica ilustra el riesgo de las vulnerabilidades descubiertas y el conteo por protocolo durante el periodo de este reporte.



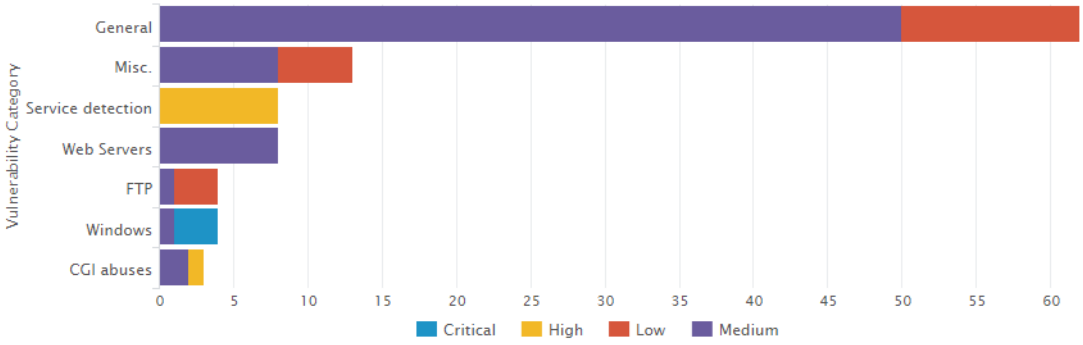
Graph: Vulnerability Category by Vulnerability Name.
Este gráfico ilustra las categorías de vulnerabilidad descubiertas y el conteo por nombre de vulnerabilidad durante este periodo de reporte.



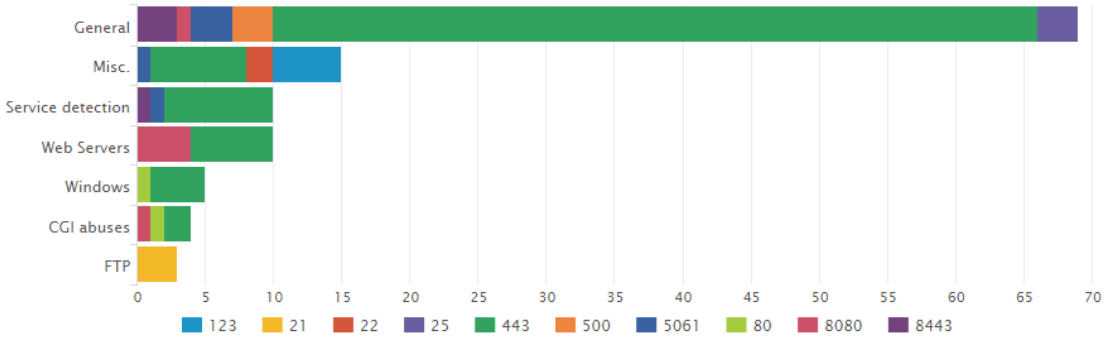
Graph: Vulnerability Category by Host.
Este gráfico ilustra las categorías de vulnerabilidad descubiertas y el conteo por hosts durante este periodo de reporte.



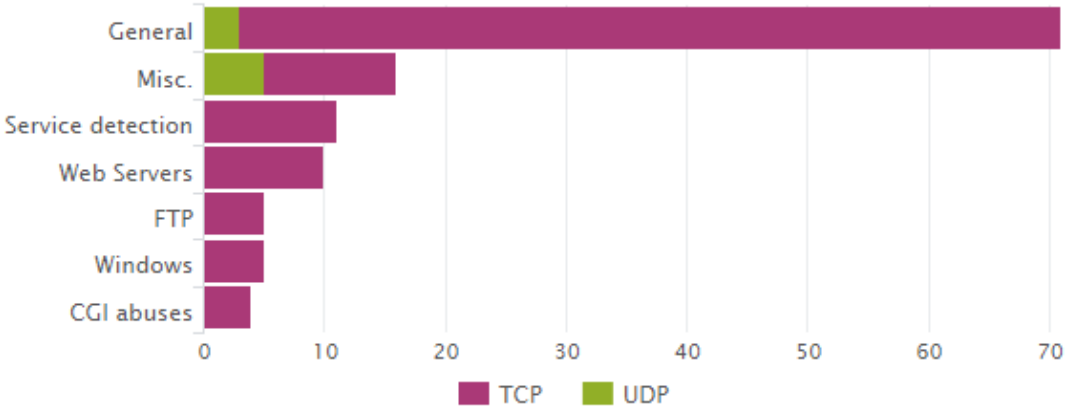
Graph: Vulnerability Category by Risk
Este gráfico ilustra las categorías de vulnerabilidades descubiertas y el conteo por riesgo durante este periodo de reporte.



