PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

INFORME FINAL CASO DE ESTUDIO PARA UNIDAD DE TITUALCIÓN ESPECIAL

TEMA:

"Análisis y Selección de una herramienta para administración y obtención de información de eventos críticos de seguridad informática para la infraestructura del Ministerio de Telecomunicaciones y de la Sociedad de la información – MINTEL"

Pablo Williams Molina Boada

Quito – 2016

Autoría

Yo, ***Pablo Williams Molina Boada***, portador de la cédula de ciudadanía No.***1709291529***, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

_____

Pablo Williams Molina Boada

Agradecimientos

Agradezco a toda mi familia, en especial a mi esposa Lucía e hijos Isabella y Esteban por toda la comprensión, sacrificio y paciencia que tuvieron que tener para poder culminar con esta maestría.

Tabla de Contenidos

Índice de Figuras

Índice de Tablas

1. Introducción

El presente caso de estudio tiene como finalidad el seleccionar una herramienta de software para la implementación de un sistema de seguridad de la información y gestión de eventos - SIEM, por sus siglas en inglés, para esto se implementarán y configurar dos herramientas de software licenciado (con versiones demo) y una herramienta de software libre con el fin de analizar los datos de fuentes críticas en seguridad de la información y con esto determinar cuál es la herramienta que tiene el mejor desempeño, bondades y que se acople de la mejor manera a la infraestructura del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

El presente caso de estudio está dividido principalmente en dos partes, la primera parte donde se presentará la introducción, la justificación, los antecedentes y los objetivos respectivos y la segunda parte considerada la más importante la cual se dividirá en varios subtemas como son: implementación y configuración de las herramientas de análisis, correlacionador de eventos, entrega de tableros de control (dashboards), evaluación en tiempo real de datos de fuentes críticas en seguridad de la información y por último la comparación de herramientas para seleccionar la que mejor ayude en la red de la institución.

2. Justificación

Hoy en día con la penetración que tiene el internet en nuestro país y en el mundo estamos más expuestos a ser atacados por hackers principalmente de otros países como son China, India y Estados Unidos entre los más importantes, por lo que es necesario estar protegidos contra estas amenazas externas que hacen que los sistemas y aplicaciones se vuelvan inestables y en algunos casos se vuelvan críticos al dejar de tener sus servicios, lo cual ocasionaría que las personas usuarias de los mismos se queden en muchos casos sin nada que hacer.

Por lo expuesto se ha vuelto indispensable tener nuevas estrategias en seguridad de la información para las redes de información ya que los ataques actualmente se han vuelto más sofisticados e inmunes a la detección por parte de dispositivos convencionales como son los Firewalls, IDS o IPS y en muchos de los casos se ha visto la obligación de no solo tener instalado nuevos equipos y/o software sofisticados sino también concientizar a la gente de cuál es el riesgo que se tiene al no tener procesos y sistemas seguros.

Una de las herramientas que en los últimos años ha tomado gran importancia para entender de mejor manera los ataques que se pueden dar a una red de datos es el Sistema de Seguridad de la Información y Gestión de eventos – SIEM por sus siglas en inglés, el cual se lo puede encontrar como una herramienta en software, como un appliance (hardware) o en algunos casos como una administración de servicios dados por terceros. Un SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por el hardware y software de una red y ayuda a entender de mejor manera lo que está

sucediendo en la misma al realizar una correlación de los eventos de los múltiples dispositivos que conforman una red, con lo cual se tiende a detectar una posible intrusión en los sistemas y aplicativos de manera temprana y oportuna. Además en una sola plataforma se tiene la administración del monitoreo, lo que actualmente existen herramientas que permiten el monitoreo de la red en forma independiente, lo cual genera dificultad al administrador al no contar con un sistema de detección centralizado.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información al ser la institución rectora en determinar y proponer nuevas tecnologías de la información, ve la necesidad de mantener su red de datos libre de amenazas externas y posibles intrusiones para lo cual a través de la Dirección de Gestión Tecnológica se realizará la implementación de una herramienta tipo SIEM para su infraestructura tecnológica, no sin antes realizar un análisis previo de algunas alternativas que se tienen disponibles en el mercado ecuatoriano y seleccionar la que mejor se adapte a sus necesidades técnicas y a los costos que se tendrán en el año debido principalmente a la baja del presupuesto que se tiene en el estado ecuatoriano.

3. Antecedentes

En la actualidad la infraestructura informática se encuentra inmersa en varios problemas de seguridad de la información debido al incremento de amenazas de seguridad, principalmente debido a nuevas tecnologías que han aparecido para vulnerar sistemas y también por el inmenso auge que la red mundial llamada internet ha tenido, lo cual deteriora el adecuado funcionamiento de los sistemas de información. Se tiene el conocimiento que no se puede tener seguridad al 100% en una red, pero aplicando algunas de las estrategias de protección actuales se podrá obtener una seguridad aceptable con la cual se podría trabajar en un ambiente de confianza informática.

Es así que al momento en una red de datos se manejan principalmente los siguientes dispositivos y servicios: endpoints (equipos terminales), dispositivos móviles (celulares y tabletas), proveedores de internet, proveedores de celulares, etc.., por lo que es necesario controlar la red tanto la LAN como la WAN y todas las aplicaciones que se tengan en ellas, por lo que se considera necesario tener un controlador de aplicaciones, controlador de ancho de banda, dar calidad de servicio a las aplicaciones, un firewall para estas aplicaciones, entre otros. Ya hablando de los servidores que se tienen en una red la principal amenaza actual que se tiene son los malwares y los hackers, algunos de ellos los más sofisticados y tecnológicos están atacando directamente al CPU del servidor lo que ocasiona que en muchos de los casos el servicio se pierda.

Para combatir estas amenazas y tener segura la red de datos, las empresas actuales se están enfocando hoy en día en tener como mínimo un antivirus, un firewall, un IPS y un IDS, pero debido a que los métodos modernos que se utilizan actualmente para

vulnerar una red también es necesario ya tener un correlacionador de eventos y aún ir un poco más allá con un Centro de Respuestas de Incidentes Computarizado (CIRT en inglés) donde ya se tiene una mitigación de amenazas persistentes avanzadas es decir ataques ya dirigidos a la institución.

Para determinar la realidad actual en temas de seguridad de la red del Ministerio de Telecomunicaciones y de la Sociedad de la Información, previo a la instalación de las herramientas SIEM, primero se decidió analizar la situación en lo referente a verificar que amenazas se tiene, que aplicaciones están usando los usuarios, consumo de ancho de banda y vulnerabilidades entre las principales; para esto se decidió instalar por 15 días (esto se realizó en el mes de Diciembre 2015) un Applaince de la marca Checkpoint, que es una de las marcas en seguridad más reconocidas a nivel mundial, así lo dice Gartner en sus cuadrantes para los años 2014 y 2015. Para realizar el análisis se colocó el equipo de checkpoint en la red de datos a través de un puerto espejo (mirror) en el switch de core y se activó todas las funcionalidades que tiene como son: IPS, Antibot, Antivirus, Control de aplicaciones (Application Control) y filtrado Web (Web Filtering). Además cabe señalar que no se utilizó el equipo UTM que se tiene ya que es una versión antigua y no cuenta con todas las funcionalidades descritas anteriormente.

Los resultados obtenidos de este previo análisis se presentan a continuación en la Figura 1, dividido por categorías:

Aplicaciones y sitios de alto riesgo:

Application / Site	Matched Category	App Risk	Sources	Traffic	Number of Events
OpenVPN	Anonymizer	5 Critical	2	43 MB	11
Ultrasurf	Anonymizer	5 Critical	2	41 KB	2
Tor	Anonymizer	5 Critical	2	4 MB	2
Hola	Anonymizer	5 Critical	2	352 KB	2
iodine	Anonymizer	5 Critical	1	5 KB	1
Kugou	P2P File Sharing	5 Critical	1	847 KB	1
Hide.me	Anonymizer	5 Critical	1	693 KB	1
BitTorrent Protocol	P2P File Sharing	4 High	1160	16 GB	1510
Dropbox	File Storage and Sharing	4 High	174	3 GB	1436
TeamViewer	Remote Administration	4 High	27	450 MB	731
BitTorrent Sync	P2P File Sharing	4 High	7	2 MB	82
sogou.com	Suspicious Content	4 High	1	159 KB	82
Remote Desktop Protocol	Remote Administration	4 High	13	8 MB	70
uTorrent	P2P File Sharing	4 High	7	9 MB	70
silkenthreadiness.info	Spam	4 High	27	387 KB	60
pixel.adsafeprotected.com	Suspicious Content	4 High	29	5 MB	39
differentia.ru	Botnets	4 High	5	2 MB	39

Source	Application / Site	Matched Category	App Risk	Sessions
10.2.4.28	OpenVPN	Anonymizer	5 Critical	10
10.2.4.66	OpenVPN	Anonymizer	5 Critical	1
10.2.0.57	Tor	Anonymizer	5 Critical	1
10.2.0.94	Hola	Anonymizer	5 Critical	1
10.0.102.31	Hide.me	Anonymizer	5 Critical	1
10.2.4.56	Tor	Anonymizer	5 Critical	1
10.0.30.57	Ultrasurf	Anonymizer	5 Critical	1
10.2.4.47	Kugou	P2P File Sharing	5 Critical	1
10.2.0.100	Hola	Anonymizer	5 Critical	1
10.0.104.236	Ultrasurf	Anonymizer	5 Critical	1
10.0.104.91	iodine	Anonymizer	5 Critical	1
10.0.105.40	TeamViewer	Remote Administration	4 High	161
10.2.0.20	TeamViewer	Remote Administration	4 High	143
10.0.104.123	TeamViewer	Remote Administration	4 High	133
10.0.105.40	Dropbox	File Storage and Sharing	4 High	110
10.0.70.82	Dropbox	File Storage and Sharing	4 High	86
10.0.106.2	sogou.com	Suspicious Content	4 High	82
10.0.30.88	TeamViewer	Remote Administration	4 High	76
10.2.0.86	TeamViewer	Remote Administration	4 High	71
10.0.70.50	Dropbox	File Storage and Sharing	4 High	70

Figura 1. Top de aplicaciones y sitios de alto riesgo detectados por Checkpoint en la red del MINTEL

En la Figura 1 se observa que Open VPN, Ultrasurf, Tor y Hola son aplicaciones que podrían crear huecos de seguridad ya que son herramientas que permiten ingreso a

los servicios del Ministerio pero de forma no confiable o autorizada por la institución. Además se observa que no son muchos los eventos (ya que con el equipo UTM que se tiene se ha bloqueado la mayoría de aplicaciones no permitidas) pero que a la larga si pueden representar una vulnerabilidad para la red.

Eventos de intrusión y ataque (IPS):

Severity	Event Name	CVE List*	Events
Critical	WordPress Slider Revolution Plugin Local File Inclusion	None	110
	Web Servers Suspicious File Upload	None	41
	China Chopper Web Shell Remote Code Execution	None	13
	Nmap Scripting Engine Scanner Over HTTP Request	None	11
	PHP Web Shell Generic Backdoor	None	9
	Web Servers Malicious URL Directory Traversal	CVE-2011-2474, CVE-2014-0130, CVE-2010-4598, CVE-2014-0780, CVE-2015-0666, CVE-2015-4068	8
	Joomla Unauthorized File Upload Remote Code Execution	None	7
	Wordpress Ajax Store Locator Arbitrary File Download	None	5
	OpenSSL TLS DTLS Heartbeat Information Disclosure	CVE-2014-0160, CVE-2014-0346	4
	ZmEu Security Scanner	None	4

Figura 2. Eventos detectados por el IPS de la herramienta

Los eventos descritos en la Figura 2 son catalogados como verdaderamente críticos para la seguridad de la red considerando que entre los dos primeros se tienen 151 eventos lo cual en 15 días de análisis significa que alguien quiere ingresar sin permiso a

los servidores de la institución. En el caso de WordPress Slider Revolution Plugin significa que algún servidor que tiene instalado este plugin está siendo atacado y en el caso del Web Server Suspicious significa que un atacante remoto está tratando de subir un archivo malicioso a un servidor web con Sistema Operativo Linux y si se logra ejecutar este archivo malicioso podría tener acceso a ejecutar código en el servidor.

Source	Destination	Severity	Event Name	CVE List
87.106.34.221	10.0.104.131	Critical	WordPress Slider Revolution Plugin Local File Inclusion	None
46.118.155.216	10.0.104.131	Critical	Web Servers Suspicious File Upload	None
84.246.210.169	10.0.104.131	Critical	WordPress Slider Revolution Plugin Local File Inclusion	None
46.105.114.103	10.0.104.131	Critical	WordPress Slider Revolution Plugin Local File Inclusion	None
37.187.24.158	10.0.104.131	Critical	WordPress Slider Revolution Plugin Local File Inclusion	None
46.118.155.216	10.0.104.238	Critical	Web Servers Suspicious File Upload	None
118.98.72.15	10.0.104.131	Critical	WordPress Slider Revolution Plugin Local File Inclusion	None
64.34.159.20	10.0.104.131	Critical	WordPress Slider Revolution Plugin Local File Inclusion	None
212.40.14.13	10.0.104.131	Critical	WordPress Slider Revolution Plugin Local File Inclusion	None
172.245.128.159	10.0.104.131	Critical	WordPress Slider Revolution Plugin Local File Inclusion	None

Figura 3. Listado de equipos que tienen eventos críticos

En la Figura 3 se puede observar que servidores son los atacados y desde que fuente con su IP, por lo que se puede buscar con algún programa buscador de IPS el país desde donde se produce el ataque y se observó que los principales ataques provienen de China y de Ucrania.

Hallazgos de seguridad de endpoints:

Total endpoints running high risk applications	1.472
Total endpoints involved in data loss incidents	0
Total endpoints involved in intrusion & attack events	270
Total endpoints involved in a malware incidents	0

Figura 4. Detalle de eventos de seguridad de los equipos terminales del MINTEL

Lo más importante de la Figura 4 es que se observa que existen 1472 hits de puntos finales (endpoints) que tienen aplicaciones de alto riesgo que están corriendo y 270 puntos finales que estaban involucrados de alguna forma en eventos de seguridad (ataques e intrusiones), además que se observa que no se tienen incidentes de malware en los puntos finales, que se considera importante para una red.

Análisis de ancho de banda:

En la Figura 5 se observa que en 15 días de análisis se determina que la aplicación que más consume el ancho de banda de la institución es el youtube con 426 Gigas y 4771 eventos y después Facebook con 74 Gigas 7769 eventos, lo cual indica que muchos de los usuarios no dedican todo su tiempo al trabajo asignado.

Application / Site	Matched Category	App Risk	Sources	Traffic	Number of Eve...
YouTube	Media Sharing	Low	461	426 GB	4771
Facebook	Social Networking	Low	485	74 GB	7769
Web Browsing	Web Browsing	Unknown	6131	36 GB	19460
Google Services	Computers / Internet	Low	565	28 GB	13547
telecomunicaciones.gob.ec	Government / Military	Unknown	14402	24 GB	28195
SSL Protocol	Network Protocols	Very Low	3172	21 GB	19209
facebook.com	Social Networking	Unknown	308	18 GB	4064
BitTorrent Protocol	P2P File Sharing	High	1160	16 GB	1510
App Store	Search Engines / Portals	Very Low	54	15 GB	133
SMTP Protocol	Network Protocols	Medium	3071	14 GB	15740
mintel.gob.ec	Government / Military	Unknown	3604	14 GB	13844
RTMP Protocol	Network Protocols	Low	31	14 GB	149
Mega	File Storage and Sharing	Medium	22	14 GB	329
nyc001.ix.nflxvideo.net	Computers / Internet	Unknown	7	13 GB	20
Google Play	Search Engines / Portals	Low	276	12 GB	2679
iTunes	Media Sharing	Low	24	11 GB	58
10.0.104.92	Uncategorized	Unknown	2574	6 GB	10479
Firefox-update	Software Update	Low	218	6 GB	538
Twitter	Social Networking	Low	379	6 GB	3418
Windows Update	Software Update	Very Low	107	5 GB	1025
nawest2.synaptic.att.com	Computers / Internet	Unknown	2	5 GB	5
mia003.ix.nflxvideo.net	Computers / Internet	Unknown	3	5 GB	11
Skype	VoIP	Medium	300	5 GB	3590
Google Cloud Storage	File Storage and Sharing	Medium	85	5 GB	327
a248.e.akamai.net	Computers / Internet	Unknown	356	5 GB	3220
WhatsApp Messenger-file transfer	Media Sharing	Medium	217	5 GB	2570
IAX2 Protocol	Network Protocols	Low	6	4 GB	9

Figura 5. Top del detalle de consumo de ancho de banda por aplicación

La herramienta instalada Check Point también permite obtener el nivel de cumplimiento normativo de los organismos internacionales y estándares de seguridad más conocidos, es así que en la Figura 6 se expone los resultados que arroja el aplicativo.

Regulation	Number of Requirements	Number of Security Best Practices	Compliance Status
CIPA	9	2	0%
NCIPA	4	2	0%
NIST 800-41	22	20	24%
PCI DSS 2.0	53	75	45%
DSD	14	48	46%
ISO 27001	27	75	48%
HIPAA Security	14	75	49%
MAS TRM	21	75	51%
GLBA	5	75	55%
GPG13	8	18	57%
ISO 27002	192	75	59%
NIST 800-53	23	48	61%
FIPS 200	23	48	61%
Firewall STIG	27	26	66%
NERC CIP	7	38	67%
CobiT 4.1	15	75	71%
SOX	15	75	71%

Figura 6. Nivel de cumplimiento de estándares de la red del MINTEL

Se puede observar que en las normas ISO 27001 y 27002 se tiene un estado de cumplimiento del 48 y 59 por ciento respectivamente y para COBIT 4.1 se tiene un 71 por ciento de cumplimiento.

Con estos resultados obtenidos se justifica y se ve la necesidad de instalar una herramienta que permita detectar tempranamente y correlacionar todos estos eventos de seguridad en una sola plataforma de administración con el fin de enviar alertas para toma de decisiones inmediatas en tiempo real y esto lo hace una herramienta del tipo SIEM.

4. Objetivos

Objetivo general

Analizar herramientas de software licenciadas o libres para la implementación de un sistema de seguridad de la información y gestión de eventos - SIEM y seleccionar la de mejor desempeño para la infraestructura del Ministerio de Telecomunicaciones y de la Sociedad de la Información

Objetivos específicos

- Implementar y configurar en servidores herramientas de software para seguridad de la información y gestión de eventos.
- Examinar datos en tiempo real y correlacionar eventos de los logs de seguridad generadas por el hardware y software de la red del MINTEL.
- Evaluar los datos para analizar fuentes críticas en seguridad de la información como son: aplicativos institucionales, correo electrónico (antispam), firewall y la red de datos.
- Comparar y seleccionar la herramienta que se adapte mejor y obtenga los óptimos resultados para la infraestructura del MINTEL tomando en cuenta su facilidad de uso, costos y niveles de dificultad en la implementación y configuración.
- Entregar tableros de control (dashboards) para toma de decisiones al oficial de seguridad de la información de la institución.

5. Desarrollo Caso de Estudio

5.1 Productos SIEM

Según David Trejo (2013) afirma que: “Security Information and Event Management (SIEM) es una herramienta capaz de monitorizar el estado en cuanto a seguridad de una organización, debe estar perfectamente integrada con todos los sistemas ya que debe entender el comportamiento de toda la infraestructura TIC. Mediante la recopilación de eventos de login, acceso a BBDD, logs de firewall, proxy, IPS, logs de aplicaciones, etc; un SIEM es capaz de monitorizar y predecir el comportamiento futuro de la plataforma TIC de tal manera que ante una conducta inusual de la plataforma puede generar una alerta y/o realizar una acción determinada”. [1]

Para Jason Soto (2015) SIEM son:

> Plataformas que proveen análisis en tiempo real de los eventos de seguridad generados por los equipos de comunicación, servidores y todo lo que estemos monitoreando. Pero para entender un poco el término y las funcionalidades, debemos entender de donde proviene, que es la combinación de **SEM** y **SIM**.
>
> **SEM**, es el segmento de la administración de la seguridad que tiene que ver con Correlación de Eventos, Análisis en Tiempo real, Flujo de trabajo, además de que toma en consideración otras fuente como es el monitoreo del tráfico.
>
> **SIM**, Este tiene que ver con el almacenamiento a largo plazo de logs para su posterior análisis y reporte. [2]

Las herramientas tipo SIEM son necesarias actualmente ya que las organizaciones de hoy en día tienen muchas aplicaciones y servicios alojados en su red de datos lo cual generará muchos eventos (logs) diariamente de los servidores, equipos de defensa, equipos de comunicación, entre los principales, lo que hace difícil la tarea para los administradores de estos sistemas ir analizando estos eventos de cada equipo ya que involucra mucho tiempo y recursos humanos, y lo que es más se lo hace en plataformas de administración independientes por cada servidor o equipo. Es así que el SIEM ayuda mucho para que en una sola plataforma de administración se tengan concentrados la mayoría de eventos de los sistemas y definiendo parámetros conocidos se puedan correlacionar los mismos y obtener como resultado desde alertas tempranas de que el servicio está comprometido o siendo atacado hasta por ejemplo ver únicamente el consumo de ancho de banda por usuario de las empresas, con la opción de tener tableros gráficos de mando (dashboards) que puedan servir para toma de decisiones por los encargados de seguridad de una empresa.

Actualmente en el mercado de la seguridad existen diversas soluciones de tipo SIEM, algunos de estos productos caen más en una u otra área del SIM o el SEM, y otros son capaces de ofrecer ambas bondades por lo que es mejor analizar las necesidades de la institución y evaluar alguno de estos u otros productos antes de adquirirlos, que será el tema de análisis en este caso de estudio. Entre los principales se tienen los siguientes:

Nombre del fabricante	**Nombre de la herramienta**
AlienVault	USM, OSSIM
ArcSight	ArcSight Enterprise Security Manager HP
Cisco	Security MARS
IBM	Tivoli Security Information and Event Manager
McAfee SIEM	Intel Security ESM
Splunk	Splunk

La mayoría de estas herramientas son licenciadas a excepción de OSSIM que es de código abierto y solo se paga el mantenimiento por actualizaciones y soporte. Para escoger cuales de estas herramientas se utilizarán para este caso de estudio se realizó una consulta en el cuadrante mágico de Gartner en lo que se refiere a productos SIEM - Security Information and Event Management, del último reporte que se tiene el 20 de julio de 2015 (ver Figura 7) se observa que las empresas líderes son IBM Security, ArcSight-HP, Splunk e Intel Security de estas se va a seleccionar Splunk e Intel Security debido a que sus costos de licenciamiento son menores que las dos primeras y además se seleccionará AlienVault que es una de las empresas visionarias ya que al tener una de sus herramientas de código libre encaja en el perfil de software que las instituciones públicas pueden usar.

Figura 7. Cuadrante mágico de Gartner año 2015 para productos SIEM, Magic Quadrant for Security Information and Event Management Kelly M. Kavanagh, Oliver Rochford 2015

5.1.1 Breve descripción de las herramientas seleccionadas

USM (OSIMM) -AllenVault

Es un sistema fácil de implementar para instituciones que pretenden instalar un SIEM por primera vez debido a que la puesta en marcha del servidor y sus servicios se realiza de manera sencilla y al poseer herramientas de código libre, se puede configurar de acuerdo a las necesidades de la institución.

Según Jason Soto (2015) indica que: “OSSIM es un SIEM Open Source que integra una gran cantidad de herramientas para asistirnos en la detección de Intrusos,

Visibilidad en la red, Seguridad informática, entre otros. OSSIM ejecuta estas funciones usando componentes de seguridad muy conocidos integrados con Debian y con una interfaz gráfica web. Todos estos componentes pueden ser manejados desde la interfaz gráfica y además de permitirnos visualizar las informaciones recolectadas" [3]

Según Gartner (2015): "La plataforma AlienVault debe ser considerado por las organizaciones que necesitan un amplio conjunto de capacidades de seguridad integradas a un costo relativamente bajo, y por las organizaciones que aceptarán un producto con soporte comercial que se basa en código abierto." [4]

Fortalezas:

• AlienVault en su versión USM ofrece una variedad de capacidades de seguridad integradas, incluyendo SIEM, monitoreo archivo integridad, evaluación de la vulnerabilidad, de descubrimiento de activos, y ambos sistemas basados en host y detección de intrusiones basado en red.

• Referencias de clientes indican que las ofertas de software y aparatos son mucho menos caras que los conjuntos de productos correspondientes de la mayoría de los competidores en el espacio SIEM.

• AlienVault ofrece un modelo de licencias simplificado basado en los aparatos utilizados, más que en eventos por segundo (EPS).

Precauciones

• Identidad y acceso a la administración (IAM) de integración se limita a Active Directory y monitoreo LDAP, y la integración de aplicaciones es principalmente con aplicaciones de código abierto.

• Las capacidades de flujo de trabajo de AlienVault no incluyen la integración con directorios externos para las tareas de flujo de trabajo.

• El promedio de las puntuaciones de satisfacción del cliente AlienVault de referencia para facilitar la creación de informes y personalización, facilidad y eficacia de las consultas ad hoc, la calidad y la estabilidad del producto, y la experiencia de soporte es menor que las puntuaciones medias para todos los clientes de referencia en esas áreas.

McAfee Enterprise Security Manager – Intel Security

En la página web de McAfee (2015) se indica que: "la solución SIEM (información de seguridad y administración de eventos) es potente y de alto rendimiento, reúne los datos de los eventos, de las amenazas y los riesgos para proporcionar la información de seguridad más amplia, responder rápidamente a los incidentes, administrar los registros de forma sencilla y generar informes de cumplimiento, lo que proporciona el contexto necesario para la gestión adaptable de riesgos para la seguridad." [5]

Según Gartner (2015): “ McAfee ESM es una buena opción para las organizaciones que utilizan otras tecnologías Intel de seguridad, así como aquellos que buscan un marco de seguridad integrado que incluye la defensa avanzada de amenazas o la vigilancia de los sistemas de control industrial ”. [4]

Fortalezas

• Fuera del soporte del hardware (appliance) dado por otros fabricantes, se cita por los usuarios finales que el soporte es muy buena y es una fortaleza. El promedio de satisfacción por los clientes a la Seguridad de Intel misma que entregan calificaciones de escalabilidad, personalización de informes, consultas ad hoc y experiencia de soporte es más alta que las puntuaciones medias para todos los demás clientes de referencia en esas áreas.

• Integraciones profundas con Intel Security´s Enterprise Security Database Event Monitor y Application Data Monitor proporcionan un monitoreo de base de datos y de aplicaciones a fondo para las tecnologías seleccionadas.

• Los clientes informan que la integración de múltiples productos de seguridad de McAfee a menudo proveen buenas sinergias y ofrece las mejores soluciones que otras soluciones de este tipo disponibles.

Precauciones

•Muchas características SIEM avanzadas de Intel de seguridad y capacidades en áreas como la inteligencia de punto final y la respuesta automatizada requieren integraciones con otros productos de la cartera de INTEL.

• NetFlow se puede utilizar para generar eventos y alertas, pero no se utiliza automáticamente para enriquecer eventos basados en registros.

Splunk

Según Ramos L. (2013): "Splunk es el proveedor líder de software de inteligencia operativa, se utiliza para controlar, informar y analizar datos que generan sus sistemas de TI en tiempo real, así como terabytes de datos históricos, almacenados en sus instalaciones o en la nube." [6]

Según Splunk (2012):" Splunk es el motor para los datos de las maquinas. Colecta, indexa y aprovecha los datos de las maquinas generados pos sus sistemas e infraestructura de TI, puede ser física, virtual o en la nube." [7]

Según Gartner (2015): "Las organizaciones que requieren una plataforma SIEM que pueda ser personalizada para apoyar extensos análisis de funciones y una gran variedad de formatos de registro y aquellas con casos de uso que abarcan soporte de seguridad y operaciones de TI, deben considerar Splunk como una alternativa". [4]

Fortalezas

• Los clientes Splunk citan visualización y análisis de comportamiento, predictivos y estadísticos como elementos eficaces de los casos avanzados de uso de monitoreo, tales como la detección de acceso de los usuarios anómala a datos sensibles.

• Splunk ha mejorado su soporte integrando una gran cantidad de información sobre amenazas externas que se alimenta de fuentes comerciales y abiertas.

Precauciones

• El App Splunk para la seguridad de la empresa proporciona soporte básico para las correlaciones predefinidas para el monitoreo de usuario. Los compradores potenciales deben anticipar modificándolos y construyendo sus propios para implementar los casos de uso de monitoreo de usuario más avanzados.

• Las funciones de gestión de flujo de trabajo se quedan atrás de la de los competidores. Las organizaciones con procesos SOC maduros pueden requerir la personalización o integraciones con las tecnologías de terceros para estas funciones.

• El modelo de licencia de Splunk se basa en el volumen de datos indexados por día. Los clientes informan de que la solución es más costosa que otros productos SIEM donde existen volúmenes elevados de datos.

5.1.2 Instalación y configuración de las herramientas SIEM

Dentro del alcance del presente caso de estudio se tomarán cuatro fuentes (dispositivos o aplicaciones) para el envió de datos (eventos) a las herramientas seleccionadas, mismas que son consideradas dentro de las más importantes y críticas dentro de la red del MINTEL; estas fuentes son:

* Un Firewall Fortinet Fortigate 310B
* Un Switch Core Cisco 4507E
* Un Servidor de McAfee Antispam
* Un(os) Servidor(es) de Aplicación web en Linux CentOs 7 (Apache, MySql)
* Un servidor de antivirus (opcional)

5.1.2.1 Splunk

Según Splunk (2012):

> Splunk es el motor para los datos de las máquinas. Fue desarrollado para superar completamente los desafíos que comprenden los datos de las maquinas; colecta, indexa y aprovecha los datos no estructurados de las maquinas. Además, colecta, indexa y aprovecha sus series de datos temporales y no estructurados de las máquinas. Splunk puede leer los datos desde casi cualquier fuente imaginable, como por ejemplo el tráfico de red, servidores web, aplicaciones personalizadas, servidores de aplicaciones, hipervisores, sistemas GPS, comentarios del mercado de valores, medios sociales y bases de datos estructuradas preexistentes. Ofrece

una comprensión de lo que está sucediendo en tiempo real y un análisis profundo de lo que ha sucedido en sus sistemas e infraestructura de TI. Convierte los datos de las máquinas en el conocimiento que necesita para tomar decisiones informadas. [7]

En la Figura 8 se presenta un tablero típico de la herramienta

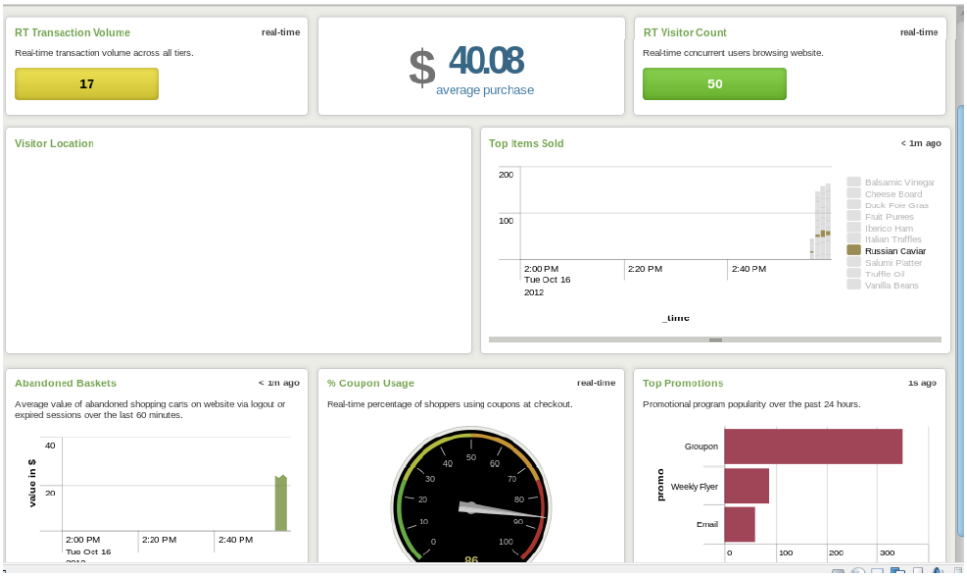


Figura 8. Dashboard ejecutivo de una tienda en línea. Guía de inteligencia de Splunk 2012

A continuación se detalla las características tanto en hardware como en software que necesita la herramienta para su instalación, recomendados para una versión demo:

Hardware:

Un Servidor con 8 cores en procesador

12 GB de memoria RAM

Disco duro de 10K o 15K RPM

300GB de espacio libre en disco.

Software:

Sistema Operativo: 64 bits (Windows server 2008 R2)

Versión de Splunk: 6.3

Dentro de la infraestructura HP de servidores que posee el MINTEL se creó una máquina virtual con las características de hardware y de software descritas arriba, la dirección del servidor virtual es: 10.0.104.164, máscara 24 y Gateway 10.0.104.1.

En la Figura 9 se presenta el tipo de licenciamiento que se instaló teniendo en cuenta que el volumen de datos que podrán ser adquiridos por la herramienta es de 500 Mbyte diarios, suficiente para tener información acerca de la red del MINTEL.

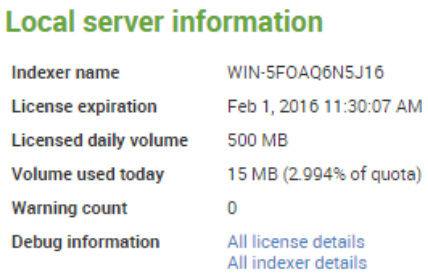
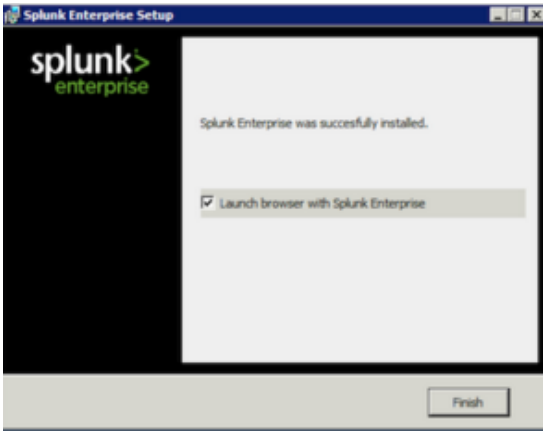


Figura 9. Nivel de licenciamiento por volumen diario para demo

Para la instalación de Splunk en Windows Server 2008, se realizan los siguientes pasos:

1. Dar doble clic en el archivo splunk.msi: el instalador corre y se despliega el panel del Splunk Enterprise Installer

2. Dar clic en “Check this box to accept the License Agreement”, esto activa las pestañas “Customize Installation” e “Install”
3. Se escogió el boton “Install”, que se instala con las configuraciones por defecto de la herramienta.
4. El instalador se ejecuta y despliega la ventana “Installation complete”

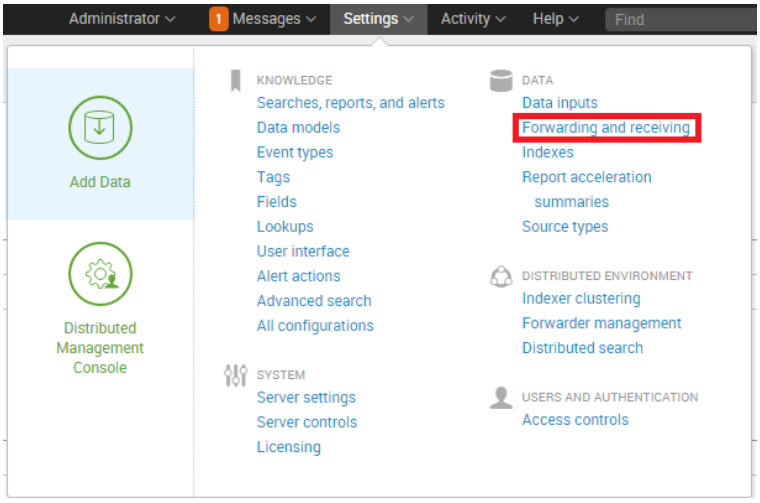


La primera vez que ya se tiene acceso al sitio web de Splunk, se debe ingresar como “username: admin” y “password: changeme”, posteriormente siempre se solicita que se cambie la contraseña y en este caso se colocó como nueva contraseña “Ecuador2015”. Para acceder al sitio web de splunk se coloca en el

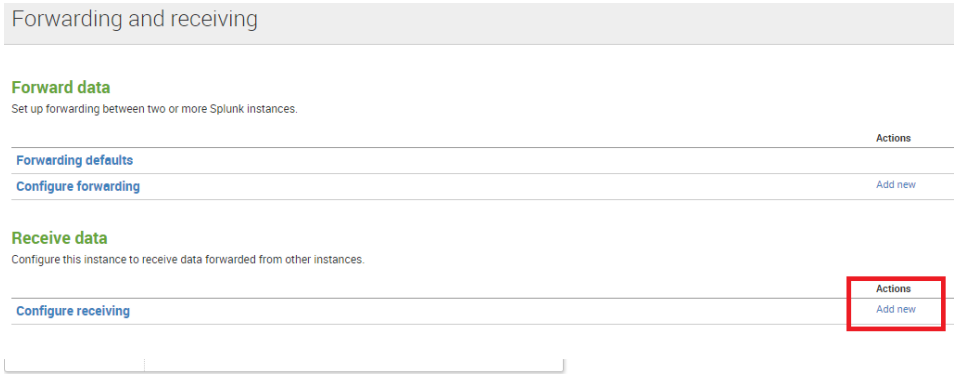
navegador: http://localhost:8000 siendo el localhost la dirección del servidor, en este caso 10.0.104.164 y el puerto por defecto es el 8000 ya que se instaló con los parámetros predefinidos de la herramienta.

Al ser Splunk una herramienta que recoge datos y los indexa, es necesario enviar los datos de los servidores que va a monitorear Splunk y si estos dispositivos no manejen algún estándar de envió de eventos (logs) o cuando al activar el protocolo syslog al servidor que enviará los datos pueda sobrecargar su procesamiento (lo que no sería deseado), es necesario buscar algún método alternativo que sea ligero y fácil de usar, por lo que para situaciones en las que los datos que se necesita no están disponibles en la red se pueden implementar los Splunk Forwarders que son ligeros y ofrecen una captura de datos universal segura, distribuida y en tiempo real. Para el caso de estudio en análisis se instaló en un servidor de aplicaciones del MINTEL (con sistema operativo Linux) y se siguió los siguientes pasos para la instalación tomados de Byteschef (2013) [8]:

1. En primer lugar hay que decirle a Splunk que esté listo para recibir los datos, para esto hay que ir a **Settings → Data** y seleccionar **Forwarding and receiving**

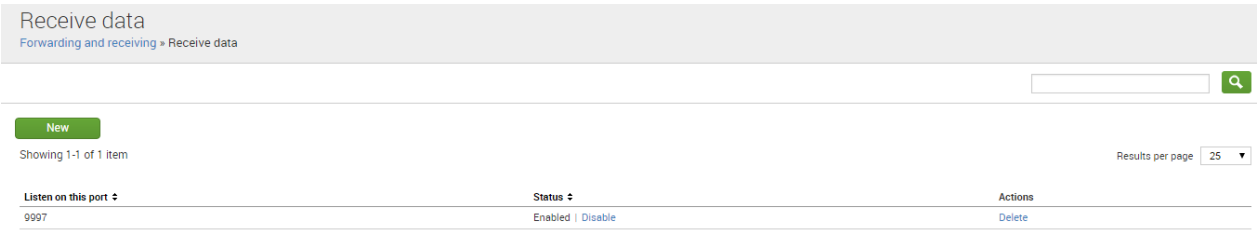


1.1 Añadir uno nuevo, en la pestaña **"Add New"**



1.2 Agregar el puerto que se desee usar para recibir los datos (se elige el por defecto)

1.3 Listo para recibir datos en el puerto especificado



2. En el servidor del que se enviara los datos se realiza la descarga del forwarder universal de Splunk (que se lo encuentra en la página web www.splunk.com), usando los siguientes comandos para Linux:

```
1 wget -O splunkforwarder-5.0.2-149561-linux-2.6-x86_64.rpm 'http://www.splunk.com/page/downl
```

Luego instalarlo usando el comando:

```
1 rpm -ivh splunkforwarder-5.0.2-149561-linux-2.6-x86_64.rpm
```

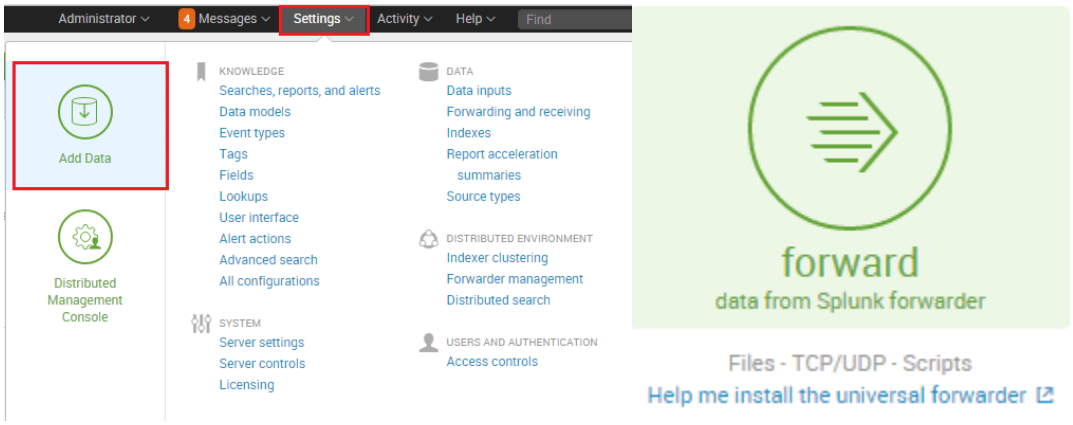
y por último se realiza la siguiente configuración para usarlo:

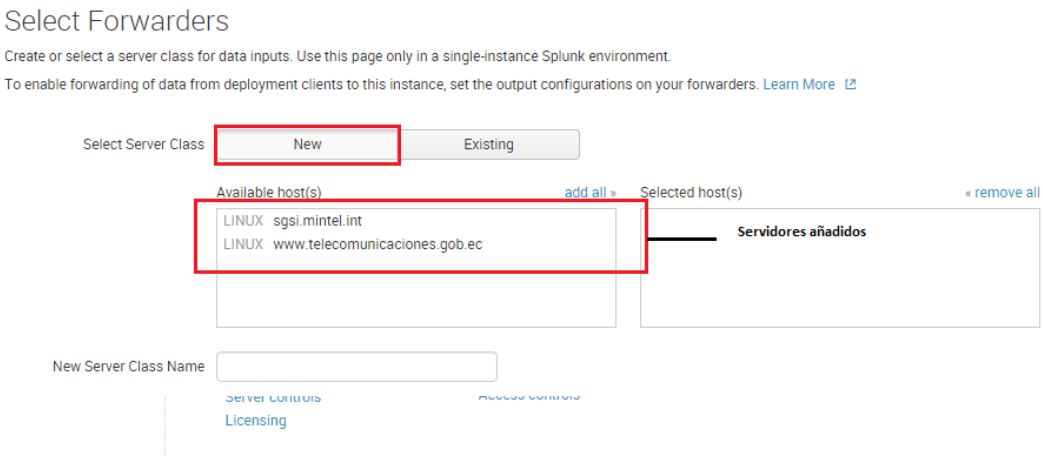
```
1 cd /opt/splunkforwarder/bin
2 ./splunk start --accept-license
3 ./splunk enable boot-start
4 ./splunk add forward-server 10.0.104.164:9997-auth admin:admin
```

3. A continuación se tiene que decir a Splunk que se va a monitorear, para esto se usará los “logs” de los servidores escogidos para lo cual se usará el siguiente comando:

```
1 ./splunk add monitor /var/log/
```

4. Por último se debe añadir los datos que se reciben a Splunk para esto hay que ingresar a la herramienta y en la pestaña **Settings → Add Data** y seleccionar la opción **Forward** y adicionar los servidores que usan Splunk Forwarder:





Si no comienza el envío y recepción de datos después de realizar estas configuraciones será necesario reiniciar el servicio para esto se usa el comanda restart y con esto splunk comenzará a recibir los datos de los servidores, como se aprecia en la Figura 10.

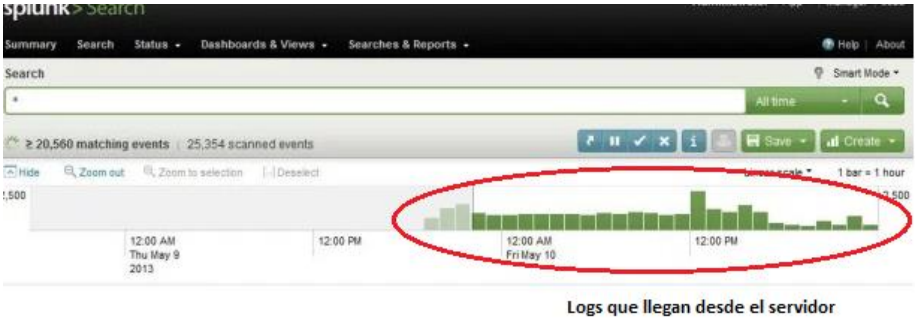


Figura 10. Pantalla que confirma que se están recibiendo logs desde un servidor

Para añadir las demás fuentes de datos, se tomó sus logs de alarmas en formato syslog y para recibirlos se configuró dentro de la herramienta en **Settings→data inputs** en la opción UDP y su recepción por el puerto 514, como se indica en la Figura 11.

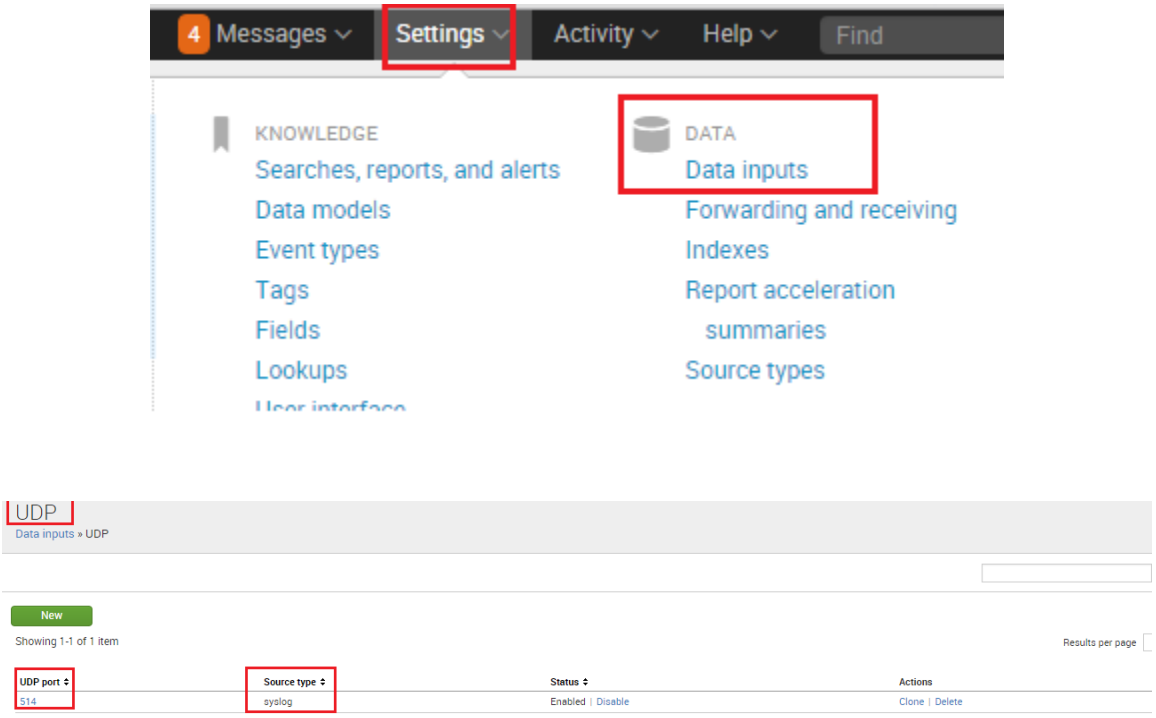


Figura 11. Configuración de equipos que envían syslog

La arquitectura de conexión de todas las fuentes de datos de análisis se presenta en la Figura 12. Cabe señalar que con esta herramienta no se pudieron utilizar los datos provenientes de antivirus y del equipo CISCO ya que en el primer caso no maneja protocolo syslog lo que hizo difícil realizar la configuración de los paneles de control ya que filtrar los datos obtenidos en crudo es una tarea muy complicada y en cuanto al switch CISCO los datos enviado por syslog son muy básicos (de administración del dispositivo) tales como: alertas, ingresos al equipo, grabaciones de memoria, etc., lo que no ayudaría en mucho al análisis que se pretende. Se intentó recibir eventos activando el protocolo NetFlow propio del equipo pero como en el primer caso se tuvo la dificultad de filtrar toda la información cruda que se recibía.

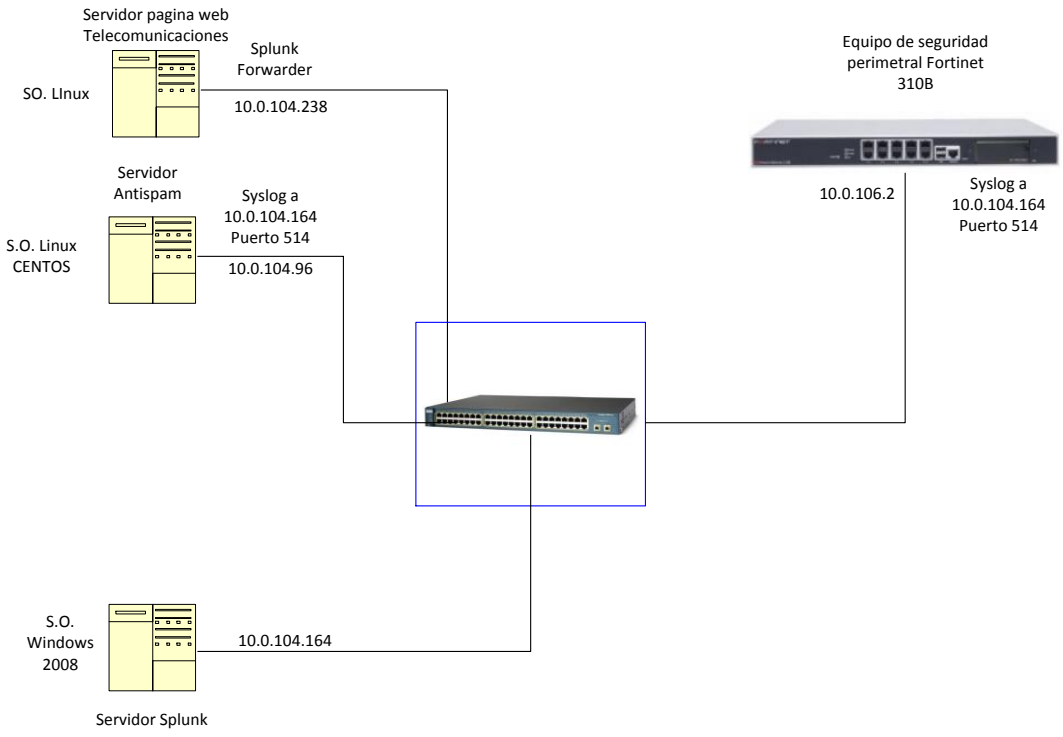


Figura 12. Esquema de conexión de red para la implementación de las herramientas

5.1.2.2 McAfee Enterprise Security Manager-ESM

Según la guía de producto de McAfee (2015):

> McAfee ESM recopila y agrega datos y eventos de dispositivos de seguridad, infraestructuras de red, sistemas y aplicaciones. A continuación, aplica inteligencia a esos datos mediante su combinación con información contextual acerca de usuarios, activos, vulnerabilidades y amenazas. Correlaciona esta información para localizar incidentes relevantes. Gracias a los paneles interactivos personalizables, es posible acceder a información detallada sobre eventos específicos a fin de investigar los incidentes. [9]

Por lo que ESM permite en general recopilar, almacenar y analizar los riesgos y amenazas a los cuales están expuestos la infraestructura y red de datos de una empresa y además permite actuar sobre estos bajo una sola plataforma de administración, para esto ESM consta de 3 etapas que se describen brevemente a continuación:

- Interfaz: es una consola de administración en forma gráfica de la herramienta
- Almacenamiento, administración y análisis de datos: esto sería el corazón de la herramienta y está conformado por dispositivos que proporcionan los servicios para la manipulación de datos para la configuración, búsqueda, visualización y presentación en informes ejecutivos. Los dispositivos que cumplen están funciones son: ESM, Advanced Correlation Engine-ACE, ESM distribuído-DESM y Enterprise Log Manager-ELM.