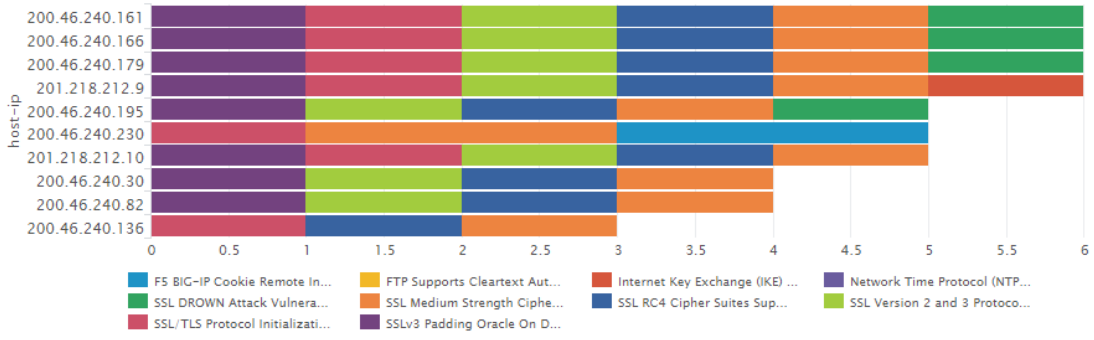
Graph: Vulnerability Category by Port
Este gráfico ilustra las categorías de vulnerabilidades descubiertas y el conteo por puerto durante este periodo de reporte.



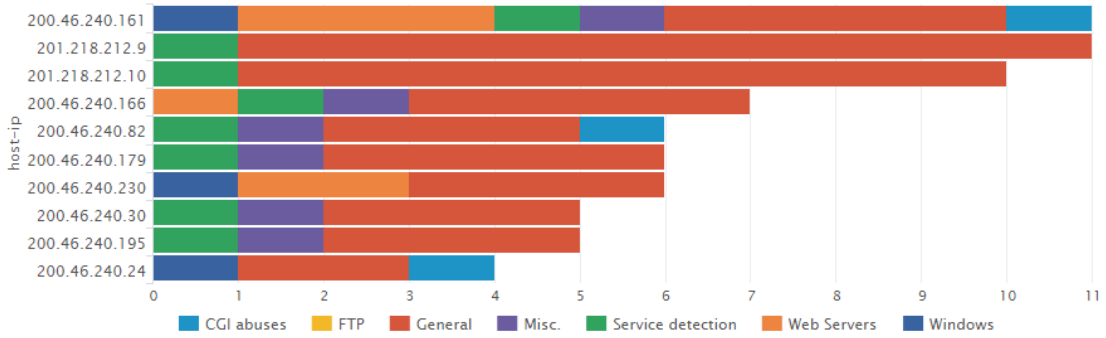
Graph: Vulnerability Category by Protocol
Este gráfico ilustra las categorías de vulnerabilidades descubiertas y el conteo por protocolo durante el periodo de este reporte.



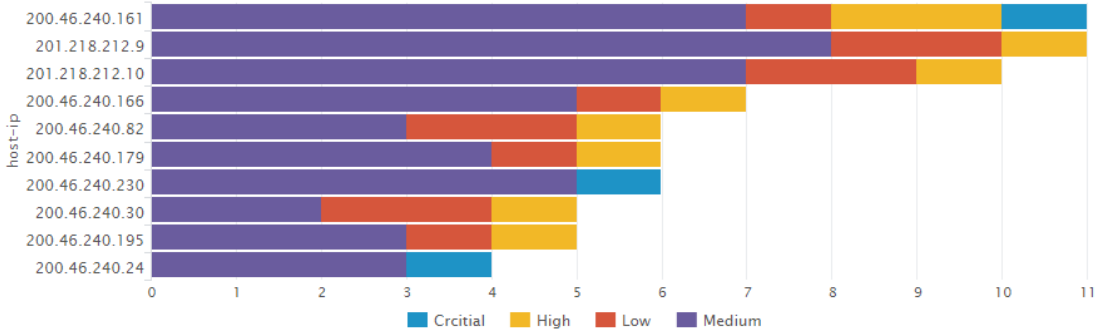
Graph: Host by Vulnerability Name.
Este gráfico ilustra las vulnerabilidades descubiertas y el conteo por equipo durante el periodo de este reporte.



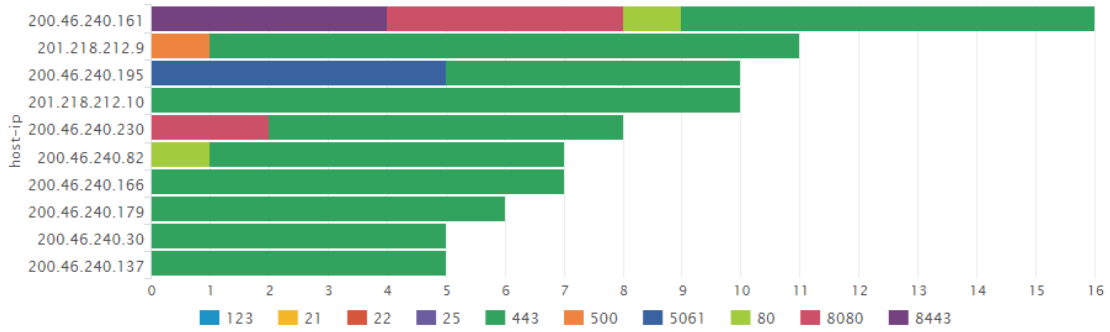
Graph: Host by Vulnerability Category.
Este gráfico ilustra las categorías de las vulnerabilidades descubiertas y el conteo por host durante el periodo de este reporte.



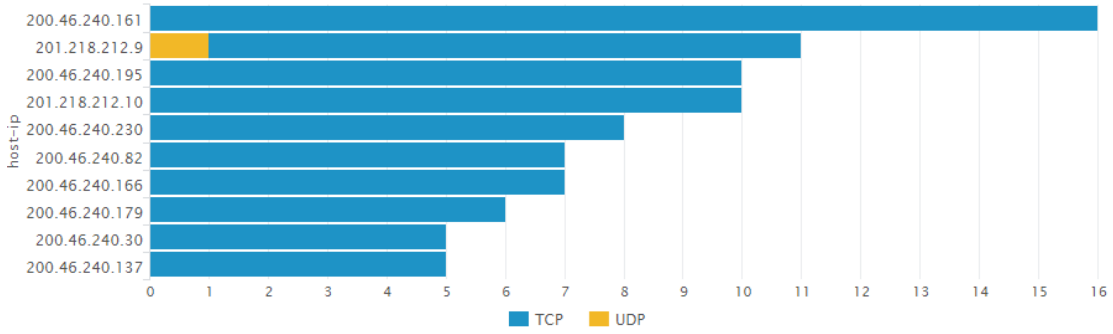
Graph: Host by Vulnerability Risk.
Esta gráfica ilustra el riesgo de las vulnerabilidades descubiertas y el conteo por equipo durante el periodo de este reporte.



Graph: Host by Port
Este gráfico ilustra el puerto de vulnerabilidad y el conteo por host durante el periodo de este reporte.



Graph: Host by Protocol
Este gráfico ilustra el protocolo de las vulnerabilidades descubiertas y el conteo por equipo durante el periodo de este reporte.



Managed Trusted Access Service (MSS-TAS)

El Managed Trusted Access Service (MSS-TAS) es un servicio holístico de seguridad que a) asegura que el acceso de los usuarios es confiable (usuario válido) y b) el dispositivo usado para autenticarse cumple con los estándares de seguridad de la organización. Esto se logra a través del servicio basado en la nube de GLESEC, que es parte de la plataforma TIP™.

El propósito de esta sección es resaltar la Inteligencia recopilada de esta y otros servicios bajo contrato, así como también de fuentes externas como honeypots, fuentes maliciosas conocidas, base de datos de vulnerabilidades, relaciones con los equipos del CERT y CSIRT que GLESEC posee, junto con otras fuentes.

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

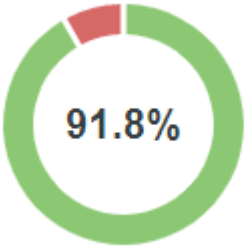
Graph: Autenticación de doble factor de los usuarios.
Este gráfico muestra el total de usuarios (activos e inactivos) para el método de doble factor de autenticación en su red.