- Adquisición de datos: son los dispositivos para la adquisición de datos de la red de la empresa. Los dispositivos que cumplen están funciones son: Nitro Intrusion Prevention System-IPS, Event Receiver-ER, Application Data Monitor-ADM y Database Event Monitor-DEM.

En la Figura 13 se presenta un diagrama en el cual se observa como todos los dispositivos mencionados anteriormente se unen como parte de la solución para conformar el SIEM, así como también se indica la manera en que se conecta con la red del usuario.

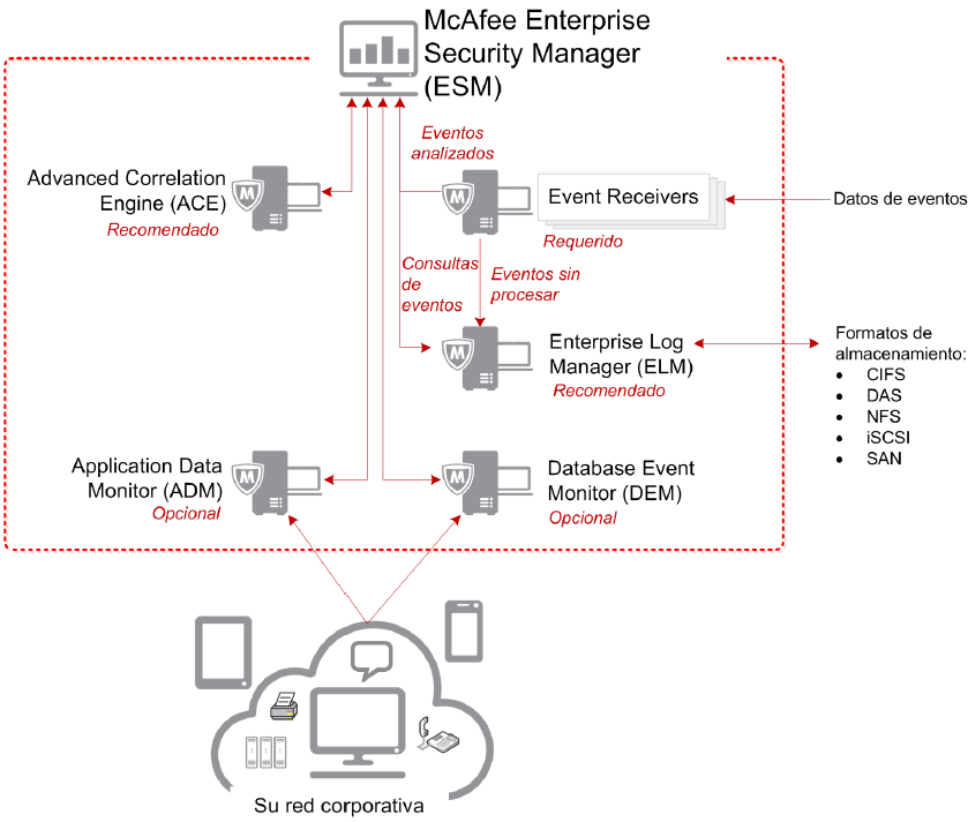


Figura 13. Diagrama de la solución completa para ESM. Intel, S. (2015). Guía de producto: McAfee Enterprise Security Manager 9.5.1. Santa Clara, California, USA.

Para el análisis del presente caso de estudio solo se usaron los elementos básicos de la solución los cuales son: Event Receivers-EM, Enterprise Log Manager-ELM y el ESM en sí, todos estos dispositivos vinieron preinstalados en una sola imagen para su instalación y posterior configuración. En el caso de necesitar el ACE, ADM o DEM se los debe instalar como appliances o como máquinas virtuales.

En la Figura 14 se presenta la consola centralizada de administración de la herramienta, la cual proporciona visibilidad en tiempo real de las actividades de los dispositivos, a continuación se describe brevemente cada parte de la misma [9]:

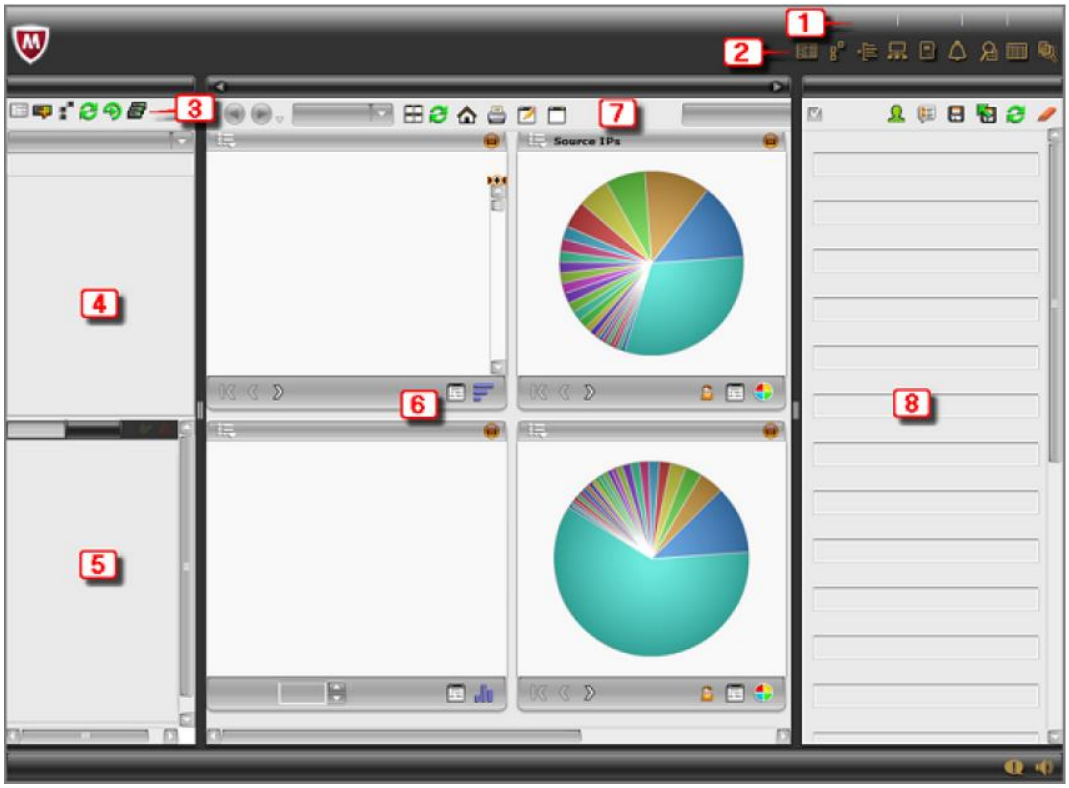


Figura 14. Consola central de administración de ESM. Intel, S. (2015). Guía de producto: McAfee Enterprise Security Manager 9.5.1. Santa Clara, California, USA

1. Barra de navegación del sistema para las funciones de configuración generales.
2. Iconos para acceder a páginas de uso frecuente.
3. Barra de herramientas de acciones para seleccionar las funciones necesarias a fin de configurar cada dispositivo.
4. Panel de navegación del sistema para ver los dispositivos del sistema.
5. Panel de alarmas y casos para ver las notificaciones de alarma y los casos abiertos asignados.
6. Panel de vistas para los datos de eventos, flujos y registro.
7. Barra de herramientas de vistas para crear, editar y administrar las vistas.
8. Panel de filtros para aplicar filtros a las vistas de datos basadas en eventos o flujos.

A continuación se presentan los requisitos mínimos en hardware y software que necesita la herramienta para su funcionamiento:

Hardware:

Procesador: de 8 núcleos y 64 bits, Dual Core2/Nehalem o superior, o bien AMD Dual Athlon64/Dual Opteron64 o superior

RAM: 4 GB o más

Espacio en disco: 250 GB o más

VMWare ESXi 5.0 o posterior

Software:

Sistema Operativo Red Hat Linux

Versión de ESM es la 9.5.0.

Para la implementación de la herramienta se usó un servidor virtual con las características de hardware descritas anteriormente y se utilizó una imagen que se obtuvo de McAfee la cual ya viene cargada con los dispositivos básicos para el funcionamiento de la solución. La dirección del servidor virtual es la 10.0.104.168, máscara 24 y Gateway 10.0.104.1.

Una vez cargada la imagen en la máquina virtual, se procede con el arranque de la misma y se inicia la sesión del ESM colocando la dirección IP del servidor virtual, donde aparecerá la pantalla indicada en la Figura 15, en la cual primero se selecciona el idioma para la consola y se coloca el usuario y la contraseña predeterminados. Nombre de usuario predeterminado: NGCP y contraseña predeterminada: security.4u, para el caso de estudio se dejó el mismo usuario y se cambió la contraseña por Mintel2015.

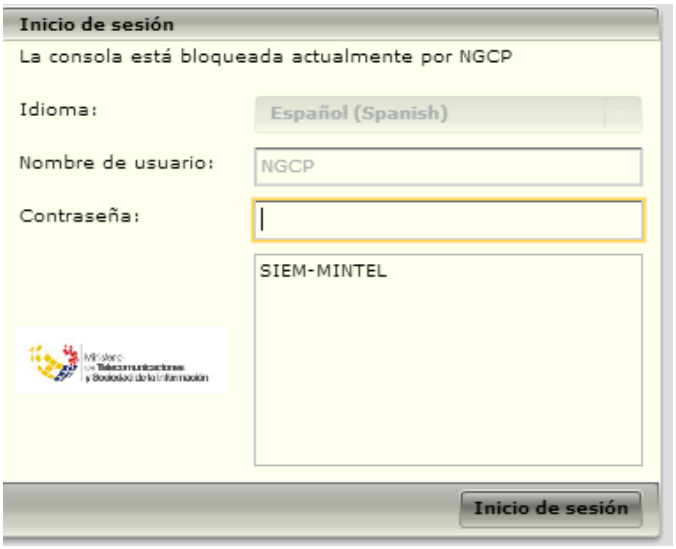


Figura 15. Pantalla de inicio de ESM con logo del MINTEL

Una vez ingresado el usuario y contraseña se accede a la consola de administración indicada en la Figura 14, donde en la barra de herramientas de acciones (3), se selecciona **Local ESM** y posterior la pestaña **propiedades** para realizar las configuraciones iniciales de la herramienta. En la Figura 16, se presenta el despliegue de las opciones que se visualizan al dar clic en propiedades; a continuación se explicará brevemente las opciones más importantes del menú herramientas.

- En la información del sistema se puede encontrar la versión de la herramienta, el hardware usado, el tiempo de caducidad de la licencia, etc...

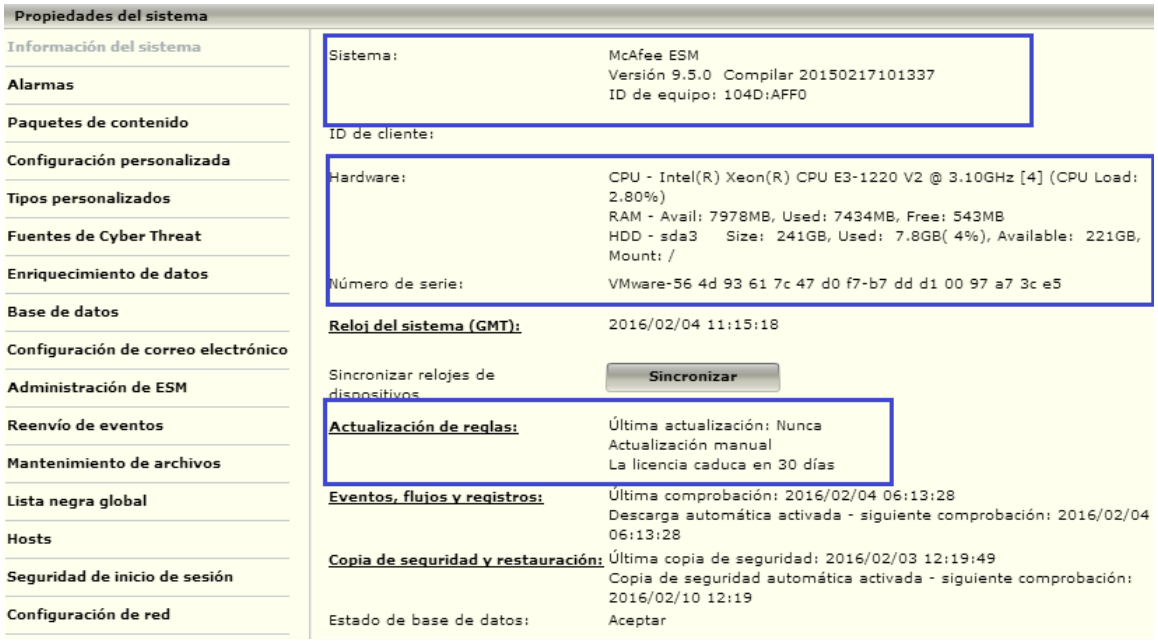


Figura 16. Pantalla de configuración inicial para el ESM – Información del sistema

- Otra pestaña importante es la administración del ESM, en la cual se encuentra la configuración, administración de claves y mantenimiento de la herramienta. En la Figura 17 se indica las opciones que se tienen para la administración del ESM.

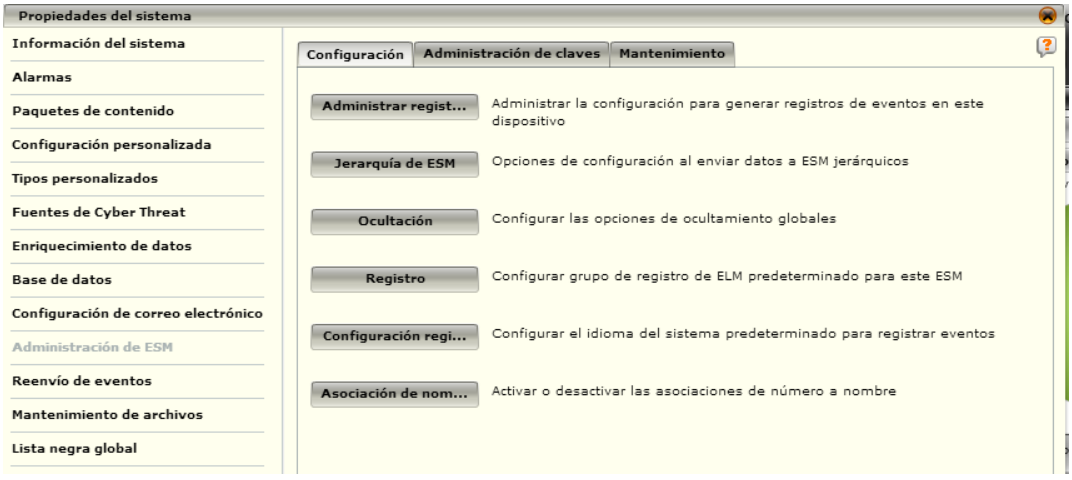


Figura 17. Pantalla para configurar la administración del ESM

- En la Figura 18 se indica las opciones que se despliegan al dar clic en la pestaña seguridad de inicio de sesión, en la misma se puede ver todas las opciones que se tienen para una autenticación segura como son: servidor RADIUS, adherirse al Active Directory, caducidad de contraseñas, etc...

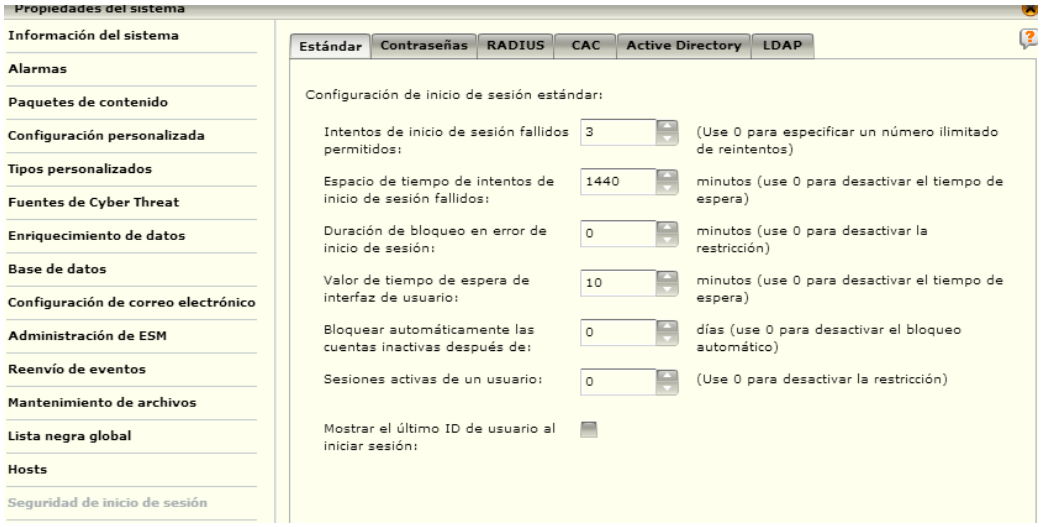


Figura 18. Pantalla de configuración para seguridad de inicio de sesión del ESM

- En la Figura 19 se visualiza la configuración de red para el servidor donde está alojada la herramienta, donde se pone: dirección de red, máscara, gateway y servidores DNS, entre los principales.

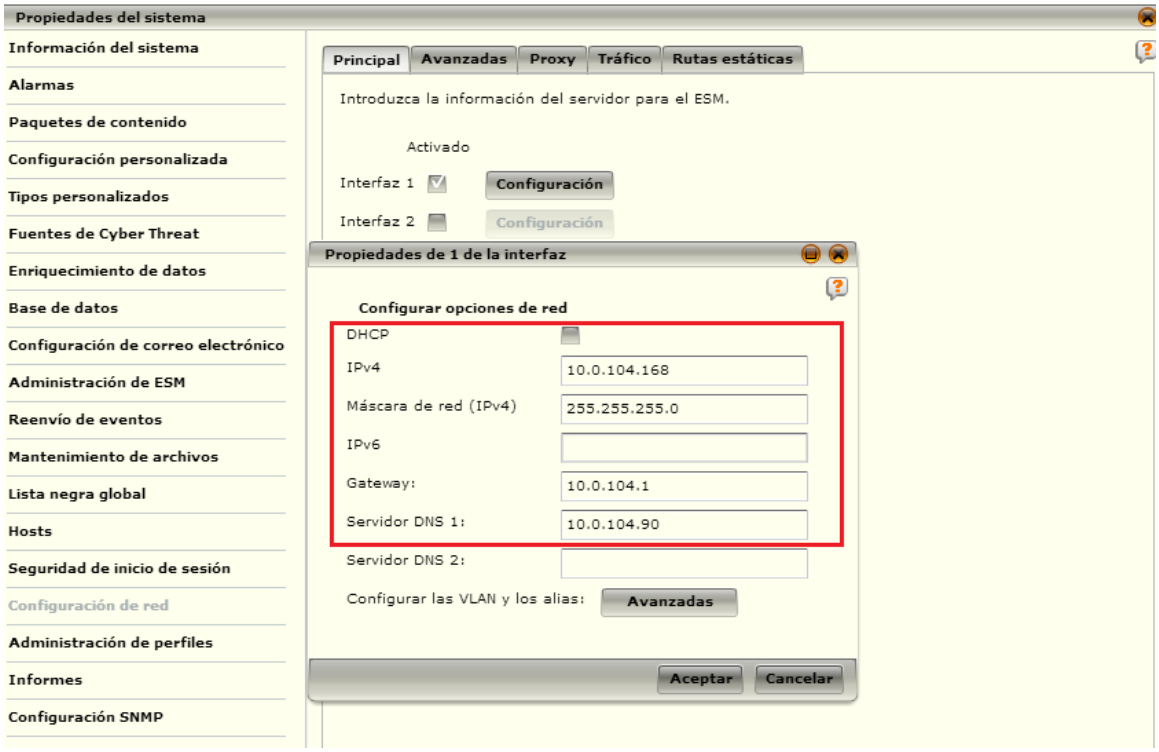


Figura 19. Pantalla de configuración de red para el ESM

- Por último, en la Figura 20 se presenta la configuración para la elaboración de informes donde se puede activar o desactivar esta opción, configurar los destinatarios que recibirán los informes, hora a la que se generarán, visualización de los mismos y una opción para ver archivos de informes pasados.

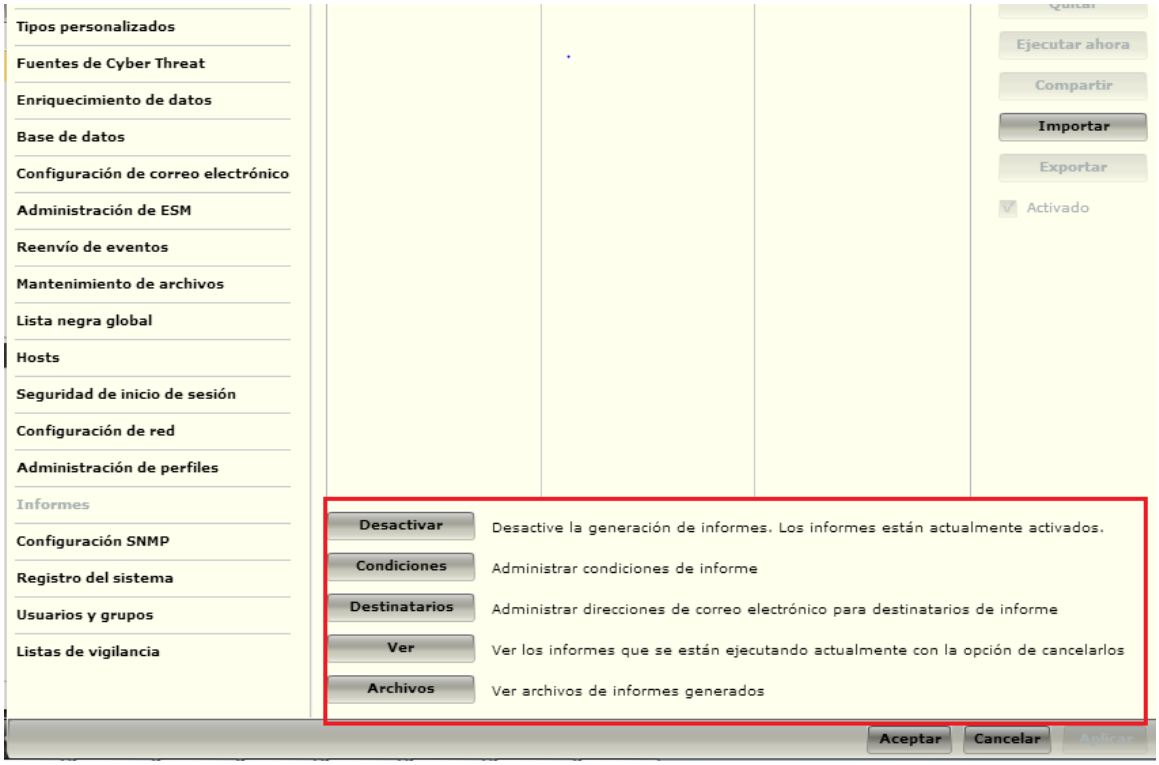


Figura 20. Pantalla para configuración de informes del ESM

Una vez que se realizan las configuraciones iniciales, a continuación se procede a añadir los dispositivos que ayudarán a la herramienta en su funcionalidad, para esto en la barra de herramientas de acciones (3), se selecciona el botón **agregar dispositivos**  con el fin de añadir a todos los aparatos que vienen dentro de la herramienta como son:

- Local ESM
- Event Receiver-ER y Enterprise Log Manager- ELM en una sola unidad

- Advanced Correlation Engine-ACE, como no se dispone de este motor avanzado de correlación, se añadió el McAfee Correlation Engine que viene intrínsecamente en la herramienta.
- Dispositivos de donde se extraerán los datos o eventos (4 fuentes definidas para el caso de estudio).

Para la visualización de los dispositivos se utiliza una estructura tipo árbol en donde su raíz será el local ESM y a partir de este se va añadiendo los demás aparatos; primero se añaden los dispositivos que sirven para la funcionalidad de la herramienta, para lo cual se debe realizar un clic en el botón agregar dispositivos  y se desplegará una pantalla con se indica en el Figura 21.

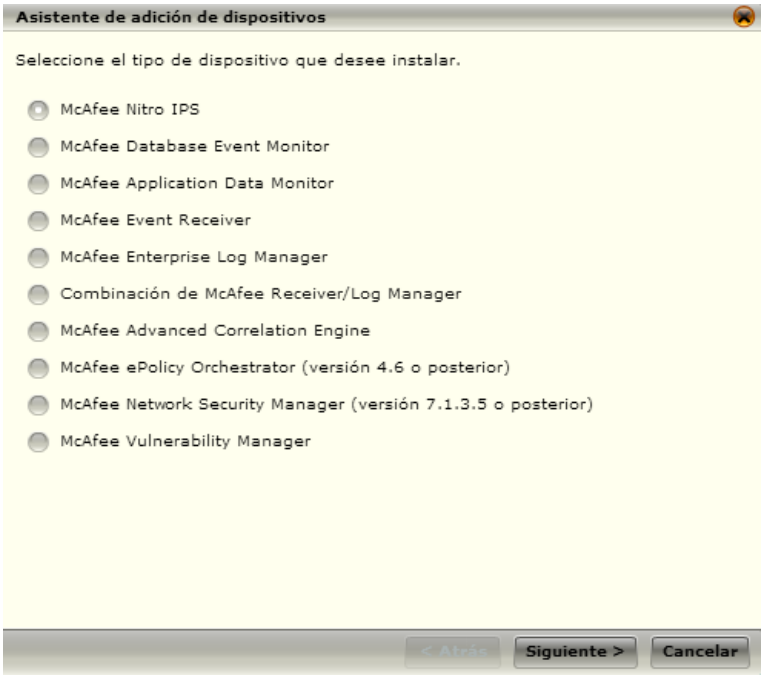


Figura 21. Pantalla de asistente de adición de dispositivos para el Local ESM

Se selecciona McAfee Event Receiver - ER y McAfee Enterpise Log que son las básicas para conformar el SIEM para este caso de estudio.

Una vez añadido el ER, el cual es el dispositivo que permite la recopilación de eventos de seguridad y datos de la red desde orígenes de varios proveedores y los normaliza a fin de obtener una solución única que se puede administrar y el ELM el cual admite el almacenamiento y la administración de los datos de registro, así como el acceso a ellos y la generación de informes, para lo cual se debe seleccionar el **Local Receiver – ELM**, dar clic en **propiedades** y se desplegará una pantalla como el de la Figura 22, donde se pueden observar las diferentes opciones de configuración.

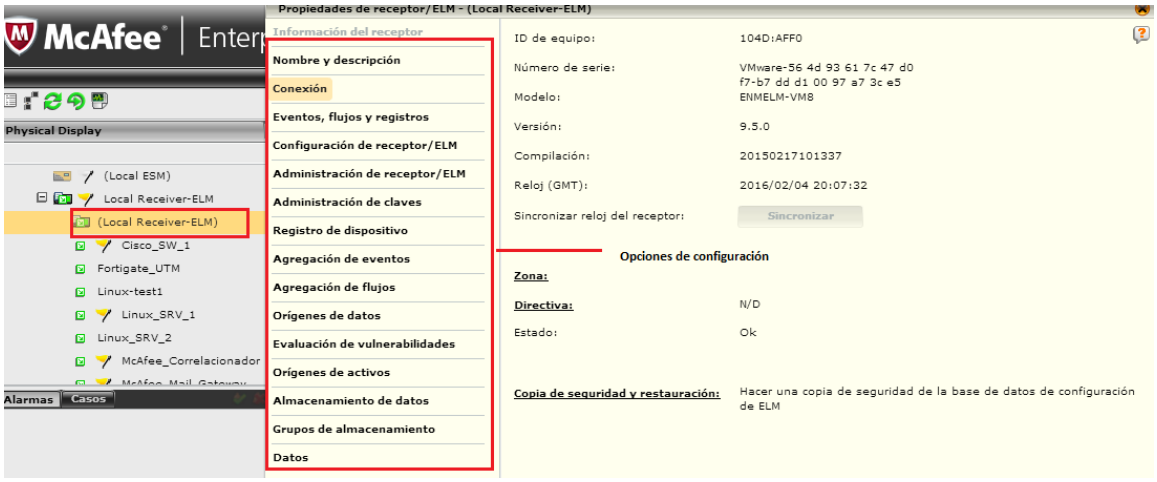


Figura 22. Pantalla de propiedades de receptor/ELM – Local Receiver ELM

Dentro de estas opciones de configuración se detallarán brevemente las más importantes y usadas. Para la recepción de eventos se da clic en la pestaña **eventos, flujos y registros** y si se desea que el ESM haga una búsqueda automática de dispositivos que

enviarán los eventos, flujos o registros se selecciona automáticamente, de esta forma se configuró en este caso de estudio, la forma de hacerlo se presenta en la Figura 23.

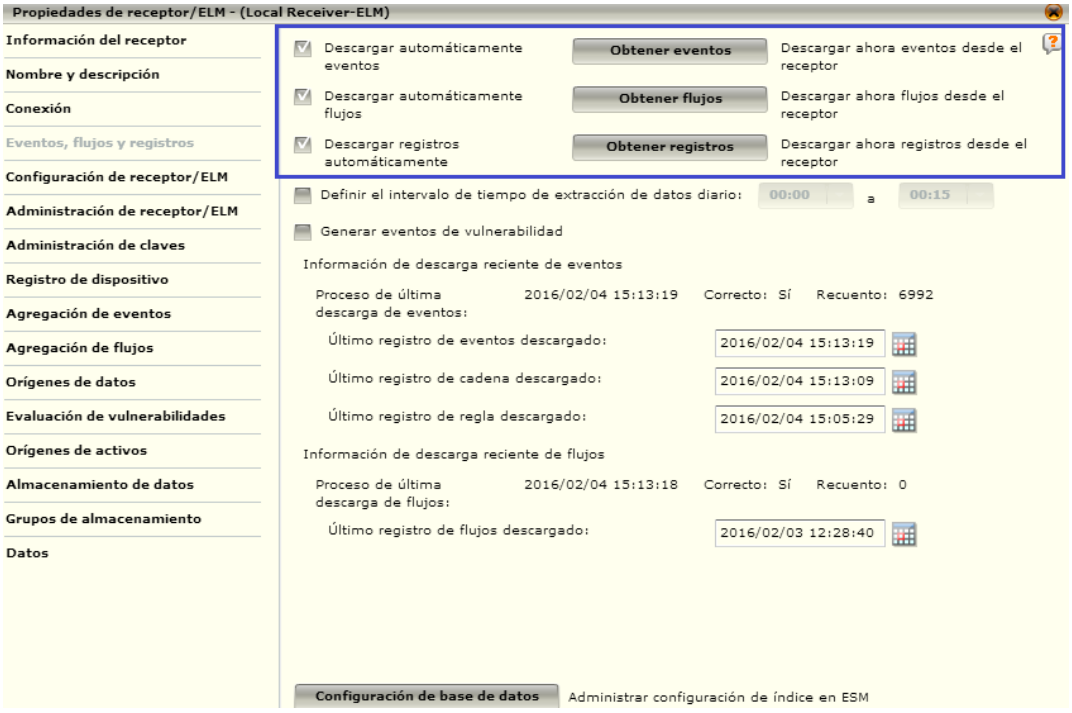


Figura 23. Pantalla para descargar eventos, flujos y registros automáticamente por ESM

Para la configuración del receptor/ELM, se da clic en la pestaña del mismo nombre y se obtendrá una pantalla como el de la Figura 24, dentro de esta lo más importante es la configuración de la **interfaz** y dentro de esta el puerto para recibir syslog. Se configuró el puerto 514 (que viene por defecto) para que reciba los syslogs de los diferentes dispositivos.

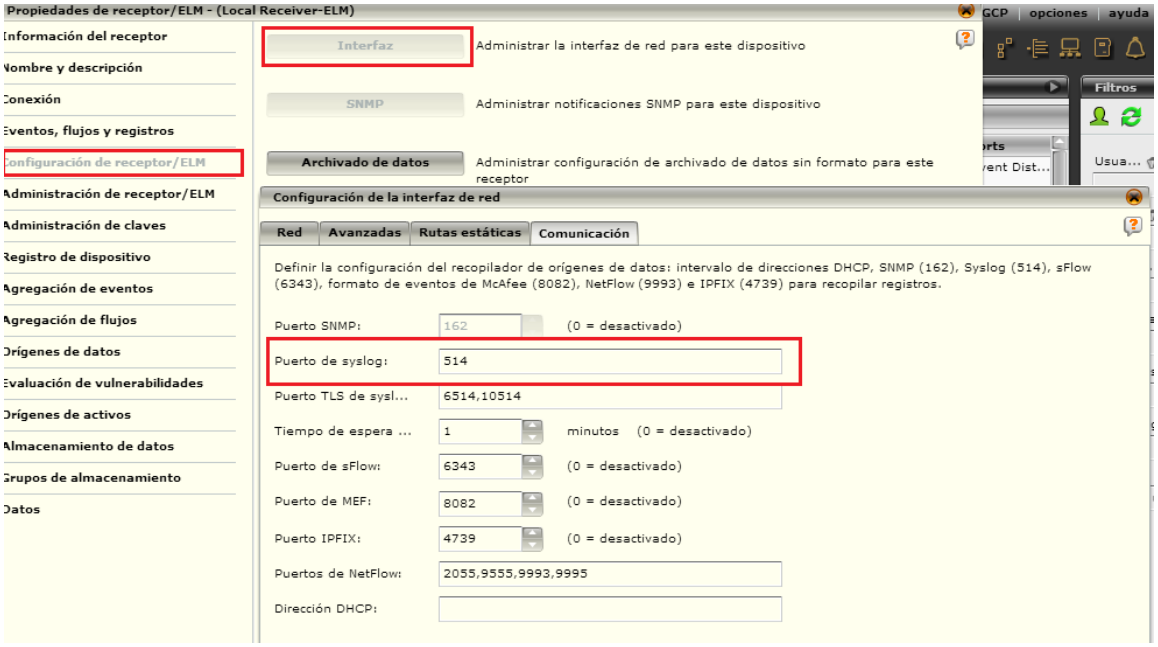


Figura 24. Pantalla de configuración de la interfaz de recepción de syslog del Receptor/ELM

Por último, se explicará la pestaña **orígenes de datos,** la cual sirve para seleccionar y configurar los orígenes de datos para el receptor, se puede usar MAYÚS+clic o CTRL+clic para seleccionar y editar varios orígenes de datos al mismo tiempo. En la Figura 25 se observa lo indicado y las fuentes de datos que se definieron para el caso de estudio.

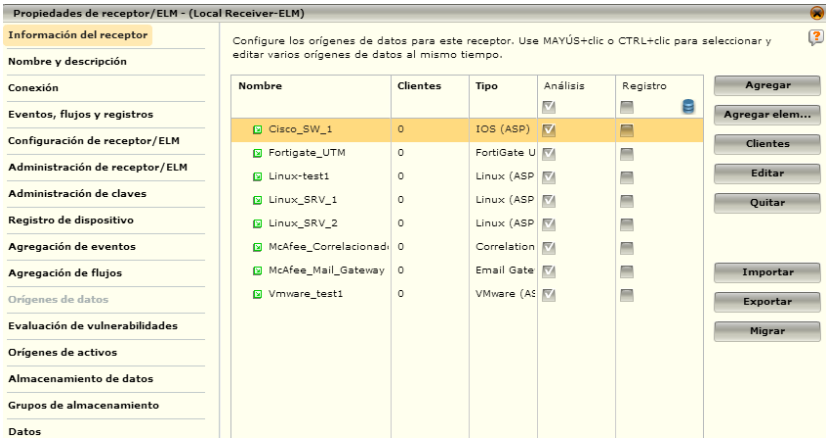


Figura 25. Fuentes de datos configurados para el caso de estudio en ESM

Dentro de esta pantalla se pueden también agregar más dispositivos desde donde se recibirán más datos para el análisis, además se tiene una opción de aprendizaje automático de las direcciones IP desconocidas para crear varios orígenes de datos. En la Figura 26 se visualiza esta última opción y la pantalla a la cual se accede al dar clic en la misma, donde se puede activar o desactivar el aprendizaje automático en varios formatos de eventos, tales como: syslog, MEF, etc…

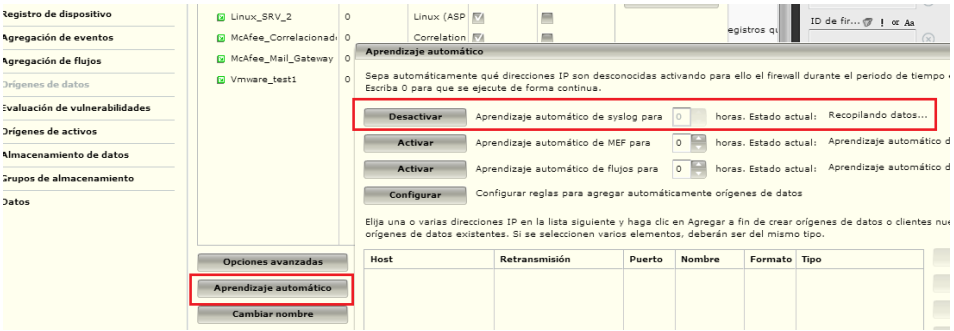


Figura 26.Pantalla de configuración para activación automático de formatos de eventos

Para finalizar con la configuración inicial del ESM, se deben añadir los dispositivos desde donde se recibirán los eventos para que posteriormente sean correlacionados. Para esto, se selecciona el **Local Receiver-ELM** añadido anteriormente y en la barra de herramientas se da clic en **agregar origen de datos**  , para añadir los dispositivos y se despliega una pantalla como la que se indica en la Figura 27.

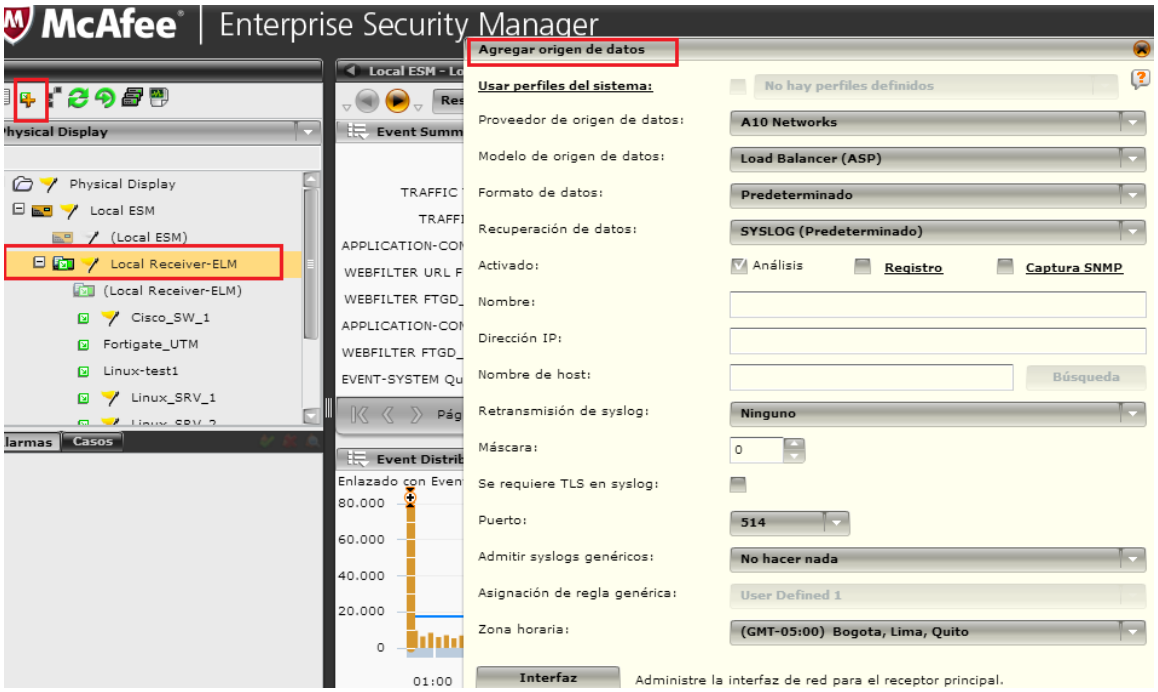


Figura 27 Pantalla para añadir nuevos orígenes de datos al ELM

En esta nueva pantalla se tienen algunas opciones, de las cuales se explicarán las necesarias y más usadas dentro de la configuración realizada en este caso de estudio.

Proveedor de origen de datos y modelo de fuente de datos: para seleccionar el proveedor y el modelo del equipo dentro de este proveedor.

Formato de datos: para seleccionar el método de análisis sintáctico, existen 3 opciones: Predeterminado, MEF (McAfee Event Forwarder) y SEF (Estándar Event Format)

Recuperación de datos: para seleccionar el método de colección de los datos, existen varias opciones, como se indica en la Figura 28. Para el caso de estudio se escogió para la mayoría de equipos syslog, que es el predeterminado que viene con la herramienta y MEF para el antispam que es una herramienta también de McAfee.

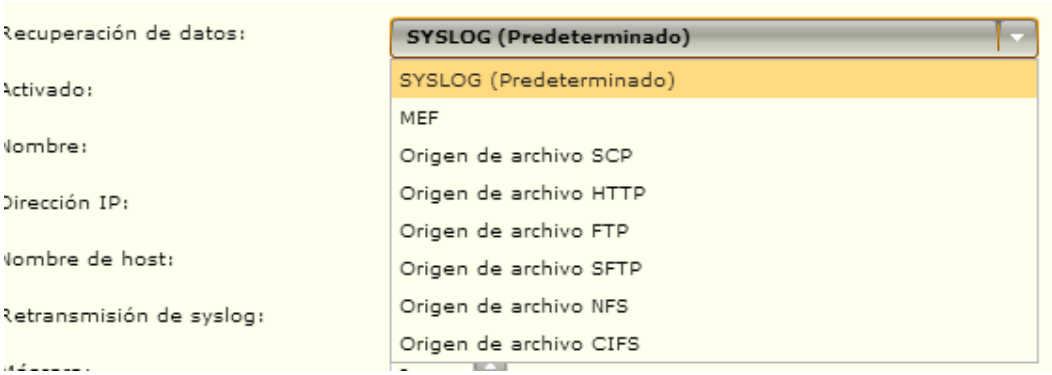


Figura 28. Opciones de configuración para la pestaña recuperación de datos

Nombre y Dirección IP: aquí se configura el nombre que aparecerá en el árbol del panel de navegación del sistema y la dirección IP del dispositivo origen de los eventos.

Como ejemplo, en la Figura 29 se presenta la configuración que se realizó a una de las fuentes de análisis del caso de estudio que es el Fortinet UTM del MINTEL.

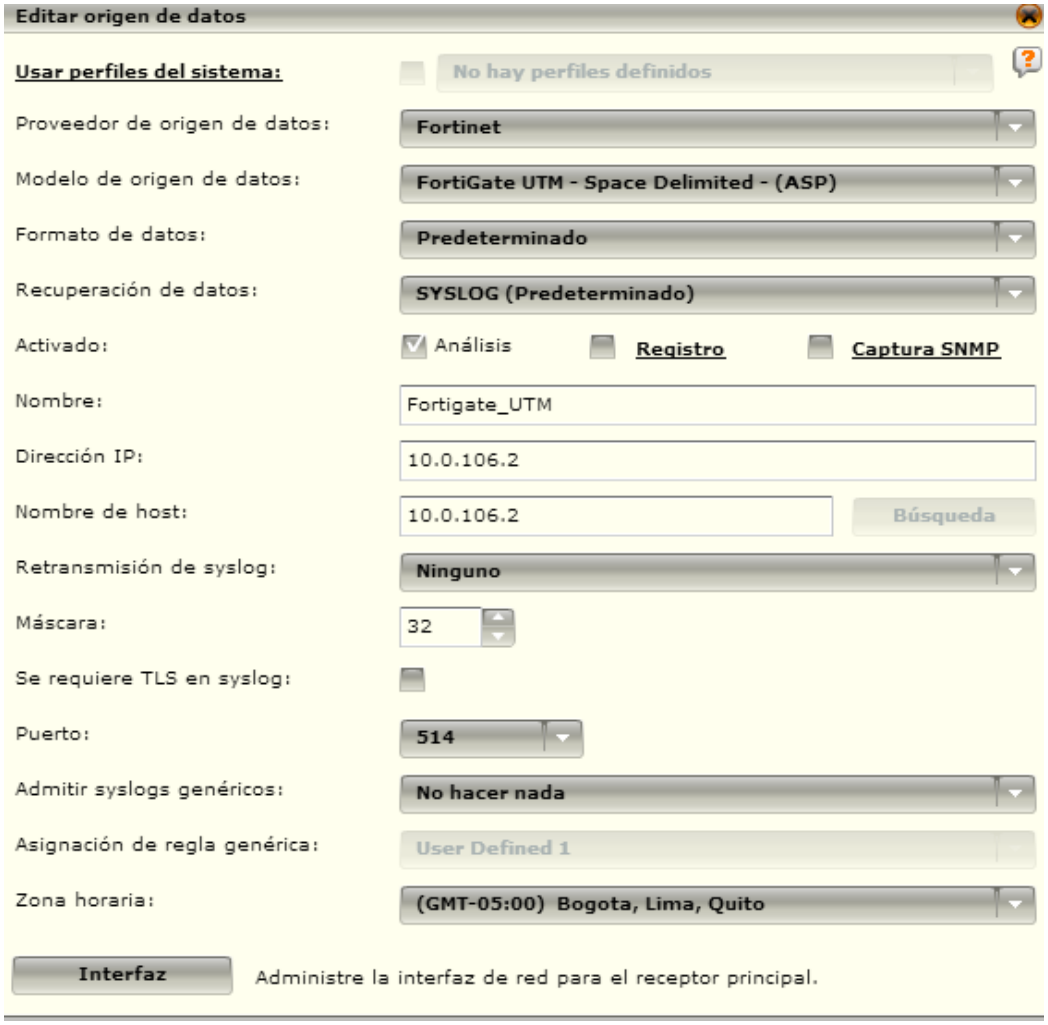


Figura 29. Configuración creada para recibir datos del equipo Fortinet del MINTEL

Para esta herramienta se añadieron los mismos dispositivos (fuentes de eventos) descritos en el numeral 5.1.2 y con la misma arquitectura de red descrita en la Figura 12, tomando en cuenta que al igual que se indicó para Splunk, los datos del servidor de antivirus no se pudieron recoger y los datos del equipo CISCO a pesar que fueron configurados solo se reciben eventos básicos y en ESM tampoco hay forma de tomar los datos para estos equipos de alguna otra forma. Además hay que tomar en cuenta que para

esta herramienta se añadieron en total 3 servidores (Linux) de aplicaciones y no solo uno como en Splunk, debido a que fueron más fáciles de ingresarlos en la herramienta.

5.1.2.3 AlienVault USM

La plataforma USM por sus siglas en inglés de Unified Security Management provee cinco funciones de seguridad en una única consola para entregar todo lo que se necesita para gestionar tanto el cumplimiento como amenazas dentro de una red lo cual ayudará a los administradores de red en la seguridad, detección de intrusos y prevención de amenazas.

Estas funciones son **descubrimiento de activos** el cual escanea activos y pasivos de una red así como también dispone de un inventario de los activos, **evaluación de vulnerabilidad** característica que realiza un monitoreo continuo de vulnerabilidades así como también un escaneo de activos autenticados y no autorizados, **detección de intrusiones** con laboratorios en Estados Unidos para redes y host IDS con monitoreo de la integridad de archivos, **monitoreo del comportamiento** con análisis de flujos de la red – netflow y monitoreo de disponibilidad de los servicios y por último incluye un **SIEM** para colección de logs, correlación de eventos y repuesta a los incidentes.

Como se indicó en uno de los objetivos de este caso de estudio, se pensó incluir dentro del análisis una herramienta de código abierto y libre, OSSIM - Open Source Security Information Management, la cual es una herramienta de AlienVAult no licenciada cuyo soporte y nuevas características son dadas principalmente en foros de

discusión creados para ello, ahí cada cual puede hacer su aporte o dar recomendaciones cuando se tenga algún problema con el aplicativo. Debido a que OSSIM es un producto libre que no tiene soporte y que además según la página web del fabricante esta herramienta tiene reportes muy básicos, no tiene un almacenador de eventos (logger) para fines forenses y principalmente no tiene un motor de correlación, objetivo principal de este caso de estudio, se decidió para poder realizar la comparación con las otras herramientas no utilizar OSSIM y usar USM que si cumple todas las funciones descritas anteriormente. En el White Paper OSIMM vs USM presentado por Alien Vault se realiza una comparación de estas dos versiones la una de código abierto y la otra comercial, se la encuentra en el link: https://www.alienvault.com/forms/document-thank-you/ossim-vs-usm-a-comparison-of-open-source-vs-commercial

Como se indicó las cinco funciones de seguridad que provee USM son las siguientes:

- Descubrimiento de activos de la red
- Evaluación de vulnerabilidades: identifica sistemas de la red que son vulnerables a la explotación
- Detección de amenazas: detecta tráfico malicioso de la red
- Monitoreo del comportamiento: detecta comportamientos sospechosos y sistemas en riesgo
- SIEM: correlaciona y analiza datos de eventos de seguridad de toda la red.

Las soluciones tradicionales SIEM integran y analizan los datos producidos por otras tecnologías de seguridad ya implementados, pero desafortunadamente la mayoría de las organizaciones del mercado medio no tienen esas otras tecnologías todavía desplegadas. AlienVault USM, además de toda la funcionalidad de un SIEM tradicional, también construye las capacidades de seguridad esenciales en una sola plataforma, sin cargos adicionales de características.

USM es la distribución comercial de AlienVault, la cual es una distribución Debian (Linux) que lleva múltiples herramientas de monitorización de seguridad para una red en una solo plataforma, se accede a la misma mediante una interfaz vía web y puede ser adquirida mediante un appliance all in one (todo en uno) o se lo puede instalar sobre una máquina virtual ya que es completamente compatible con VMware ESXi. Los requerimientos de hardware y software que necesita esta plataforma se describen a continuación:

Hardware:

Al igual que las otras herramientas evaluadas, los requerimientos de hardware dependen del número de eventos por segundo y el rendimiento de la red que se desea proteger, siendo los mínimos los siguientes:

Procesador: de 8 núcleos y 64 bits, Intel Xeon E5620 o equivalente

RAM: 8 GB o más

Espacio en disco: 500 GB o más

VMware ESXi 5.x (recomendado)

Software:

Sistema Operativo Debian 3.5

Versión de USM: versión 5.0

Para la implementación de la herramienta se usó un servidor virtual con las características de hardware descritas anteriormente y se cargó la imagen ISO que se descargó de la página web de AlienVault. La dirección del servidor virtual es la 10.0.104.170, máscara 24 y Gateway 10.0.104.1

Para cargar la imagen en la máquina virtual, se desplegó un OVF usando el cliente vSphere con la opción de menú '**File > Deploy OVF Template'**, posteriormente se utilizaron las opciones de configuración predeterminada y se abre la consola de línea de comandos de AlienVault. En la Figura 30 se observa la pantalla para desplegar el OVF.

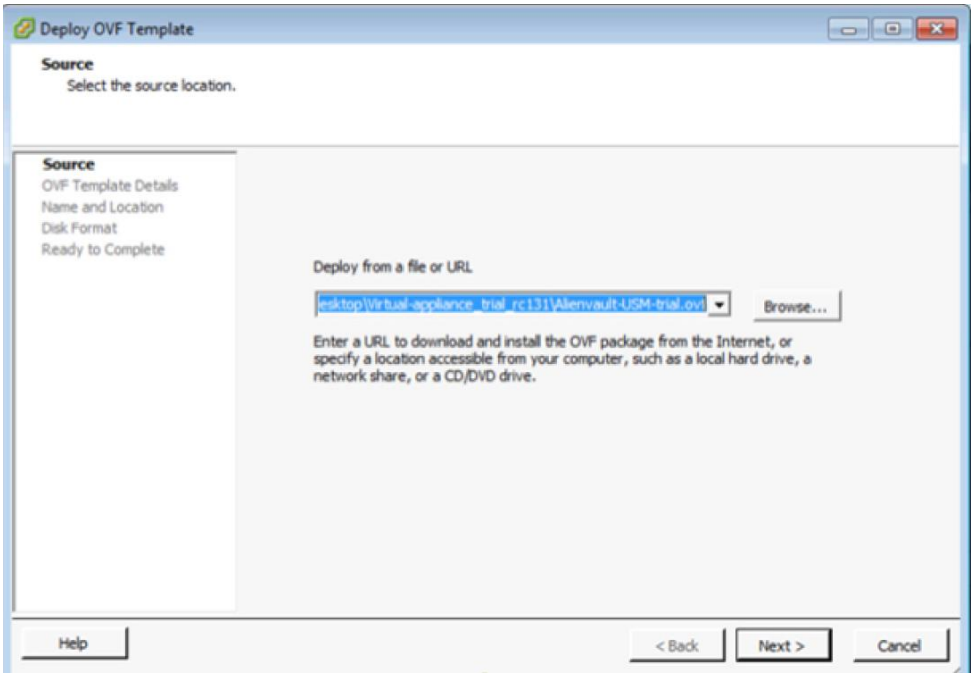


Figura 30. Pantalla para desplegar el modelo OVF de instalación de USM

Las configuraciones iniciales toman algunos minutos, lo básico que se debe configurar es la dirección IP del servidor, con su máscara y gateway y lo demás lo hará directamente USM, posteriormente se pide las credenciales de acceso, las cuales se encuentran en la pantalla inicial; hay que tener en cuenta que se debe cambiar el password del root, como se observa en la Figura 31

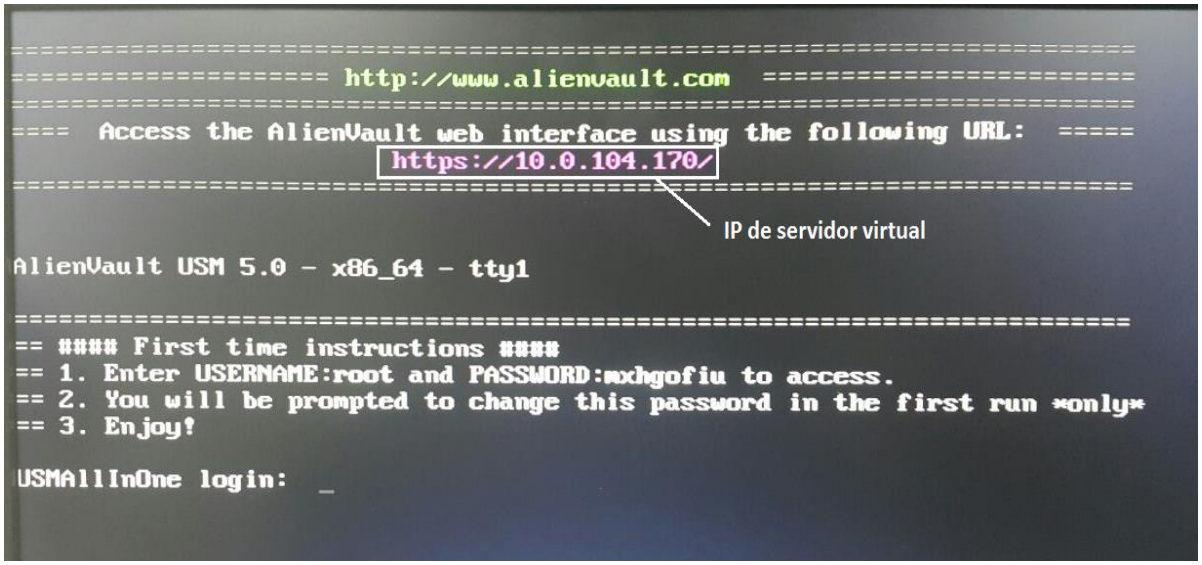


Figura 31 Pantalla de instalación inicial con comandos Linux

Por último se accede a la interface web de la herramienta usando el URL provisto (IP del servidor virtual), donde además se debe ingresar una dirección de email (que es la misma que se usó para bajarse la versión demo), se llena la forma de bienvenido y se registra el usuario y contraseña para posteriormente iniciar con las configuraciones iniciales usando el asistente de introducción rápido (Getting Started Wizard). En la Figura 32 se presenta la pantalla de registro.

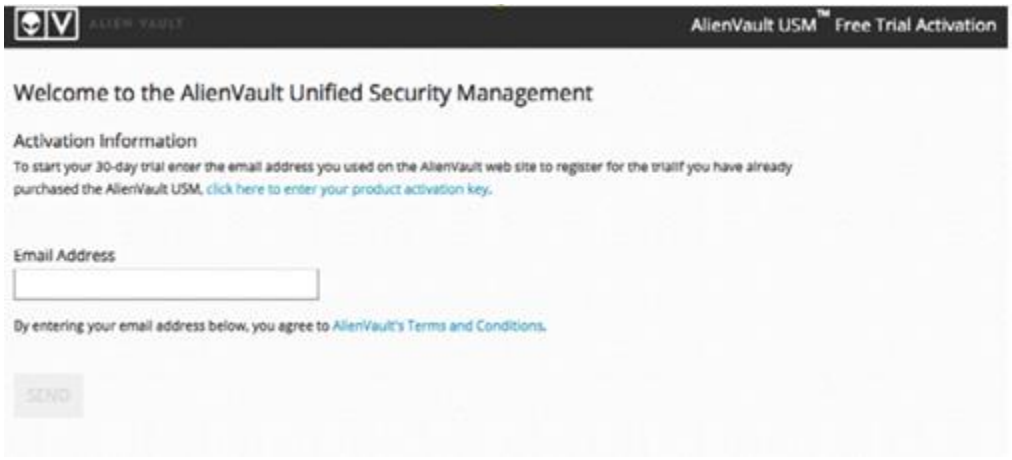


Figura 32. Pantalla de inicio de instalación de USM

El nombre de usuario predeterminado para ingresar vía web es: admin y la contraseña predeterminada: alienvault. Para el caso de estudio se dejó el mismo usuario y se cambió la contraseña por Mintel2016, la contraseña se la cambia ingresando en las opciones de configuración que tiene la herramienta por Linux.

Una vez que se ingresa en la herramienta se realiza un inicio rápido de 5 pasos para configurar el USM y poder usarlo inmediatamente para detectar amenazas en la red.

A continuación se explican estos pasos de configuración rápida:

1. Lo primero que se debe configurar son las interfaces de red que vienen predefinidas, en total son 6 y cada interface puede ser configurada como: no en uso, monitoreo de red y recopilación y análisis de eventos. La interface eth0 sirve para administración de la herramienta, es decir para la comunicación con el servidor virtual creado y poder conectarse vía web. La IP de la eth0 se la

configuró inicialmente al ingresar vía consola y posteriormente este valor es presentado en la sección de interfaces por defecto como se visualiza en la Figura 33, donde además se configura las otras interfaces de red disponibles.

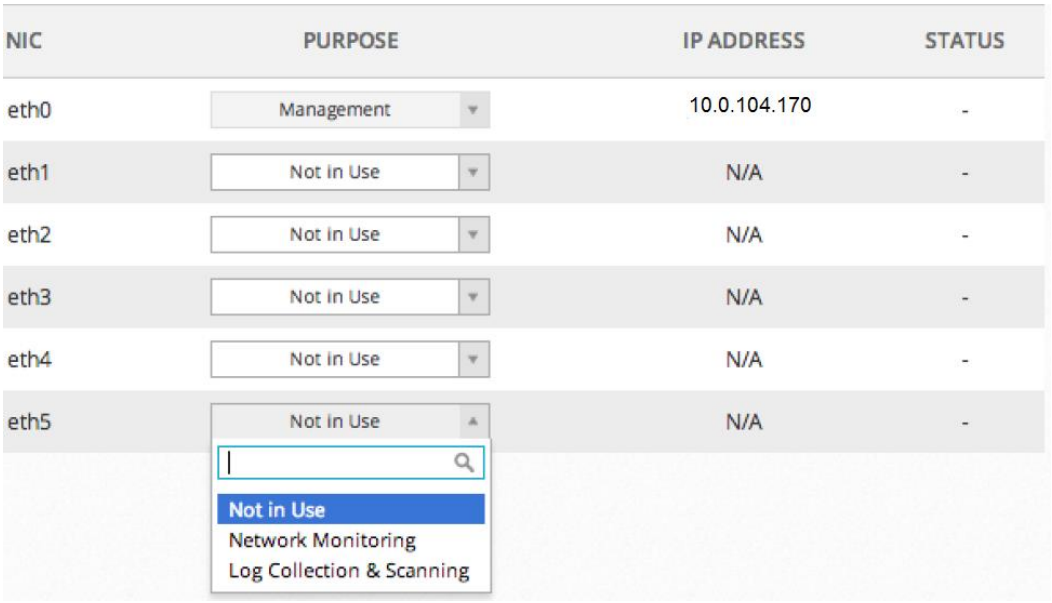


Figura 33. Pantalla para configurar las interfaces eth1 a eth5 de USM

Se configuró la interface eth1 como monitoreo de red que significa modo de escucha pasivo, referido como modo promiscuo. La interface escuchará el tráfico que viene por el "cable", esta interface físicamente se conectó a un puerto del switch de core del MINTEL y se configuró este puerto como espejo para que el tráfico fluya a la interfaz de red asignada para que pueda buscar eventos. No se configuró ninguna interface para recopilación y análisis de eventos. En la Figura 34 se observa que la interface eth1 está siendo usada para monitoreo de red -

Network Monitoring por que la herramienta automáticamente colocará la interface para escuchar el tráfico de entrada. Para saber que la misma está recibiendo datos el led de estado se pondrá en verde.

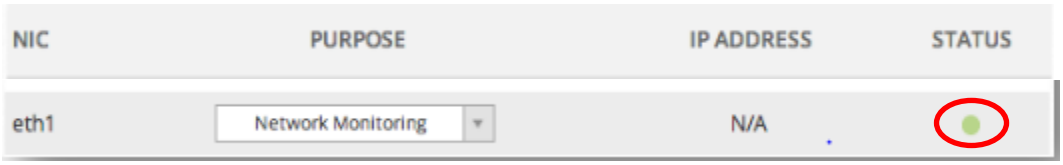


Figura 34. Estado de la interface eth1 configurada para monitoreo de red

2. Descubrir los activos de la red, para esto existen tres formas de descubrimiento: la primera es descubrir automáticamente los activos, la segunda es ingresar manualmente los activos y la último se puede importar activos de un archivo del tipo CVS; además la herramienta cuenta con una base de datos de las marcas de equipos más conocidas para que con esto se pueda añadir de una forma más sencilla manualmente nuevos activos que se tengan en la infraestructura de la red. Para este caso de estudio se realizó un descubrimiento automático de activos y además se ingresó de forma manual algunos dispositivos que fueron evaluados con las otras herramientas.

   Para escanear automáticamente la red y encontrar nuevos activos, primero se da clic en el botón **Scan Networks**, como se visualiza en la Figura 35.

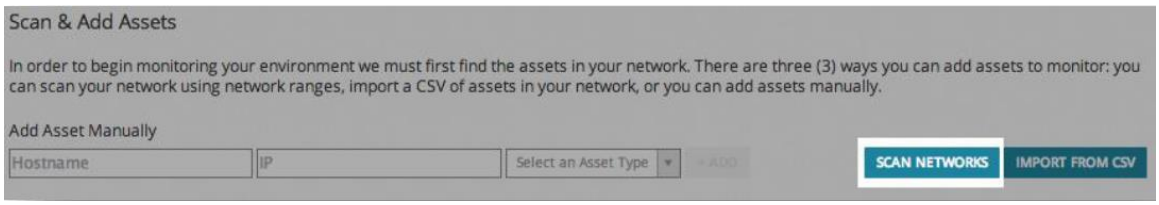


Figura 35. Escaneo automático de activos de la red del MINTEL

Posteriormente se escoge una o más redes que se desea escanear, para este caso se configuró 3 redes para descubrir activos: red de servidores 10.0.104.x, red wifi 10.20.0.x y la red de prueba del departamento de gestión tecnológica 10.0.105.x. En la Figura 36 se pueden visualizar las redes adicionadas.

RED	CIDR	PROPIETARIO(S)	SENSORES
Red WIFI	10.2.0.0/16	MINTEL	USMAllInOne
Red DGT	10.0.105.0/24	DGT	USMAllInOne
Local_10_0_104_0_24	10.0.104.0/24		USMAllInOne

Figura 36. Declaración de redes para descubrimiento de activos de eventos

Una vez adicionadas las redes por último se da clic en el botón **Scan Now** y aparece una pantalla donde se indica el número de activos que van a ser descubiertos en base a las configuraciones de las redes colocadas. Se da clic en el botón **aceptar** (ver Figura 37) y comienza el escaneo lo cual puede durar algunos minutos dependiendo de cuantas redes se hayan colocado para ser escaneadas y de cuantos equipos está conformada la red.

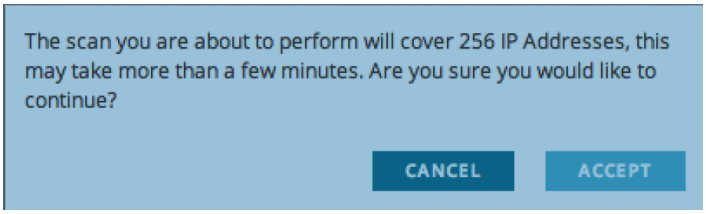


Figura 37. Pantalla para aceptar el número de equipos que serán descubiertos por USM

Una vez finalizado la búsqueda se preguntará si se desea calendarizar nuevos escaneos para descubrir nuevos elementos en las redes periódicamente, se dejó en la opción por defecto que es mensualmente.

Finalmente se adicionó 6 dispositivos (activos) manualmente, los cuales son: 3 servidores Linux de página web y aplicaciones del MINTEL, el switch de core, el Wireless Lan Controller - WLC para comunicaciones inalámbricas y el equipo de seguridad perimetral Fortinet. Para ingresar manualmente un activo se debe seleccionar la opción **manualmente**, proveer los datos de: nombre, IP y tipo de activo de una lista que se despliega en la última ventana y a continuación dar clic en el botón **ADD**. En la Figura 38 se da un ejemplo de la adición del switch de core y en la Figura 39 se presenta algunos de los dispositivos adicionados manualmente en la herramienta.

Figura 38. Ingreso manual del switch de core del MINTEL al USM

NOMBRE EQUIPO	IP	TIPO DE DISPOSITIVO	SISTEMA OPERATIVO	VALOR ACTIVO
WLC	10.0.104.7	Network Device		2
USMAllInOne	10.0.104.170		AlienVault OS	2
SWdeCore	10.0.1.1	Network Device		2
SrvWebTeleco	10.0.104.238		Linux	2
SrvWebSGSI	10.0.104.253		Linux	2
SrvWebObtic	10.0.104.131		Linux	2

Figura 39 Lista de equipos adicionados manualmente en la herramienta

3. El paso 3 consiste en implementar un agente para la detección de intrusiones basado en host (HIDS) para los servidores, a fin de realizar la supervisión de integridad de archivos, y recopilación de registros de eventos. Para las máquinas Windows el agente HIDS se instala localmente. Los sistemas Unix/Linux son controlados de forma remota y sólo incluyen la capacidad de supervisión de integridad de archivos. Para que esto funcione se debe ingresar en la herramienta las credenciales de administración del dispositivo en el que se desee desplegar el HIDS. Solo se instaló este agente en los 3 servidores LINUX: página web, Infocentros y observatorio TIC.

   Para implementar HIDS en estos servidores, se debe ingresar las credenciales vía SSH, y en la pantalla de la herramienta escoger los dispositivos en los cuales se desee instalar el HIDS y desplegar el agente usando el botón **Deploy**. Una vez que el agente este configurado correctamente, un círculo de color verde aparece y se

desplegará los siguientes mensajes: “Plugin Enabled” y “Receiving Data”. En la Figura 40 se presenta los servidores en los cuales están desplegados el agente HIDS.

NOMBRE EQUIPO	IP	USUARIO	ESTADO	DESCRIPCIÓN
SrvWebObtic	10.0.104.131	madmin	✔	
SrvWebSGSI	10.0.104.253	madmin	✔	
SrvWebTeleco	10.0.104.238	madmin	✔	

Figura 40. Lista de equipos Linux desplegados el agente HIDS

4. El paso 4 consiste en configurar la administración de registros (logs), la cual consiste en recopilar datos externos desde dispositivos de red, dispositivos de seguridad y de servidores. Los datos recopilados permiten a la herramienta hacer la correlación de eventos para ver los patrones de actividad y avisar vía una alarma. Una vez que se hayan descubierto los dispositivos sean automáticos o ingresados manualmente, el asistente de inicio rápido permite configurar fácilmente cada uno estos activos con el plugin adecuado para recopilar los logs de estos dispositivos. Por cada dispositivo, se selecciona el correcto proveedor, modelo y número de versión y se da clic en el botón **Enable** para habilitarlos; para el caso de estudio se seleccionó 3 dispositivos: el switch de core, el WLC y el Fortinet. En la Figura 41 se indica un ejemplo de la configuración para el switch de core.

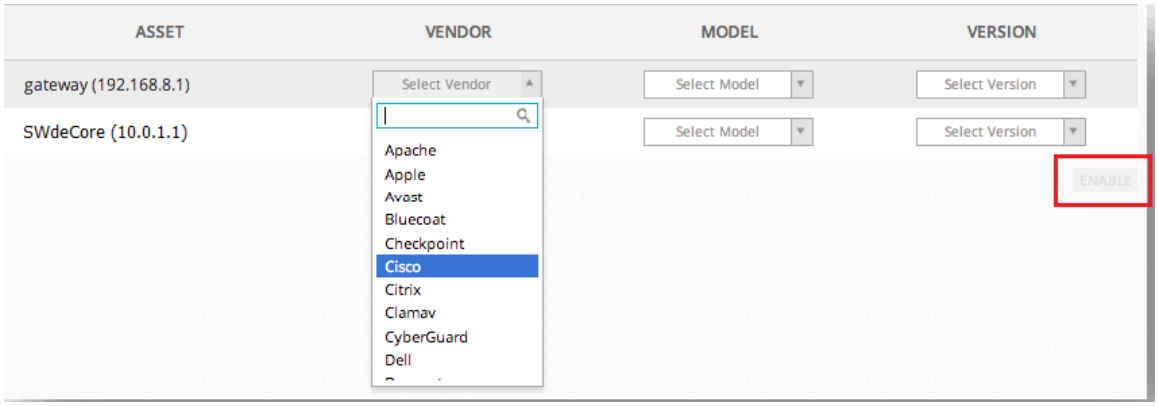


Figura 41. Configuración para recibir logs del switch de core del MINTEL

Una vez que el plugin está perfectamente instalado, aparecerá un indicador en color verde que indica una instalación correcta y se podrá comenzar a recibir registros de ese dispositivo. Una vez que se instaló todos los plugins en los dispositivos seleccionados, se da clic en **Finish** y se terminará la configuración inicial rápida.

5. El último paso es registrarse en la comunidad OTX – Open Threat Exchange, que es una red de compartimiento y análisis para amenazas, creada para poner medidas de seguridad efectivas al alcance de todas las organizaciones. OTX proporciona en tiempo real, información procesable para todos aquellos que quieran participar, al registrarse en OTX permite que se comparta información de amenazas automáticamente con la comunidad y al mismo tiempo recibir nuevas amenazas de otros ambientes. El registro además se lo puede hacer en redes sociales.

Al finalizar este paso, se desplegará una pantalla de felicitaciones, indicando que los datos están llegando al USM como se indica en la Figura 42.

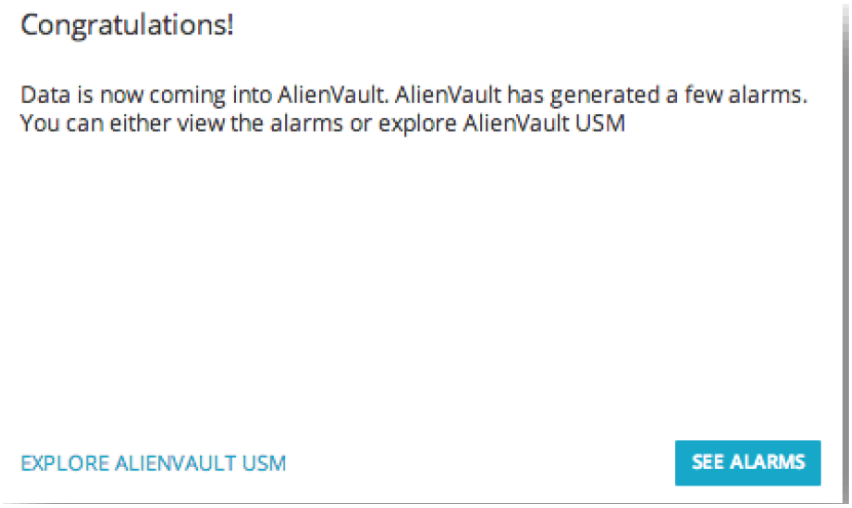


Figura 42. Pantalla de finalización de instalación rápida de USM

Al finalizar todos los pasos descritos anteriormente ya se puede ingresar a la herramienta dando clic en **Explore AlienVault USM** o ver las alarmas ya generadas dando clic en **See Alarms**. En la Figura 43 se indica las alarmas iniciales generadas por

la herramienta después de realizar la configuración rápida.

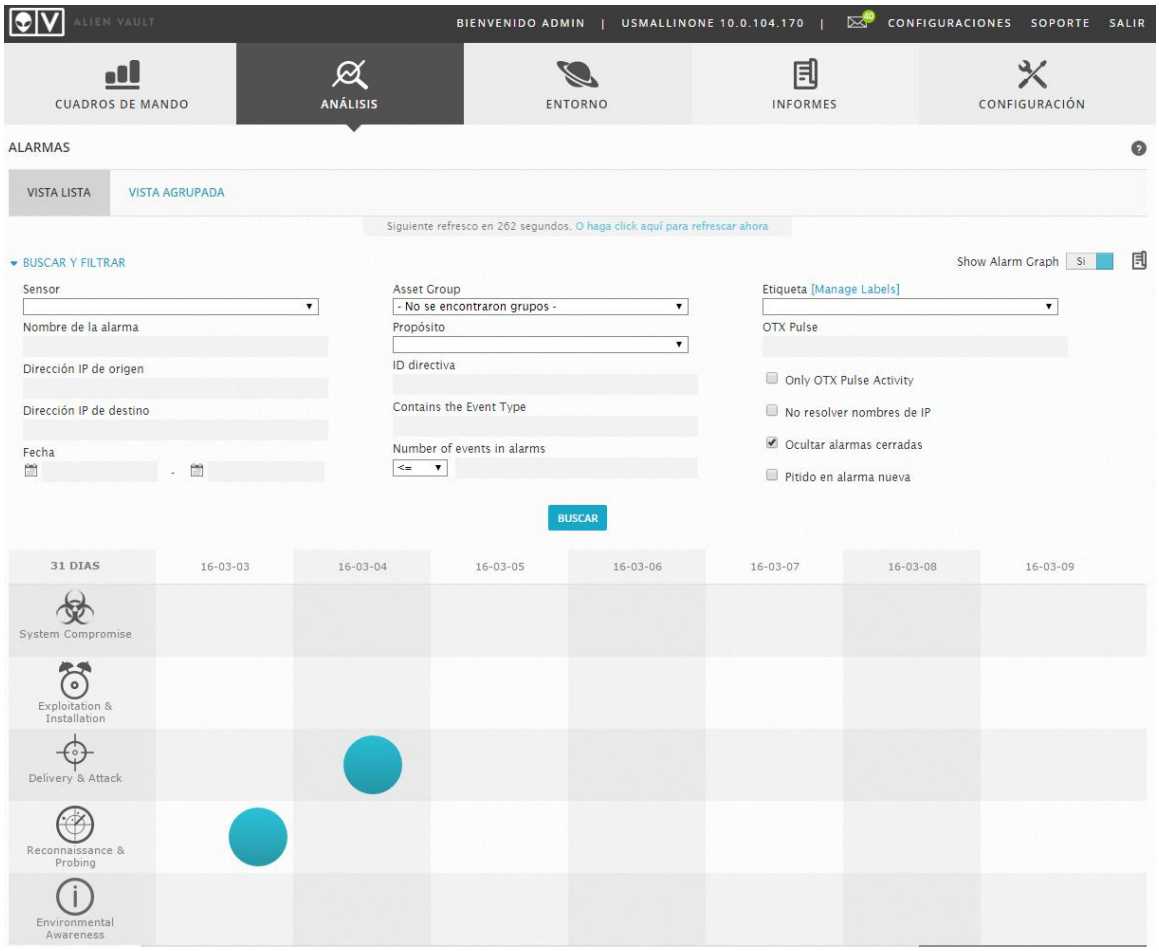


Figura 43. Pantalla de alarmas encontradas al finalizar la instalación rápida de USM

Se utilizó la misma arquitectura de red descrita en la Figura 12, tomando en cuenta que los datos del servidor de antivirus tampoco se pudieron recoger ya que no maneja syslog pero si se pudo añadir los datos de equipos CISCO. Al igual que en ESM también se añadieron en total 3 servidores de aplicaciones que fueron descritos anteriormente.

5.2 Correlación de eventos de seguridad

Una vez que las herramientas SIEM seleccionadas fueron instaladas y configuradas para recibir los datos de las fuentes de información elegidas para la infraestructura del MINTEL, se tiene que realizar la configuración para correlacionar los eventos que llegan y presentarlos en forma de tableros gráficos de control. En este capítulo se irá describiendo el análisis realizado con cada herramienta con la respectiva configuración de correlación de los eventos; este análisis se lo hizo de acuerdo a la forma de presentar los eventos que tiene cada herramienta tratando que el producto final sea parecido y así poder analizarlo posteriormente y seleccionar la mejor herramienta SIEM.

5.2.1 Splunk

Una vez ingresadas las credenciales de acceso para la herramienta, se ingresa vía web a la pantalla de inicio, donde se creó un nuevo App llamado MINTEL a parte de los que vienen por defecto que son: search & reporting y el App de Fortinet creado exclusivamente para Splunk. En la Figura 44 se visualiza lo indicado.

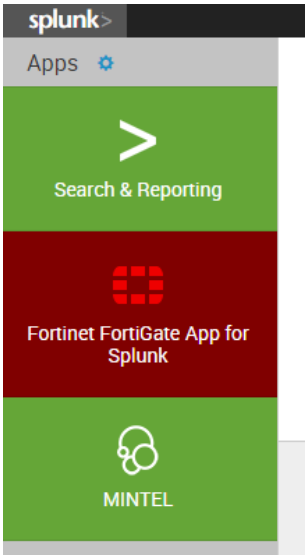


Figura 44. Pantalla inicio de Splunk

Al seleccionar **search & reportering** se ingresa a una pantalla donde se podrá hacer cualquier búsqueda de la información que se tienen de los eventos que están llegando a la plataforma y con estos datos crear tableros de control. En la Figura 45 se ven las opciones que se tienen al ingresar en esta pestaña, se observa que se han recibido aproximadamente tres millones de eventos (en 1 mes y medio que se tuvo activa la licencia demo).

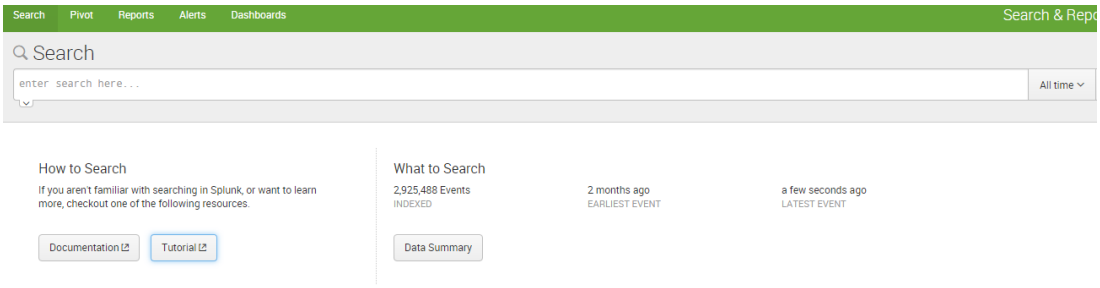


Figura 45. Pantalla de búsqueda inicial de Splunk

Al dar clic en **Data Summary** se podrá observar 3 sub-pestañas: **Hosts, sources y sourcetypes,** como se visualiza en la Figura 46. Los hosts son los dispositivos que están siendo monitoreados por la herramienta, en este caso están ingresados 5.

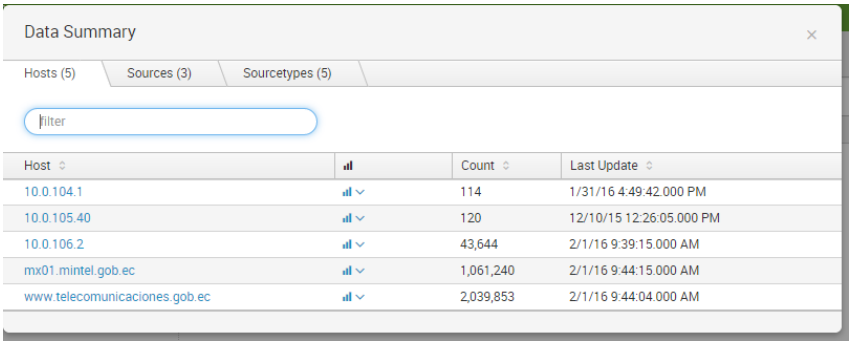


Figura 46. Pantalla de resumen de datos y equipos ingresados en Splunk

En la Figura 47 se presenta los tipos de fuentes (sourcetypes) que para este caso de estudio igual son 5, donde se puede visualizar la cantidad de eventos recibidos por cada fuente de información con su última actualización. Al dar clic en cualquiera de estos tipos de fuente se despliega toda la información de los eventos recibidos, con estos datos se puede analizar los casos de uso que se requieran correlacionar.

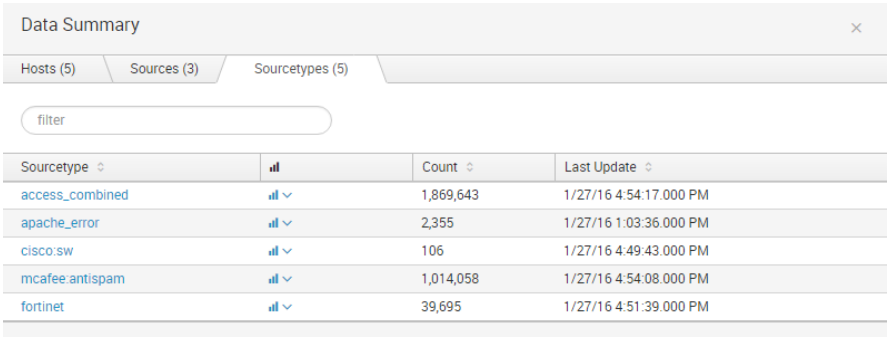


Figura 47. Lista de tipos de fuente ingresados en Splunk

En la Figura 48, se indica la pantalla donde se presentan los eventos de la fuente de información seleccionada, de acuerdo al siguiente detalle:

- En la parte superior la línea de tiempo de eventos recibidos por: minuto, hora, día o mes.
- En la parte izquierda se visualizan todos los campos de interés de esos datos y además los campos seleccionados para un análisis futuro de correlación filtrando o dejando pasar solo los datos de interés que se necesiten.
- En la parte derecha se presentan todos los campos de los registros recibidos con fecha y hora. Al mismo tiempo se puede seleccionar y visualizar los registros en tiempo real o en los últimos minutos, última hora, últimos días e inclusive en el último mes almacenados en una base de datos propia de la herramienta.

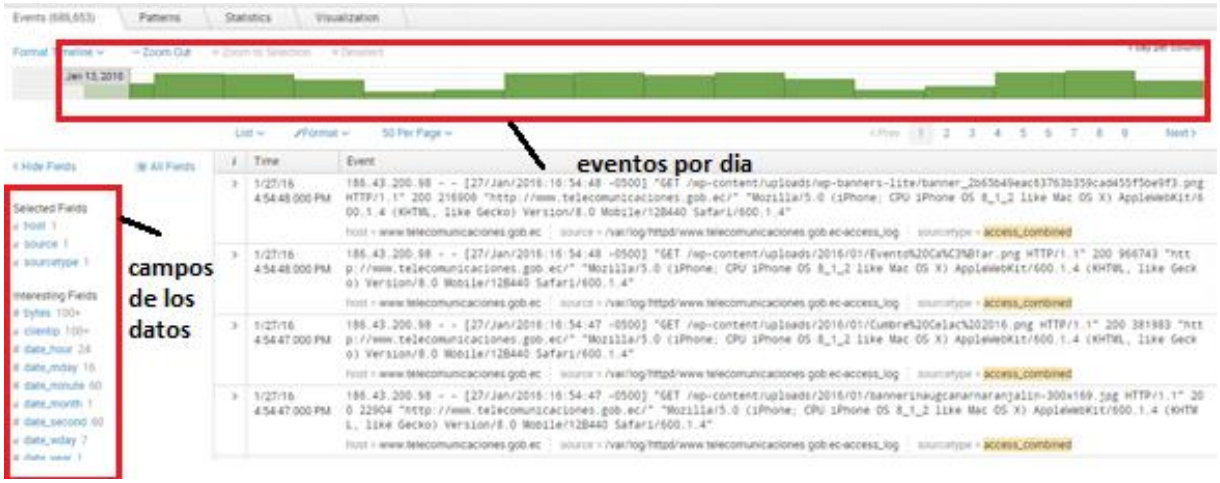


Figura 48. Registros de eventos que llegan a la herramienta

Con los datos de estas 5 fuentes se procedió a correlacionar los eventos tanto para las aplicaciones web, equipo UTM (Fortinet) y Antispam, no se pudo realizar nada con el equipamiento de Networking (CISCO) ya que los syslogs enviados por el equipo son demasiado básicos como para realizar algún tipo de análisis o correlación, al igual que con el servidor de Antivirus que no envía syslog.

Para realizar correlaciones con la herramienta se tiene que ingresar en cualquiera de los 5 tipos de fuentes que se tienen y seleccionar **New search** y ahí colocar la configuración en lenguaje SPL de acuerdo a los eventos que se tengan del tipo de fuente. Cabe señalar que para realizar la configuración y correlación de los eventos se tuvo que investigar sobre búsqueda y reportería en Splunk usando comandos de SPL, toda la información necesaria sobre cómo usar este lenguaje se encuentra en los manuales de la herramienta, lo primero que se debe realizar es entender que tipos de búsquedas existen y que tipos de comandos se usan con su sintaxis. Por ejemplo para filtrar información que no se necesita o para extraer más información, o para cálculo de estadísticas, etc., se deben usar comandos y además hay que tomar en cuenta que se lo tiene que hacer a partir de los logs en bruto obtenidos desde las fuentes de datos. A continuación se presentan las correlaciones realizadas para la herramienta:

1. **Servidor página web de telecomunicaciones:**

   Disponibilidad del sitio

   sourcetype=access_combined status!="3*"| eval isUp=if(status==200,1,0) | stats avg(isUp) as average | eval average=round(average*100,2)

Visitas al sitio

sourcetype=access_combined | stats count as Visitas

Visitas únicas al sitio

sourcetype=access_combined | dedup clientip | stats count as Visitas

Resultados de consultas

sourcetype=access_combined | stats count by status_description | sort 10 – count

Top 10 de los lugares más visitados dentro de la página

sourcetype=access_combined status=200 NOT referer="-" | stats count as Visitas by referer | sort 10 - Visitas

Visitas al sitio por ubicación (dentro de un mapa geo referenciado)

sourcetype=access_combined | iplocation clientip | geostats count

IP con múltiples accesos a página de "wp_login.php"

sourcetype=access_combined status=200 NOT referer="-" referer="http://www.telecomunicaciones.gob.ec/wp-login.php"| stats count AS Accesos by clientip | sort 10 -Accesos | search Accesos > 50

Países según IP accediendo al sitio "wp_login.php"

sourcetype=access_combined status=200 NOT referer="-" referer="http://www.telecomunicaciones.gob.ec/wp-login.php" | iplocation clientip | geostats count by clientip

Consumo ancho de banda (últimas 24 horas)

sourcetype=access_combined | eval MB=bytes/(1024*1024) | timechart sum(MB) AS AnchoBanda

Ataques bloqueados

host="10.0.106.2" dstip=10.0.104.238| top limit=20 attack | rename count as Ataques attack as TipoAtaque | fields – percent

2. **Equipo UTM (Fortinet)**

Amenazas por severidad

|tstats summariesonly=true count FROM datamodel=ftnt_fos where nodename="log.utm" log.utm.gseverity!="" log.devname="*" log.vd="*" log.subtype="*" log.srcip="*" log.dstip="*" log.dstport="*" GROUPBY _time log.utm.gseverity | timechart values(count) by log.utm.gseverity

Amenaza por IP de origen

| tstats summariesonly=true count FROM datamodel="ftnt_fos" WHERE nodename="log.utm" log.utm.gseverity!="" log.devname="*" log.vd="*" log.subtype="*" log.srcip="*" log.dstip="*" log.dstport="*" GROUPBY log.srcip | sort -count | head 30

Amenaza por IP de destino

| tstats summariesonly=true count FROM datamodel="ftnt_fos" WHERE nodename="log.utm" log.devname="*" log.vd="*" log.subtype="*"

log.srcip="*" log.dstip="*" log.dstport="*" log.utm.gseverity!=""

GROUPBY log.dstip| sort-count | head 30

Amenazas por usuario

| tstats summariesonly=true count FROM datamodel="ftnt_fos" WHERE

nodename="log.utm" log.utm.gseverity!="" log.user!="" log.devname="*"

log.vd="*" log.subtype="*" log.srcip="*" log.dstip="*" log.dstport="*"

GROUPBY log.user | sort -count | head 20

Ataques contenidos por Fortinet (top 5 todo el tiempo)

host="10.0.106.2"| top limit=5 attack

Ataques contenidos por Fortinet (top 20 últimas 24 horas)

host="10.0.106.2"| top limit=20 attack

Ataques contenidos (últimos 60 minutos limitado a 10 ataques)

host="10.0.106.2"| timechart count by attack limit=10

3. **Antispam**

Total de correos recibidos

sourcetype="mcafee:antispam" | dedup msgid | stats count as Mensajes

Top 10 correos recibidos

sourcetype="mcafee:antispam" NOT From="<>" | dedup msgid| top

limit=10 From | rename count as "Mensajes Recibidos"

Top 10 correos envíados

sourcetype="mcafee:antispam" NOT (to="<>" OR to="<unknown>") | dedup msgid| top limit=10 to | rename count as "Mensajes Enviados"

Correos spam limitados a 20

sourcetype="mcafee:antispam" NOT From="<>" OR subject Undeliverable spam | top limit=20 subject | fields - percent | rename count as "Mensajes SPAM"

Top 10 de correos spam recurrentes en porcentajes

sourcetype="mcafee:antispam" NOT From="<>" OR subject Undeliverable spam | top limit=10 subject | fields - percent

Top 20 **e**stado de correos en porcentajes

sourcetype="mcafee:antispam"| top limit=20 status | fields - percent

Número de correos recibidos por funcionario

sourcetype="mcafee:antispam" NOT From="<>" | dedup msgid | eval correo = From + " -> "+ to| top limit=20 correo | rename count AS CorreoEnviado | fields – percent

Para estas reglas de correlación creadas se configuraron tableros de control (dashboards) para visualizar los eventos de mejor manera, la creación de estos tableros será explicado en el siguiente capítulo.

5.2.2 McAfee ESM

El propósito fundamental del motor de correlación de la herramienta es analizar los datos que fluyen desde el ESM, detectar patrones dentro del flujo de datos, generar alertas que representan estos patrones e insertar estas alertas en el receptor de la base de datos una alerta; el motor de correlación se activa cuando un origen de datos es configurado teniendo en cuenta que sólo una fuente de datos de correlación puede ser configurada por receptor. Una vez que el origen de datos de correlación está configurado, se puede editar el conjunto de reglas de correlación mediante el editor de reglas de correlación. Se permite habilitar o deshabilitar cada regla de correlación y establecer un valor de criticidad de cada regla definible por el usuario.

Dentro de esta herramienta existen dos formas de correlacionar los eventos: la primera mediante el correlacionador propio del aplicativo y la otra según las necesidades que se tenga asociando los eventos que llegan de los dispositivos. Para el primer caso y para que funcione con éxito el correlacionador automático de la herramienta, se necesita que lleguen eventos de muchos dispositivos de la red para que se tenga muchas fuentes de información y se puedan correlacionarse entre ellos.

Para el segundo caso, existen dos formas: la primera tomar los reportes automáticos de eventos que tiene la herramienta y generar alarmas en base a ellos y la segunda configurar las correlaciones necesarias para asociar eventos de las distintas fuentes de datos que llegan a la herramienta según lo que se necesite; esta opción al igual que en Splunk sería la que más ayuda para el análisis de seguridades en una red pero así

mismo es la más difícil de configurar ya que se requieren conocimientos profundos sobre los formatos de los eventos al igual que la configuración en la herramienta.

Para este caso de estudio se realizarán varios ejemplos utilizando los 3 formatos de correlación descritos anteriormente.

5.2.2.1 Correlación automática

Para usar la correlación automática propia de la herramienta es necesario incluir el módulo McAfee correlation engine, mismo que correlaciona automáticamente todos los eventos de las fuentes de datos ingresadas. Solo se puede configurar un origen de datos de correlación en un receptor y el mismo es encargado de analizar los datos que fluyen de un ESM, detectar patrones sospechosos dentro del flujo de datos, generar alertas de correlación que representan estos patrones e insertar estas alertas en la base de datos de alertas del receptor.

La finalidad principal del motor de correlación es analizar los datos que fluyen del ESM, detectar patrones interesantes en el flujo de datos, generar alertas que representen esos patrones e insertar las alertas en la base de datos de alertas del receptor. El motor de correlación se activa cuando se configura un origen de datos de correlación.

Dentro del motor de correlación, un patrón interesante tiene como resultado datos interpretados por una regla de correlación. Una regla de correlación es distinta e

independiente de una regla estándar o de firewall, y dispone de un atributo que especifica su comportamiento. “Cada receptor obtiene un grupo de reglas de correlación de un ESM (grupo de reglas de correlación desplegado), el cual se compone de cero o más reglas de correlación con un conjunto cualquiera de valores de parámetros definidos por el usuario. Al igual que en el caso de los grupos de reglas estándar y de firewall, se incluirá un grupo de reglas de correlación de base en cada ESM (grupo de reglas de correlación básico).” [9]

En la Figura 49, se presentan las reglas de correlación automáticas existentes en la herramienta, para esto hay que ir a la consola de ESM, hacer clic en el icono de inicio rápido **Correlación**  y ahí se abrirá el **Editor de directivas** con el tipo de regla de correlación existente, se puede verificar que todas las reglas de correlación automáticas existentes están activadas.

Figura 49. Reglas de correlación predefinidas de ESM

Una vez que se añadió el dispositivo correlacionador se observó que inmediatamente comienza a trabajar y en menos de dos días detectó un posible ataque, mismo que se describe a continuación.

Tipo de evento: Recon-Possible Probing by a single IP

Descripción: Esta regla detecta la posible actividad de sondeo desde una única dirección IP de origen. El sondeo es el acto de aprender todo lo que pueda acerca de una red de

diseño, los usuarios, sistemas, aplicaciones y debilidades. El tipo más común de palpación es escaneado o de reconocimiento, que se utiliza para la detección de redes. Otras formas de sondeo pueden ser más perjudiciales, tales como diversos ataques de malware. Un gran número de posibles eventos de sondeo se ha detectado procedente de una única dirección IP de origen, esto probablemente significa que un atacante está recopilando información y se prepara para lanzar un ataque a su red.

Acción posible: Inmediatamente bloquear la dirección IP de origen de la comunicación en la red. Si la fuente es local, investigar el host para detectar signos de compromiso. Determinar los patrones de comportamiento del atacante para que pueda ser reconocido o prevenirse en el futuro.

Esta detección busca para múltiples eventos en cualquiera de las siguientes categorías de normalización, que se producen dentro de un período de tiempo especificado: "Recon", "denegación de servicio", "Exploit", "malware", "actividad sospechosa". (Este texto fue tomado de la descripción que da la herramienta para el evento descrito).

Como se observa alguien intentó ingresar a la red del MINTEL sin permiso, por lo que inmediatamente se acogió la recomendación dada por la herramienta de bloquear esas 5 direcciones IP en el equipo de seguridad perimetral Fortinet una vez que se verifiquen que no son IP´s confiables.

Una vez que el correlacionador automático detecte algún posible ataque a la red, será necesario generar alarmas para avisar a la persona encargada de seguridad y que se

tome alguna acción al respecto. La configuración de alarmas en las herramientas será realizada en el capítulo 5.4.

En la Figura 50 se observa el panel gráfico de detección del ataque indicado por el correlacionador automático de la herramienta, donde se observa también la dirección origen y destino del evento así como también los puertos por donde se realizó el ataque.

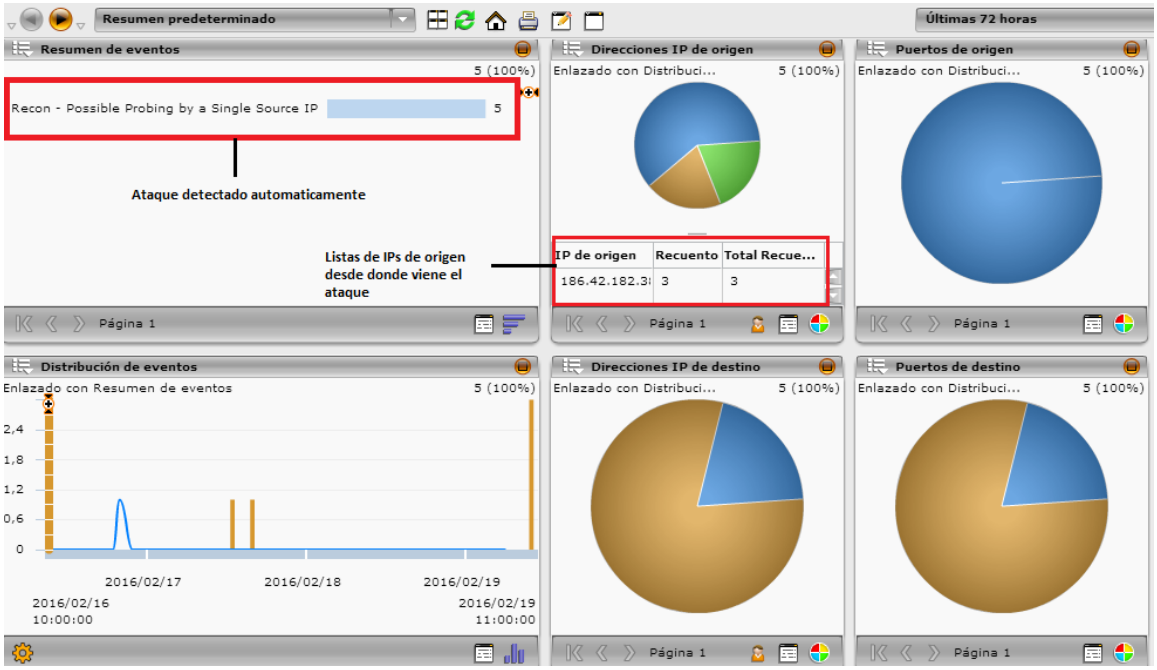


Figura 50. Panel gráfico del correlacionador automático de ESM

5.2.2.2 Reportes de eventos generados por la herramienta

Al seleccionar alguno de las fuentes (dispositivos) de eventos añadidos en la herramienta, se da un resumen de los eventos da cada uno de ellos, así como también tableros gráficos de direcciones IP origen-destino, puertos de origen-destino y una distribución de los eventos. En la Figura 51 se presenta la captura de la pantalla al seleccionar el equipo de seguridad Fortinet.

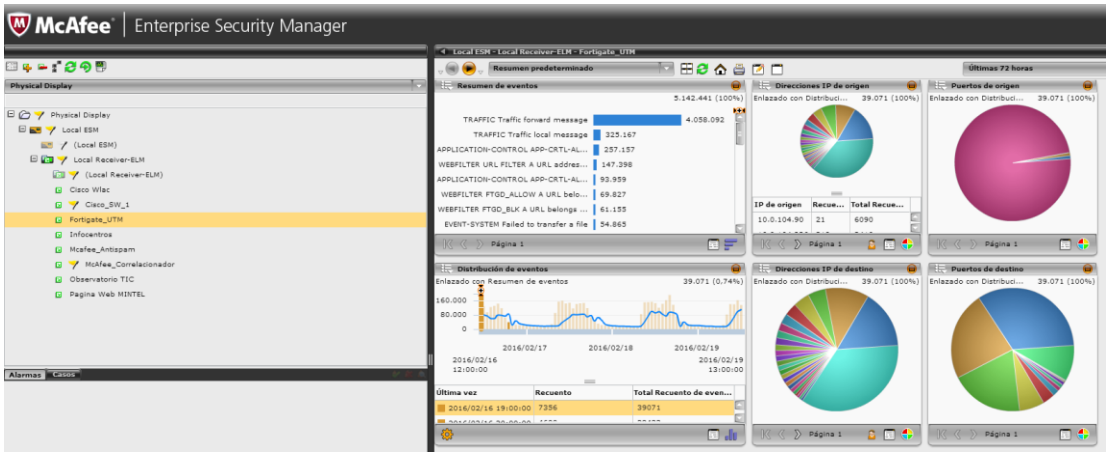


Figura 51. Pantalla de paneles gráficos de eventos para el equipo Fortinet

Además se puede seleccionar cada evento de la lista **resumen de eventos** y ver en detalle los paneles de direcciones origen-destino, puertos de origen-destino y distribución de eventos. En la Figura 52 se indica la pantalla que sale al seleccionar el evento **Traffic local message.**

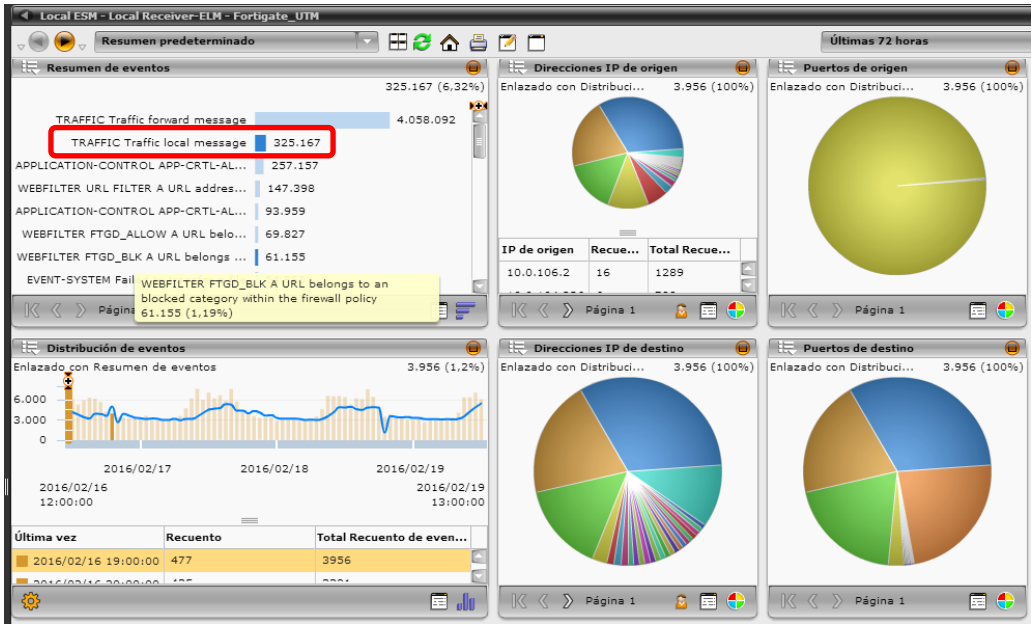


Figura 52. Pantalla de ejemplo al seleccionar el evento Traffic local message

Otra forma de ver reportes de eventos en la herramienta, es seleccionar en la barra de herramientas de vistas, una de las vistas predefinidas que se tiene. A continuación se detallan los diferentes tipos de vistas predefinidas que vienen con ESM tomadas de la Guía de producto de ESM [9]:

• Las vistas de Activo, amenaza y riesgo: da un resumen de los datos de activos, amenazas y riesgos, así como su posible efecto sobre el sistema.

• Vistas de conformidad: ayudan a simplificar las actividades de conformidad con normativas.

• Vistas de panel: proporcionan una descripción general de aspectos específicos del sistema.

• La vista Estado del dispositivo muestra el estado de los dispositivos seleccionados en el árbol de navegación del sistema. Si se hace clic en un dispositivo de la vista, la información de estado sobre el dispositivo seleccionado aparece en la mitad inferior de la vista.

• Búsqueda de ELM mejorada proporciona capacidad de rastreo en tiempo real del progreso de la búsqueda y los resultados. Esta vista solo está disponible si existe un ELM en el sistema.

• Las Vistas de eventos desglosan la información generada por eventos asociados con el dispositivo seleccionado en el árbol de navegación del sistema.

• Las Vistas ejecutivas proporcionan una descripción general de aspectos del sistema de mayor interés para empleados ajenos al departamento de TI.

• Las Vistas de flujo desglosan la información registrada sobre cada flujo (o conexión) que se realiza mediante Nitro IPS.

• McAfee Event Reporter incluye vistas específicas para varios productos de McAfee.

• Las Vistas de riesgo se utilizan con el administrador predeterminado de ACE-Advanced Correlation Engine. A fin de ver correctamente los datos en los administradores personalizados, es necesario crear vistas personalizadas.

• Entre las Vistas de flujo de trabajo de evento se incluyen las vistas siguientes:

- Alarmas activadas: permite ver y administrar las alarmas que se han activado al cumplirse las condiciones de alarma.
- Administración de casos: ver y administrar los casos del sistema.