486

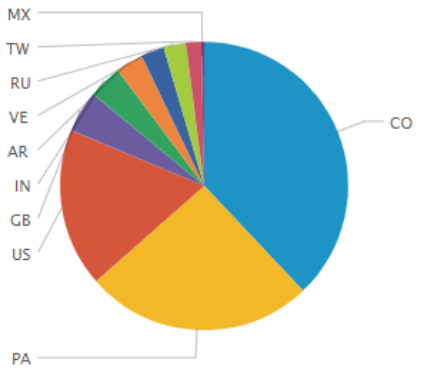
Graph: Total Endpoints.
Este gráfico muestra el número de puntos finales diferentes usado para acceder al sistema de su organización durante este periodo.

335

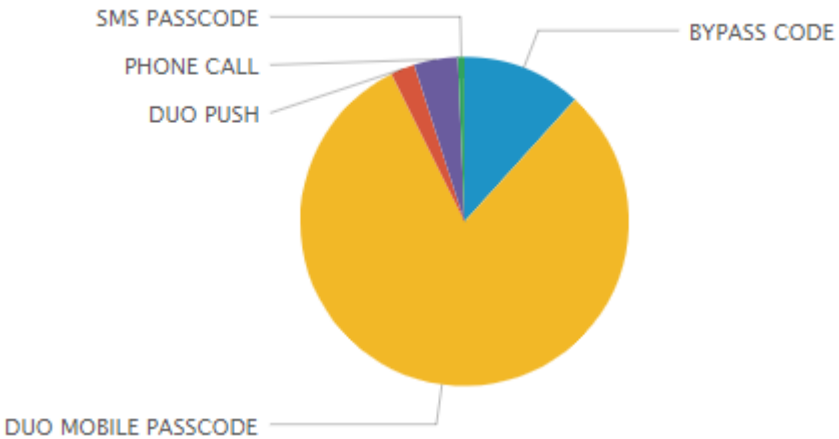
Graph: Overview
Este gráfico muestra la tasa de todas las autenticaciones exitosas.



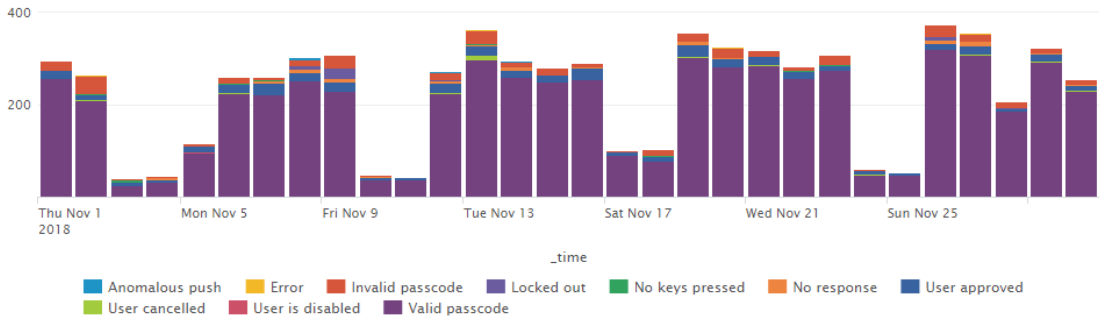
Graph: Authentication Per Country
Este gráfico muestra la proporción de autenticaciones de los diferentes países de origen.



Graph: Successful Authentications by Factor
Este gráfico muestra los diferentes métodos de autenticación utilizados cuando se otorgó el acceso.