Dentro de las vistas descritas una de la más importante es la vista: activo, amenaza y riesgo. Para llegar a esta vista se da clic en **resumen predeterminado** en la barra de herramientas, se selecciona **activo, amenaza y riesgo** y se despliega tres opciones: resumen de amenazas de activos, resumen de amenazas recientes y resumen de vulnerabilidades. En la Figura 53 se indica cómo se debe seleccionar este tipo de reportes.

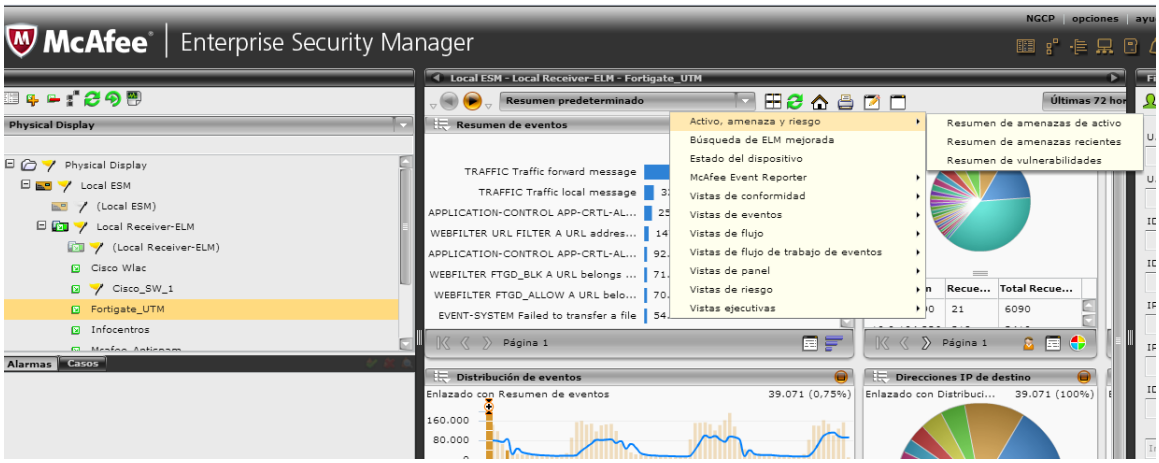


Figura 53. Pantalla para selección de vista de activo, amenaza y riesgo

En la Figura 54. se indica la pantalla que sale al seleccionar la opción **resumen de amenazas más recientes**, donde se puede observar el top de las amenazas recientes, amenazas por proveedor y protección frente a amenazas de producto entre las principales.

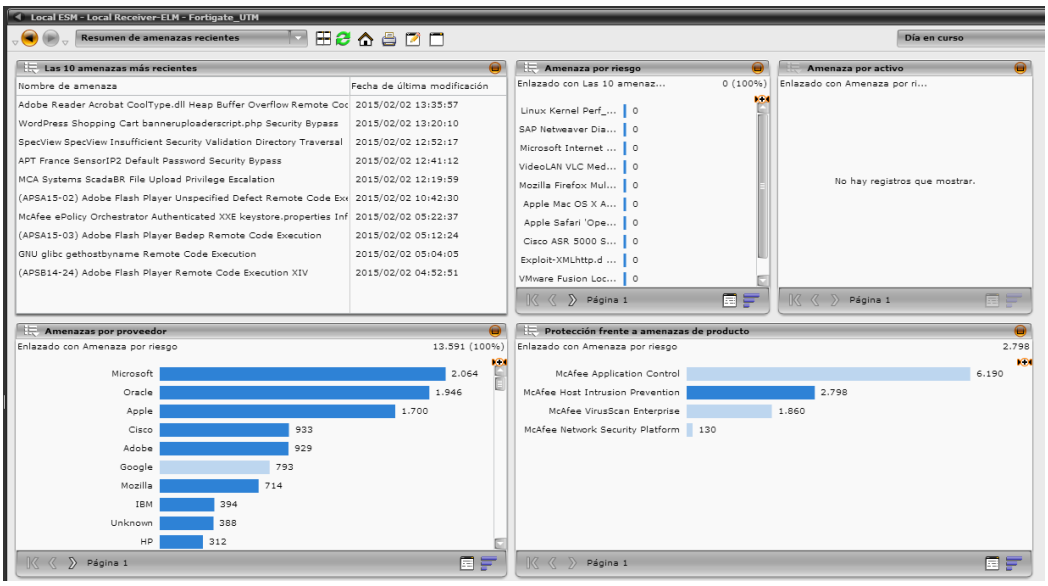


Figura 54. Pantalla de resumen de amenazas recientes

Otra vista que puede ayudar mucho es la opción **análisis de eventos**, donde se puede ver los eventos de origen de un evento de correlación, estos eventos se pueden visualizar de cualquiera de las fuentes de eventos añadidos en la herramienta. Por ejemplo para ver los orígenes de eventos del motor de correlación automático se realiza los siguientes pasos:

- En el árbol de navegación del sistema, se selecciona el receptor y se da clic en **McAfee Correlacionador**
- En la lista de vistas, se da clic en **Vistas de eventos** y se selecciona **Análisis de eventos.**
- En la vista **Análisis de eventos**, se da clic en el signo más **(+)** en la primera columna junto al evento de correlación.

Hay que destacar que solo aparecerá el signo + si el evento de correlación tiene eventos de origen al realizar los pasos descritos. En la Figura 55, se muestran los eventos origen del evento **Possible Probing by a single source IP**, que se explicó anteriormente y fue detectado automáticamente por el correlacionador de la herramienta.

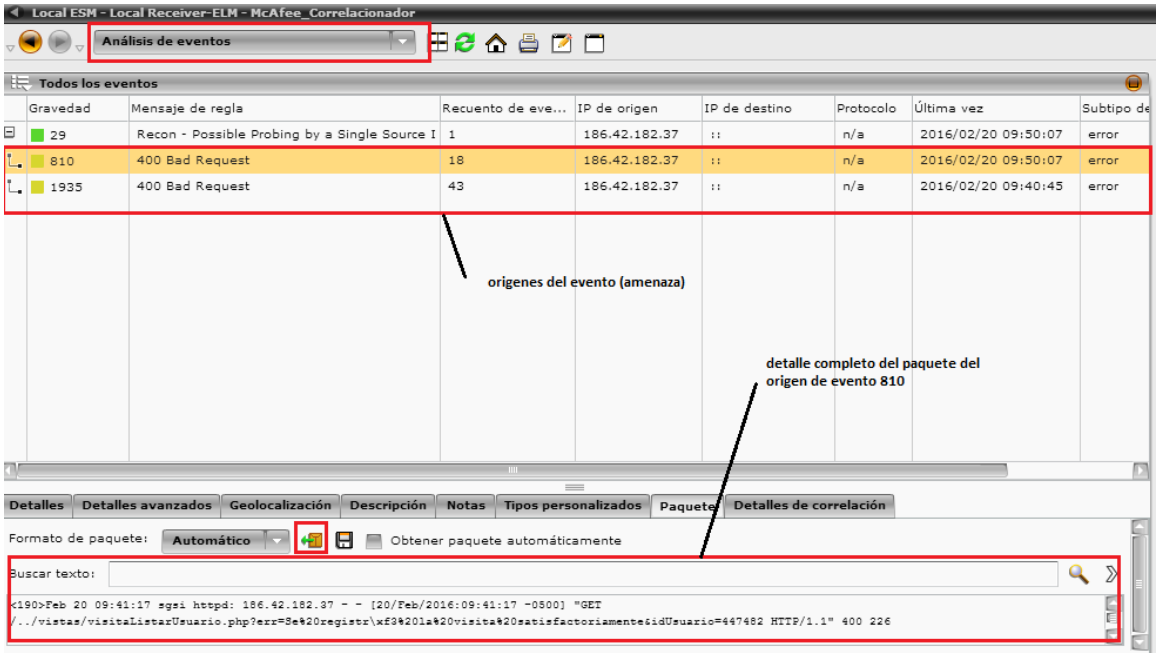


Figura 55. Pantalla de análisis de eventos de ESM

Además se puede obtener el detalle del paquete de los eventos de origen, para esto se selecciona el evento y en las opciones inferiores se escoge paquete y se da clic en recuperar paquete  y se mostrará todo el detalle del paquete del evento en bruto (algo parecido a lo que obtiene Splunk directamente), en la Figura 55 se indica el detalle del paquete del evento origen 810.

Otro parámetro importante de los eventos es el ID de firma, mismo que servirá para hacer reglas manuales de correlación y creación de alarmas, esto se lo puede ver dentro de la pestaña de **detalles.**

En la Figura 56, se presenta otro ejemplo de análisis de eventos, en este caso se seleccionó el dispositivo Fortinet y se escogió la opción **análisis de eventos**, se puede observar que en esta ocasión los eventos del dispositivo no tienen eventos de origen, pero como se observa en la parte inferior de la figura se podrá ver los detalles del paquete de cualquiera de los eventos, al igual que el caso anterior.

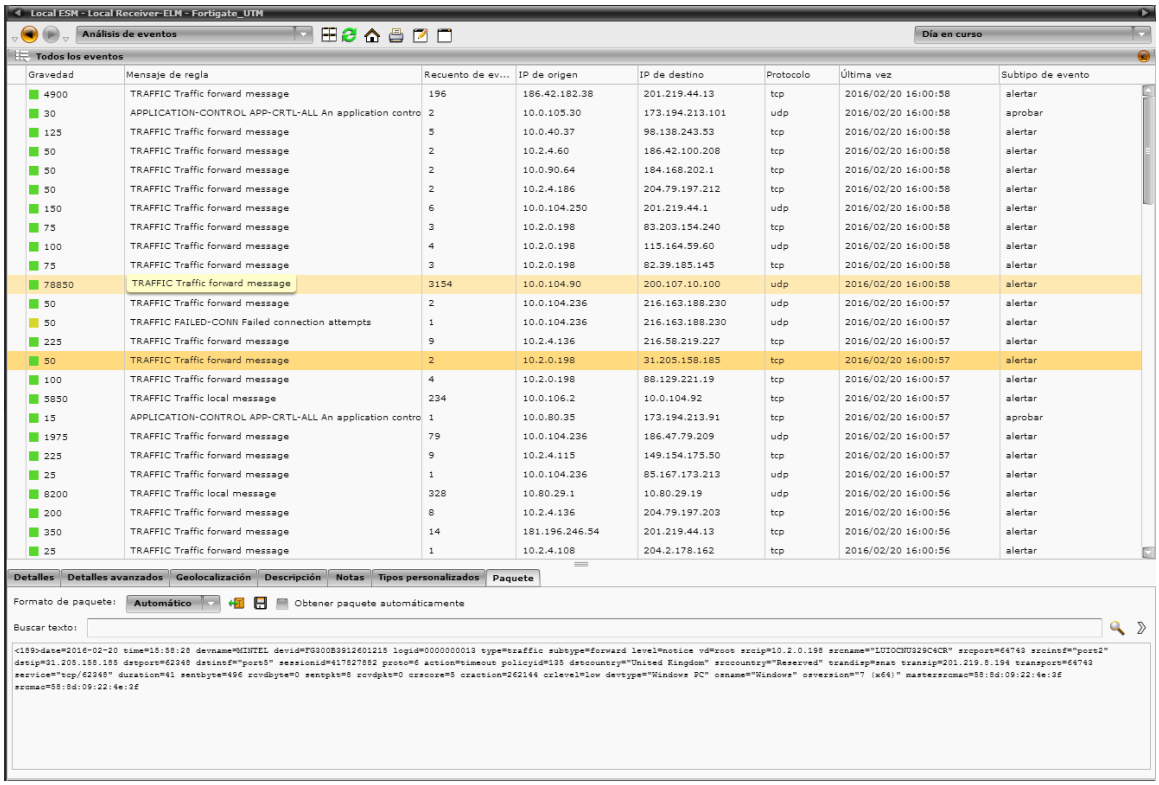


Figura 56. Pantalla análisis de eventos para el equipo Fortinet

Dentro de la misma opción de vistas de eventos, se puede seleccionar por fuente de eventos, la opción **eventos por gravedad**. Se desplegarán cuatro pantallas en las cuales se tienen datos de: total de gravedad, direcciones IP de origen-destino y distribución de los eventos. Así como en los demás casos de puede seleccionar una de las

gravedades y visualizar los datos relacionadas solo con esta. En la Figura 57 se indica lo que se obtiene al seleccionar el dispositivo McAfee antispam y eventos por gravedad. Cabe señalar que en cualquiera de las vistas que procesa la herramienta se puede seleccionar el tiempo de análisis, teniendo opciones como: último minuto, últimos 10 minutos, día en curso, día anterior, semana en curso, semana anterior, etc., con los eventos que son tomados de la base de datos que tiene ESM.

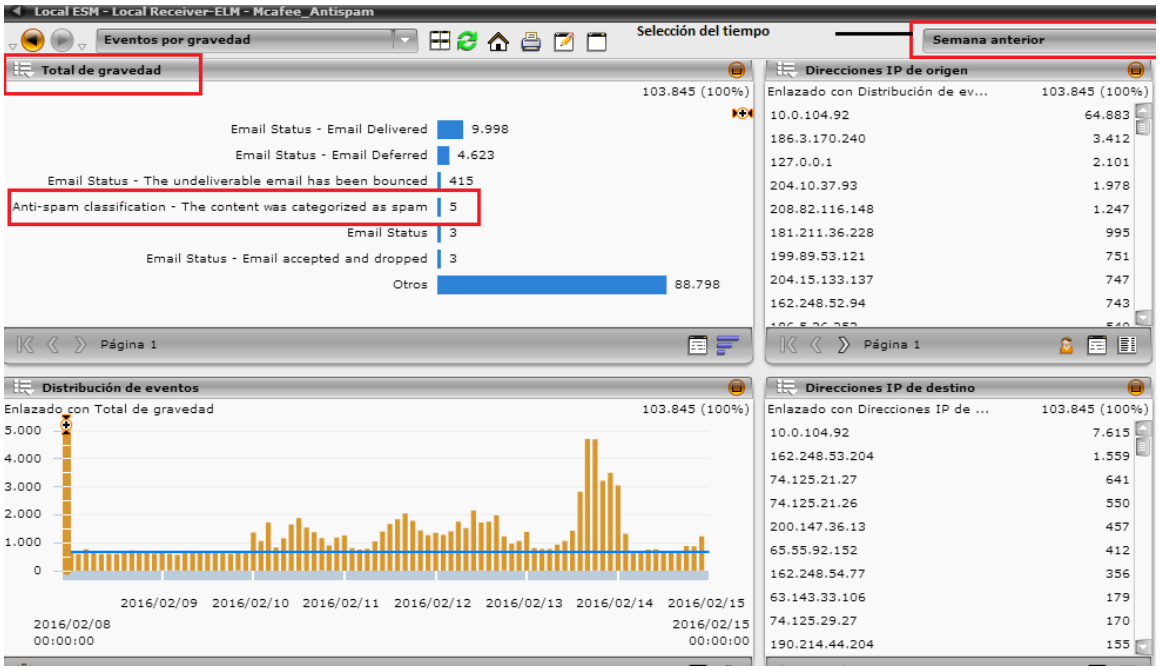


Figura 57. Pantalla de eventos por gravedad del equipo Antispam

Tanto en Splunk como en ESM, se puede realizar una consulta geo referenciada de los eventos de alguno de las fuentes de datos añadidos a la herramienta, para esto en la misma opción de **vista de eventos**, se debe seleccionar **Geolocalizacion de destino de origen de eventos** y se visualizará los orígenes de eventos por país, un resumen de eventos normalizado y la geo localización de origen (con 3 opciones: por país,

provincia/estado y ciudad), en la Figura 58 se presenta la geolocalización para el dispositivo McAfee Antispam.

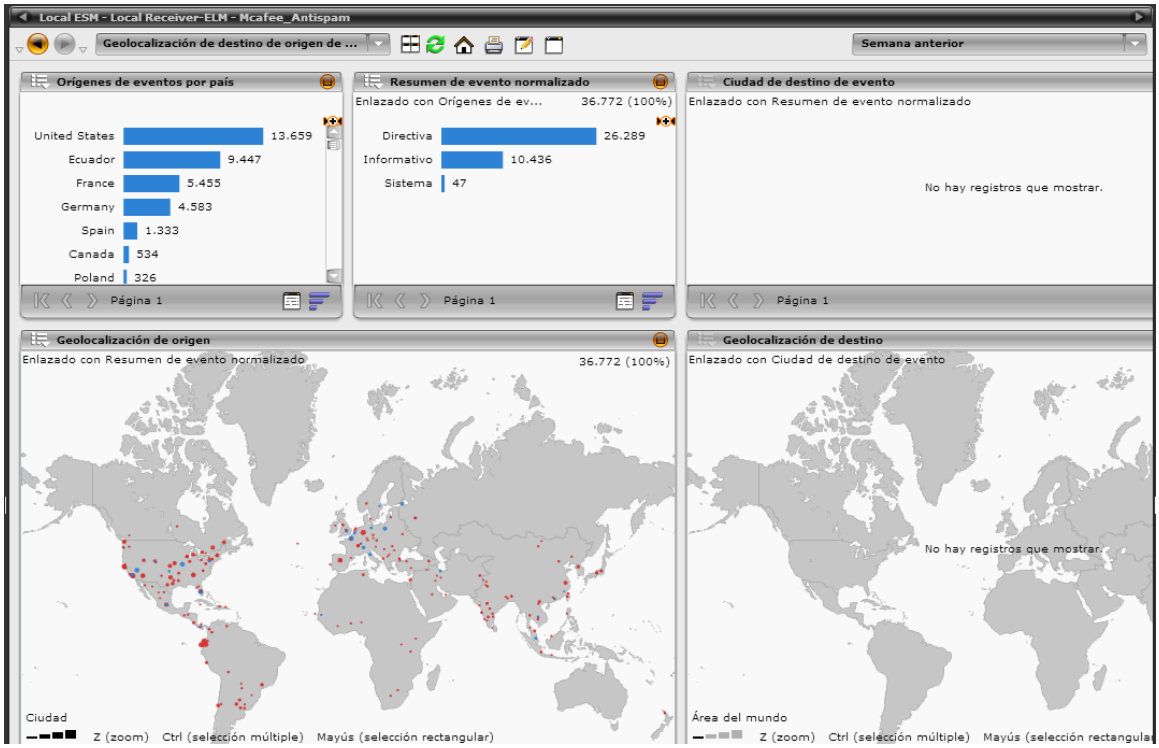


Figura 58. Pantalla de geolocalización de destino de origen de eventos del equipo antispam

Por último para cada fuente de datos, dentro de la opción **vista de eventos**, se puede seleccionar **rastreo de usuarios-usuario origen**, que sirve para visualizar las conexiones georreferenciadas de cierto usuario asignado como fuente de origen. En la Figura 59, se presenta las pantallas que salen al escoger como fuente de datos al Fortinet de la institución

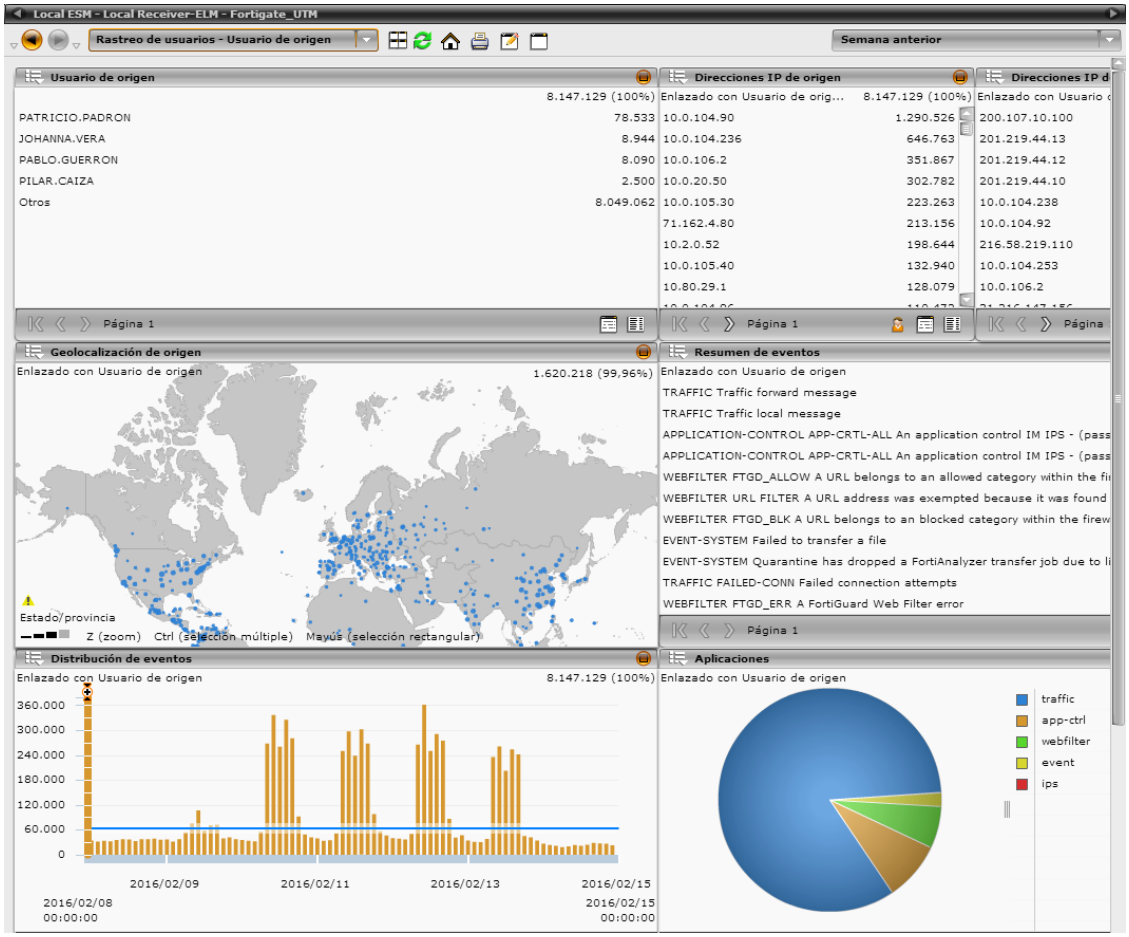


Figura 59. Pantalla de rastreos de usuario-usuario origen del equipo Fortinet

5.2.2.3 Correlación manual creando reglas

Para la correlación manual, al igual que en Splunk, se necesita analizar los eventos que llegan de los dispositivos para poder relacionarlos entre ellos y generar una correlación con el fin de alertar cuando suceda el evento que pueda comprometer a la seguridad de la red.

Para este caso de estudio, se realizaron algunos casos de uso (correlaciones) analizando los eventos que llegaban a la herramienta de las distintas fuentes de datos descritas anteriormente.

Se crearon los siguientes casos de uso para posteriormente obtener las reglas de correlación:

Caso 1:

Fuente 1: Fortinet (tráfico malicioso, tráfico mal formado) – Por IP, Puerto, Protocolo

Fuente 2: Servidores web incluidos (acceso exitoso, fallido, errores de acceso) – Por IP, Puerto, Protocolo

De la Fuente 1 se tomará el tráfico malicioso, tráfico mal formado, etc. (Por IP, Puerto, Protocolo) y se relacionará con la Fuente 2 de acceso a sitio web exitoso, fallido y con errores (Por IP, Puerto y Protocolo), con esto se verificara si el tráfico que es y no detenido por el Fortinet está accediendo o intentando acceder a los servidores de aplicaciones web.

Caso 2:

Fuente 1: Fortinet (tráfico de salida y entrada malicioso, navegación a páginas bloqueadas) – Por IP, Puerto, Protocolo

Fuente 2: Antispam (Correos spam, bloqueos, correos maliciosos, entrada y salida) – Por IP, Puerto, Protocolo

De la Fuente 1 se tomará el tráfico malicioso, tráfico de navegación bloqueado, etc (Por IP, Puerto, Protocolo) y se relacionará con la Fuente 2 de envío y recepción de Spam,

correos bloqueados, maliciosos, etc, de entrada y salida (por IP), con esto se verificará si las IP´s que son detenidas su tráfico por el Fortinet son las mismas que las que envían SPAM o correo malicioso.

Caso 3:

Fuente 1: Fortinet (Tráfico normal de entrada y salida) – Por IP, Puerto, Protocolo

Fuente 2: Antispam (correos enviados y recibidos) – Por IP, Puerto, Protocolo

De la Fuente 1 se tomará el tráfico normal de Fortinet, tráfico de navegación, etc (Por IP, Puerto, Protocolo) y se relacionará con la Fuente 2 de envío y recepción de Correos, de entrada y salida (por IP), con esto se verificará las IP´s que navegan y envían y reciben correos.

Para verificar las reglas de correlación creadas se da clic en el icono **correlación**  en la barra de navegación del sistema y se despliega una pantalla como el de la Figura 60, para ver las reglas de correlación creadas y las automáticas se selecciona dentro de DEM, la opción **Correlación**.

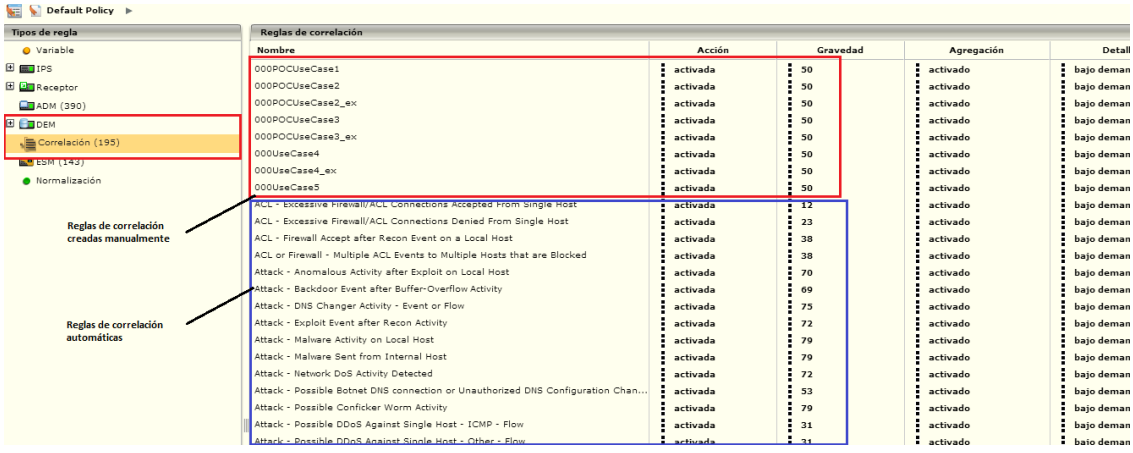


Figura 60. Reglas de correlación: creadas y por defecto de la herramienta

Para crear una nueva regla de correlación se siguen los siguientes pasos:

- Dentro del editor de directivas se selecciona el dispositivo para crear una nueva regla, en este caso se seleccionará **Correlación** para crear una regla de correlación.
- En la pestaña nueva, se selecciona nueva regla de correlación y se llenan los siguientes datos:
    - Nombre: nombre de la regla
    - Severidad: para seleccionar la severidad , se puede escoger del 1 al 100, siendo 100 la máxima severidad
    - Etiquetas: para seleccionar etiquetas que definen la categoría a la cual la regla pertenece
    - Agrupar por: crea una lista de campos para que los eventos puedan ser agrupados para cuando entran al motor de correlación.
    - Parámetros: personaliza las instancias de un componente de regla y reutilización.
    - AND, OR, SET: arrastra y suelta en el área de la lógica de correlación para establecer la lógica de la regla.
    - Descripción: adicionar una descripción de la regla.
- Se crea la nueva regla usando los operadores lógicos o el SET arrastrándolos al panel de configuración.
- Para la creación de la regla se lo puede hacer con los ID de firma de los eventos que llegan al ELM, esto lo recomienda McAfee.

En la Figura 61 se presentan las pantallas de los pasos descritos arriba.

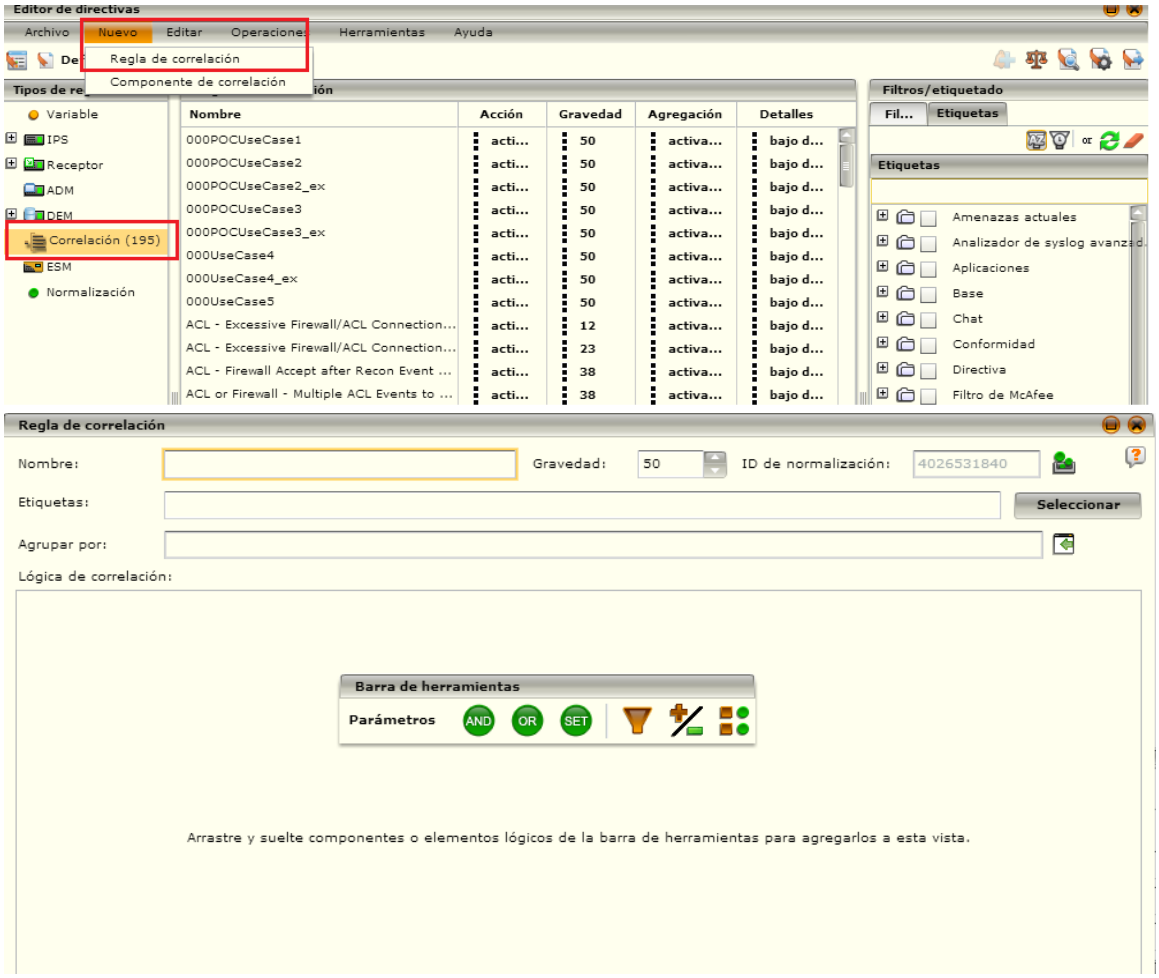
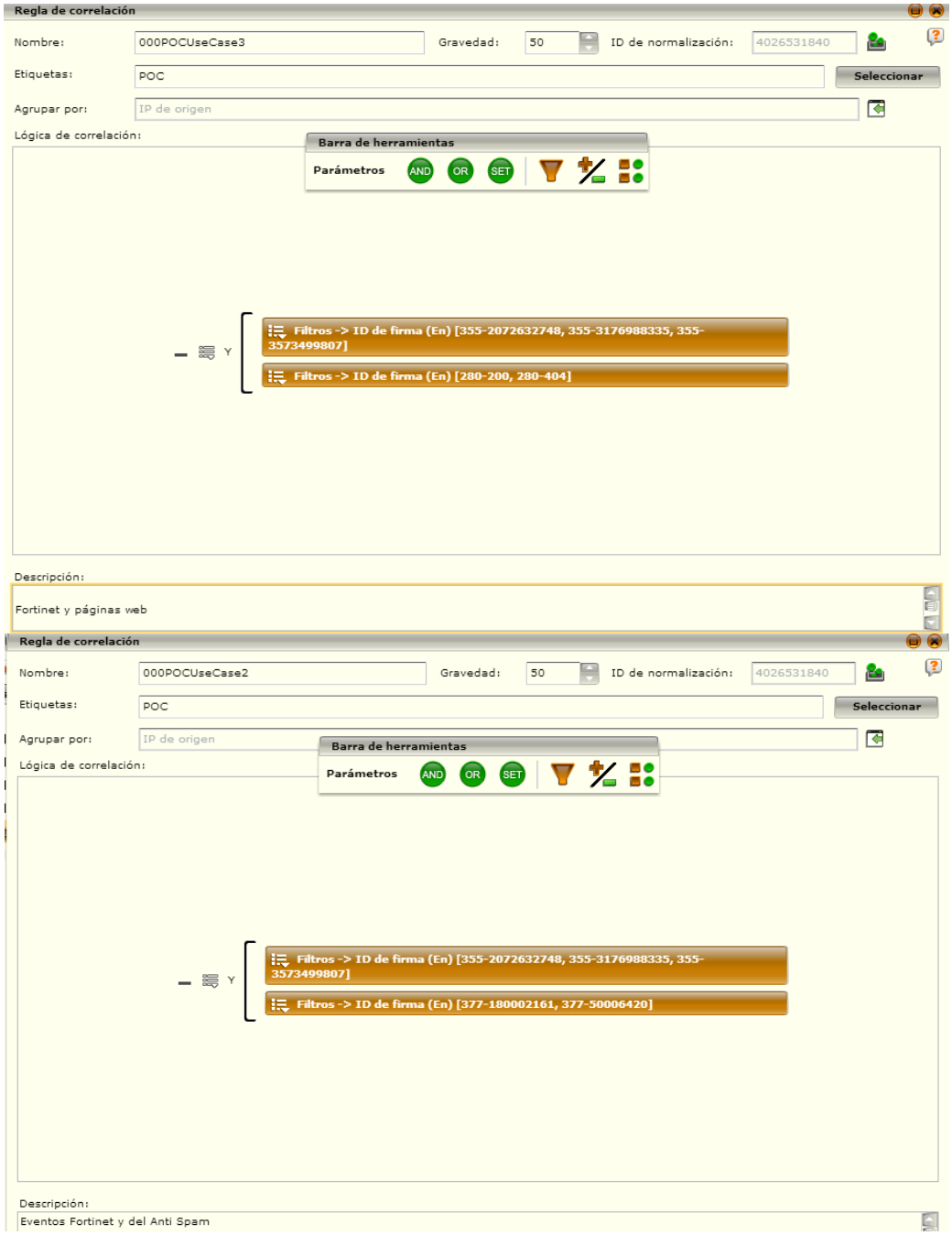


Figura 61. Pantallas para la configuración de una regla creada manualmente

En la Figura 62, se presentan todas las reglas creadas manualmente para los 3 casos de uso descritos anteriormente.


Regla de correlación
Nombre:
000POCUseCase3
Gravedad:
50
ID de normalización:
4026531840
Etiquetas:
POC
Seleccionar
Agrupar por:
IP de origen
Lógica de correlación:
Barra de herramientas
Parámetros
AND
OR
SET
Y
Filtros -> ID de firma (En) [355-2072632748, 355-3176988335, 355-3573499807]
Filtros -> ID de firma (En) [280-200, 280-404]
Descripción:
Fortinet y páginas web
Regla de correlación
Nombre:
000POCUseCase2
Gravedad:
50
ID de normalización:
4026531840
Etiquetas:
POC
Seleccionar
Agrupar por:
IP de origen
Lógica de correlación:
Barra de herramientas
Parámetros
AND
OR
SET
Y
Filtros -> ID de firma (En) [355-2072632748, 355-3176988335, 355-3573499807]
Filtros -> ID de firma (En) [377-180002161, 377-50006420]
Descripción:
Eventos Fortinet y del Anti Spam

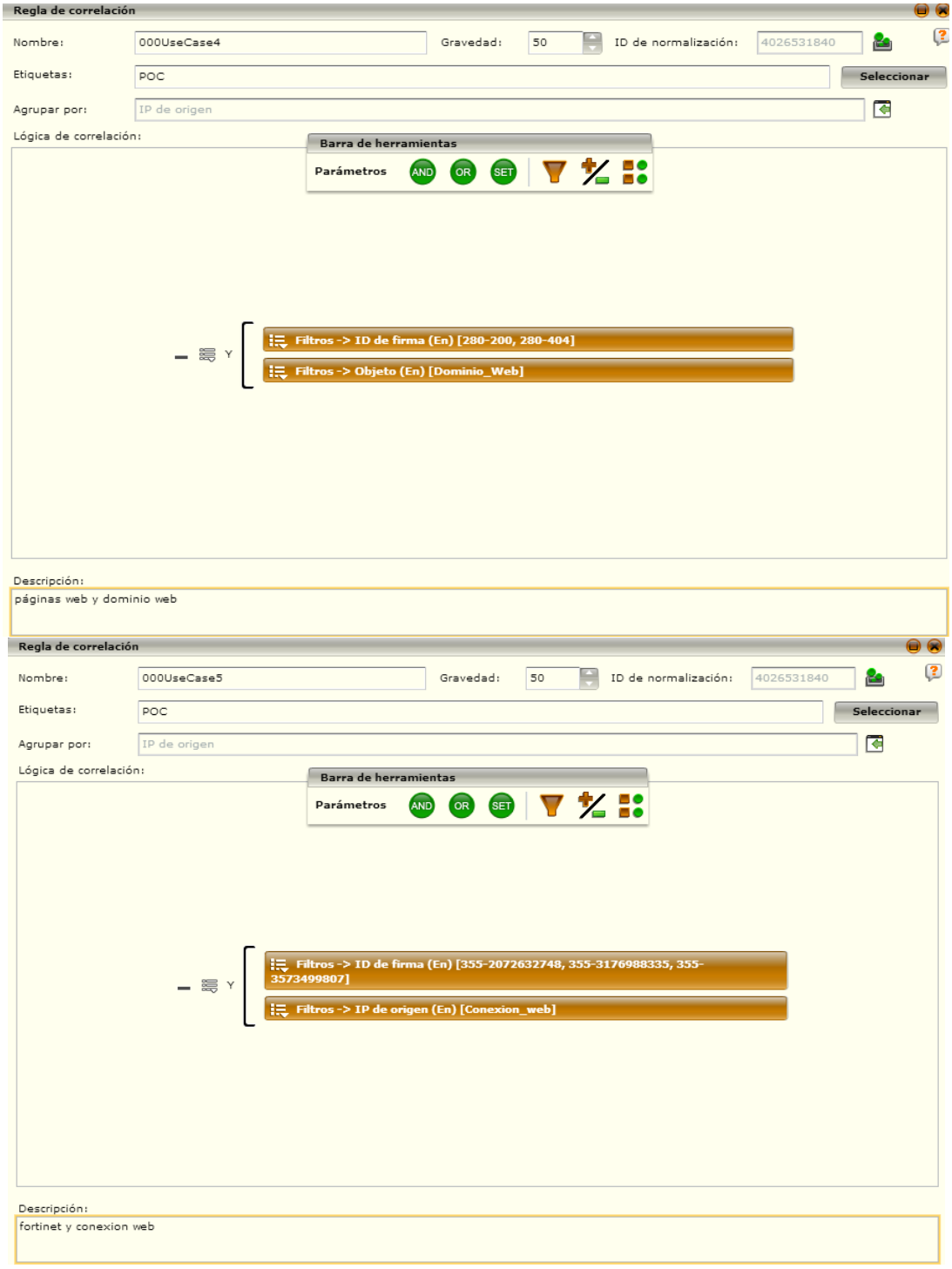


Figura 62. Creación de reglas de correlación manuales para los casos de uso

Una vez creadas las reglas de correlación se pueden generar alarmas que alerten tanto en el navegador de la herramienta o con un sonido o también enviando mails a usuarios configurados en el ESM. En la Figura 63 se indica dónde está el ID de la regla creada ya que con este identificativo será más fácil crear una nueva alarma cuando suceda esa regla de correlación.

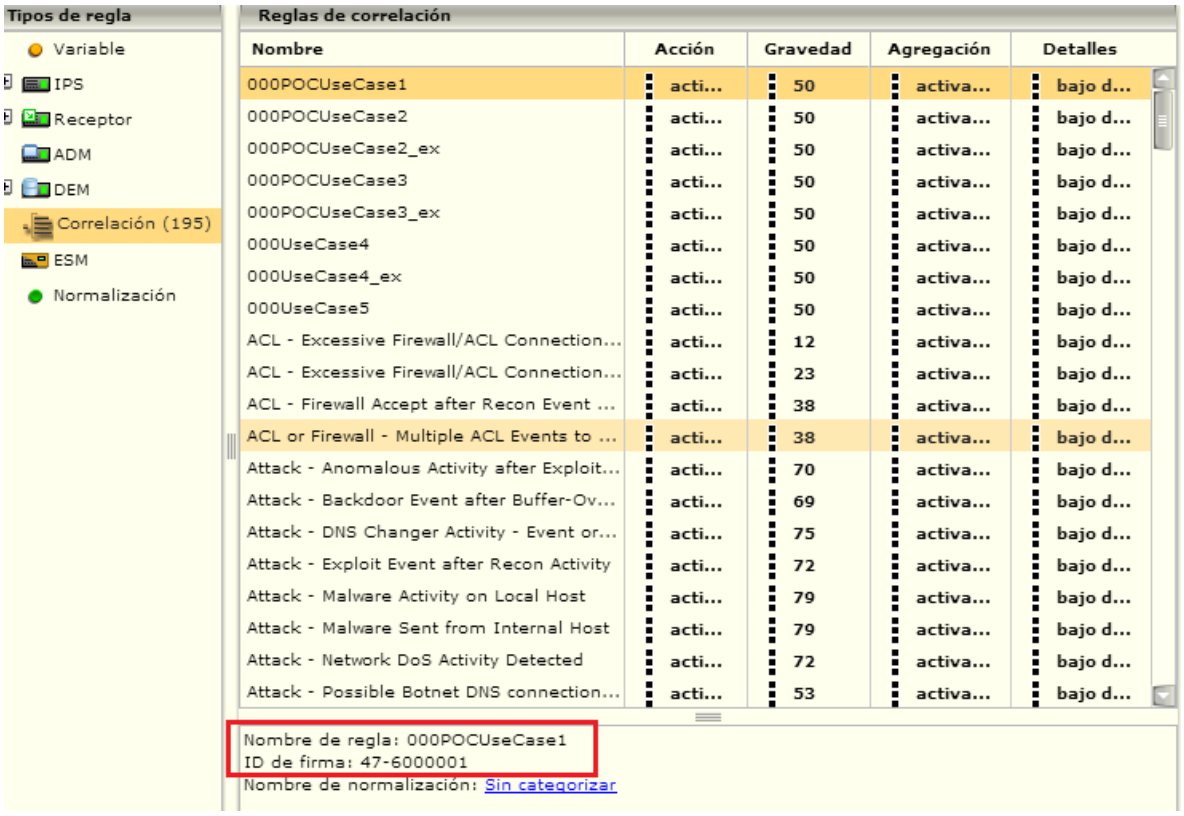


Figura 63. Ubicación del ID de firma de una regla de correlación

5.2.3 AlienVault USM

USM tiene muchas opciones para obtener datos de la red a más del correlacionador propio que ya viene instalado en la herramienta. Dispone de un SIEM incluido para obtener eventos normalizados y también eventos en bruto, para los eventos normalizados se los puede filtrar por varias categorías en diferentes líneas de tiempo o también agrupa eventos de cierto tipo para poder analizarlos.

USM ayuda a las empresas para monitorizar los cambios en el panorama de las amenazas sin mucha dificultad ya que proporciona conocimientos sobre seguridad, mediante la automatización del proceso de correlación de eventos, para esto tiene los siguientes componentes:

- Recopilación de datos: identificación de los datos de los logs para su importación e integración automática, tanto desde las tecnologías incluidas en la plataforma USM como desde herramientas de terceros mediante la instalación de plugins, algunos ya vienen en la herramienta predefinidos y otros si no existen se puede solicitar a AlienVault la creación de uno nuevo, esto demora entre 1 semana a 10 días en crearlos. Además si se tiene conocimiento en desarrollos de plugins se los puede crear uno mismo para el caso de aplicaciones personalizadas o dispositivos antiguos siguiendo el instructivo que se encuentra en la página web de AlienVault.

- Normalización: como se indicó la herramienta normaliza los eventos que llegan desde los diferentes activos por lo que se puede analizar, normalizar e integrar datos de logs en el motor de análisis integrado del SIEM.
- Correlación: la herramienta en su versión completa, posee más de 2000 reglas de correlación de activos, vulnerabilidades, red, tráfico y datos de amenazas.
- Alarmas: evaluación de la severidad y priorización de alertas, con instrucciones detalladas de remediación sensible al contexto
- Detección de amenazas emergentes: actualizaciones automáticas de nuevas reglas de correlación y firmas para nuevas amenazas y vulnerabilidades.

La principal diferencia que se tiene con otras herramientas es que casi no es necesario escribir nuevas reglas de correlación o realizar una investigación para esto como sucedió con Splunk o ESM, además en los laboratorios de AlienVault se realizan continuas actualizaciones incluyendo nuevas directivas de correlación. De ser necesario la herramienta entrega la posibilidad de crear nuevas reglas de correlación en caso que se desee tener una directiva particular a partir de algún análisis previo que la misma herramienta puede arrojar.

Adicionalmente la herramienta permite detectar amenazas más recientes y con las opciones que tiene se puede crear alarmas y casos para corregirlos, inclusive algunas veces se da la solución para corregir la vulnerabilidad o amenaza detectada gracias a su conexión directa con OTX, el cual es una gran base de datos de eventos de seguridad y

amenazas de AlienVault que es alimentada por los mismos usuarios o por los laboratorios de la empresa.

Para ver los informes provenientes de las reglas de correlación que vienen por defecto con la herramienta, se tiene que ir a la sección de informes y ahí se puede encontrar las directivas de correlación expuestos en forma de informes. En la Figura 64 se presenta la forma de encontrar estos informes.

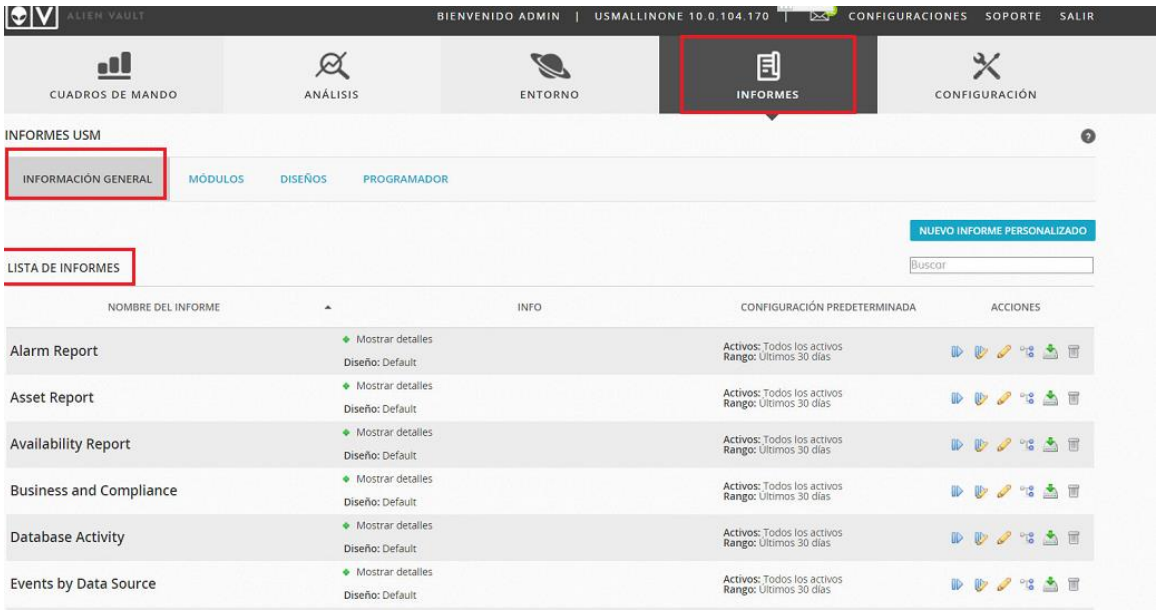


Figura 64. Informes de directivas de correlación de USM

Para editar un informe de una regla se da clic en el lápiz  y con esto se puede observar que eventos intervienen para la regla seleccionada. En la Figura 65 se puede observar como ejemplo de una regla de correlación el informe de **malware alarms**, teniendo que para esta regla intervienen los eventos: malware alarms-lista, malware

alarms – top alarmas, salto de página, malware alarms-mapa, malware alarms-top equipos atacantes y malware alarms-top equipos atacados. Además se puede seleccionar un rango de fechas para el análisis, teniendo algunas opciones de tiempo como: semana actual, hoy, ayer, últimos 30 días, etc. y también se puede configurar para que estos informes estén disponibles para ciertos usuarios que lo necesiten.

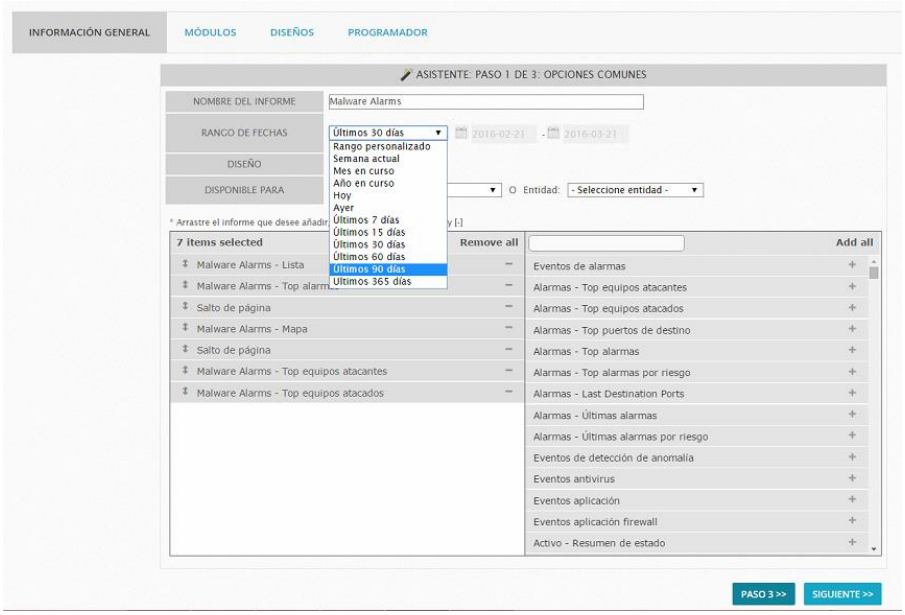


Figura 65. Edición de directiva de malware alarms

Además se puede encontrar para que activos se aplicaría el informe para esta regla teniendo que para las reglas por defecto están siempre seleccionados todos los activos. En la Figura 66 se presenta esta opción.

Figura 66. Pantalla de selección de activos de la directiva malware alarms

Siguiendo con la explicación de los informes, en la pestaña de **módulos** se puede encontrar los 2631 módulos de informes disponibles. En la Figura 67 se presenta la pantalla que se despliega al dar clic en módulos.

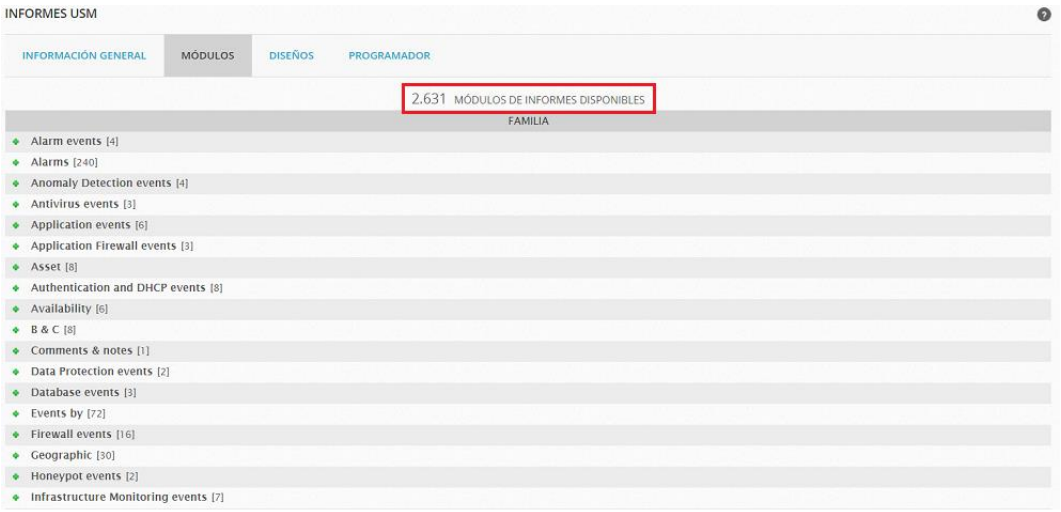


Figura 67. Pantalla de módulos de informes de la herramienta

En la siguiente pestaña de **diseño** se pueden personalizar estos informes incluyendo logos de la empresa, colores de las fuentes, del fondo, etc. En la Figura 68 se

presenta la opción de diseños del informe en donde al dar clic en el lápiz se pueden modificar los parámetros que vienen por defecto.

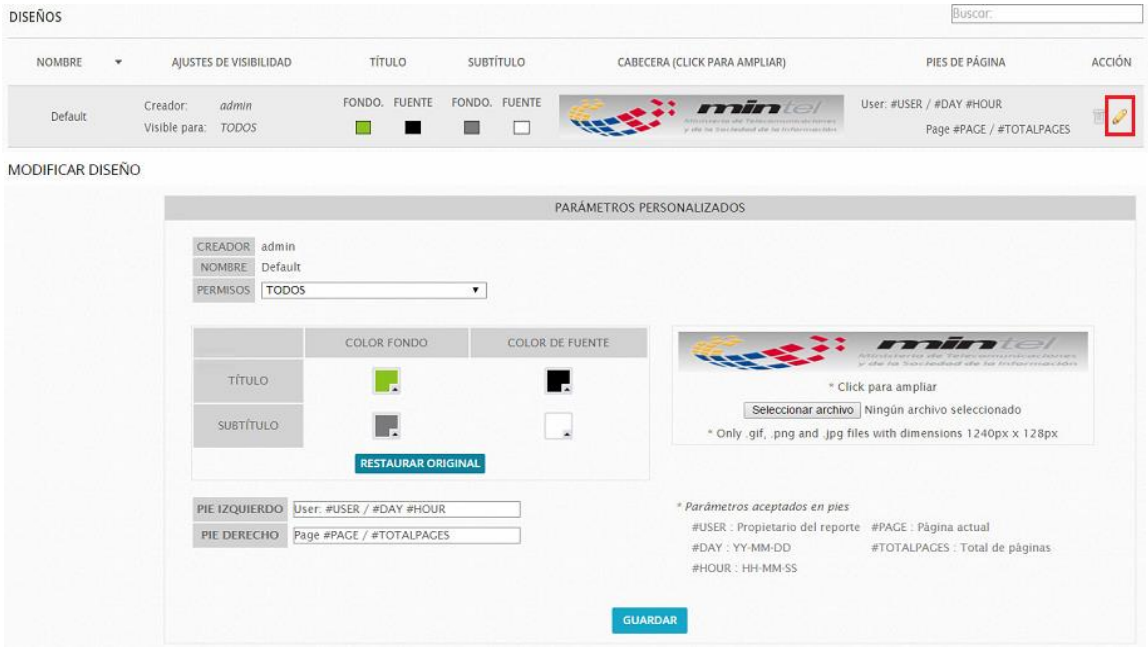


Figura 68. Pantalla para modificar el diseño de los informes

Para terminar en la última pestaña **programador**, se puede añadir programar un informe con el fin de que estos puedan llegar por ejemplo vía correo electrónico al personal de seguridad para que pueda tomar acciones inmediatas en caso que se detecte alguna amenaza o ataque de las reglas de correlación por defecto que vienen con la herramienta.

En la Figura 69 se presentan las programaciones de informes realizadas como demo.

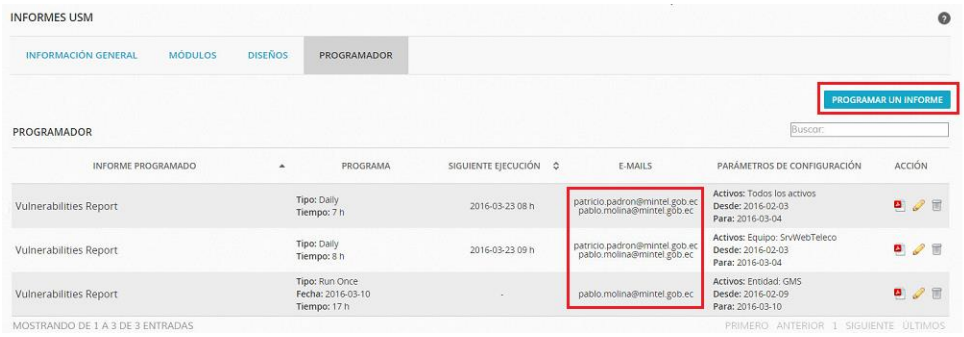


Figura 69. Pantalla de programaciones de informes realizadas para el caso de estudio

En la parte superior derecha de la Figura 69 se tiene la opción de programar un informe, en donde se puede visualizar la forma de seleccionar las directivas para el reporte, los mails a donde debe llegar, la periocidad de entrega del informe, los activos a los cuales se va a aplicar la directiva y por ende de donde se obtendrán los eventos para la elaboración automática del informe.

Cabe señalar que mientras más activos estén correctamente ingresados en la herramienta, llegarán más eventos con los cuales se obtendrán datos para los informes, ya que de no suceder los eventos pertenecientes a un informe simplemente el documento saldrá en blanco. En la Figura 70 se indican con recuadros en rojo las opciones de configuración para programar un informe.

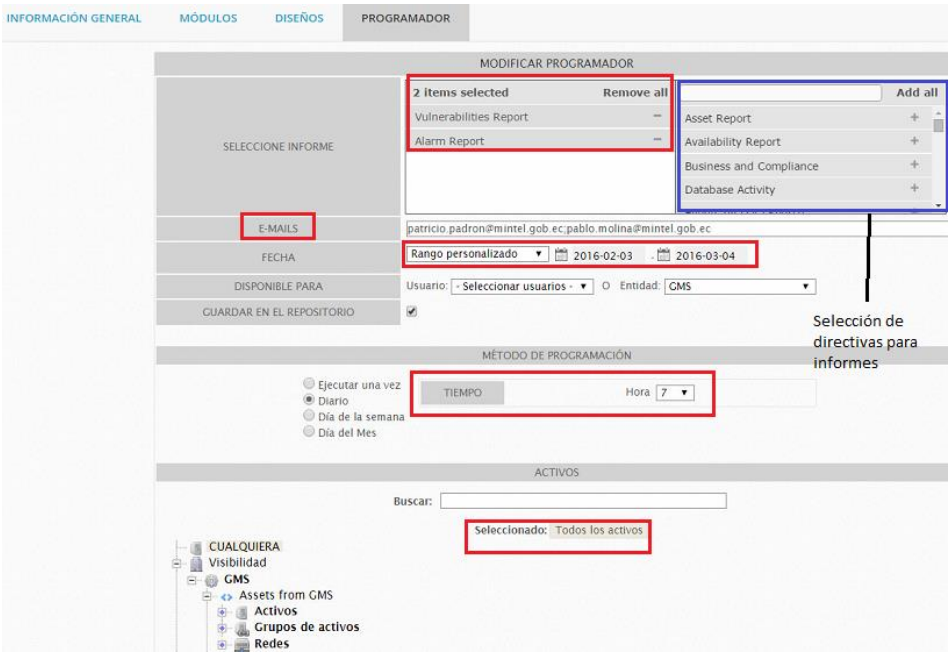


Figura 70. Pantalla con opciones para programar un informe

Una vez explicado las opciones para los informes de correlación, a continuación de explicarán las directivas de correlación que vienen por defecto en la herramienta, para verlas se debe ir a la pestaña de **configuración** y dar clic en **Info. sobre amenazas** y escoger la opción **directivas**, se puede visualizar todas las directivas de correlación pre definidas que tiene la herramienta, son en total 2813 directivas en el sistema subdivididas en algunas categorías, cabe indicar que las directivas de correlación por defecto no pueden ser modificadas, pero si se desea modificarlas se puede realizar un clon de ellas y personalizarlas con los ajustes que se necesiten. En la Figura 71 se puede visualizar todas las directivas que tiene USM.

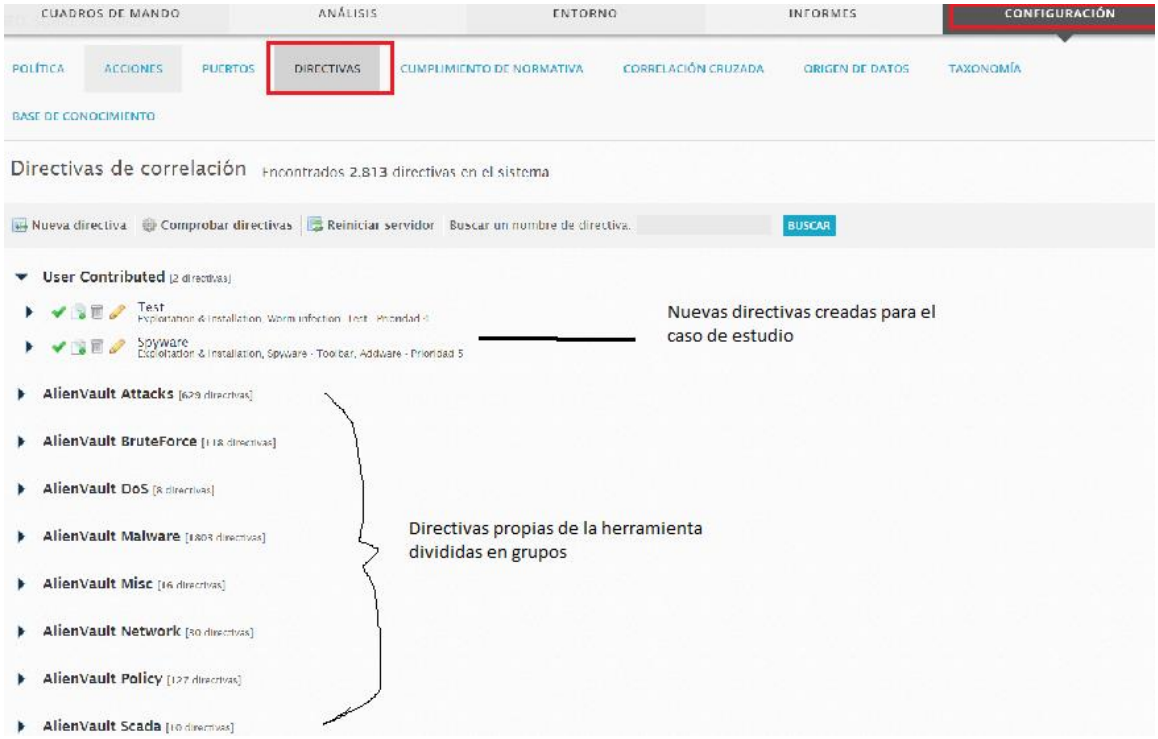


Figura 71. Lista de directivas de correlación de la herramienta

Para crear una nueva directiva de correlación dentro de la misma pestaña de directivas se selecciona **nueva directiva**, se da nombre a la directiva y se llena la taxonomía de datos como: propósito, estrategia y método de la directiva y una prioridad en escala del 0 al 5, siendo 5 la de mayor prioridad. En la Figura 72 se visualiza los datos iniciales a ser llenados para la nueva directiva de correlación, una vez llenados todos los datos se da clic en siguiente.

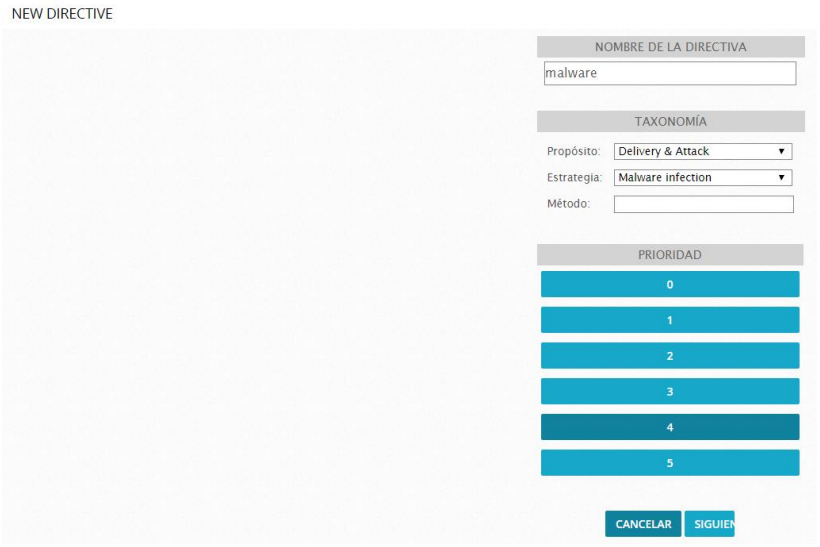


Figura 72. Pantalla inicial de creación de una nueva directiva de correlación

En la siguiente pantalla se da un nombre a la directiva de correlación, en la Figura 73 se visualiza la pantalla y para continuar se da clic en siguiente.

Figura 73. Pantalla para poner nombre a la directiva de correlación

A continuación se selecciona los tipos de eventos o taxonomía de entre algunas que proporciona la herramienta, con esto el aplicativo insertará un nuevo plugin. Si se deja vacía la selección, la herramienta escogerá cualquier tipo de producto. En la Figura 74 se presenta la pantalla y para continuar se da clic en siguiente.

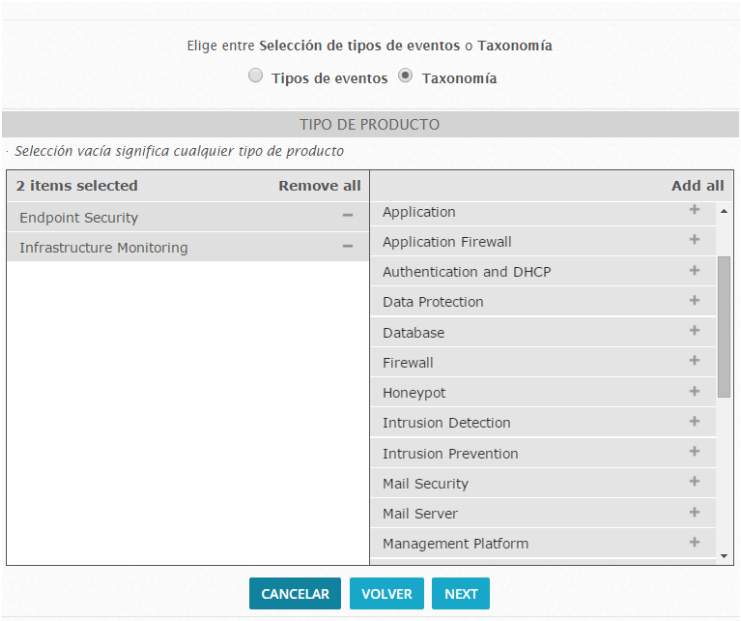


Figura 74. Pantalla para seleccionar los tipos de eventos y productos de la directiva de correlación

A continuación se seleccionarán los activos tanto de origen como de destino para los cuales se aplicará esta directiva de correlación, si se deja vacío significará cualquier activo. En la Figura 75 se visualiza esta pantalla y para continuar se da clic en siguiente.

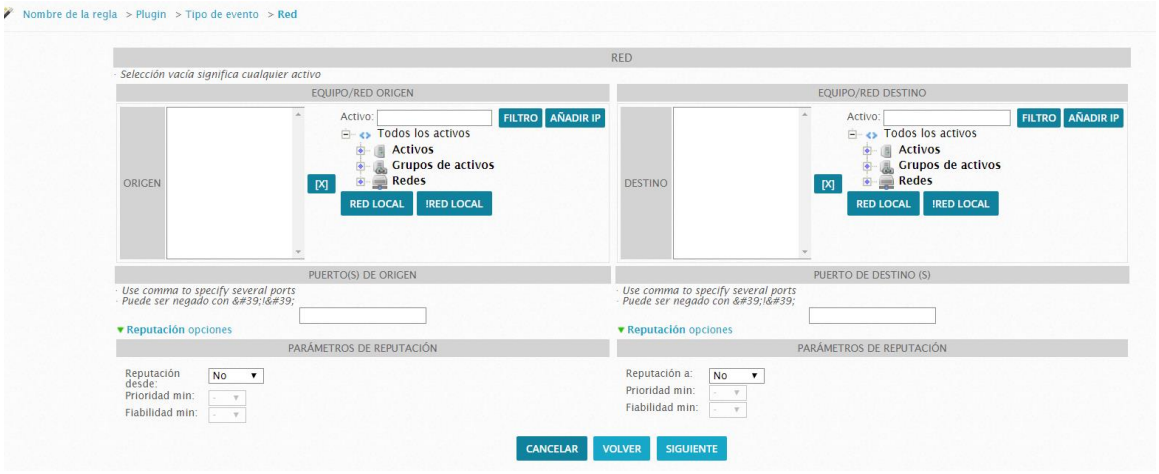


Figura 75. Pantalla para seleccionar los activos que intervendrán en la directiva de correlación

Y por último se la da una categoría de fiabilidad para la nueva directiva. En la Figura 76 se presenta la pantalla de fiabilidad y luego se da clic en siguiente y la regla se termina de crear completamente.

Figura 76. Pantalla de fiabilidad de la directiva de correlación

Como ejemplos del caso de estudio se crearon 3 nuevas reglas de correlación que se detallan como sigue:

- para detectar algunas amenazas del tipo spyware y de botnet en la red (2).
- para ver si el ingreso a los principales servidores de las aplicaciones web del MINTEL se lo está haciendo por las personas autorizadas (1).

En la Figura 77 se presentan las 3 reglas o directivas de correlación creadas.

Figura 77. Lista de directivas de correlación creadas como ejemplo del caso de estudio

5.3 Tableros de control

Todas las herramientas seleccionadas en este caso de estudio tienen la opción de crear tableros de control (dashboards) de los eventos que llegan de las diferentes fuentes de datos, algunas de estas tienen tableros predefinidos como ESM y USM. En este capítulo se presentará la forma de crear nuevos tableros de control, usar los que ya vienen predefinidos y además se presentará algunos tableros de información de ataques, amenazas y vulnerabilidades al oficial de seguridad de la información de la institución.

5.3.1 Splunk

Para esta herramienta hay algunas formas de crear tableros de control, entre las más usadas se describirán dos:

1) Grabar una búsqueda como un tablero: para crear un tablero usando este método se da clic en **New Search** y se buscan las fuentes de eventos de seguridad que se necesiten o la correlación deseada usando el lenguaje SPL para que con los datos obtenidos se cree el tablero. Como ejemplo se buscará el top 20 de los ataques realizados y detectados por el equipo Fortinet, para esto se coloca en la ventana de búsqueda la sintaxis que cumpla con lo indicado, se da clic en el botón de búsqueda y se desplegarán todos los eventos que coincidan con esto, en la Figura 78 se presenta la pantalla al realizar la búsqueda.

	attack	count	percent
1	TCP.Out.Of.Range.Timestamp	6647	72.478465
2	SMTP.Local.Overflow	1089	11.874387
3	HTTP.Null.Session	235	2.562425
4	Joomla.Core.Session.Remote.Code.Execution	201	2.191691
5	WordPress.Slider.Revolution.File.Inclusion	173	1.886381
6	HTTP.Unknown.Tunnelling	134	1.461127
7	China.Chopper.Webshell.Client.Connection	109	1.188529
8	TCP.Overlapping.Fragments	88	0.959546
9	Bash.Function.Definitions.Remote.Code.Execution	81	0.883219
10	Muieblackcat.Scanner	70	0.763276
11	SSH.Client.Request.Mimicking	65	0.708756
12	ZmEu.Vulnerability.Scanner	60	0.654236
13	HTTP.Request.Smuggling	48	0.523389
14	SMTP.Unknown.Command	34	0.370734
15	TCP.Inconsistent.Retransmssion	19	0.207175
16	HTTP.URI.SQL.Injection	19	0.207175
17	Traceroute	13	0.141751
18	MS.IIS.File.Extension.Processing.Security.Bypass	9	0.098135
19	WordPress.xmlrpc.Pingback.DoS	8	0.087231

Figura 78. Búsqueda en Splunk para equipo Fortinet

En esta pantalla se da clic en la pestaña de **visualization** y se selecciona la forma como se desea presentar los datos obtenidos, se tiene como opciones gráficos en forma de barras, de pie, etc... En la Figura 79, se presenta la pantalla que sale al escoger el tablero en forma de pie.

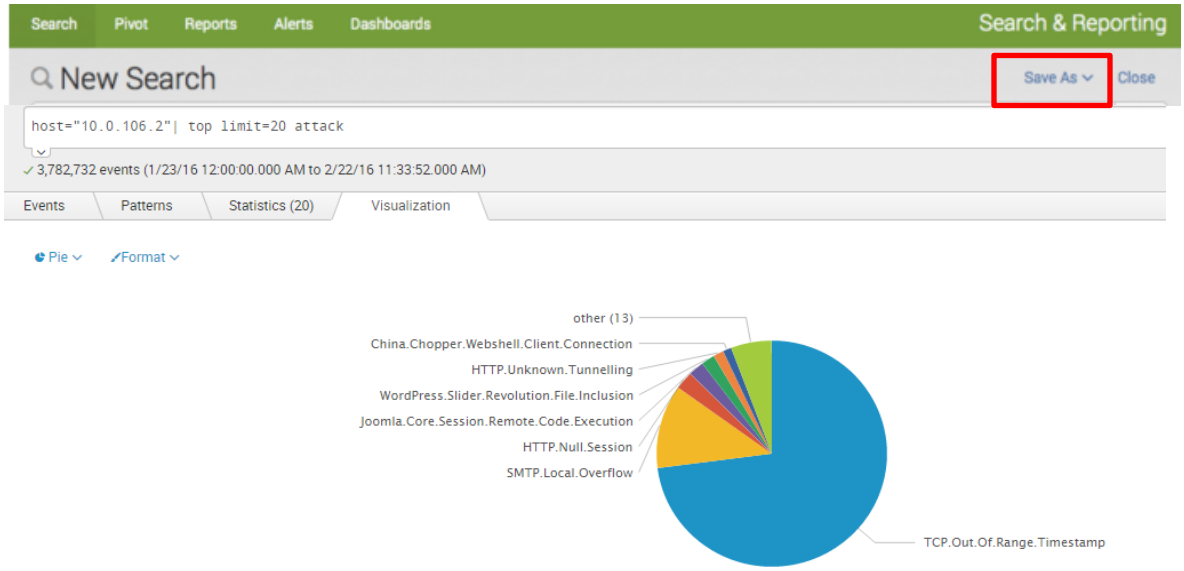


Figura 79. Tablero de ataques recibidos por el equipo Fortinet

Una vez obtenido el gráfico, se da clic en **Save as** y se selecciona **Dashborad Panel**, como se indica en la Figura 80.

Figura 80. Pantalla para grabar los datos de la búsqueda como un panel gráfico

Posteriormente se abrirá una caja de dialogo en la cual se define los datos del nuevo panel de control, con las opciones de crear uno nuevo o adicionar a un tablero ya existente. Además se deben llenar los datos como: título del tablero, un ID, una descripción, si el tablero será privado o se desplegará en todos los apps

creados, título del panel, etc. y por último dar clic en **save**. En la Figura 81 se indican las opciones de creación del tablero de control.

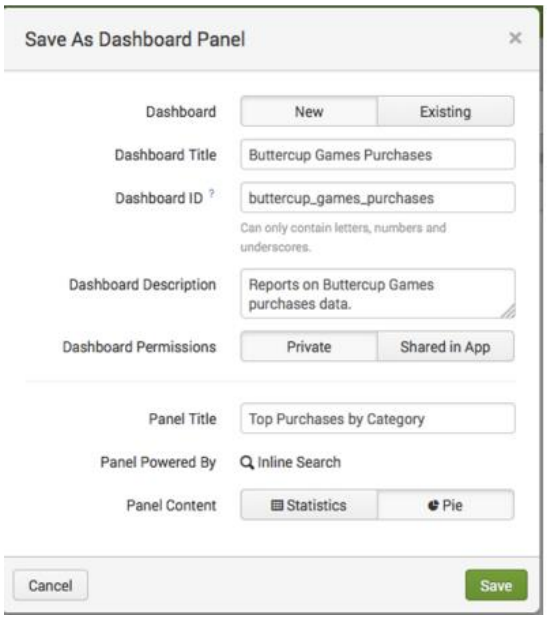


Figura 81. Opciones para llenar en la creación de un tablero gráfico

Hay como adicionar entradas a los tableros de control creados, por ejemplo entre las principales entradas de tiempo, de texto, de múltiple selección. La más usada es la entrada de tiempo, con la cual se selecciona el tiempo de visualización de los datos en el tablero de control, teniendo varias opciones, en la Figura 82 se presentan todas las opciones al seleccionar la entrada tiempo.

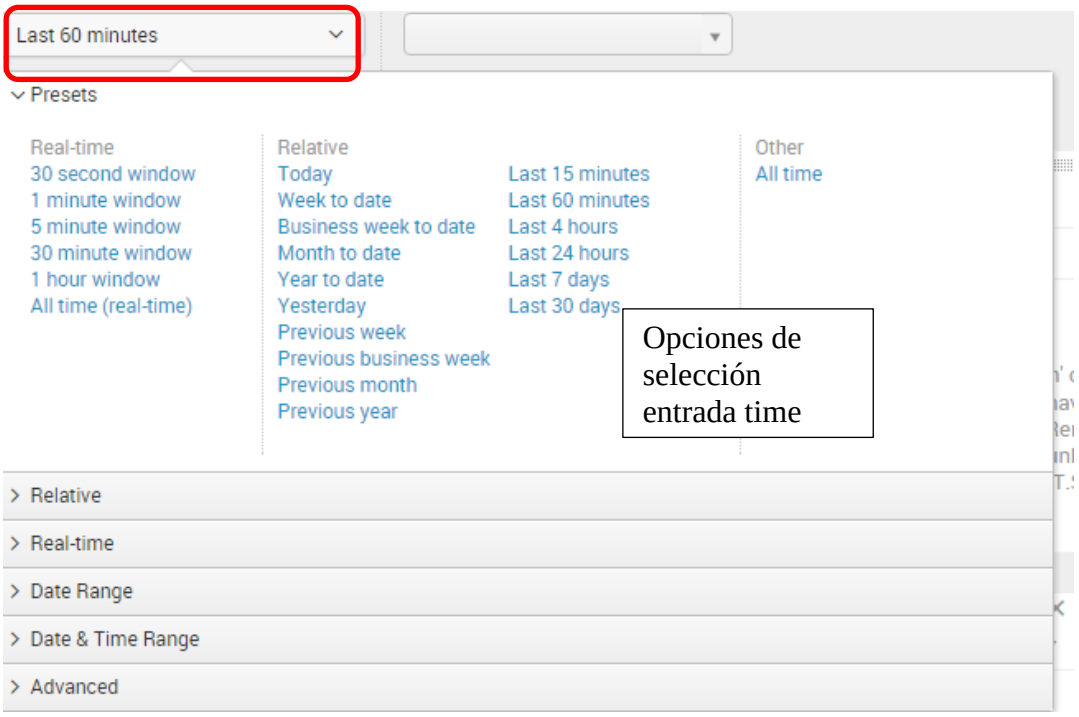


Figura 82. Entrada de tiempo con sus opciones de selección para un tablero

2) La segunda forma es añadir paneles a tableros de control ya creados, para esto en la opción de **edit** del tablero de control se selecciona la opción **edit panels,** y después **add panel** y se despliega un nuevo menú en el cual se selecciona **New from Report,** al realizar esto aparecerá otra pantalla con todos los paneles que se hayan creado y se tengan disponibles. Se selecciona uno de ellos y se da clic en **Add dashboard** y el nuevo panel formará parte de todo ese tablero de control. En la Figura 83 se indica los pasos a seguir para adicionar un panel a un tablero de control ya creado.

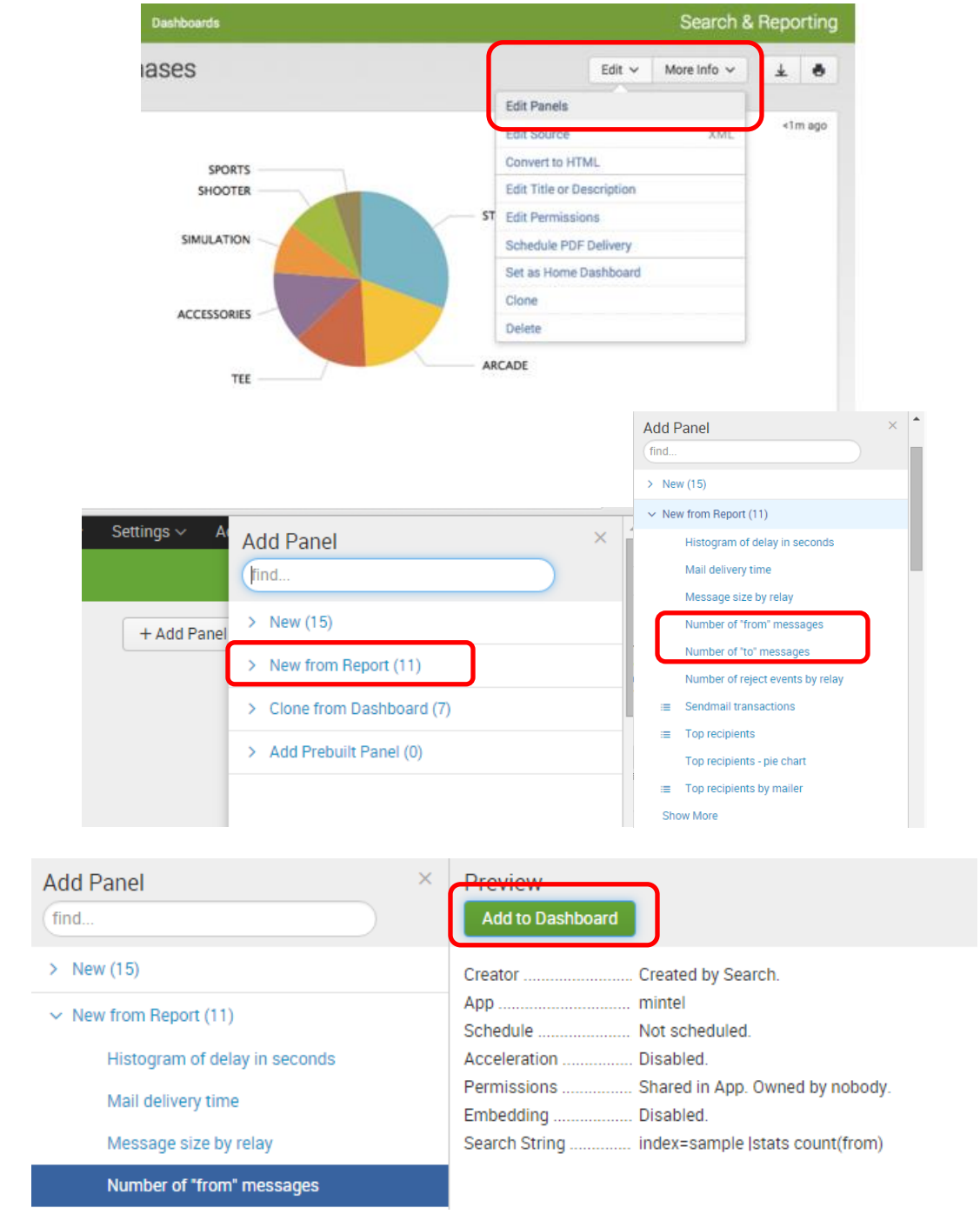


Figura 83. Creación y adición de un panel a un tablero de control existente

Como dato adicional, en la parte inferior de cada panel existen 4 opciones: búsqueda (search), exportar (export), inspeccionar (inspect) y refrescar (refresh)

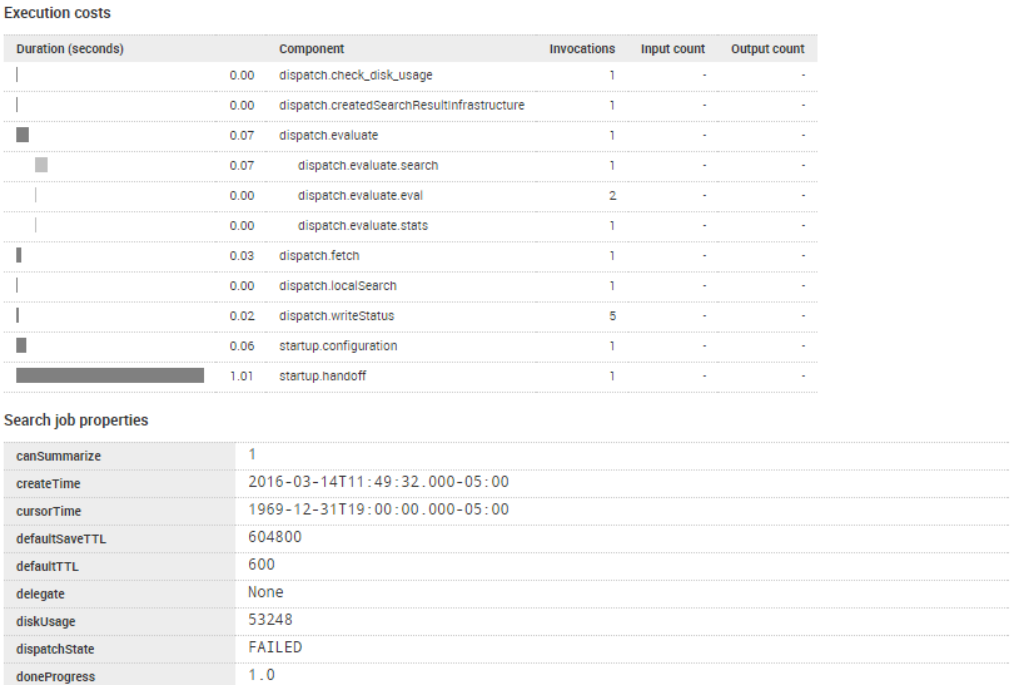
Búsqueda: Al dar clic en búsqueda,  se visualiza la sintaxis del lenguaje SPL para la creación de ese panel y además 4 pestañas en orden de izquierda a derecha para obtener eventos (en bruto), los patrones, las estadísticas y la visualización. En la Figura 84 se presenta la pantalla que se despliega al dar clic en búsqueda de uno de los paneles del equipo Fortinet.

Figura 84. Pantalla de búsqueda en un panel del equipo Fortinet

Exportar: se pueden exportar los datos de los paneles en 4 formatos diferentes: eventos brutos, formato CSV, formato XML y formato JSON. Para esto se da clic en el botón

exportar , se selecciona el formato de datos que se desee teniendo en cuenta que se puede limitar el número de resultados.

Inspeccionar: el Inspector de trabajo de búsqueda muestra dos paneles diferentes. Los costos de ejecución muestran información acerca de los componentes de la búsqueda y cómo cada componente tiene mucho impacto sobre el rendimiento global de la búsqueda. Cuando termina la búsqueda, el inspector de trabajo indicará cuántos resultados encontrados y el tiempo que se tardó en completar la búsqueda, también indica mensajes de error en la parte superior de la pantalla en caso de haberlos, para acceder a esta inspección se da clic en . En la Figura 85 se visualiza la pantalla después de dar clic en inspeccionar.



Execution costs

Duration (seconds)		Component	Invocations	Input count	Output count
	0.00	dispatch.check_disk_usage	1	-	-
	0.00	dispatch.createdSearchResultInfrastructure	1	-	-
	0.07	dispatch.evaluate	1	-	-
	0.07	dispatch.evaluate.search	1	-	-
	0.00	dispatch.evaluate.eval	2	-	-
	0.00	dispatch.evaluate.stats	1	-	-
	0.03	dispatch.fetch	1	-	-
	0.00	dispatch.localSearch	1	-	-
	0.02	dispatch.writeStatus	5	-	-
	0.06	startup.configuration	1	-	-
	1.01	startup.handoff	1	-	-

Search job properties

canSummarize	1
createTime	2016-03-14T11:49:32.000-05:00
cursorTime	1969-12-31T19:00:00.000-05:00
defaultSaveTTL	604800
defaultTTL	600
delegate	None
diskUsage	53248
dispatchState	FAILED
doneProgress	1.0

Figura 85. Pantalla de inspeccionar para un tablero de control del equipo Fortinet

Refrescar: sirve para refrescar los datos de los paneles, se da clic en  para acceder al refresco de datos de un panel.

Después de completar la elaboración de un panel o tablero de control se puede expórtalos en formato PDF o imprimirlos usando los botones que existen en la parte superior derecha  .

Se obtuvieron tableros de control para la página web, para el equipo de seguridad perimetral Fortinet y para la herramienta de Antispam de la institución, mismos que se obtuvieron de las correlaciones configuradas en el numeral 5.2.1. A continuación se presentan los tableros de control y paneles que se configuraron para las fuentes de datos seleccionadas.

Página web MINTEL:

Para la página web se crearon paneles para visualizar por ejemplo el tiempo de disponibilidad de la misma, número de visitas, desde que parte del mundo ingresaron, consumo de acho de banda y los ataques que se están dando a la página. Como se explicó anteriormente se pueden visualizar los tableros de control en una línea de tiempo, es decir por ejemplo cada 60 minutos, la última semana, el último mes, etc., esta selección se la puede hacer debido a que la herramienta posee una base de datos donde se guardan los

eventos en el tiempo. En la Figura 86 se presenta el tablero de control con sus paneles para la página web en los últimos 60 minutos.

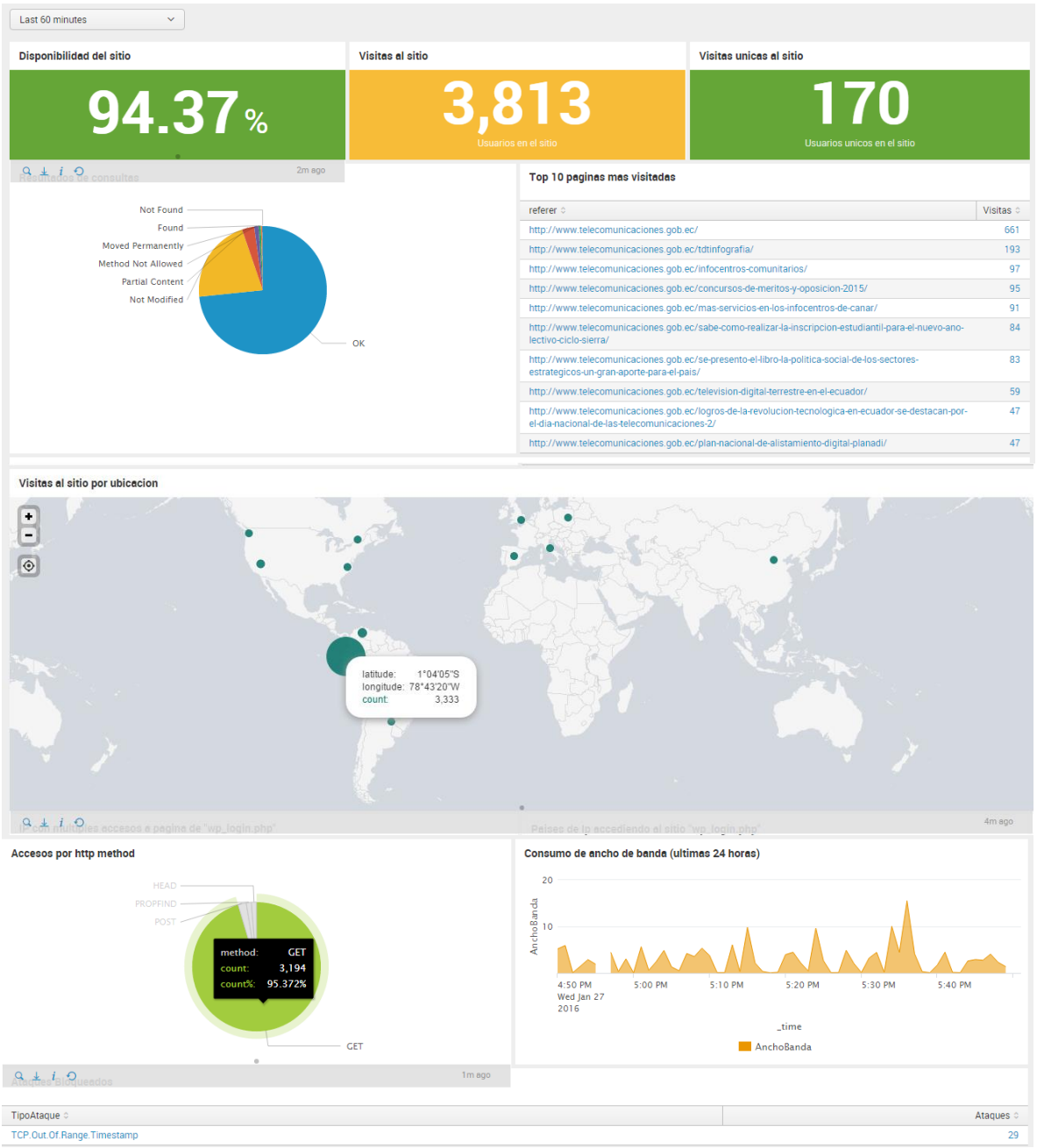


Figura 86. Tablero de control de la página web – últimos 60 minutos

Además en lo que se refiere al mapa de geo localización se puede hacer zoom para ver con más detalle en caso de ser necesario, ahí se puede visualizar por ejemplo el sitio exacto desde donde se tiene la mayor cantidad de ingresos a la página, esto se presenta en la Figura 87.

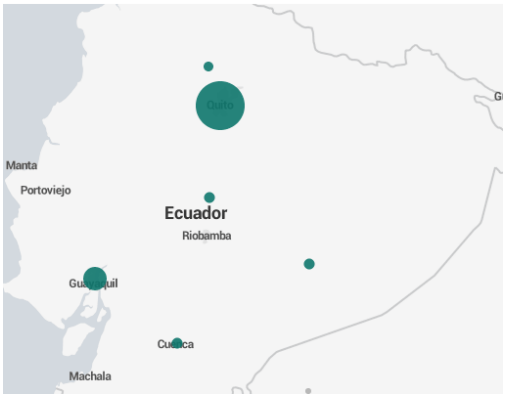
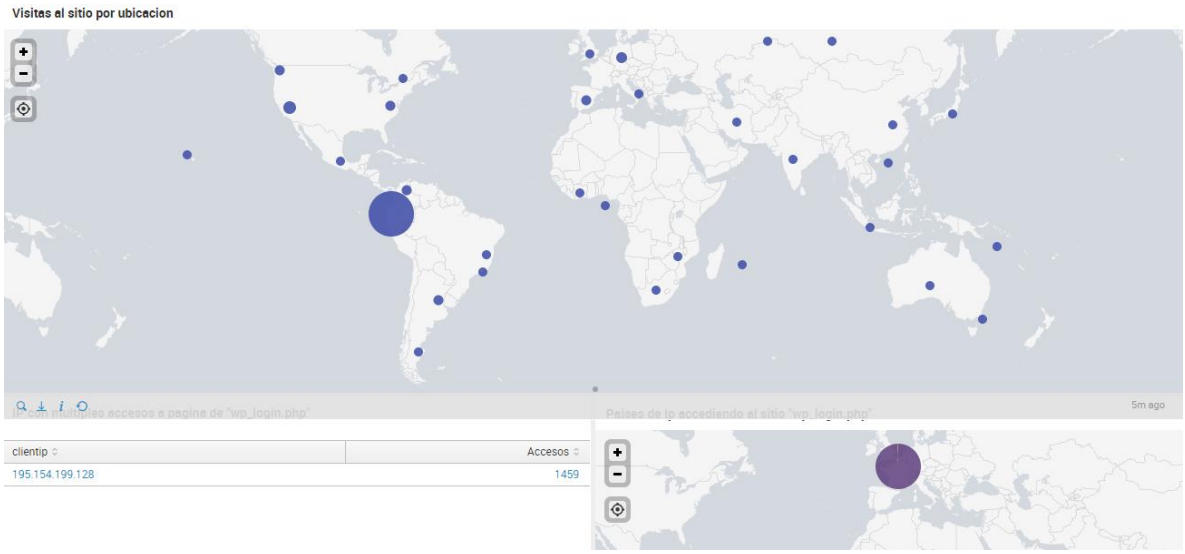


Figura 87. Acercamiento de mapa de geo localización

En la Figura 88 se presenta el tablero de control de la página web para los últimos 30 días.



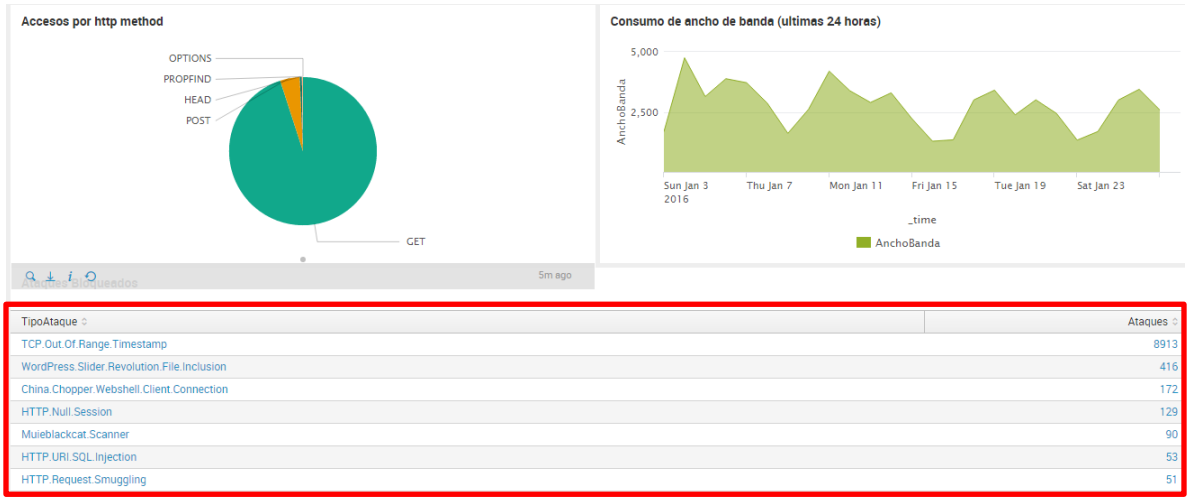


Figura 88. Tablero de control de la página web – últimos 30 días

Se puede observar en esta figura en el panel resaltado en rojo el **top de ataque**s donde se visualiza las formas con las cuales están tratando de ingresar a la página web para realizar un ataque, este resultado concuerda con el estudio previo que se realizó con la herramienta Check Point explicado en los antecedentes de este caso de estudio.

Fortinet:

Para el equipo de seguridad perimetral existen ya tableros de control predefinidos, uno de los tableros de control más importante es el de amenazas, para acceder a este tablero se da clic en **Fortinet Fortigate App for Splunk** en la pantalla inicial y después se visualizará cuantos dispositivos de esta marca se tienen en la red y aparecen algunas opciones de tableros propias para Fortinet. Para ver las amenazas se selecciona la pestaña **Unified Threat Management** y se da clic en la pestaña **Threat Dashboard**, en la cual se visualizan paneles tales como: Amenaza por severidad, Ataque IPS por dispositivo,

amenaza por subtipo, amenazas por dirección origen y destino. En la Figura 89 se presenta como ingresar a los tableros predefinidos de Fortinet.

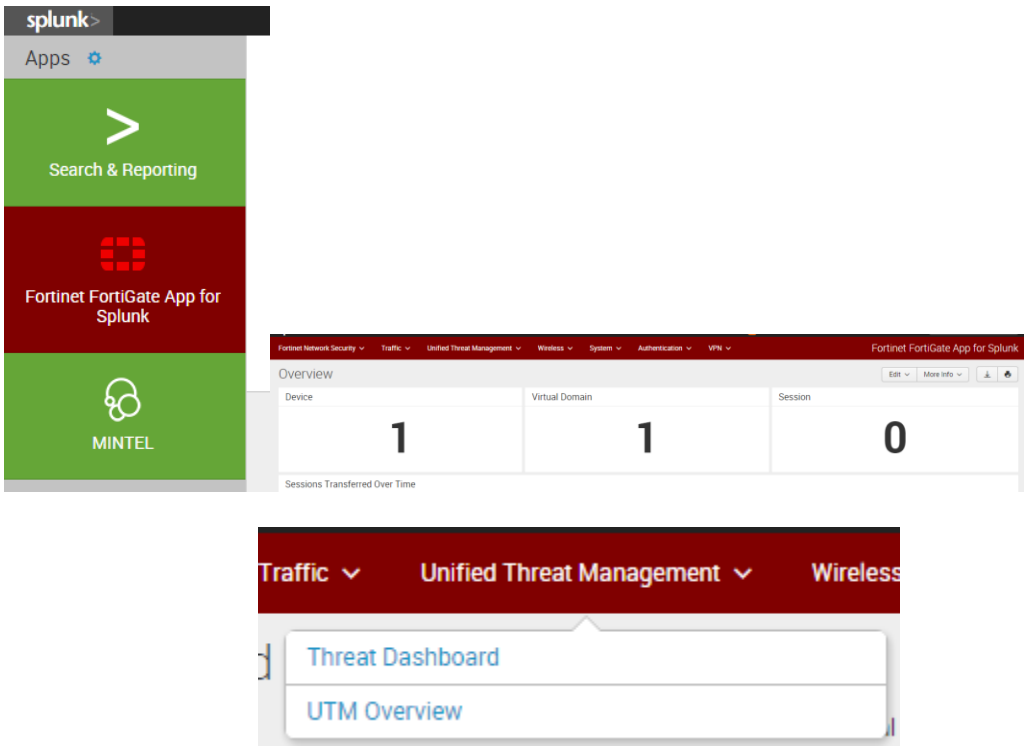


Figura 89. Pantalla de ingreso a tablero de control del equipo Fortinet

En las figuras 90 y 91 se presentan las pantallas de los tableros de control para el Fortinet utilizando una línea de tiempo de 15 minutos y 30 días.

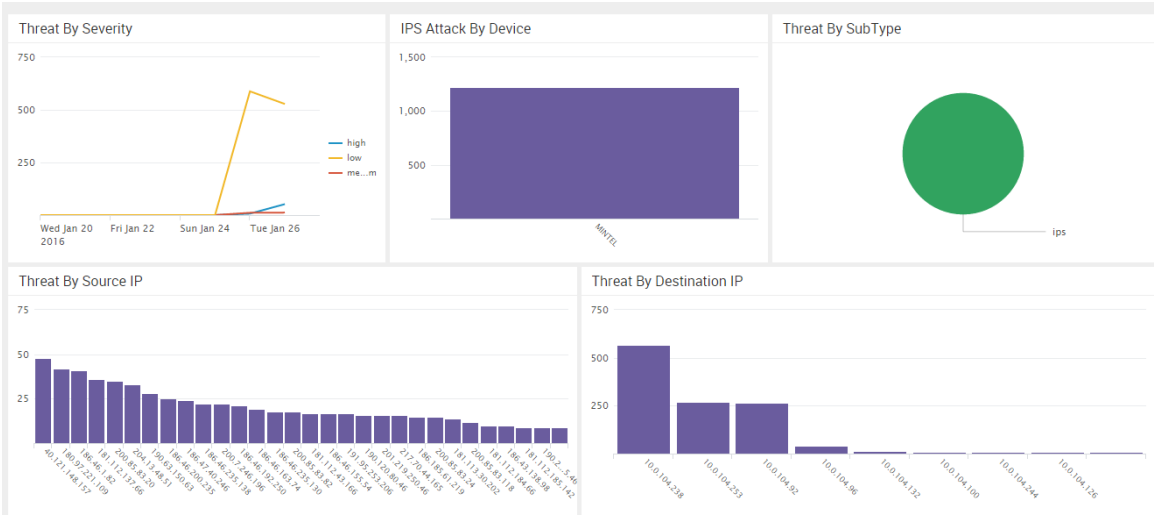


Figura 90. Tablero de control de equipo Fortinet – últimos 30 días

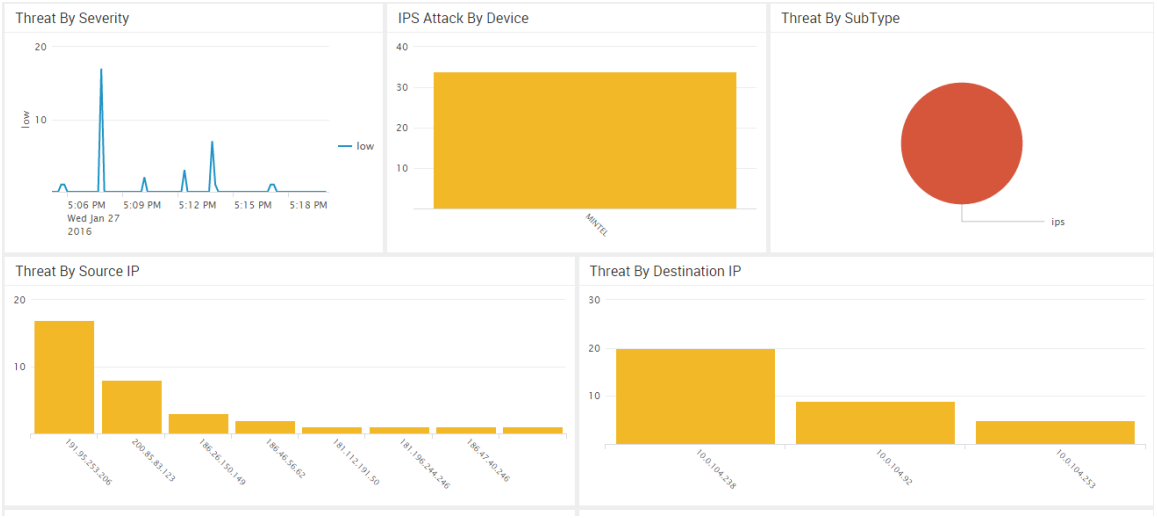


Figura 91. Tablero de control de equipo Fortinet – últimos 15 minutos

Al dar clic en alguno de los paneles se puede visualizar los datos exactos del número de veces que sucedió ese evento, por ejemplo cuantos intentos de ataques hubo o

cuantas amenazas hubo de la IP X.X.X.X de origen; en la Figura 92 se presenta la pantalla que se despliega al dar clic en el panel IPS Attack by device.