Graph: Successful and failed authentication



Graph: Users with failed authentications

Username	Date	IP Address	Reason	Application
sliu	Fri Nov 30 19:29:13 2018	0.0.0.0	Invalid passcode	COPA Airlines
lbenavides	Fri Nov 30 14:20:15 2018	177.39.97.180	Invalid passcode	COPA Airlines
jhernandezp	Fri Nov 30 14:02:20 2018	0.0.0.0	Invalid passcode	COPA Airlines
josrodriguez	Fri Nov 30 13:38:32 2018	0.0.0.0	Invalid passcode	COPA Airlines
tlaverde	Fri Nov 30 13:36:07 2018	0.0.0.0	Invalid passcode	COPA Airlines
ggomez	Fri Nov 30 09:24:05 2018	0.0.0.0	Invalid passcode	COPA Airlines
vmakkena	Fri Nov 30 07:10:25 2018	0.0.0.0	Invalid passcode	COPA Airlines
adey	Fri Nov 30 02:43:39 2018	0.0.0.0	Invalid passcode	COPA Airlines
adey	Fri Nov 30 02:42:46 2018	0.0.0.0	Invalid passcode	COPA Airlines
sliu	Fri Nov 30 01:03:51 2018	0.0.0.0	Invalid passcode	COPA Airlines
jhernandezp	Thu Nov 29 22:08:59 2018	0.0.0.0	Invalid passcode	COPA Airlines
iestribi	Thu Nov 29 18:45:13 2018	0.0.0.0	Invalid passcode	COPA Airlines
livelasquez	Thu Nov 29 11:08:14 2018	0.0.0.0	Invalid passcode	COPA Airlines
livelasquez	Thu Nov 29 11:07:13 2018	0.0.0.0	Invalid passcode	COPA Airlines
livelasquez	Thu Nov 29 11:04:48 2018	0.0.0.0	Invalid passcode	COPA Airlines
mmontes	Thu Nov 29 09:41:09 2018	190.217.26.80	Invalid passcode	COPA Airlines
mahurtado	Thu Nov 29 08:23:43 2018	0.0.0.0	Invalid passcode	COPA Airlines
mahurtado	Thu Nov 29 07:36:09 2018	0.0.0.0	Invalid passcode	COPA Airlines
vsarode	Thu Nov 29 06:33:09 2018	0.0.0.0	Invalid passcode	COPA Airlines
edsantamaria	Wed Nov 28 11:37:03 2018	0.0.0.0	Invalid passcode	COPA Airlines
mmontes	Wed Nov 28 10:56:10 2018	0.0.0.0	Invalid passcode	COPA Airlines
mmontes	Wed Nov 28 10:53:04 2018	0.0.0.0	Invalid passcode	COPA Airlines
mmontes	Wed Nov 28 10:51:26 2018	0.0.0.0	Invalid passcode	COPA Airlines
mmontes	Wed Nov 28 10:51:08 2018	0.0.0.0	Invalid passcode	COPA Airlines
mmontes	Wed Nov 28 10:46:56 2018	190.217.26.80	Invalid passcode	COPA Airlines
lsutar	Wed Nov 28 06:41:13 2018	0.0.0.0	Invalid passcode	COPA Airlines
lsutar	Wed Nov 28 06:39:54 2018	0.0.0.0	Invalid passcode	COPA Airlines
mnieva	Wed Nov 28 06:35:50 2018	0.0.0.0	Invalid passcode	COPA Airlines
lsutar	Wed Nov 28 02:47:26 2018	0.0.0.0	Invalid passcode	COPA Airlines
swomack	Tue Nov 27 23:46:57 2018	0.0.0.0	Invalid passcode	COPA Airlines
swomack	Tue Nov 27 23:46:42 2018	0.0.0.0	Invalid passcode	COPA Airlines
nlotake	Tue Nov 27 21:21:35 2018	0.0.0.0	Invalid passcode	COPA Airlines
ddelrio	Tue Nov 27 15:20:12 2018	0.0.0.0	Invalid passcode	COPA Airlines
swomack	Tue Nov 27 15:10:03 2018	0.0.0.0	Invalid passcode	COPA Airlines
aurgonzalez	Tue Nov 27 13:44:43 2018	0.0.0.0	Invalid passcode	COPA Airlines
myrigay	Tue Nov 27 13:31:51 2018	0.0.0.0	Invalid passcode	COPA Airlines
acruzado	Tue Nov 27 13:24:19 2018	0.0.0.0	Invalid passcode	COPA Airlines
kpena	Tue Nov 27 11:45:33 2018	0.0.0.0	Invalid passcode	COPA Airlines
lsutar	Tue Nov 27 11:20:04 2018	0.0.0.0	Invalid passcode	COPA Airlines
macosta	Tue Nov 27 11:04:53 2018	0.0.0.0	Invalid passcode	COPA Airlines

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.

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 se muestran todos los tickets de administración de cambios e incidentes para este mes.

Monthly Reports Copa 2018-11-01 00:00:00-2018-11-[..]

Number	Ticket#	Title	Created
1	2018110710000012	Reporte de Operaciones e Inteligencia, Octubre 2018	2018-11-07 11:05:28

Durante el mes de noviembre se envió el comunicado SSL-TLS, donde se hace referencia a las vulnerabilidades presentes en los sistemas respecto a al protocolo SSL-TLS.

Definiciones

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

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

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

Info@glesec.com
www.glesec.com