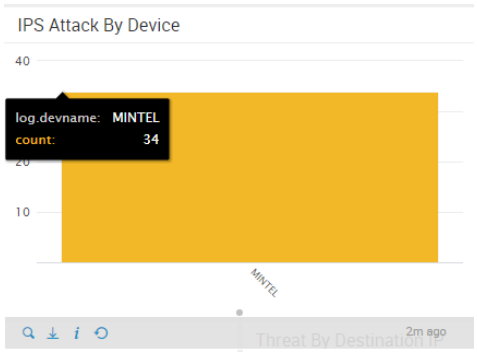


Figura 92. Número de veces de ataques IPS del equipo Fortinet – últimos 15 minutos

Dentro del equipo Fortinet, un tablero de control que se creó fue para ver los ataques contenidos por el mismo, teniendo como opciones del tablero los paneles: top 10 de ataques contenidos, ataques contenidos (últimas 24 horas) y ataques contenidos (últimos 60 min). En la Figura 93 se visualiza este tablero de control.

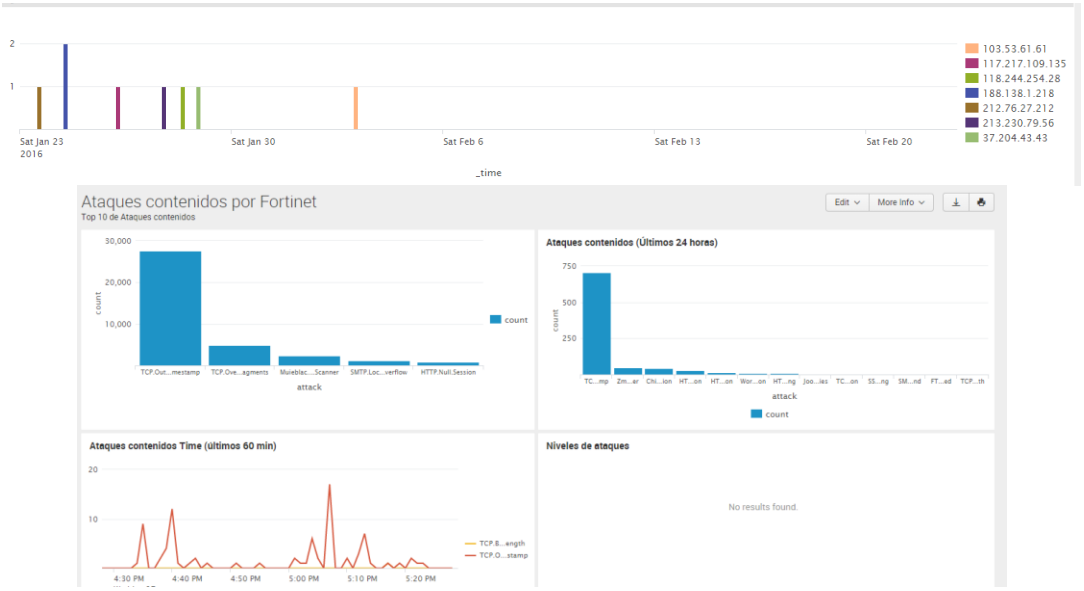


Figura 93. Tablero de control ataques contenidos por equipo Fortinet

Así mismo se puede visualizar la cantidad de eventos en cada panel gráfico, en la Figura 94 se presenta lo que sale si se da clic en algunas de las barras de control para los ataques contenidos en las últimas 24 horas.

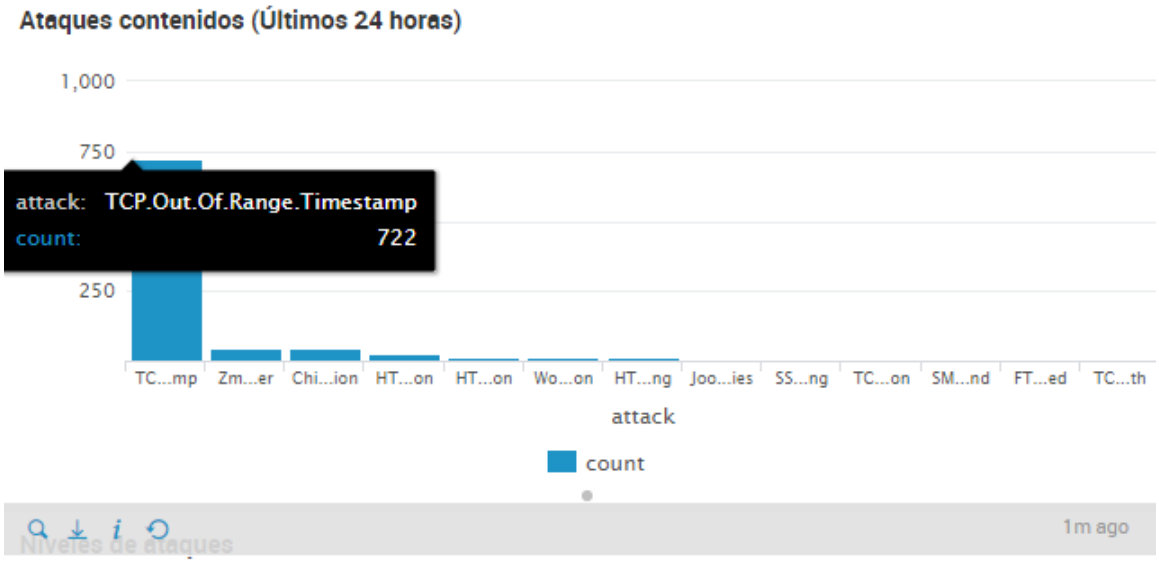


Figura 94. Número de ataques del tipo TCP out of Range Timestamp contenidos en las últimas 24 horas

Antispam:

Para el Antispam se creó paneles para verificar cuantos mails se han enviado y recibido, número de mensajes spam recibidos, **e**stado de correos en porcentajes y número de correos recibidos por funcionario. En las figuras 95 y 96 se presentan estos paneles en diferentes líneas de tiempo.

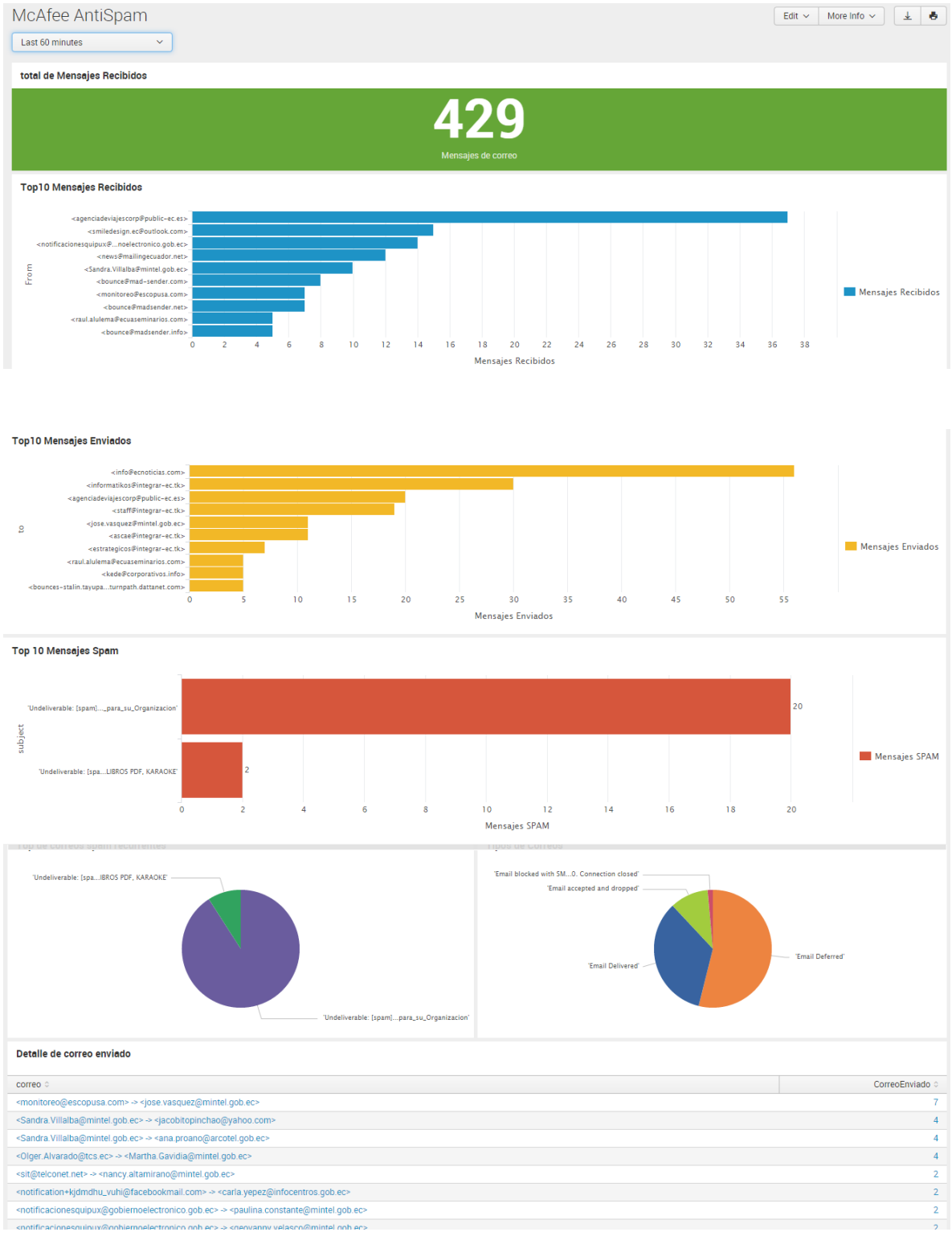


Figura 95.Tablero de control de equipo Antispam – últimos 60 minutos

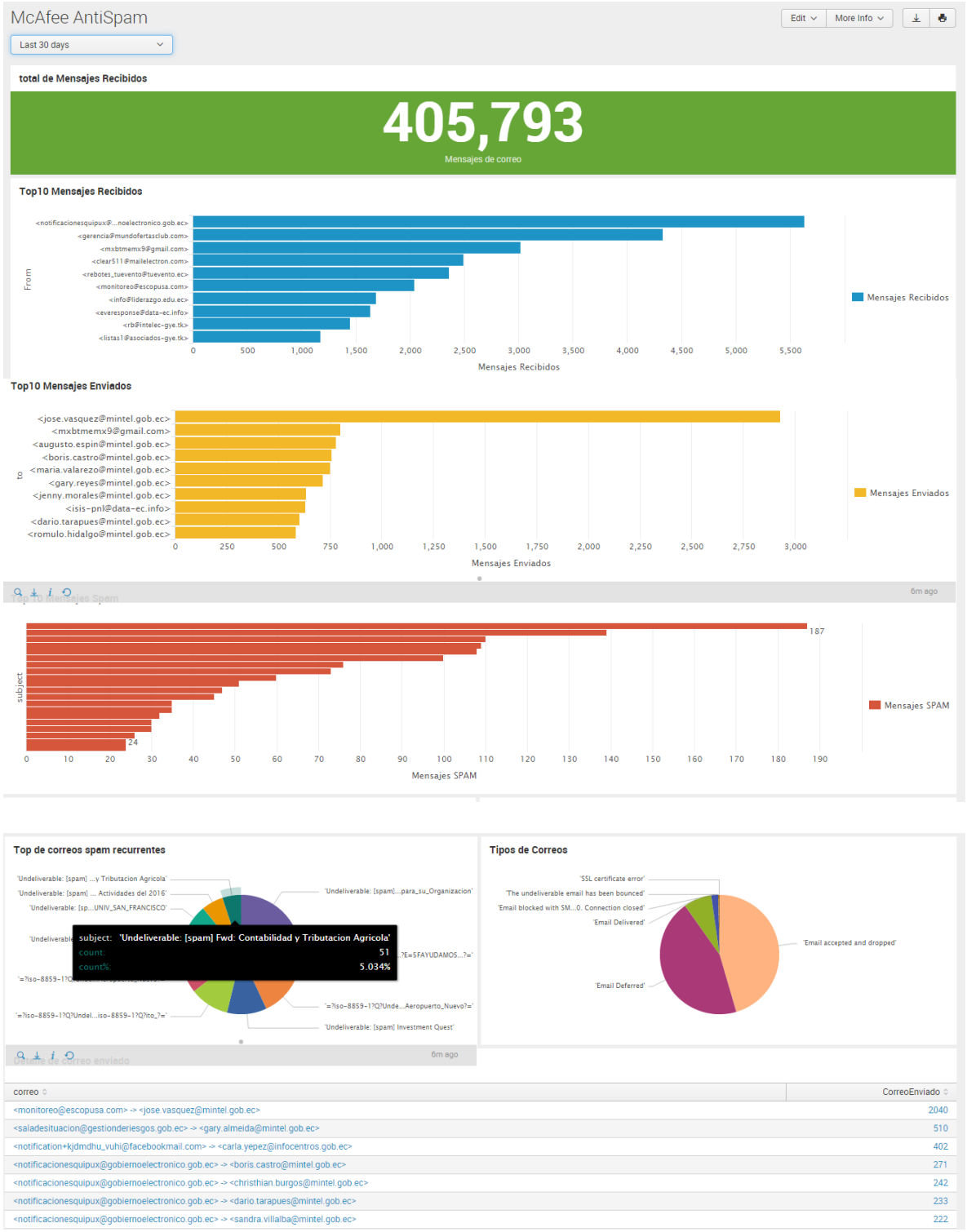


Figura 96. Tablero de control de equipo Antispam – últimos 30 días

Además como se explicó anteriormente en cualquiera de los paneles se puede dar clic en **búsqueda**  y después seleccionar **estadísticas** y se observa con más detalle las cantidades de eventos que se tienen en los paneles de los tableros de control. En la Figura 97 se indica las estadísticas del correo bloqueado por Antispam.

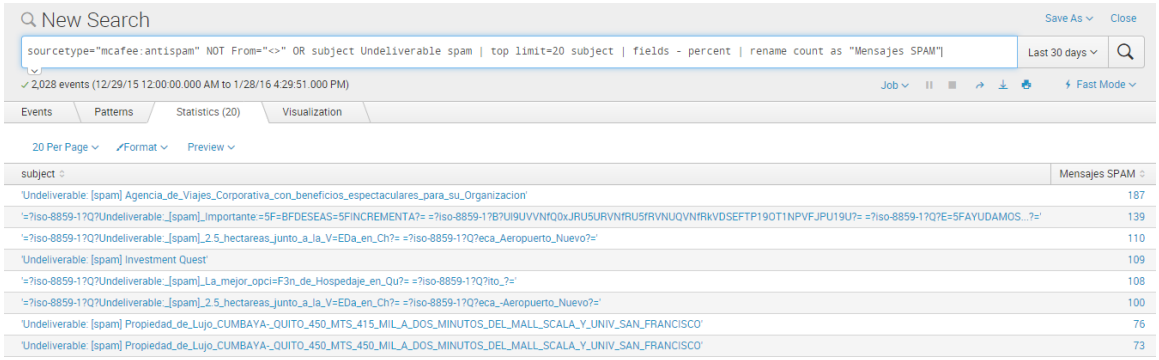


Figura 97. Estadísticas del correo bloqueado por equipo Antispam

5.3.2 McAfee ESM

Los tableros de control para esta herramienta pueden ser de dos tipos: tableros de control o también llamados vistas, los cuales son generados por la herramienta automáticamente y que pueden ser obtenidos para cada fuente de datos y la segunda opción tableros que se los puede crear con los datos recolectados por cada fuente.

Para obtener reportes o tableros de control automáticamente se usa la sección de vistas de la herramienta, cabe señalar que ya se explicó cómo acceder al uso de las vistas con reportes ya existentes en el ítem 5.2.2.2.

Entre las vistas principales que vienen automáticamente en la herramienta son: el resumen predeterminado, activo-amenaza-riesgo, estado del dispositivo y vistas de eventos.

Como ejemplo en la Figura 98 se presenta el tablero de control para verificar el estado del servidor que aloja la página web del MINTEL, para esto en la sección de barra de herramientas para crear, editar y administrar se selecciona la opción **estado del dispositivo** y a continuación se selecciona la fuente página web MINTEL desde el árbol de equipos principal.

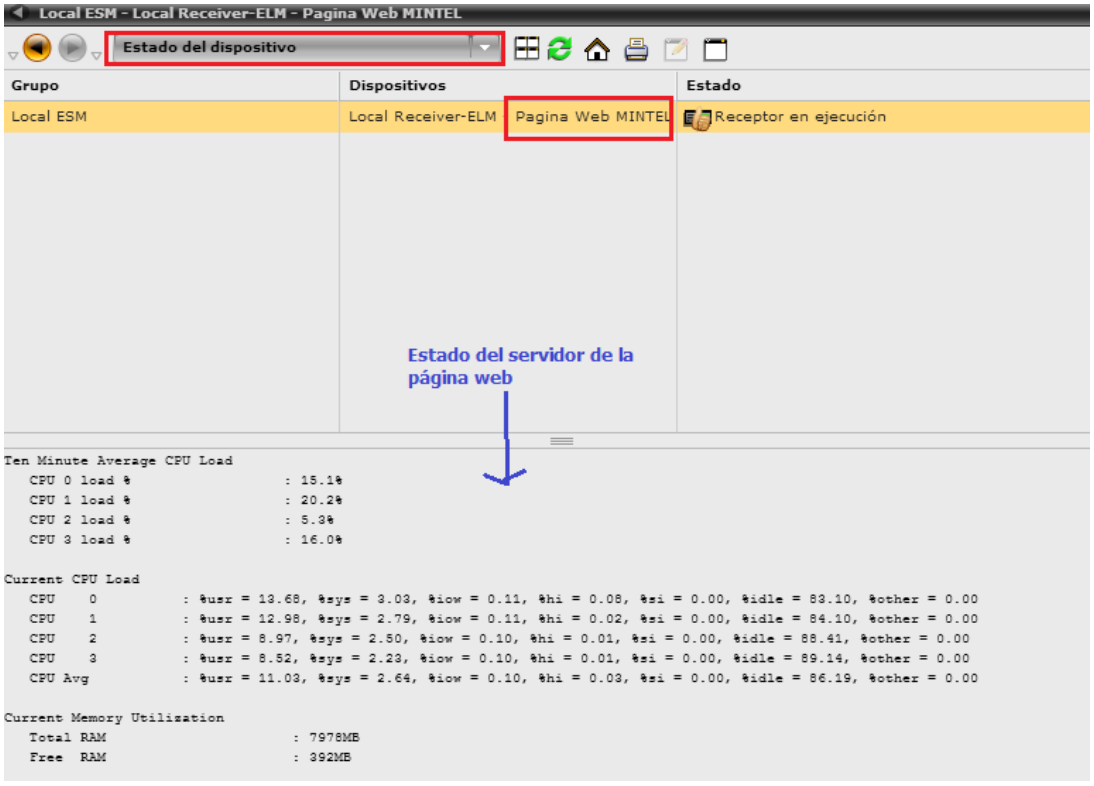


Figura 98. Tablero de control estado del servidor página web

Para crear un nuevo tablero con los eventos de las fuentes de datos, en la barra de herramientas de vistas para crear, editar y administrar las vistas, se selecciona la opción **crear vista nueva**, después de lo cual se abrirá un nuevo tablero de control en el cual se pueden añadir componentes de la barra de herramientas de edición de vistas que aparece junto con el nuevo tablero de control creado. En la Figura 99 se visualiza lo indicado.

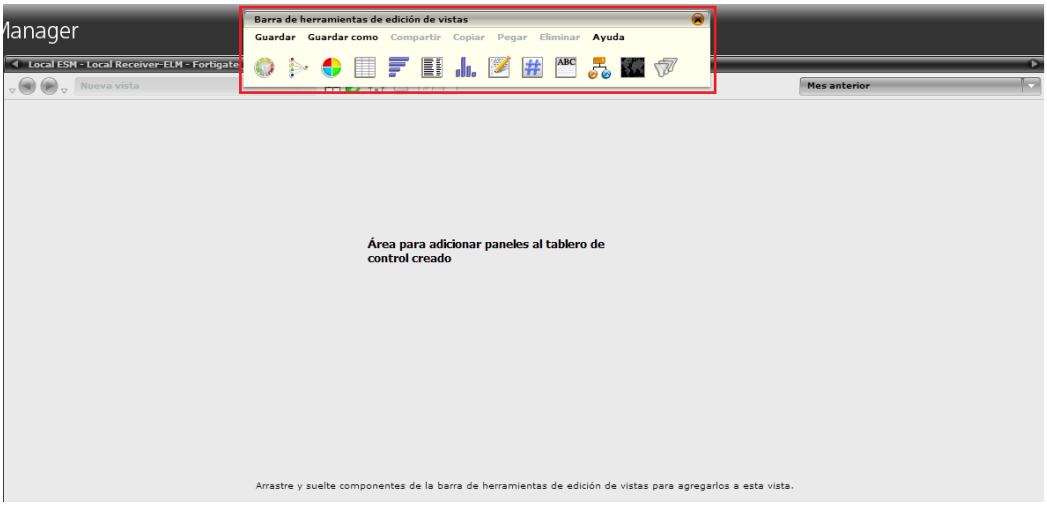


Figura 99. Pantalla para creación de un nuevo tablero de control

En la barra de herramientas para la edición de vistas hay algunas opciones de creación de los paneles, entre las principales se tiene: gráfico circular, gráfico de barras, tabla, distribución, gráfico de origen y destino. Se creó como ejemplo un panel de tipo gráfico circular y otro de gráfico origen y destino para el equipo Fortinet.

1) Para adicionar el gráfico circular, se debe arrastrar el componente  al área del tablero de control y se despliega el panel y un asistente de consultas en el cual se puede seleccionar 5 tipos: consultas de eventos, consultas de flujo, administración de casos, activos y vulnerabilidades y estado de riesgo; para cada opción de las consultas descritas existen sub categorías para seleccionar y según las necesidades que se tenga se escogen algunas de estas para crear paneles dentro del tablero de control. Se seleccionó como ejemplo la consulta de eventos y dentro de esta se escogió geo localización de destino por ciudad para ver desde que ciudades del mundo se ha intentado ingresar el equipo de seguridad perimetral. En la Figura 100 se indica las pantallas para la creación del panel y en la Figura 101 se muestra el resultado final del panel en forma circular con los datos de las ciudades.

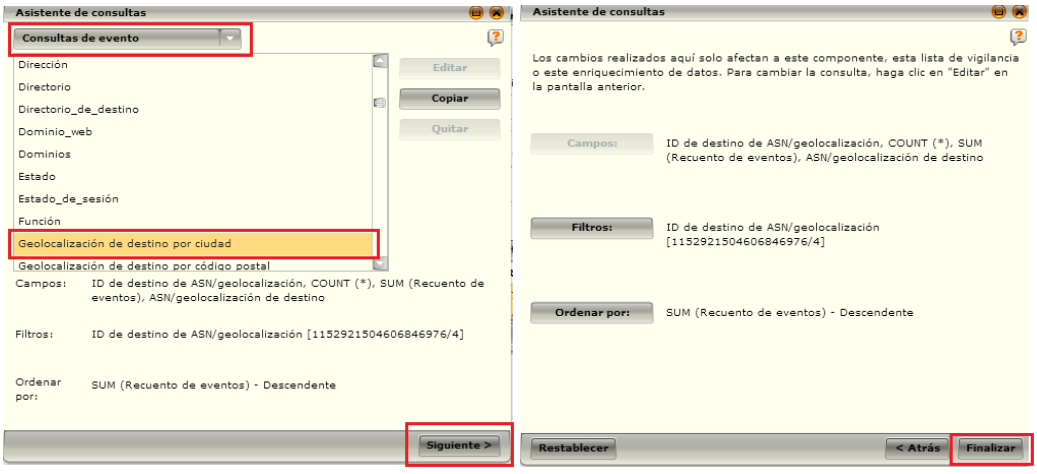


Figura 100. Opciones para configurar consultas de eventos por geo localización

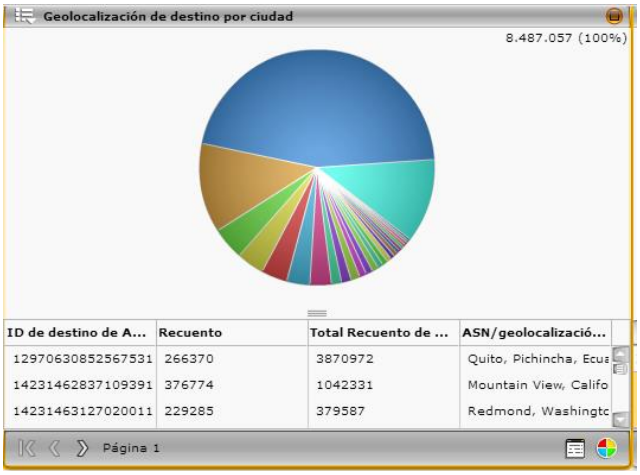


Figura 101. Pantalla de consulta de eventos en forma circular por ciudad

2) Para el caso del panel con la opción de gráfico origen y destino se seleccionó la opción consulta de evento para obtener el gráfico de red de eventos origen y destino para el equipo de seguridad perimetral. . En la Figura 102 se indica las pantallas para la creación del panel y en la Figura 103 se muestra el resultado final del panel con el gráfico de la red de eventos.

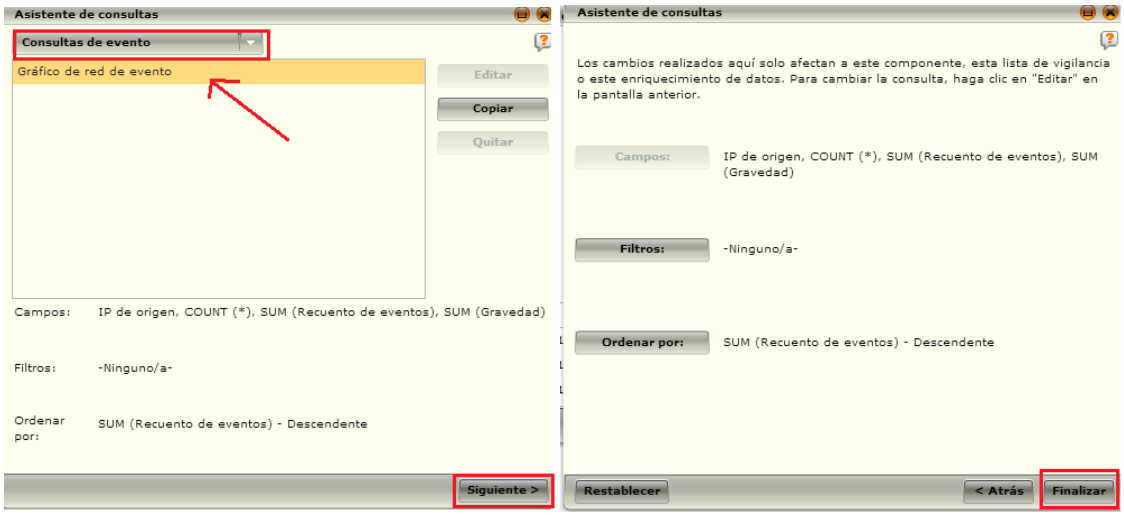


Figura 102. Opciones para configurar consultas de red eventos por origen y destino

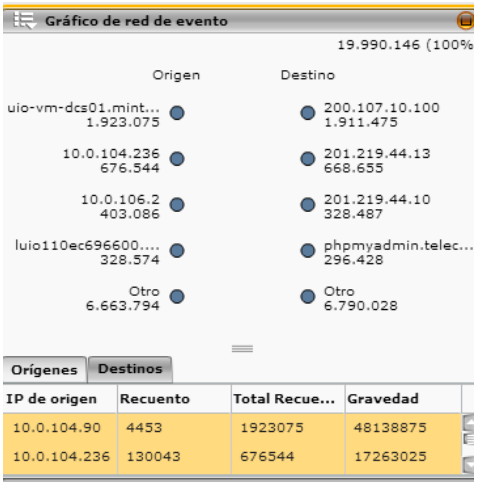


Figura 103. Pantalla de consulta de red eventos por origen y destino

El tablero de control final con los dos paneles creados de ejemplo se indican en la Figura 104, ahí también se puede visualizar en la parte superior derecha que se puede cambiar los datos de los paneles en el tiempo, pudiendo ver los resultados del día en curso, semana anterior, mes anterior, entre otros.

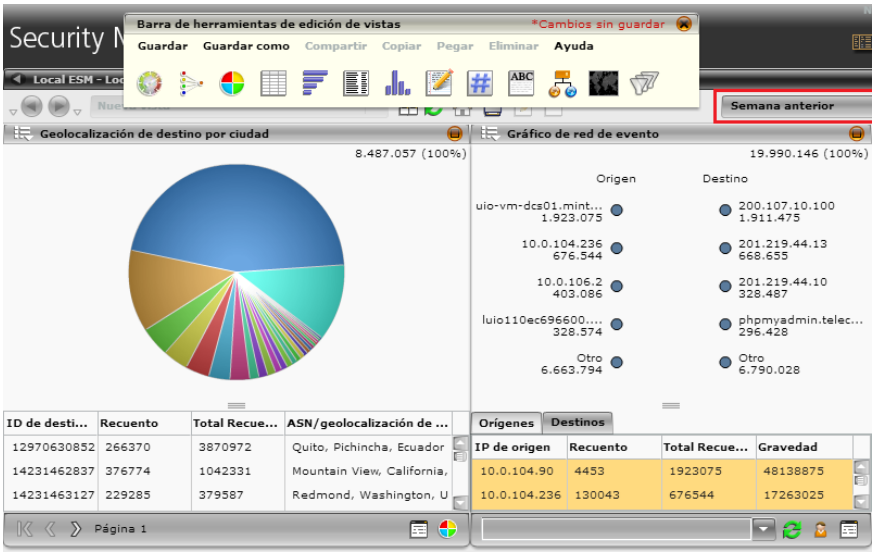


Figura 104. Tablero de control con paneles de geo localización de destino por ciudad y red de eventos del equipo Fortinet

Una vez finalizado el tablero de control con los paneles creados, se escoge la opción **guardar como**, se le da un nombre y se guardará el tablero de control en la sección de vistas que posee la herramienta. En la Figura 105 se indica el tablero de control que se creó como ejemplo y se colocó el nombre equipo fortinet, mismo que podrá ser usado para visualizar los datos que contiene cuando se lo necesite y poder tomar decisiones. En la misma figura se puede observar otros tableros creados como ejemplos para obtener datos que se necesitaban para la red del MINTEL como son: Casos_Test y Prueba WEB.

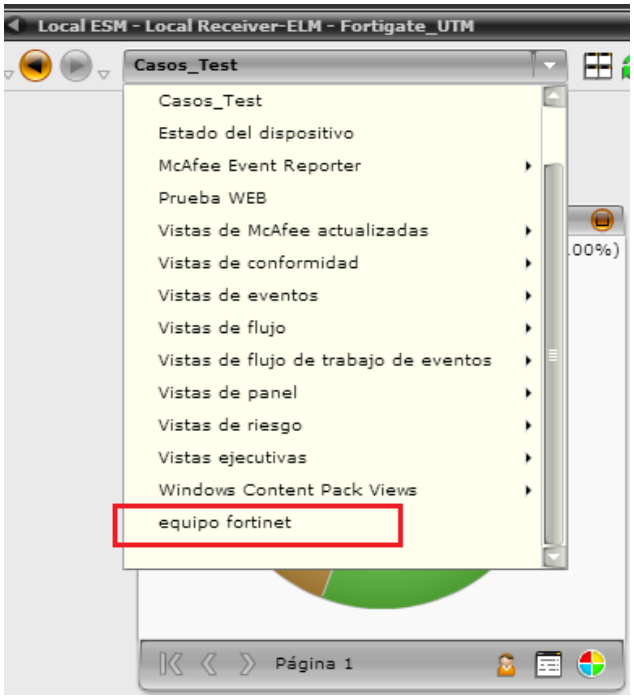


Figura 105. Tableros de control disponibles en la herramienta

5.3.3 AlienVault USM

Como se explicó anteriormente mientras más activos (dispositivos) se tengan ingresados en la herramienta se obtendrán mejores estadísticas de amenazas, vulnerabilidades y datos SIEM que se los podrá visualizar en forma gráfica. Esta herramienta tiene algunos tableros de control predefinidos que se los encuentran distribuidos en algunas categorías dentro del aplicativo. En la pestaña cuadro de mandos contiene la mayoría de tableros de control divididos en las siguientes categorías:

- Información general: ejecutivos, de seguridad, de taxonomía, de vulnerabilidades y de conformidad o cumplimiento.
- Estado despliegue: visibilidad global, visibilidad de activos y visibilidad de la red.
- Mapas de riesgo: información general y gestión de mapas.
- Intercambio de amenazas: reputación IP, IP´s maliciosas por actividad y top 10 de países.

No hay como modificar estos paneles pero si se desea cambiarlos se debe editar el tablero y realizar una copia del mismo (clon) y en esta copia si se podrá modificar lo que se desee, además se puede dar permisos para que ciertos usuarios visualicen estos paneles. Cabe señalar que los paneles son construidos con los datos que vienen del SIEM propio que tiene la herramienta, aquí se pueden encontrar todos los eventos tanto en crudo o eventos en bruto así como también eventos ya procesados o normalizados y que como se dijo son utilizados en los paneles que vienen por defecto con la herramienta.

A continuación se describen brevemente los tableros de control más importantes y que ayudarán para visualizar elementos de seguridad para encontrar posibles amenazas y vulnerabilidades en la infraestructura del MINTEL.

Información general: como su nombre lo describe en esta pestaña se encontrarán tableros de control que contienen paneles con la información general obtenida de los eventos que llegan a la herramienta y que serán los más importantes para analizar que está sucediendo en la red. Al dar clic en el tablero de tipo **ejecutivo** se podrá encontrar paneles que describen el top 5 de alarmas en eventos de seguridad, el top 10 en la categoría de eventos, eventos de seguridad versus logs de eventos, top 10 de activos con múltiples eventos, top actividad OTX en al ambiente de análisis (red MINTEL). En la Figura 106 se indica los paneles de información general.

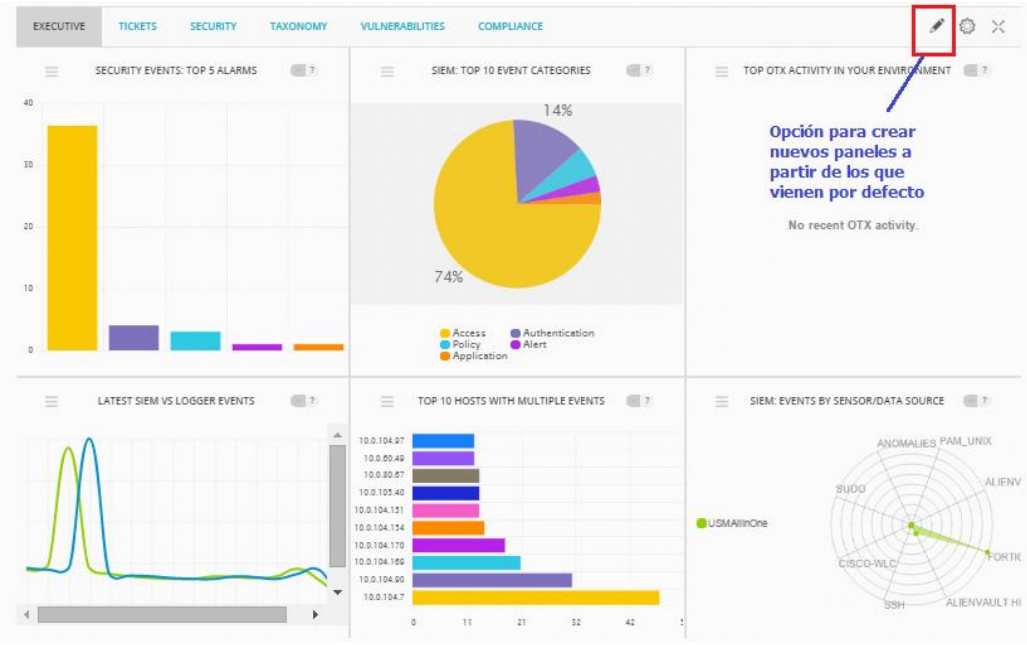


Figura 106. Paneles gráficos del tablero de control de información general USM

El siguiente tablero de control es para **seguridades**, en el cual se pueden encontrar los siguientes paneles: top 10 activos promiscuos, top 5 alarmas de eventos de seguridad, top 5 de eventos de seguridad, top 10 de activos con múltiples eventos y tendencia de eventos de seguridad por último día o por última semana. En la Figura 107, se presenta el tablero de control de seguridades obtenido para los activos declarados de la red del MINTEL.

Figura 107. Paneles gráficos del tablero de control de seguridades USM

Otro de los tableros es el de **taxonomía** donde se encuentra paneles como top 10 de activos con virus detectado, eventos de autenticación fallidos versus eventos de autenticación exitosos, eventos del sistema y eventos malware clasificados por tipo, este tablero trata de agrupar paneles que tienen características comunes de ahí su nombre de taxonomía. En la Figura 108 se presenta este tablero con sus paneles la mayoría desplegados en forma de pastel y uno en forma de barras.

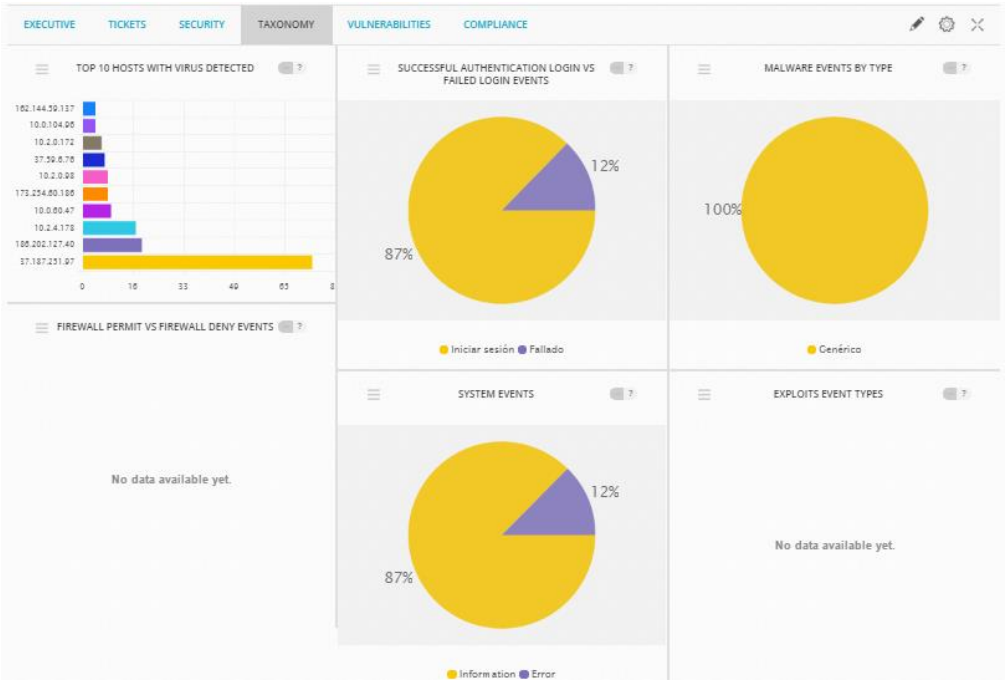


Figura 108. Paneles gráficos del tablero de control de Taxonomía USM

Otro tablero es de **vulnerabilidade**s de la red, catalogadas en cuatro tipos por gravedad, por servicio, por equipos y por redes. La vulnerabilidad por gravedad se despliega en forma de pastel indicando 4 formas de vulnerabilidades: serias, altas, medias y bajas, el panel para vulnerabilidad por servicio también es en forma de pastel y despliega el top 10 de servicios y puertos que han sido vulnerados. La otra categoría es el top 10 de equipos o activos vulnerados y se los presenta en forma de barra y en el último panel se presenta el top 10 de las redes que han sido vulneradas. En la Figura 109 se presentan todas las opciones para este tipo de tablero de control.

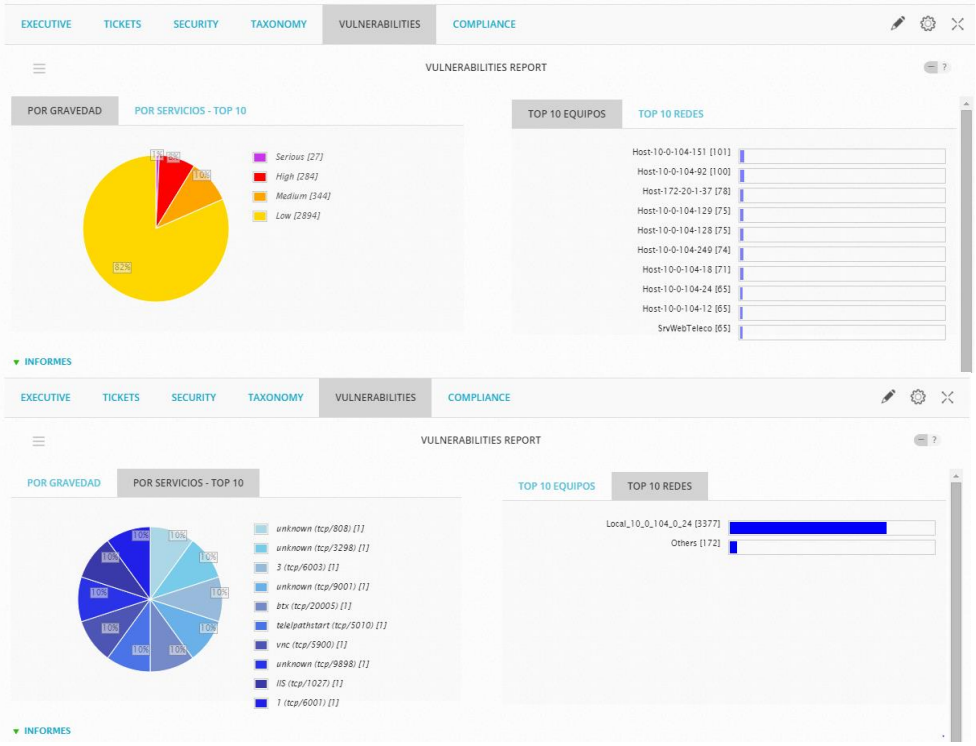
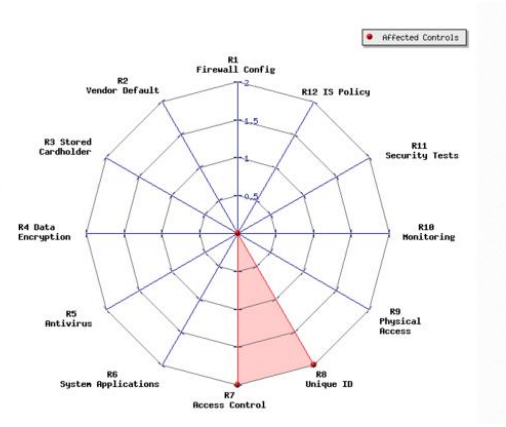
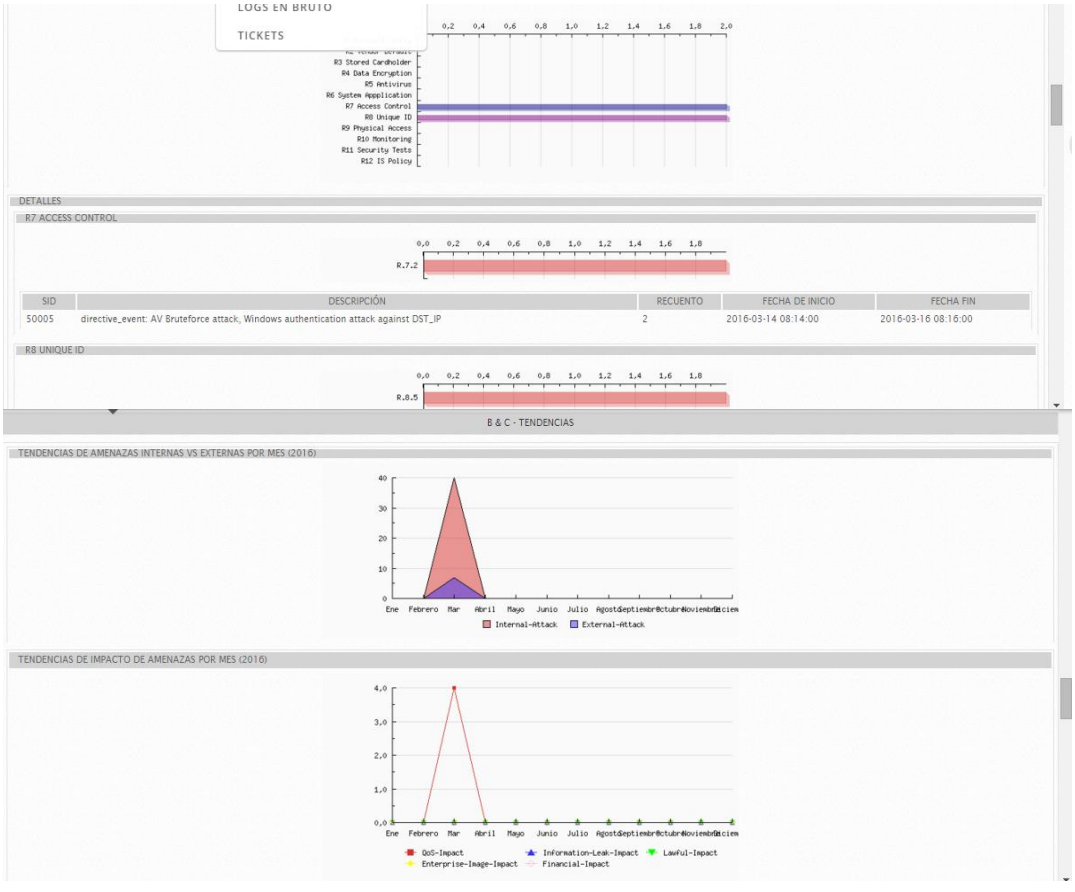


Figura 109. Paneles gráficos del tablero de control de vulnerabilidades USM

El último tablero de control de información general es el de **cumplimiento o conformidad**, en este tablero se encuentra mucha información en forma de paneles para ver si la red que se está analizando está cumpliendo estándares internacionales como por ejemplo ISO 27000 o PCI DSS. Además se puede encontrar información del número de amenazas internas o externas, un mapa con geo localización de las amenazas, tendencias de impacto de amenazas e impactos potenciales presentados en distintas formas de diagramas. En la Figura 110 se presentan los principales paneles obtenidos del tablero de control de cumplimiento.


Affected Controls
R1
Firewall Config
R12 IS Policy
R11
Security Tests
R10
Monitoring
R9
Physical
Access
R8
Unique ID
R7
Access Control
R6
System Applications
R5
Antivirus
R4 Data
Encryption
R3 Stored
Cardholder
R2
Vendor Default


LOGS EN BRUTO
TICKETS
R3 Stored Cardholder
R4 Data Encryption
R5 Antivirus
R6 System Application
R7 Access Control
R8 Unique ID
R9 Physical Access
R10 Monitoring
R11 Security Tests
R12 IS Policy
DETALLES
R7 ACCESS CONTROL
R7.2
SID
DESCRIPCIÓN
RECUENTO
FECHA DE INICIO
FECHA FIN
50005
directive_event: AV Bruteforce attack, Windows authentication attack against DST_IP
2
2016-03-14 08:14:00
2016-03-16 08:16:00
R8 UNIQUE ID
R.0.5
B & C - TENDENCIAS
TENDENCIAS DE AMENAZAS INTERNAS VS EXTERNAS POR MES (2016)
Ene
Febrero
Mar
Abril
Mayo
Junio
Julio
Internal-Attack
External-Attack
TENDENCIAS DE IMPACTO DE AMENAZAS POR MES (2016)
QoS-Impact
InFormation-Leak-Impact
LawFul-Impact
Enterprise-Image-Impact
Financial-Impact

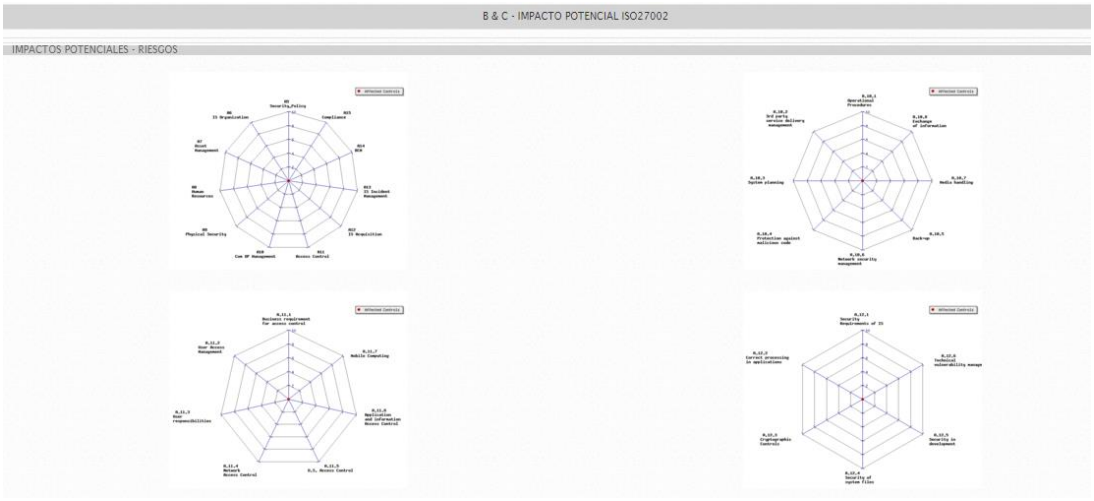


Figura 110. Paneles gráficos de tablero de control de conformidad USM

En cualquiera de los paneles se puede dar clic en las barras o en el pastel y se despliega una nueva ventana con todos los eventos de esa selección, por ejemplo en la Figura 111 se presenta la pantalla que se despliega luego de dar clic sobre una de las partes del pastel del top 10 de los eventos por categoría para ver la autenticación de los activos.

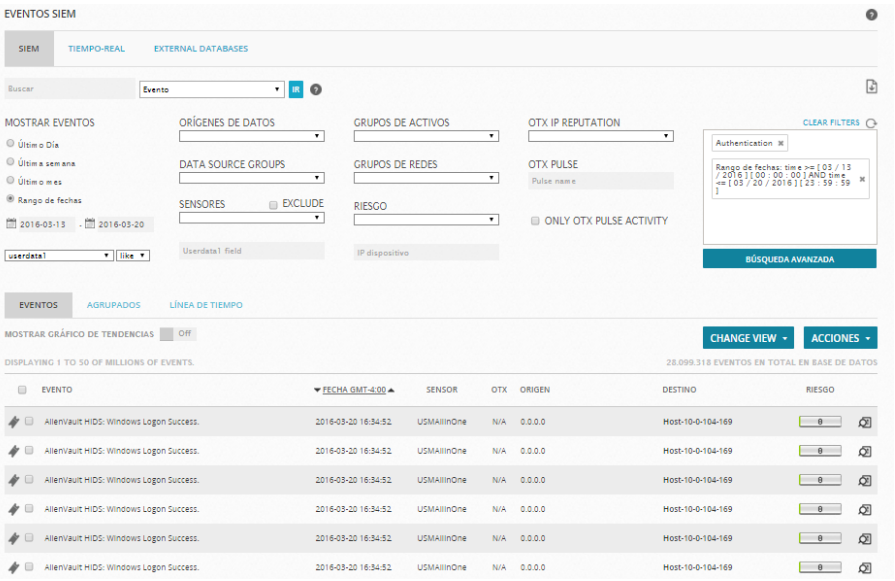


Figura 111. Eventos de autenticación de activos

Estado de despliegue: donde se presenta una visibilidad del estado de la herramienta, teniendo tres opciones: la visibilidad global que está al 100 % de los equipos y redes que se declaró previamente, la visibilidad de activos de la red configurados para entregar los eventos al correlacionador teniéndose un 12 % de equipos configurados y un 100 % en servidores y por último la visibilidad de red donde no se tiene el 100 % en escaneo de vulnerabilidades e inventario de activos. Todos estos cuadros deben estar casi siempre al 100 % para obtener mejores resultados con la herramienta. En la Figura 112 se presenta el estado del despliegue de la red del MINTEL al momento de elaborar este documento.

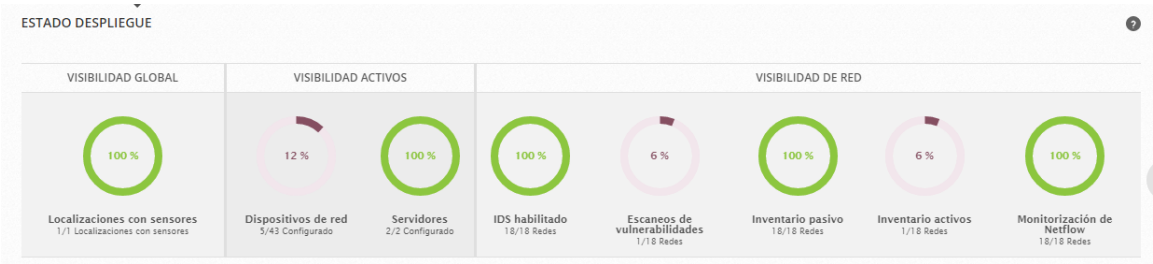


Figura 112. Panel gráfico de estado de despliegue de la herramienta USM

El tercer tipo de tableros por defecto que tiene la herramienta son los mapas de riesgos, donde se puede visualizar desde que países se tienen los ataques con mayor frecuencia. Existen dos paneles dentro de este tablero de control, el primero es de información general y el otro sirve para gestionar los mapas. En la Figura 113 se puede visualizar el mapa de riesgos de información general.

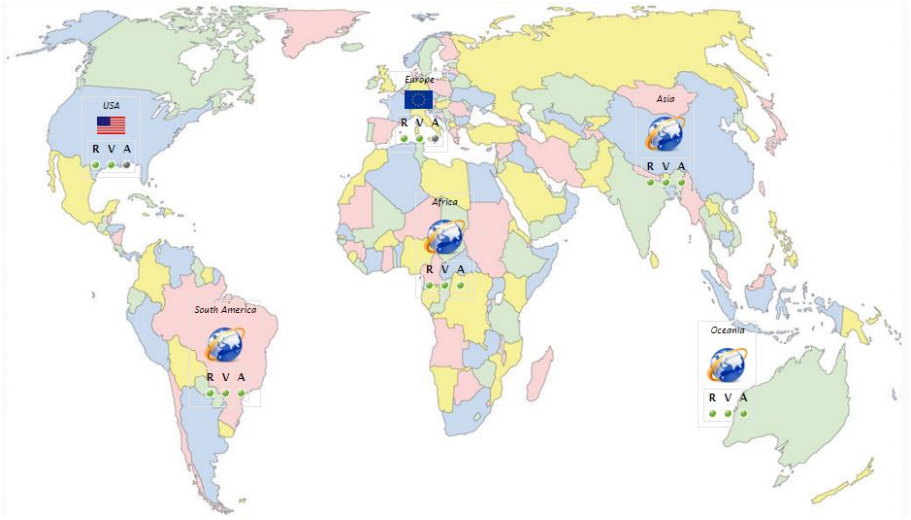
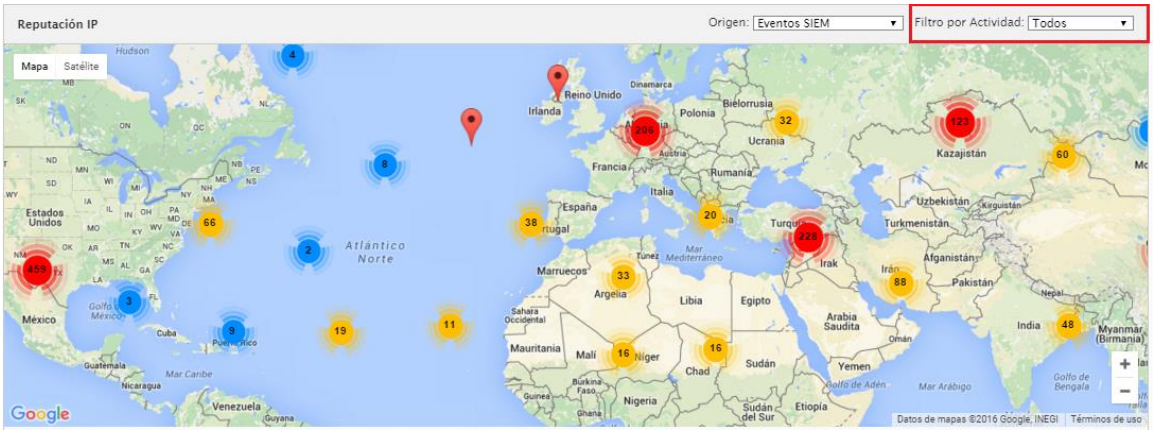


Figura 113. Panel gráfico de mapas de riesgos

El último tablero de control es el intercambio de amenazas donde se puede visualizar en el mapa diferentes tipos de amenazas según el origen del ataque, para esto en la parte superior derecha se puede seleccionar algunas opciones usando **filtro por actividad** y se visualizará desde donde proviene algún tipo de ataque. En la Figura 114 se presenta la pantalla escogiendo el filtro según la amenaza y se presenta dos ejemplos de selección para scanning y spamming como fuentes de ataques.



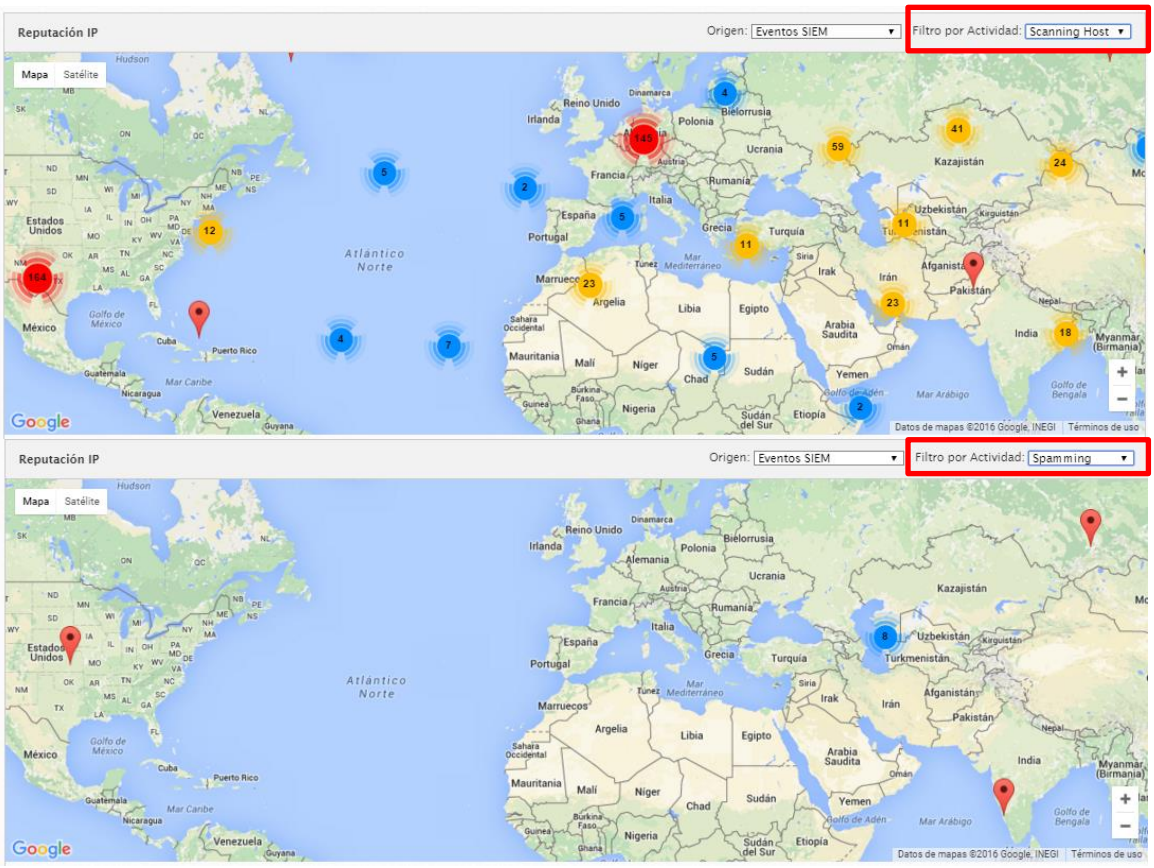


Figura 114. Paneles gráficos de intercambio de amenazas con varias opciones de filtro de actividad

Además dentro de este mismo tablero se encuentran dos paneles donde se encuentran un gráfico en forma de pastel de los ataques maliciosos por actividad y el top 10 de los países de donde provienen esos ataques. En la Figura 115 se visualizan estos paneles gráficos.

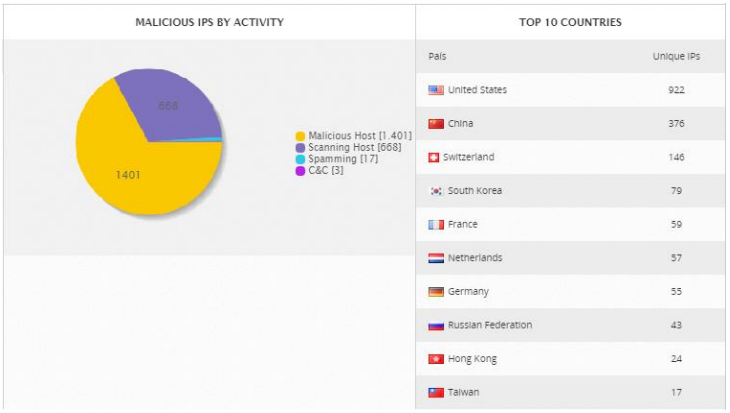


Figura 125. Paneles gráficos ataques maliciosos por actividad y países de origen

A más de estos tableros de control que se localizan en la opción **cuadros de mando,** también se tienen otros paneles que pueden ayudar para ver el comportamiento de la red, estos paneles se los puede encontrar en la opción **entorno** y los más importantes son el de netflow, disponibilidad y detección. En **netflow** se puede visualizar el tráfico de la red de tipo TCP,UDP, ICMP medidos en flujos por segundo, además se puede mostrar este tráfico por día, por semana, por mes, etc. En la Figura 116 se presenta la visualización del tráfico de una semana de la red del MINTEL

Figura 116. Tablero de control de netflow de la red del MINTEL

En la opción **disponibilidad** se puede monitorear a los diferentes activos que fueron ingresados en la herramienta para observar su disponibilidad teniendo algunas opciones de visualización. En la Figura 117 se presenta dos pantallas de disponibilidad de dos servidores, en la primera en forma general y la segunda escogiendo la opción detalle del equipo.

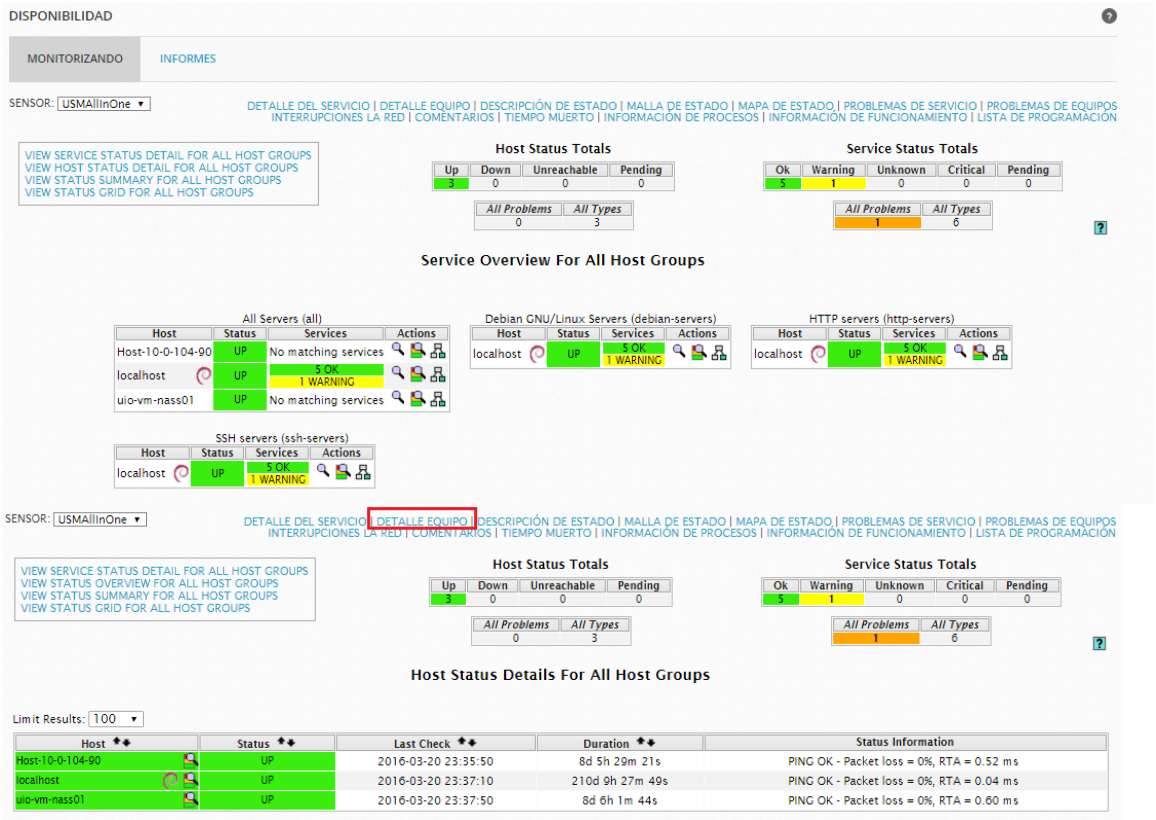


Figura 117. Tableros de control para ver disponibilidad de algunos equipos del MINTEL

En **detección** se visualizan dos paneles para visualizar los dispositivos HIDS, el uno con una tendencia y el otro las fuentes de datos HIDS, en la Figura 118 se indican

estas pantallas.

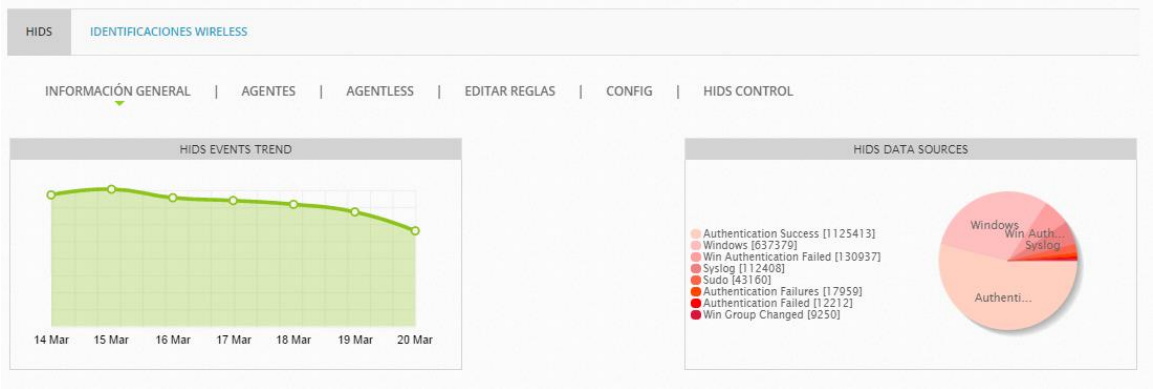


Figura 118. Tablero de control de detección para dispositivos HIDS

En el siguiente capítulo con los resultados obtenidos tanto en los tableros de control creados o con los que vienen por defecto en las herramientas, así como también con las correlaciones realizadas se analizará el comportamiento de la red del MINTEL en temas de seguridad, se crearán alertas e informes con el objetivo de indicar las vulnerabilidades, amenazas y ataques que está expuesta la infraestructura de la institución. Además con esa información se escogerán los más significativos para presentarlos al oficial de seguridad de la información de la institución y analizar los posibles huecos de seguridad que se tengan.

5.4 Evaluación de los resultados

Una vez realizadas las configuraciones de algunos casos de correlación y con los tableros de control que se obtuvieron en unos casos y otros que vienen incorporados en las herramientas, en este capítulo se realizará un análisis de las amenazas, vulnerabilidades y ataques encontrados con cada aplicativo y que acciones se tomarán para tratar de mitigar esos huecos de seguridad que se tienen en la infraestructura del MINTEL. Además se explicará brevemente como crear alarmas para cada herramienta y con esta opción alertar mediante un mail o mediante la creación de un caso al encargado de seguridad de la institución para que tome alguna acción al respecto.

5.4.1 McAfee – ESM

Una vez creados los casos o reglas de correlación, la herramienta da un ID de firma para cada nombre de las reglas configuradas, con este ID de firma se puede crear una alarma para ejecutar alguna acción en caso de que llegue a suceder. En la Figura 119 se presenta los casos de correlación creados y en la parte inferior se puede ver el ID de firma de cada regla, cabe señalar que las reglas de correlación por defecto también tienen su ID de firma.

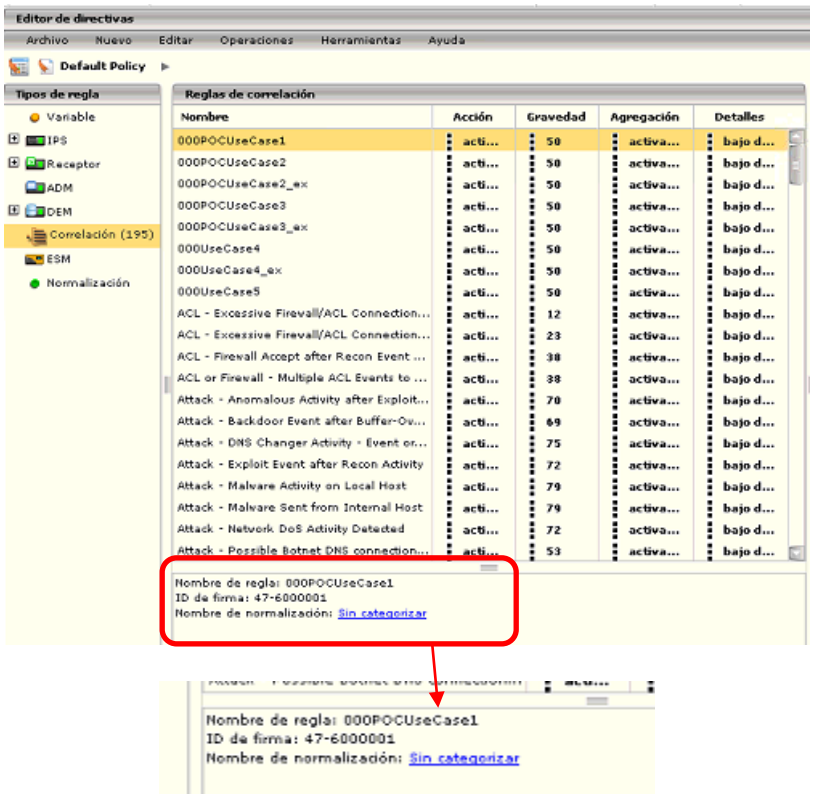
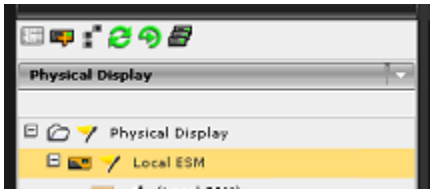


Figura 119. Reglas de correlación de herramienta ESM con sus ID´s de firma

Una vez que se tiene el ID de firma de cada regla de correlación, se escoge en el panel de navegación del sistema el dispositivo **local ESM**



y posterior se selecciona la opción de **propiedades**, de las opciones que se despliegan se selecciona la opción **alarmas** y ahí aparecerá una lista completa de todas las alarmas que se tienen dentro de la herramienta, algunas vienen por defecto y las demás son las creadas para este caso de estudio. En la Figura 120 se

presenta la pantalla dentro del cuadro en rojo se indican las alarmas configuradas para las reglas de correlación creadas y también las alarmas que vienen predefinidas.

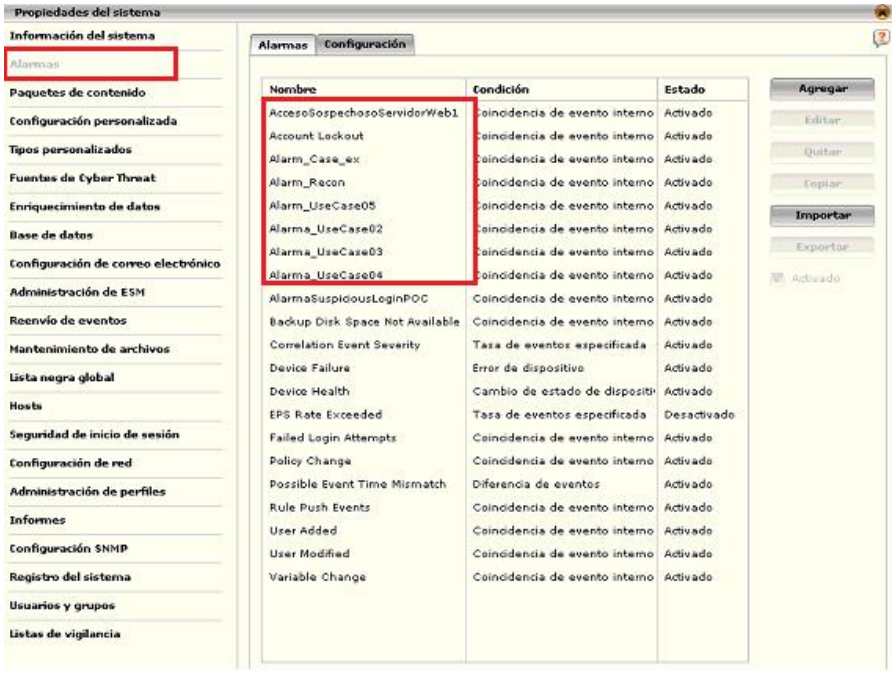


Figura 120.Alarmas creadas y por defecto de ESM

Para crear una nueva alarma se da clic en el botón de **agregar** y se desplegará una nueva pantalla con 5 opciones para configurar: **resumen, condición, dispositivos, acciones y escalación**. En la primera opción da un **resumen** de la alarma, ahí se coloca el nombre de la alarma (si se desea también se coloca una descripción), la condición de la alarma, las acciones que se toman al suceder esta alarma (en el ejemplo se seleccionó registro evento, alerta visual y alerta de audio), se asigna un usuario (en este caso será el NGCP) y por último se coloca un número de gravedad. En la Figura 121 se presenta la pantalla de resumen.

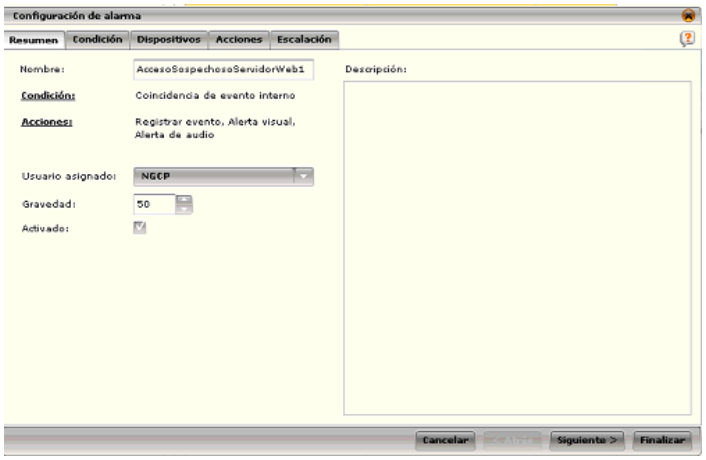


Figura 121. Pantalla para configuración de una nueva alarma

En la pestaña de **condición**, en la opción **tipo** se escoge el tipo de alarma que es y según esto la herramienta determina los campos que se deberán llenar, en este caso se seleccionó **coincidencia de evento interno**, después en la opción **campo** se escoge la condición que debe suceder para que se active la alarma, en este caso se escogerá con el ID de firma de las reglas de correlación creadas, posteriormente se ingresa el valor del ID que se obtuvo y por último la frecuencia de activación de la condición, en este caso se escogió que cada 10 minutos se den notificaciones en caso de suceder la alarma. En la Figura 122 se presenta la configuración explicada.

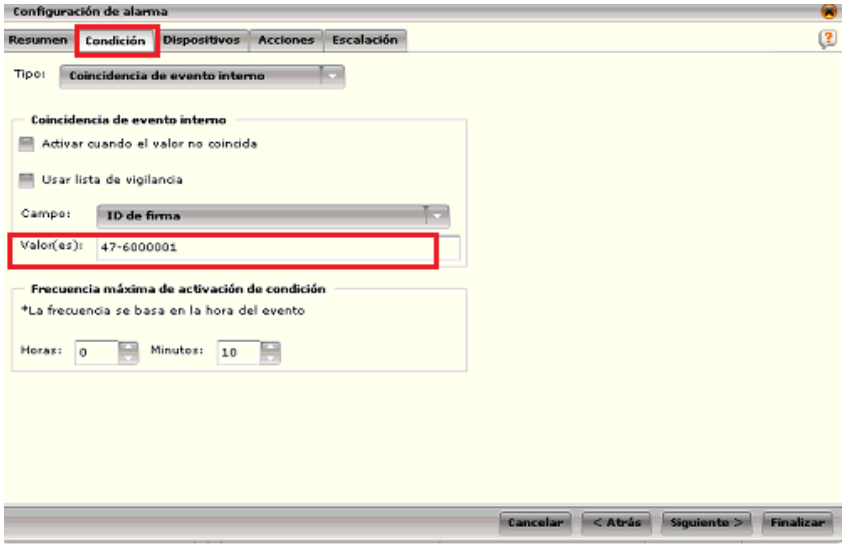


Figura 122. Pantalla de configuración para la condición que activa a la alarma

En la pestaña de **dispositivos** se seleccionan los equipos para los cuales se desea que la alarma creada los monitoree, para este caso de estudio se escogieron todos los activos ingresados en la herramienta. En la Figura 123 se presenta la pantalla de configuración de dispositivos.

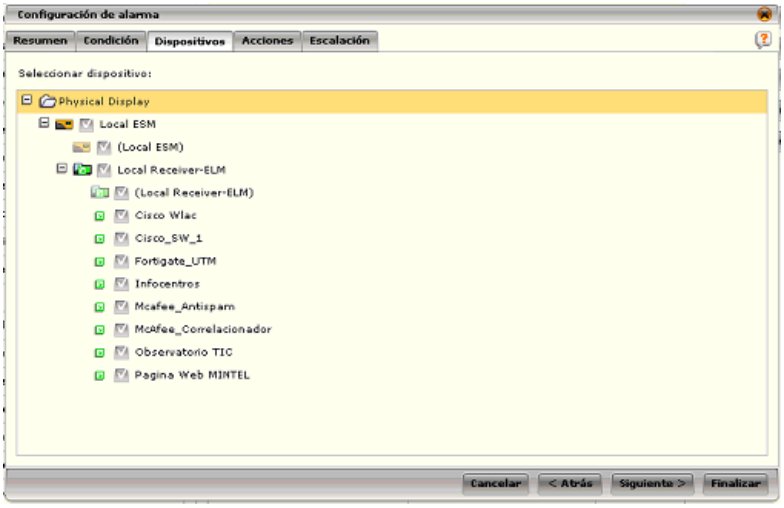


Figura 123. Pantalla de configuración para escoger dispositivos monitoreados por la alarma

En la pestaña **acciones** se define las acciones que se tomarán cuando la alarma se activa. Para este caso de estudio se crearon las siguientes acciones: registro de evento, alerta visual, enviar mensaje a un destinario y crear un caso. En general, cada cuadro de configuración de la herramienta tiene un signo de interrogación, al momento de dar clic ahí se abre en el navegador un tutorial en forma de ayuda donde se explican todas las opciones que se tengan para configurar. En la figura124 se presenta la opción de enviar mensaje y automáticamente se despliega **agregar destinatarios.**

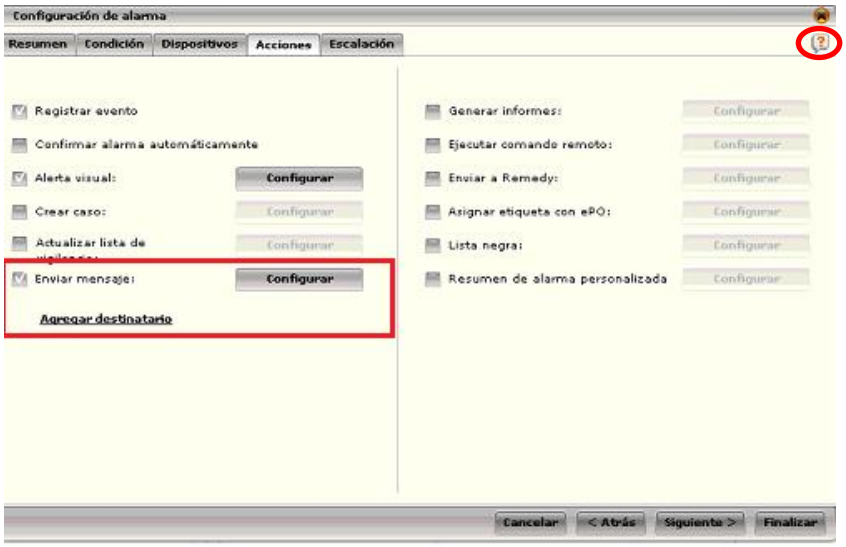


Figura 124. Pantalla de configuración de acciones que serán tomadas para la alarma

Al dar clic en **agregar destinarios** se presenta una pantalla como el de la Figura 125 donde se selecciona los destinarios a los cuales les llegara un correo electrónico cuando suceda o se active la alarma.

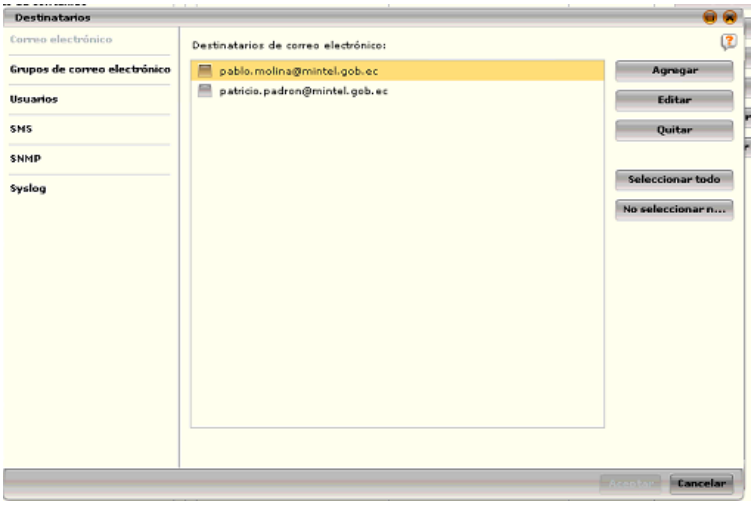


Figura 125. Configuración de destinatarios de correo electrónico cuando la alarma se active

Por ejemplo está llegando al correo de Pablo Molina las alarmas como se indica en la Figura 126.

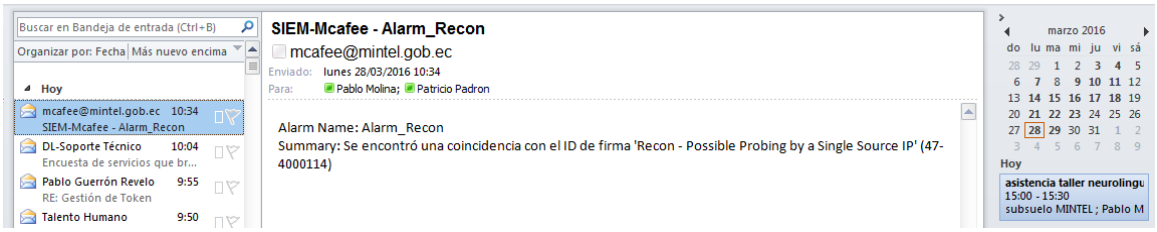


Figura 126. Verificación de recepción de correo electrónico al activarse la alarma Alarm_Recon

Además, para crear un caso cuando la alarma se activa, se da clic en **crear caso** y se abrirá otra pantalla donde se asignará el caso a una persona o a un grupo de personas si se ha creado el grupo. En la Figura 127 se presenta la pantalla al seleccionar la opción crear un caso.

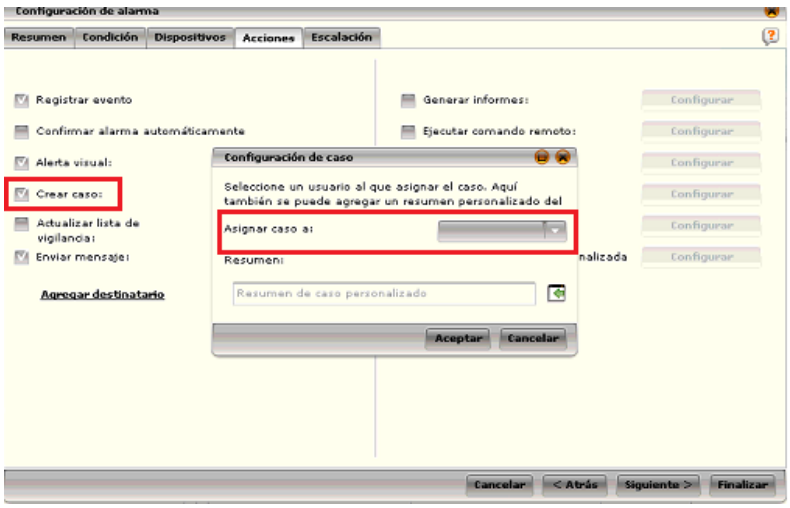


Figura 127. Creación de un caso para asignar a un usuario que resuelva la alarma presentada

Por último en la pestaña **escalación**, sirve para escalar una alarma cuando no ha sido atendida en un período determinado de tiempo, en este caso de estudio no se configuró esta opción ya que no es necesario. En la Figura 128 se presenta la pantalla de escalación.

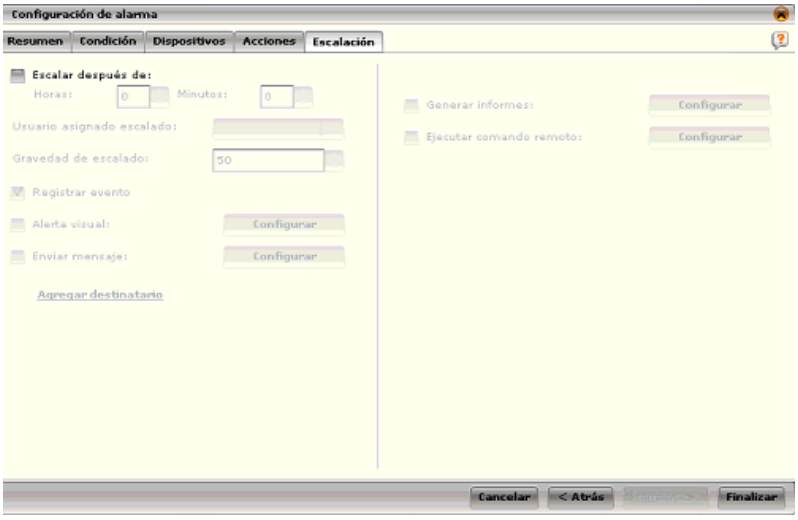


Figura 128.Pantalla para escalar una alarma ESM

En la Figura 129 se presentan todas las alarmas que se activaron durante el tiempo que se tuvo la herramienta funcionando en la red del MINTEL durante el tiempo de prueba, se puede ver en el cuadro inferior izquierdo que se activaron 171 alarmas.

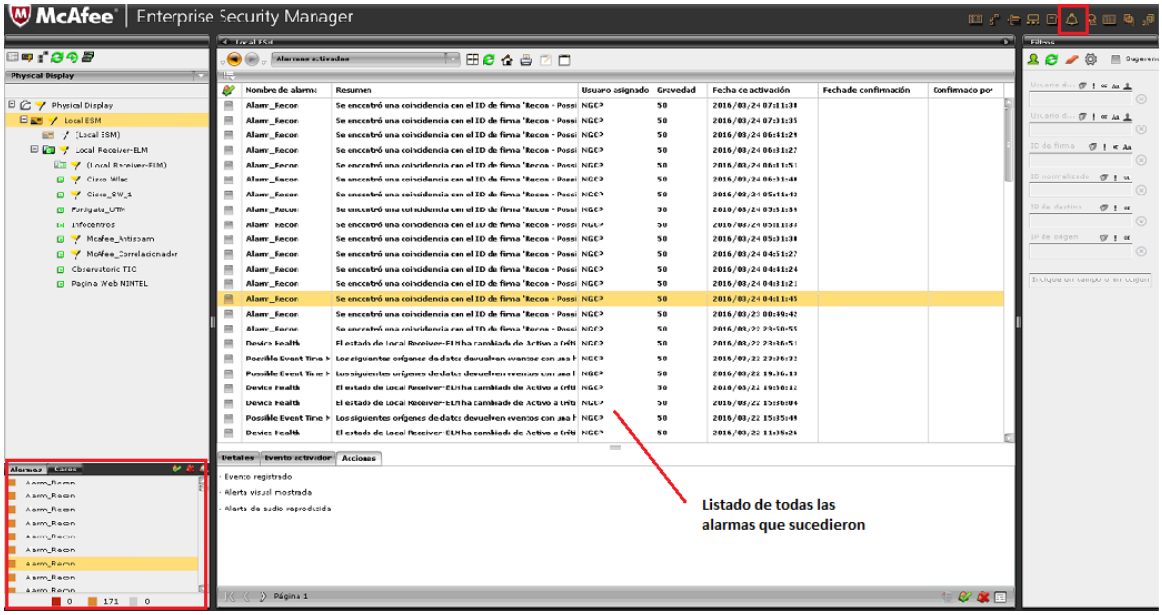


Figura 129. Lista de alarmas activadas para la red del MINTEL

Todas las 171 alarmas activadas son de gravedad media y analizándolas se determinó que la alarma cuyo nombre es **alarm recon** que significa un posible sondeo desde una misma IP es la que puede afectar la seguridad de la red del MINTEL, por lo que hay que darle alguna atención. Se observa que el servidor afectado es el 10.0.104.238 que es el servidor de la página web del MINTEL y el ataque proviene de la IP 5.9.83.211 localizada en Alemania, la explicación de esta alarma fue dada en el ítem 5.2.2.1. En la Figura 130 se indica la alarma seleccionada y en la opción **evento activador** se encontró

los datos expuestos de las IPS de origen y destino indicadas.

Figura 130. Alarma detectada y de criticidad para la red del MINTEL

A continuación se analizarán los eventos de correlación que sucedieron dentro del tiempo que se tuvo activa la herramienta, en la Figura 131 se presenta el resumen de los eventos obtenidos de las correlaciones realizadas y de las que vienen por defecto con la herramienta.

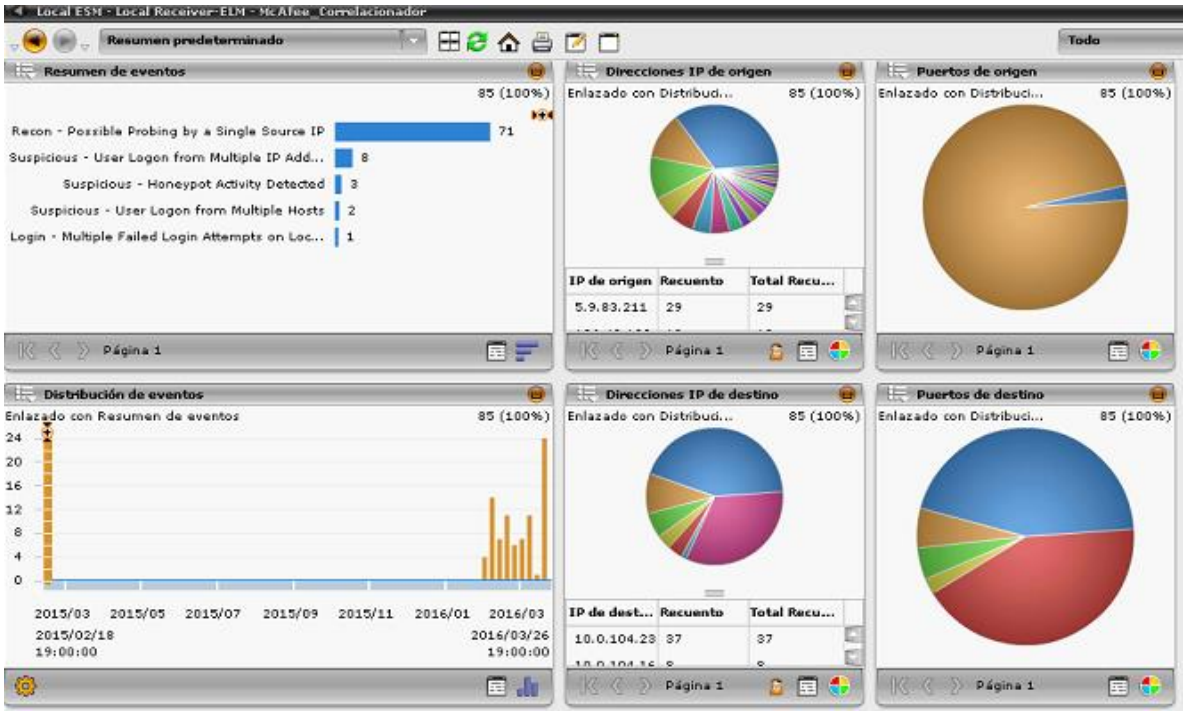


Figura 131. Resumen de eventos obtenidos con el correlacionador automático de la herramienta

En este tablero de control se puede observar que 71 veces se presentó un posible sondeo desde una misma IP (explicada en el párrafo anterior) y en los paneles de dirección de IP de origen y dirección IP de destino se puede observar las IP´s desde donde provienen los ataques y las IP´s de los servidores afectados del MINTEL respectivamente. Se aplicaron los bloqueos a estas IP´s para que no vuelvan a tratar de atacar a la red de la institución. De este mismo tablero se puede observar que se tiene una posible actividad de **Honeyspot detectado**, se tienen 3 eventos de este tipo afectando al servidor 10.0.104.236 desde la IP 198.51.100.11 en Estados Unidos; al realizar averiguaciones de esta IP se trata de una red de prueba localizada en los Ángeles que trata de simular ser una computadora vulnerable o débil para ser atacada, por lo que igualmente se bloqueó esta IP en el equipo de seguridad perimetral. Los otros eventos de correlación son referidos a ingresos fallidos al servidor de ESM y a otros equipos pero que no representa un riesgo de seguridad en la red.

Por último para esta herramienta se analizaron los tableros de control obtenidos de los equipos ingresados en la herramienta obteniéndose los siguientes resultados y análisis:

Equipo de seguridad Fortinet.

Dentro de todos los eventos detectados por este equipo, el que puede representar peligro para la red del MINTEL es el evento del tipo **backdoor: China Chopper Webshell**. Los backdoor son programas diseñados para abrir una "puerta trasera" en el sistema de

modo tal de permitir al creador del backdoor tener acceso al sistema generalmente con fines maliciosos y espionaje. Este ataque China Chopper es un backdoor ampliamente utilizado por atacantes chinos y de otro tipo para acceder remotamente a un servidor web infectado. El despliegue de este malware en el servidor es bastante básico, como la carga útil del servidor en una única línea insertada en cualquier página ASPX; una vez instalado el atacante puede acceder al Shell del servidor y atacarlo.

El ataque se lo está haciendo al servidor 10.0.104.238 (página web del MINTEL) y se observa que se tiene dos IPS realizando este ataque la 49.246.230.40 con un 80 % y la ip 118.193.199.71 con el 20 % de los ataques, provenientes de Hong Kong y China respectivamente, a pesar que estos ataques fueron contenidos por este equipo de seguridad (es decir no sucedieron) por precaución se procedió a bloquear estas IPS para que no traten en un futuro intentar desplegar este programa malicioso en el servidor. En la Figura 132 se presenta la pantalla donde se indica este ataque.

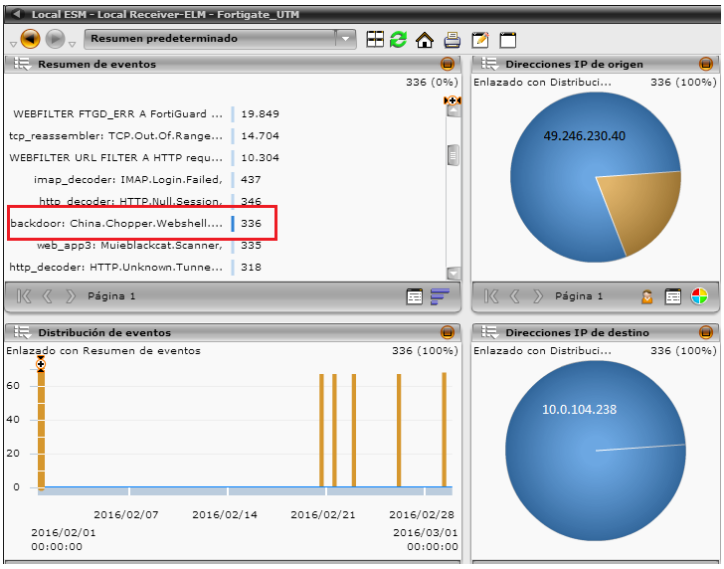


Figura 132.Paneles de ataque China Chopper, número de intentos, IP´s origen-destino

Otro ataque que se está teniendo la página web de la institución y que fue contenido por el Fortinet es el **web_app3: WordPress Slider Revolution File Inclusion** que significa que se está tratando de instalar un archivo en este servidor con el fin de instalar malware en el equipo y poder ingresar para ver los contenidos de cualquier archivo del servidor. Empleando esta técnica podemos leer por ejemplo el archivo wp-config.php y obtener las credenciales de la base de datos del blog WordPress y modificar su contenido lo que causaría un gran impacto en la página web de la institución, como ya ha pasado en otras páginas web de otras instituciones públicas.

El origen de estos ataques se está realizado desde varias IPS siendo la que mayor concurrencia tiene la 37.187.39.2 proveniente de Austria con 18 intentos, se procedió igualmente a bloquear a esta IP en el equipo de seguridad perimetral por seguridad futura.

Otro ataque importante y que tiene muchos eventos es el **web_app3: Muieblackcat Scanner**, que es un scrip/bot, supuestamente de origen ucraniano, que intenta explotar las vulnerabilidades PHP o configuraciones incorrectas del servidor. El origen de este ataque es proveniente de China de la IP 119.188.4.3 teniendo la mayor cantidad de ocurrencias llegando a 115 y queriendo ingresar a algunos servidores como son el del sistema Alfresco (documentación iinterna), página web, correo electrónico, SGSI – Infocentros, por lo que igualmente se analizó la IP en internet encontrando que no es confiable por lo que se procedió a bloquearla así mismo para seguridad futura. En la Figura 133 se presenta la información de estos dos ataques.

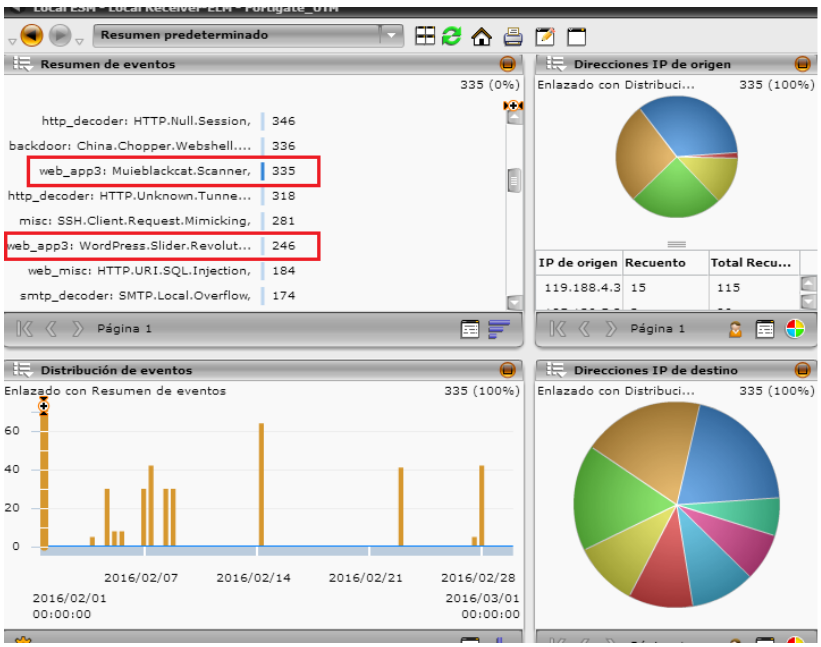


Figura 133. Ataques de riesgo que tiene la página web del MINTEL

Cabe señalar que hay como exportar en forma de un documento cualquiera de los paneles dentro de un tablero de control que tiene la herramienta a un formato tipo texto o pdf, para esto hay que dar clic en  del panel que se quieren sacar los datos y seleccionar la opción **exportar**. En el anexo 1 se presenta el informe del ataque de tipo Scanner.

Servidores Linux: SGSI-Infocentros, Observatorio TIC

No se detectó mayores amenazas a estos servidores conforme los resultados de eventos obtenidos con la herramienta, como datos se puede indicar que en el último mes se han conectado 984.004 veces (teniendo en cuenta que cada clic dentro de la aplicación

se toma como un evento). En la aplicación de observatorio TIC se han conectado 87.068 veces. En la Figura 134 se presentan los eventos para la página web de Infocentros.

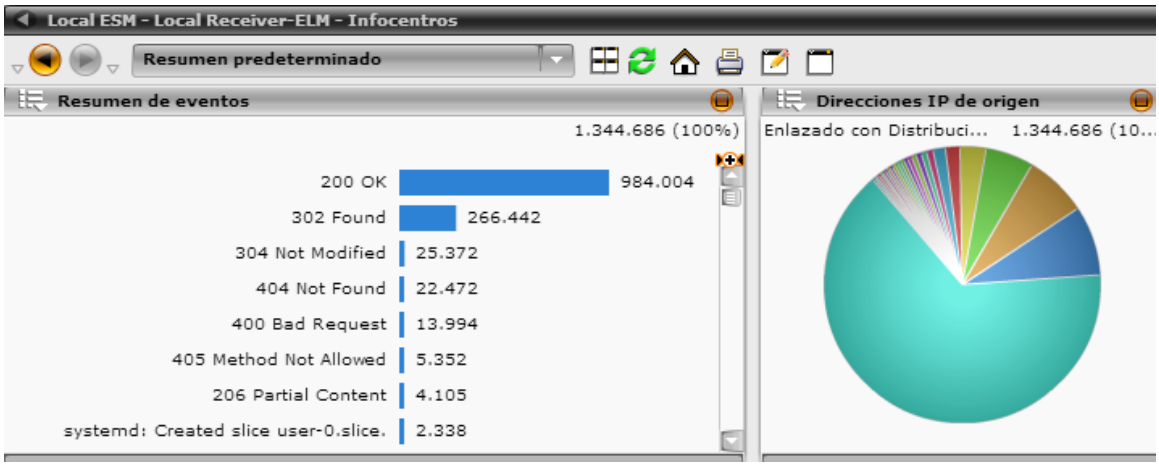


Figura 134. Panel gráfico del resumen de eventos de la página de Infocentros

Servidor de Antispam

Al analizar el tablero de control presentado por la herramienta se observa que durante el último mes se tiene que 240.000 mails fueron entregados y 43.000 fueron categorizados como spam. En la Figura 135 se observa los datos anteriormente mencionados.

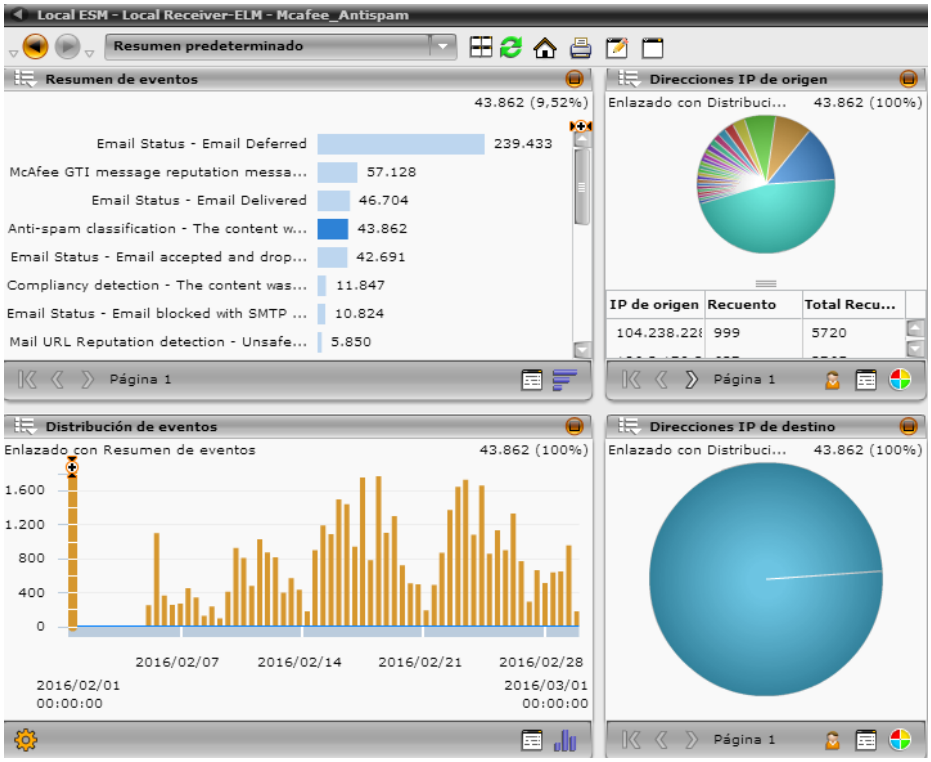


Figura 135. Resumen de eventos del equipo de antispam del MINTEL

Como dato curioso, se pudo detectar en el resumen de eventos del antispam, el evento **user logon SSH logon failed**, cuya IP de origen es la 10.0.104.170 que corresponde al servidor demo de Alienvault-USM, con esto se comprobó el por qué no se estaba recibiendo correos desde esta herramienta en las pruebas realizadas ya que al analizar el detalle de este evento se deduce que USM está utilizando un solo tipo de autenticación el cual no es compatible con lo que se tiene configurado en el servidor de correo del MINTEL actualmente. En la Figura 136 se presenta lo indicado.

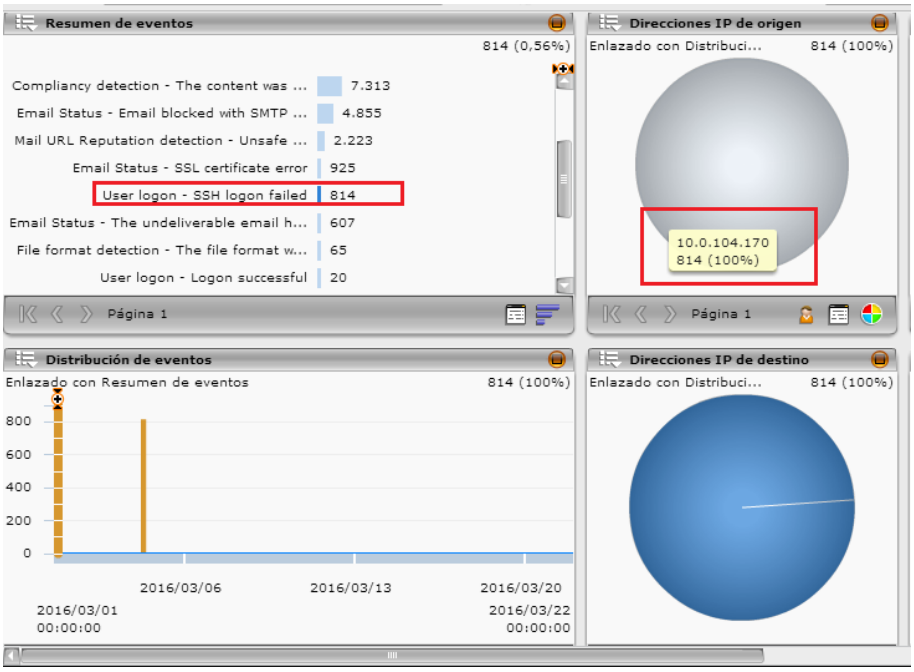


Figura 136. Evento User logon – SSH logon failed

Switch de core

Analizando los eventos para este activo, se puede ver los cambios realizados al equipo, en cisco **IOS router configuration change** en el cual se indica que las IP´s 10.0.105.53 y la 10.0.105.40 realizaron cambios en el equipo en la última semana. Con este tipo de datos se puede verificar las fechas que se han realizado cambios en este equipo y con esto por ejemplo entregarlo en una auditoria de red o para cumplimiento de hitos de acceso dentro del Esquema Gubernamental de Seguridad de la Información – EGSI implementado por la SNAP. Si se da clic en análisis de eventos se puede visualizar los eventos en crudo y también la fecha del evento, lo cual puede servir para realizar un análisis más profundo en caso de ser necesario.

En la Figura 137 se presentan las pantallas de lo expuesto y se ve que el usuario Patricio Padrón ha ingresado el 12 de marzo a realizar un cambio en la configuración por consola.

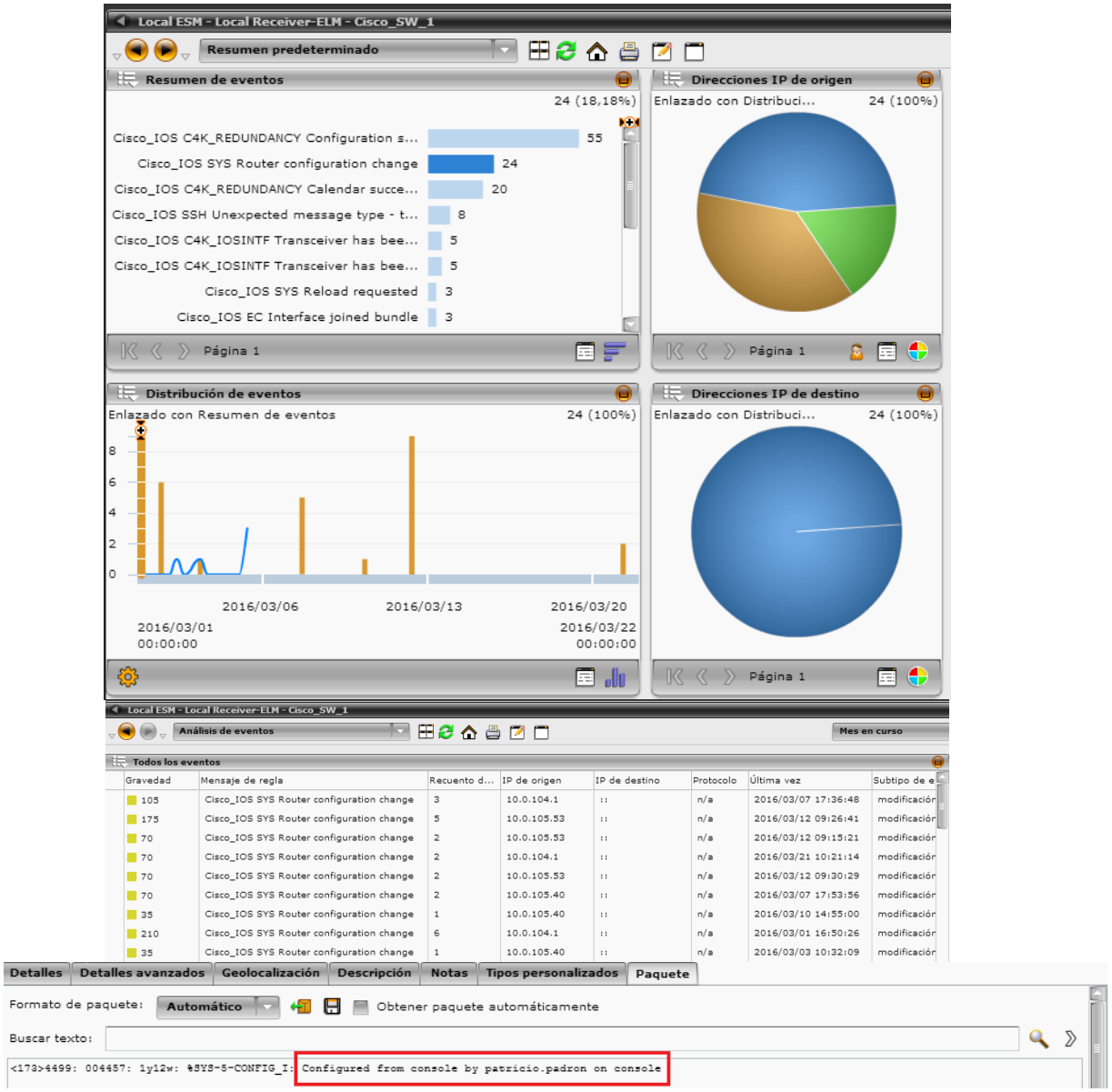


Figura 137. Pantallas obtenidas por ESM de cambios realizados al switch de core del MINTEL

5.4.2 AlienVault-USM

Para esta herramienta las alarmas de seguridad ya vienen predeterminadas en cinco categorías: System compromise, Explotationn & Installation, Delivery &, Reconnaissance & Probing y Environmental Awareness, cada una cumple una función diferente por ejemplo la primera indicará que el sistema operativo puede estar comprometido, lo que puede hacer que el equipo se torne lento ya que se está consumiendo recursos por alguna causa.

Para ver las alarmas que se detectaron con USM se debe dar clic en **análisis** y seleccionar la opción **alarmas**, en la Figura 138 se indica la pantalla de alarmas que se obtuvieron para la red del MINTEL en el tiempo de prueba, cabe señalar que las alarmas se presentan en forma de burbujas para el usuario, mientras la burbuja sea más grande significa que la alarma ha sucedido muchas veces en el mismo día.

Figura 138. Pantalla de alarmas de la herramienta USM

A continuación se realiza un análisis de las alarmas encontradas en el tiempo que se tuvo en prueba la herramienta para este caso de estudio.

Alertas System Compromise:

Solo se encuentra una alarma en esta categoría y la cual indica que se está usando el método **Sinkhole-Anubis** como método de ataque, el mismo redirige robots en una botnet para máquinas específicas y poder capturar datos de ellas, es decir utiliza un equipo con un botnet para hacer spam, con esto el equipo de la red del MINTEL será un repetidor para enviar al mundo spam y verían a este equipo como un emisor del spam. El equipo comprometido es el 10.0.104.90 que es el servidor de active directory y el ataque proviene de la IP pública 195.22.26.248 que buscando en foros es un servidor de botnet proveniente de Portugal y que es reconocido por sus ataques por lo que se procedió a bloquear esta IP en el equipo de seguridad perimetral. En la Figura 139 se presentan los detalles del evento de este ataque al dar clic en esta alarma.

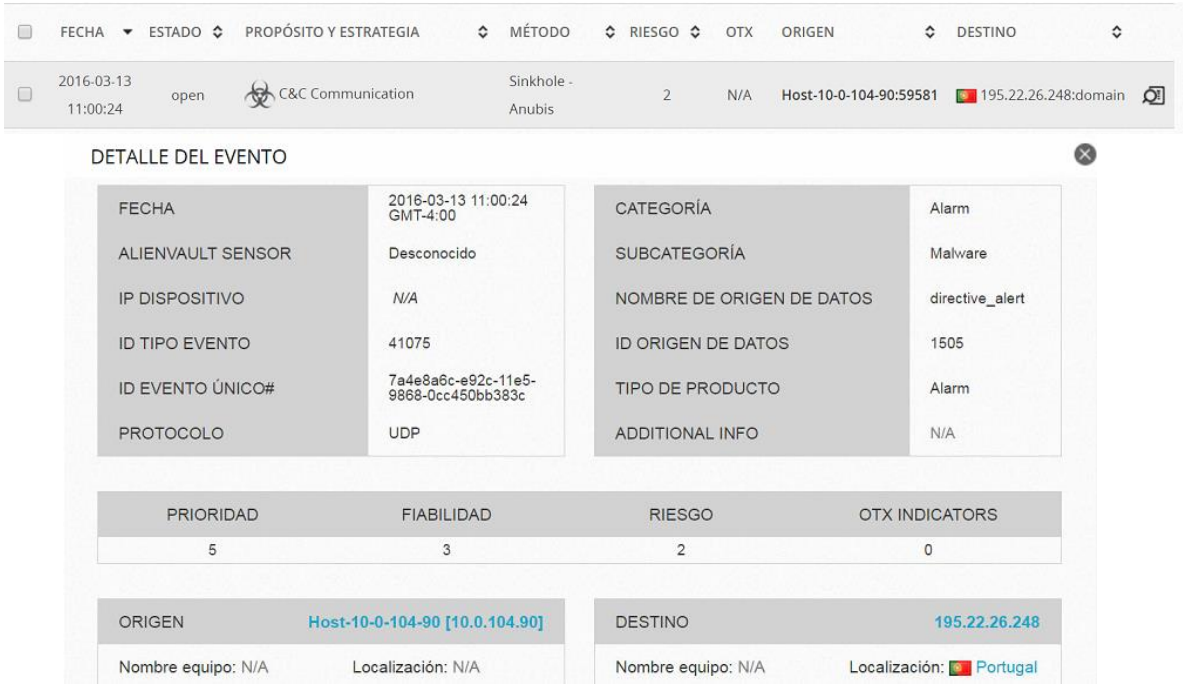


Figura 139. Detalles de evento Sinkole-Anubis

Alarmas Explotationn & Installation

No se activó ninguna alarma de este tipo.

Alarmas Delivery and attack

Se tienen muchas alarmas de este tipo en diferentes días pero analizando cada una de ellas se observa que utilizan el mismo método y que consisten en la autenticación de fuerza bruta cuyo origen y destino es la misma IP 10.0.104.90 – servidor de active directory, en la Figura 140 se presenta la pantalla que se obtiene al dar clic en alguna burbuja de esta categoría de alarma.

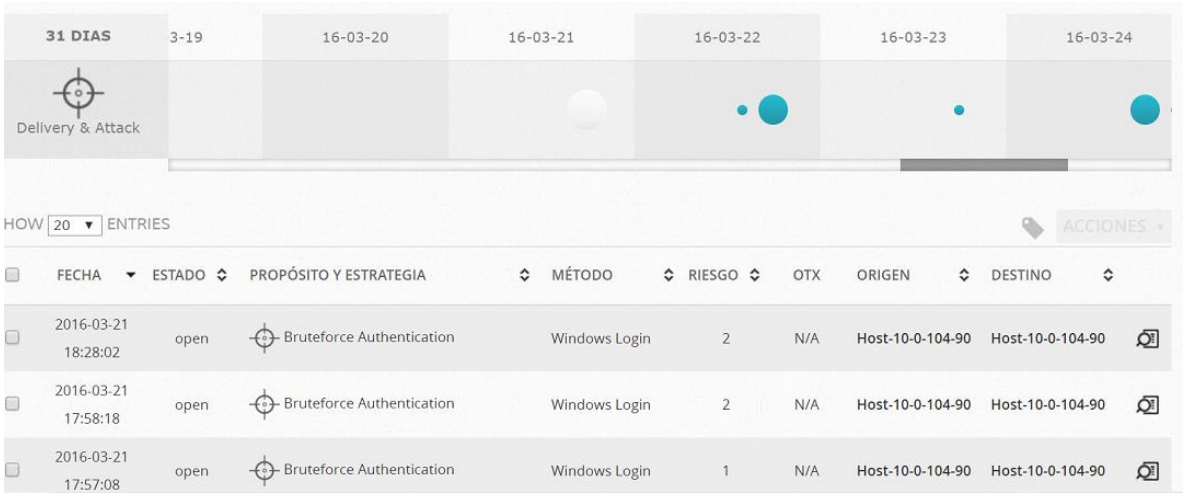


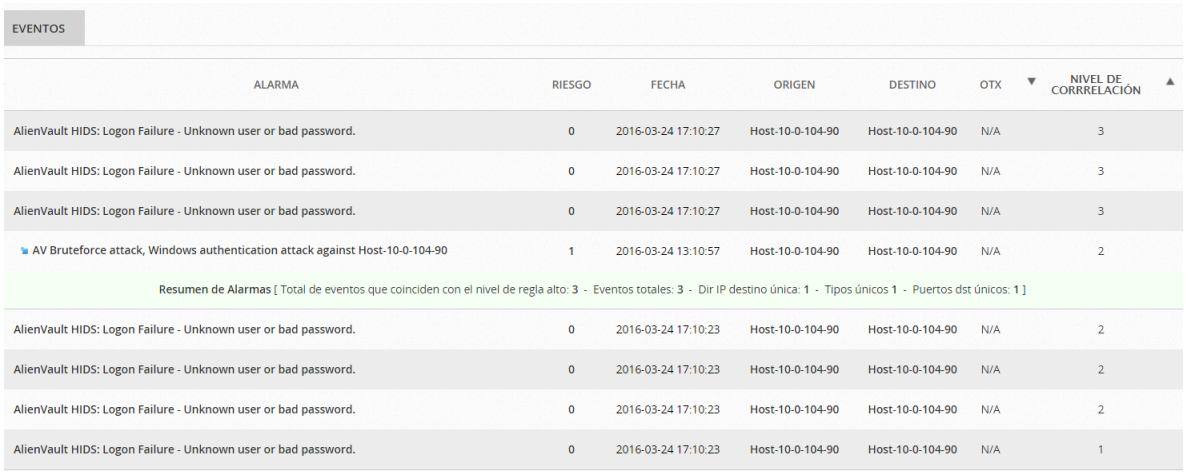
Figura 140. Lista de alarmas del tipo Delivey-Attack

Por lo tanto se tuvo que profundizar más en las características del evento para analizarlo, para esto se da clic en cualquiera de las entradas de la alarma y se llega a una pantalla como el de la Figura 141, donde se específica el número total de eventos, la fecha en la cual se produjeron, la duración y el tiempo transcurrido en días que no se ha dado atención a la alarma.

Figura 141. Información del evento de la alarma Bruteforce Authentication

Al dar clic en **ver detalles** se obtiene una nueva pantalla con más características del evento y en donde se pueden ver los siguientes datos del evento: alarmas, riesgo,

fecha, origen, destino, OTX y nivel de correlación. En la Figura 142 se presenta lo indicado.



EVENTOS

ALARMA	RIESGO	FECHA	ORIGEN	DESTINO	OTX	NIVEL DE CORRELACIÓN
AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-03-24 17:10:27	Host-10-0-104-90	Host-10-0-104-90	N/A	3
AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-03-24 17:10:27	Host-10-0-104-90	Host-10-0-104-90	N/A	3
AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-03-24 17:10:27	Host-10-0-104-90	Host-10-0-104-90	N/A	3
AV Bruteforce attack, Windows authentication attack against Host-10-0-104-90	1	2016-03-24 13:10:57	Host-10-0-104-90	Host-10-0-104-90	N/A	2
Resumen de Alarmas [Total de eventos que coinciden con el nivel de regla alto: **3** - Eventos totales: **3** - Dir IP destino única: **1** - Tipos únicos **1** - Puertos dst únicos: **1**]						
AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-03-24 17:10:23	Host-10-0-104-90	Host-10-0-104-90	N/A	2
AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-03-24 17:10:23	Host-10-0-104-90	Host-10-0-104-90	N/A	2
AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-03-24 17:10:23	Host-10-0-104-90	Host-10-0-104-90	N/A	2
AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-03-24 17:10:23	Host-10-0-104-90	Host-10-0-104-90	N/A	1

Figura 142. Detalles del evento de la alarma y nivel de correlación

Al dar clic en alguno de estos eventos de la alarma seleccionada se presenta un detalle más profundo y ahí se pudo observar que en todos los casos una máquina del MINTEL cuyo host es LUIONXMFJAL001 tiene muchos intentos de ingresos fallidos - logon failure, por lo que se presume que esta máquina ha sido atacada e infectada y está corriendo algún tipo de troyano que está intentando robar credenciales por lo que se procedió a formatear la máquina; cabe señalar que el antivirus no lo detectaba. En la Figura 143 se presenta la pantalla con el detalle de los eventos.

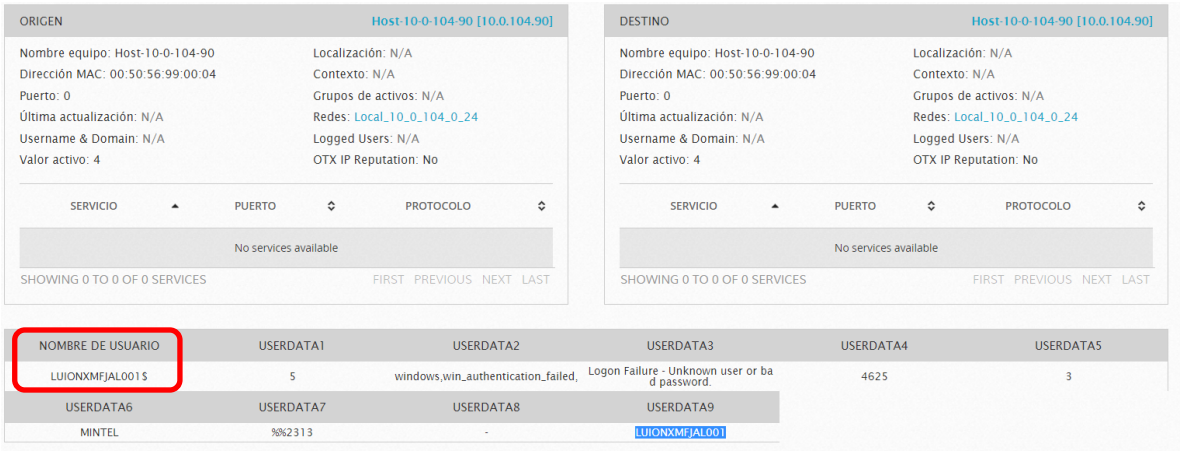


Figura 143. Información detallada de los eventos de la alarma

Alarmas Reconnaissance and probing

Solo se tiene una alarma en esta categoría y el método de ataque que está utilizando es **portscan** que es una técnica para hacer un escaneo de los puertos utilizando un programa llamado nmap y con esto tratar de ingresar a algún equipo, hay dos servidores comprometidos con este escaneo y que son: página web y el servidor de Lync, se presume que son atacados ya que los dos servidores tienen servicios hacia el mundo lo que los hace más vulnerables a cualquier tipo de ataque; el origen de los ataques son desde las IP´s 190.171.118.143 de Costa Rica y de la IP 61.240.144.67 de China, por lo que se procedió a bloquear estas IPS en el equipo de seguridad perimetral. En la Figura 144 se presenta el detalle de este ataque.

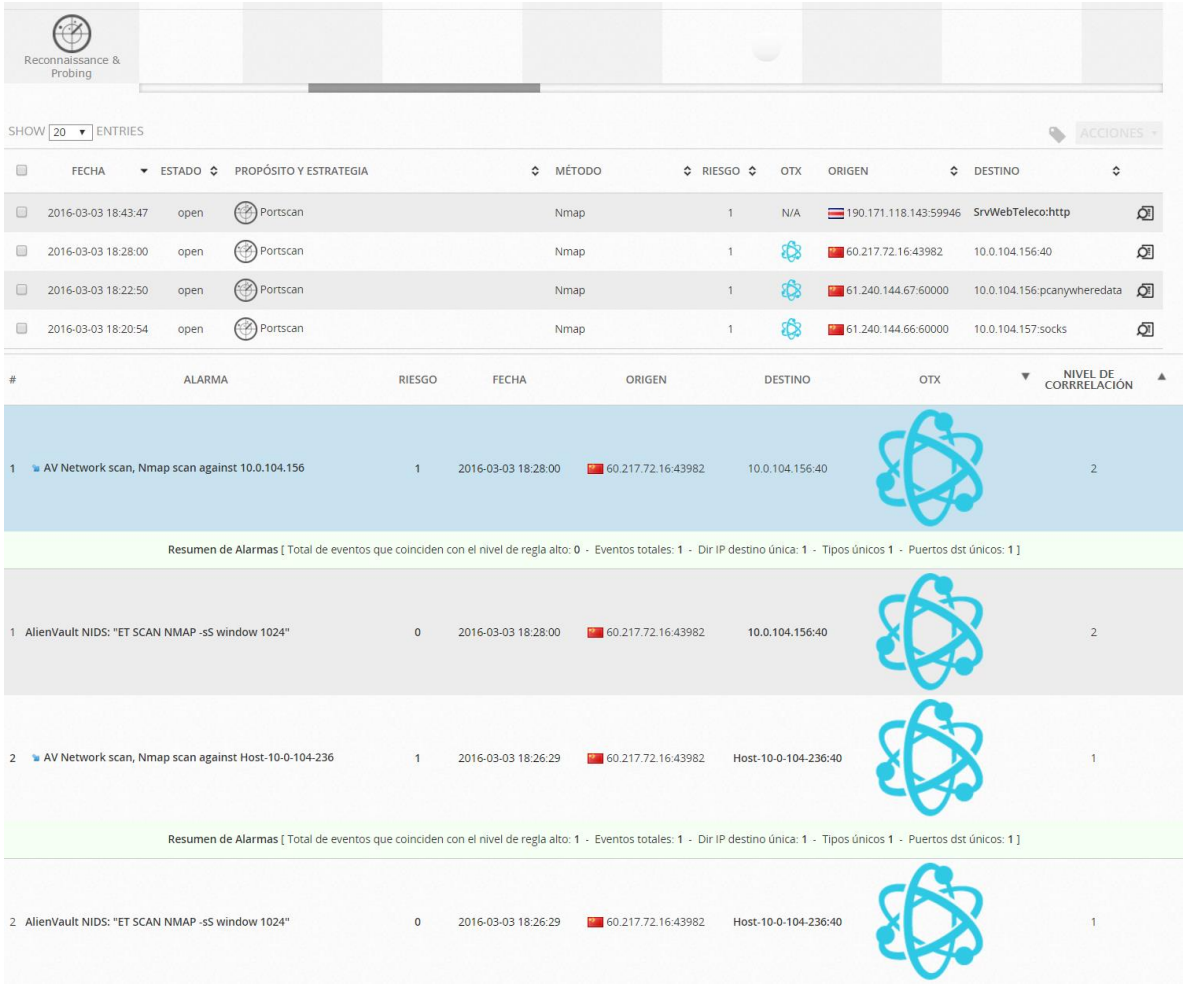


Figura 144. Detalles de la alarma Reconnaissance and probing

Se pudo observar para este caso que el ataque tiene reputación en OTX lo cual significa que este tipo de ataques ya fue identificado y se lo tiene agregado a la base de datos que tiene AlienVault, para ver los detalles en OTX se da clic en el símbolo celeste de OTX y se presenta una pantalla como el de la Figura 145 donde se encuentran los datos de la reputación de la IP.

Figura 145. Detalles de reputación de la IP de OTX

Al dar clic en  se conecta con la página web de OTX y ahí se presenta un resumen del tipo de ataque con sus causas y en algunos casos se da los consejos de como remediarlo.

Alarmas Environmental Awareness

Todas las alarmas detectadas en esta categoría son del tipo **acount lockout** que corresponde directamente con el active directory y suceden cuando los usuarios tratan de ingresar y se les bloquea la cuenta por cualquier motivo, por lo que no representan un riesgo para la red. Lo que sí se ejecutó es verificar a que usuarios les está pasando esto y conversar con ellos para ver porque se les está bloqueando sus cuentas de usuario. En la Figura 146 se presenta los detalles de esta alarma.

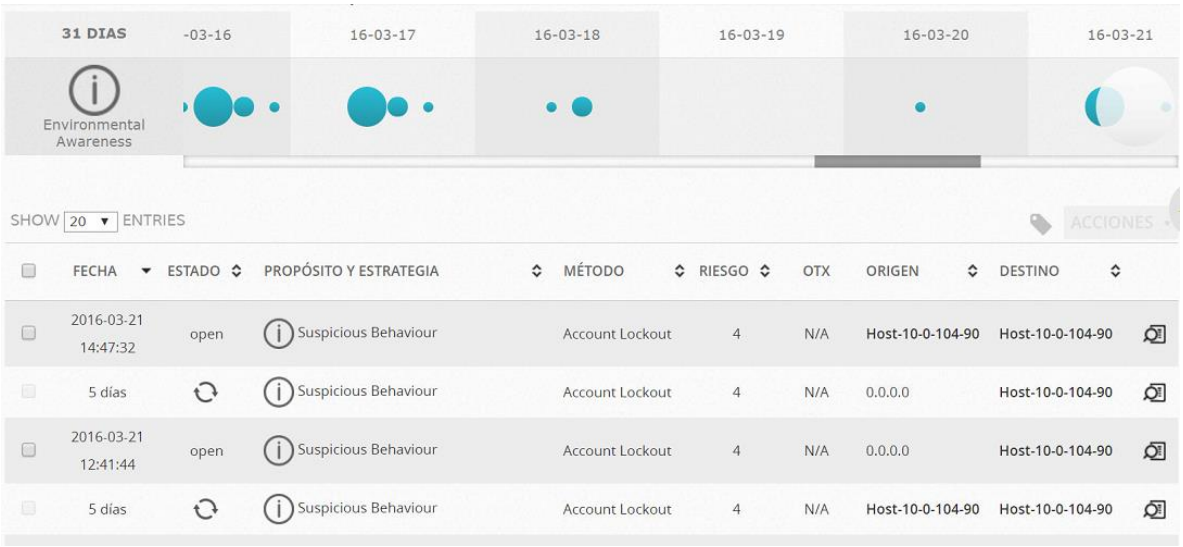


Figura 146. Detalles de la alarma Environmental Awareness

Lo que resta de hablar sobre alarmas para esta herramienta es realizar alguna acción cuando estas se activen, se tienen las siguientes opciones: crear ticket, cerrar alarma, borrar la alarma o aprender más sobre la alarma. En la Figura 147 se presentan las opciones detalladas anteriormente.

Figura 147. Acciones que se pueden tomar para las alarmas

Para crear un **ticket** se selecciona esta opción y aparecerá una pantalla como el de la Figura 148, en donde se tiene que llenar los siguientes datos: asignar a, prioridad, tipo, IP´s de origen y destino y la fecha de inicio y fin de los eventos citados.

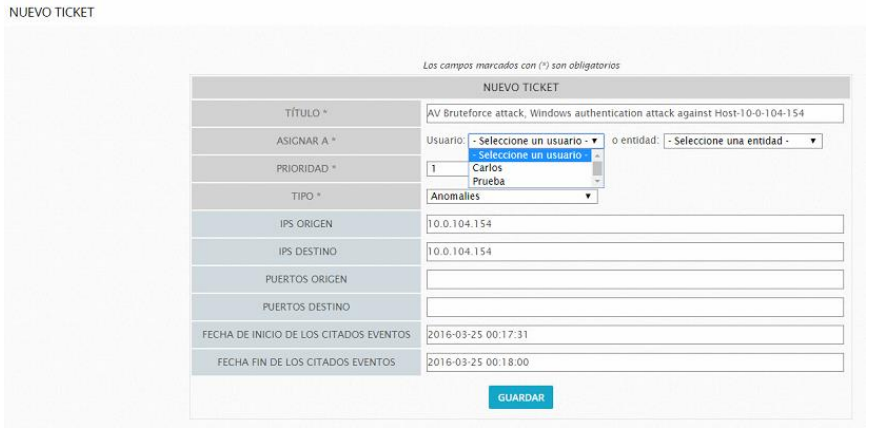


Figura 148. Pantalla para configurar un ticket a partir de una alarma

Al dar clic en **aprender más** –learn more, se despliega una pantalla con una explicación más detallada del evento entregada por una base de conocimiento de AlienVault. En la pantalla 149 se observa la pantalla de aprender más de la alarma seleccionada.

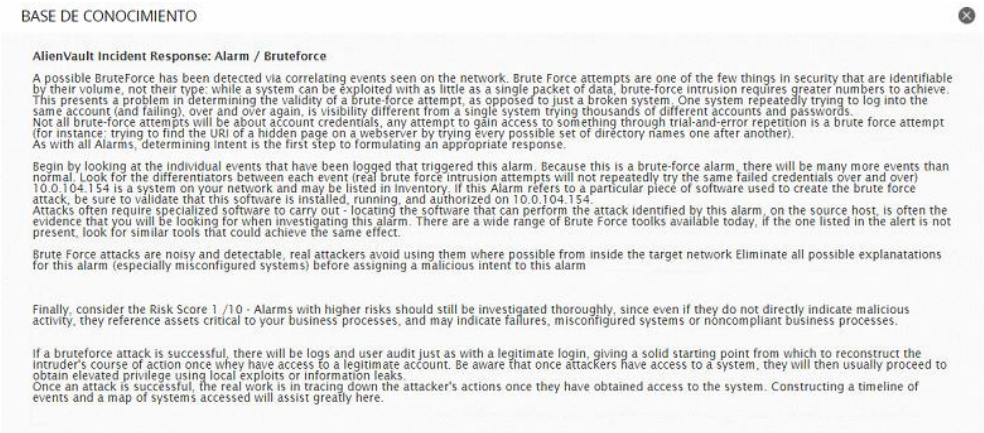


Figura 149. Pantalla de base de conocimiento dado por AlienVault para la alarma seleccionada

Una vez analizadas las alarmas de la herramienta, a continuación se procederá al análisis de las vulnerabilidades encontradas en la red obtenidas por la aplicación, para detectar la mayoría de vulnerabilidades se debe primero ingresar la mayor cantidad de activos (equipos) y después realizar un escaneo de vulnerabilidades. Para realizar esta acción se selecciona la pestaña de **entorno**, se escoge la opción **vulnerabilidades** y después se elige la pestaña **trabajo de escaneo**, esto se puede visualizar en los cuadros en rojo resaltados en la Figura 150.

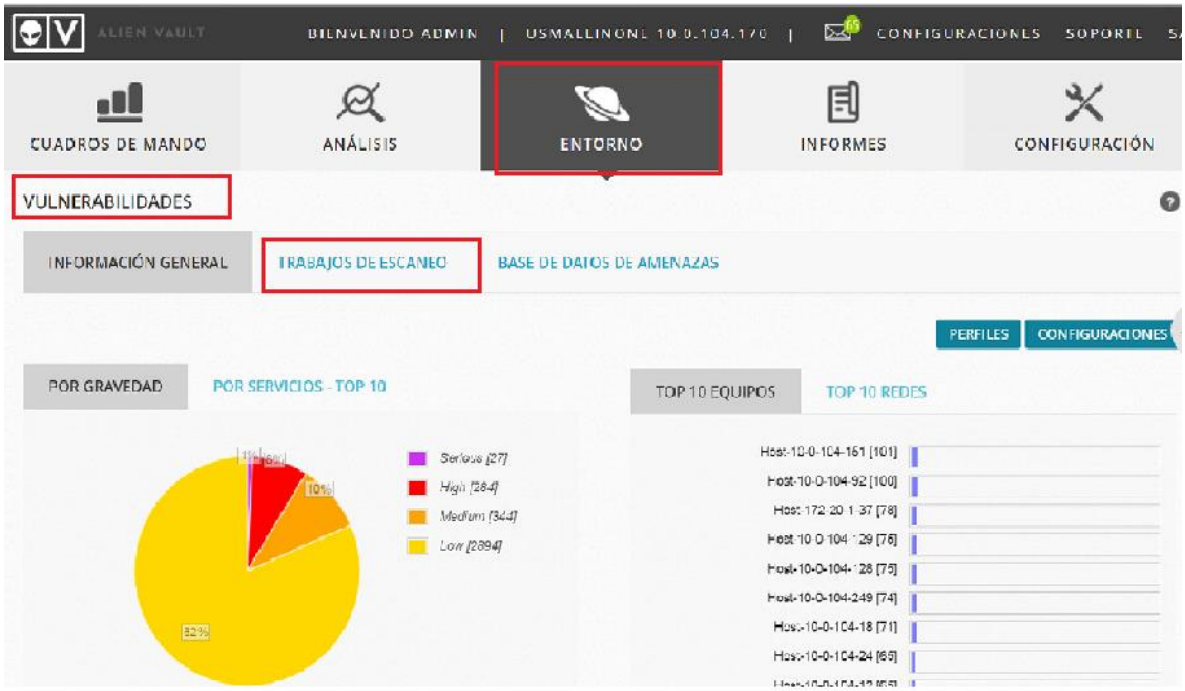


Figura 150. Pantalla inicial para configurar un nuevo trabajo de escaneo de vulnerabilidades

A continuación se selecciona **nuevo trabajo de escaneo**, donde se presentará una pantalla como el de la Figura 151., aquí se llenaran los siguientes datos: nombre del trabajo, por ejemplo escaneo red de servidores, el sensor que realizará el trabajo (en este

caso USM), el perfil de trabajo (se selecciona por defecto para no saturar ningún equipo), la calendarización del escaneo con su inicio, frecuencia y a qué hora se lo realizará y por último se selecciona los activos a los cuales se realizará el escaneo de vulnerabilidades.

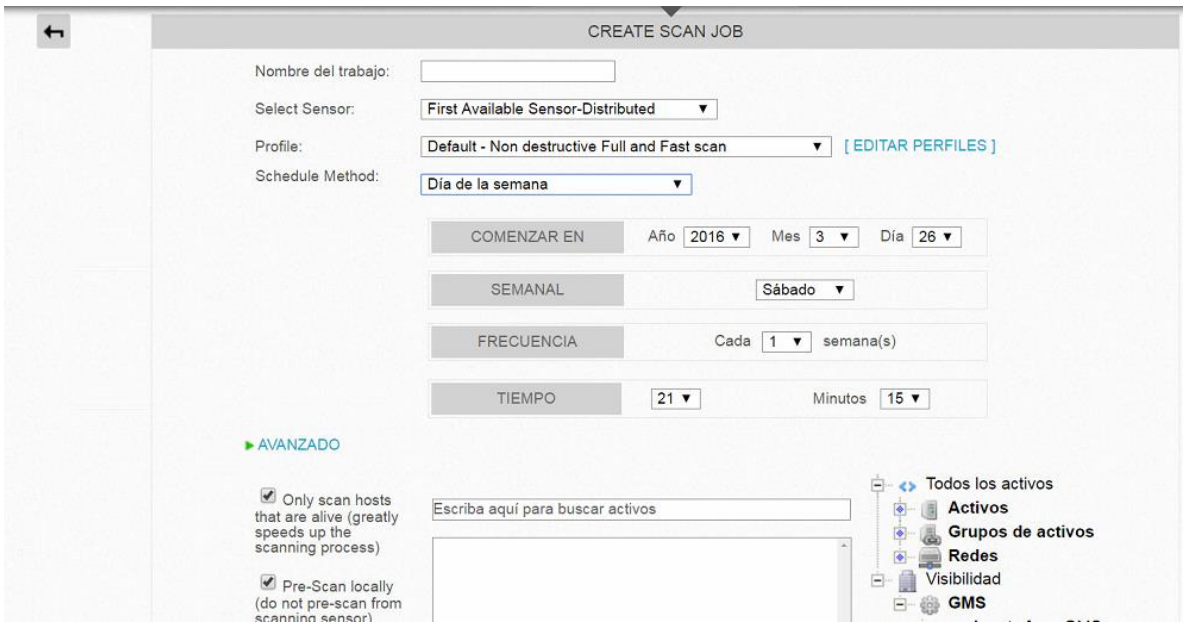


Figura 151. Pantalla para crear un nuevo trabajo de escaneo de vulnerabilidades

El escaneo de vulnerabilidades puede ser realizado por ejemplo cada semana para toda la red y así encontrar nuevas vulnerabilidades en caso de existir. Una vez realizado el escaneo, ingresando a la opción de **vulnerabilidades** se despliega el gráfico en forma de pastel donde se indican todas las vulnerabilidades categorizadas por gravedad que se han encontrado en la red. En este caso de estudio se analizarán todas las vulnerabilidades con gravedad **serius**, que en total son 27, también se puede ver que existen 284 vulnerabilidades con categoría **high**. En la Figura 152 se presenta el gráfico de vulnerabilidades.

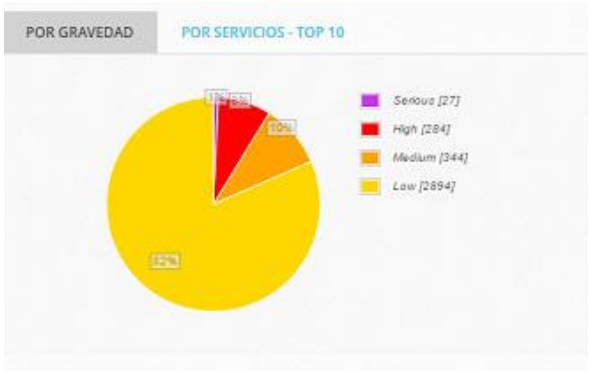


Figura 152. Panel gráfico de número de vulnerabilidades categorizadas

En la Figura 153 se presenta la lista de vulnerabilidades clasificadas por su gravedad que se encuentran en la parte inferior del gráfico de pastel.

EQUIPO - IP	FECHA/TIEMPO	PERFIL	SERI	HIGH	MEDI	LOW	INFO	
All	-	-	27	284	344	2894	0	
Host-10-0-104-151 (10.0.104.151)	2016-03-04 15:48:18	Default	0	2	17	82	0	
Host-10-0-104-92 (10.0.104.92)	2016-03-04 15:48:18	Default	0	2	18	80	0	
Host-172-20-1-37 (172.20.1.37)	2016-03-04 15:48:18	Default	1	5	10	62	0	
Host-10-0-104-129 (10.0.104.129)	2016-03-04 15:48:03	Default	1	2	8	64	0	

Figura 153. Detalle de vulnerabilidades categorizadas por gravedad y número

Se puede ver detalles de la vulnerabilidad mediante documentos, mismos que se presentan en tres tipos de formatos: html, pdf y exel, una vez que se abrió estos documentos se observó que el documento más fácil de entender fue en formato exel ya que presenta una forma estructurada. En el anexo 2 se presenta un archivo en exel con detalles de la vulnerabilidad para el servidor de impresiones.

En la Figura 154 se presenta el documento en html para una vulnerabilidad detectada en el equipo 172.20.1.37 que pertenece a la red de una adscrita al MINTEL que es la ARCOTEL, este equipo se lo puede visibilizar dentro de la red ya que se tiene comunicación entre estas dos entidades para compartir un servicio desde la red de la adscrita y se puede observar en el recuadro en rojo la solución o remediación para esta vulnerabilidad la misma que consiste en realizar una actualización del sistema operativo Windows en ese equipo.

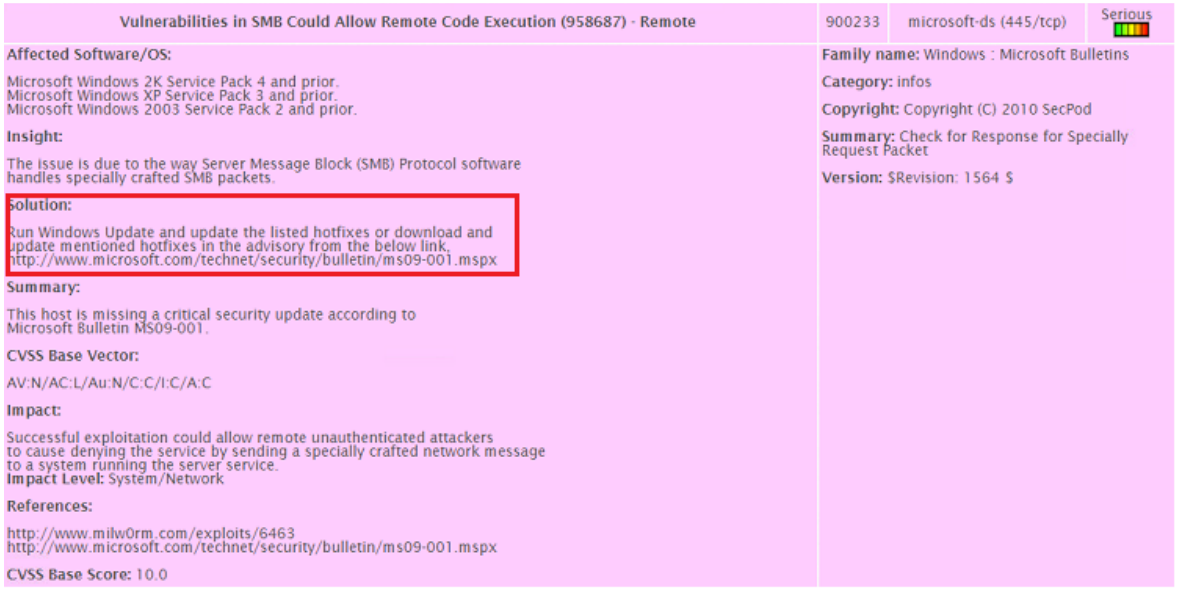


Figura 154. Documento en html de una de las vulnerabilidades categorizada serius detectadas

Para todas las vulnerabilidades con gravedad “serius” encontradas se analizó poder aplicar la solución recomendada por la herramienta y en algunos casos si se lo pudo hacer, en otros tocará hacerlo solicitando una ventana de mantenimiento y en muy pocas se deberá analizar bien que afectaciones puede tener en el servicio al realizar el trabajo indicado. En la tabla 1 se presenta un resumen de las vulnerabilidades

categorizadas como “serius” en cuyas columnas se presenta el equipo comprometido, que vulnerabilidad se detectó y que acción se debe tomar para mitigarla.

Tabla 1. AlienVault: I.T Security Vulnerabiliy Report

Host IP	Vulnerability	Remedation
172.20.1.37 máquina de ARCOTEL	Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote Family name: Windows : Microsoft Bulletins Category: infos Copyright: Copyright (C) 2010 SecPod Version: $Revision: 1564 $	Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx
10.0.104.129 Vcenter 2, centro de administración virtual	VMSA-2015-0007 VMware vCenter Server Multiple Vulnerabilities Family name: General Category: infos Copyright: This script is Copyright (C) 2014 Greenbone Networks GmbH Version: $Revision: 2435 $	Apply the missing patch(es).
10.0.104.128 Vcenter 1, centro de administración virtual	VMSA-2015-0007 VMware vCenter Server Multiple Vulnerabilities Family name: General Category: infos Copyright: This script is Copyright (C) 2014 Greenbone Networks GmbH Version: $Revision: 2435 $	Apply the missing patch(es).

10.0.104.18 Servidor de cintas de respaldo-Data Protector	HP Data Protector Multiple Vulnerabilities Family name: General Category: attack Copyright: Copyright (C) 2014 Greenbone Networks GmbH Version: $Revision: 2780 $	Apply the patch from below link, https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04373818
10.0.104.24 10.0.104.12 10.0.104.22 10.0.104.23 10.0.104.11 10.0.104.13 10.0.104.19 10.0.104.15 10.0.104.21 10.0.104.10 10.0.104.20 10.0.104.16 Servidores Vmware Esxi, software que admisnistra los servidores de las cuchillas	VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check) Family name: General Category: infos Copyright: This script is Copyright (C) 2015 Greenbone Networks GmbH Version: $Revision: 2748 $	Apply the missing patch(es).
10.0.104.164 Servidor virtual para Splunk	Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387) Family name: Windows : Microsoft Bulletins Category: infos Copyright: Copyright (C) 2012 SecPod & ITrust Version: $Revision: 2752 $	Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://technet.microsoft.com/en-us/security/bulletin/ms12-020

10.0.104.130 Servidor de pruebas	VMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check) Family name: General Category: infos Copyright: This script is Copyright (C) 2015 Greenbone Networks GmbH Version: $Revision: 2748 $	Apply the missing patch(es).
10.0.104.118 Servidor de pruebas para nueva aplicación del MINTEL llamado SIADI	PostgreSQL no password Family name: Default Accounts Category: attack Copyright: This script is Copyright (C) 2013 Greenbone Networks GmbH Version: $Revision: 2064 $	Set a password as soon as possible.
10.0.104.254 Servidor de SQL base de datos	MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) Family name: Web application abuses Category: attack Copyright: This script is Copyright (C) 2015 Greenbone Networks GmbH Version: $Revision: 2646 $	Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-034
10.0.104.254 Servidor de SQL base de datos	HP Data Protector Multiple Vulnerabilities Family name: General Category: attack Copyright: Copyright (C) 2014 Greenbone Networks GmbH Version: $Revision: 2780 $	Apply the patch from below link, https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04373818

10.0.104.252 Servidor de impresiones	MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) Family name: Web application abuses Category: attack Copyright: This script is Copyright (C) 2015 Greenbone Networks GmbH Version: $Revision: 2646 $	Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-034
10.0.104.97 Servidor de actualizaciones de windoes WSUS	MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) Family name: Web application abuses Category: attack Copyright: This script is Copyright (C) 2015 Greenbone Networks GmbH Version: $Revision: 2646 $	Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-034
10.0.104.251 Servidor de almacenamiento NAS	HP Data Protector Multiple Vulnerabilities Family name: General Category: attack Copyright: Copyright (C) 2014 Greenbone Networks GmbH Version: $Revision: 2780 $	Apply the patch from below link, https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04373818
10.0.104.110 Servidor para control de accesos al despacho	Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability Family name: Windows : Microsoft Bulletins Category: infos Copyright: Copyright (C) 2009 SecPod Version: $Revision: 1564 $	n/a

10.0.104.110 Servidor para control de accesos al despacho	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) Family name: Windows : Microsoft Bulletins Category: attack Copyright: Copyright (C) 2010 SecPod Version: $Revision: 1564 $	Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx
10.0.104.152 Servidor de Lync	Microsoft SQL Server Multiple Vulnerabilities (3065718) - Remote Family name: Windows : Microsoft Bulletins Category: infos Copyright: Copyright (C) 2015 Greenbone Networks GmbH Version: $Revision: 2646 $	Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from this link, https://technet.microsoft.com/library/security/MS15-058
High		
10.0.104.253 Servidor de aplicativo SGSI	http TRACE XSS attack Family name: Web application abuses Category: infos Copyright: This script is Copyright (C) 2003 E-Soft Inc. Version: $Revision: 2435 $	Disable these methods.
10.0.104.238 Servidor de página web	SSL Certification Expired Family name: General Category: infos Copyright: This script is Copyright (C) 2013 Greenbone Networks GmbH Version: $Revision: 2011 $	Replace the SSL certificate by a new one.

10.0.104.238 Servidor de página web	http TRACE XSS attack Family name: Web application abuses Category: infos Copyright: This script is Copyright (C) 2003 E-Soft Inc. Version: $Revision: 2435 $	Disable these methods.

Por otro lado, con la opción de SIEM que viene incluido dentro de la herramienta se analizó los eventos que llegaron a USM y gracias a las varias opciones de filtros que vienen instalados se pudo determinar ciertos eventos que pueden considerarse nocivos para la red. Para ingresar al SIEM, se selecciona la pestaña de **análisis** y se escoge la opción **eventos SIEM** y se despliega una pantalla como el de la Figura 155, ahí en el recuadro en rojo se puede observar los diferentes filtros que vienen por defecto con la herramienta, cada filtro tiene algunas opciones para seleccionar según lo que se desee analizar.

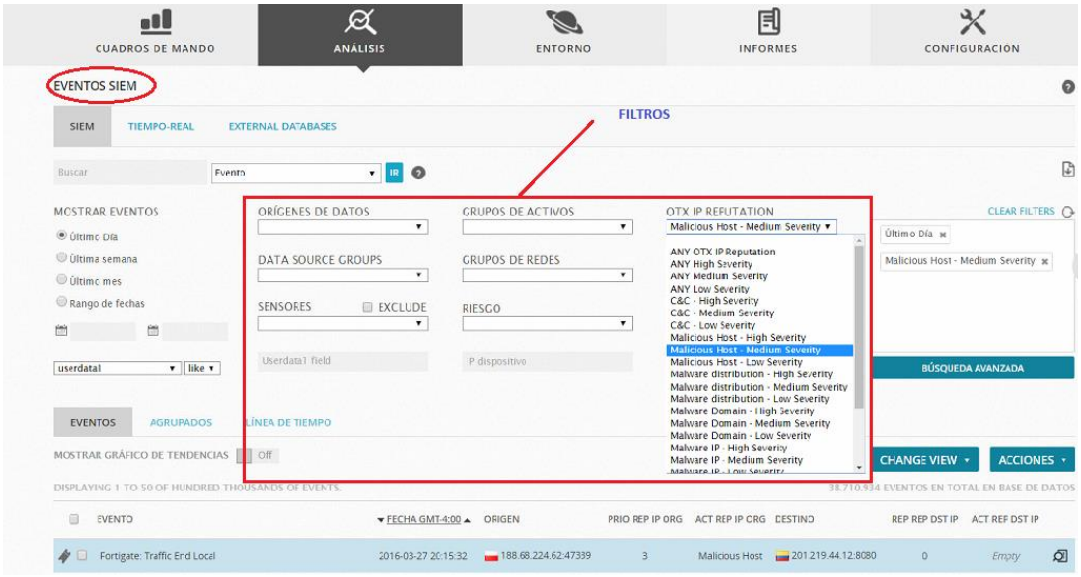
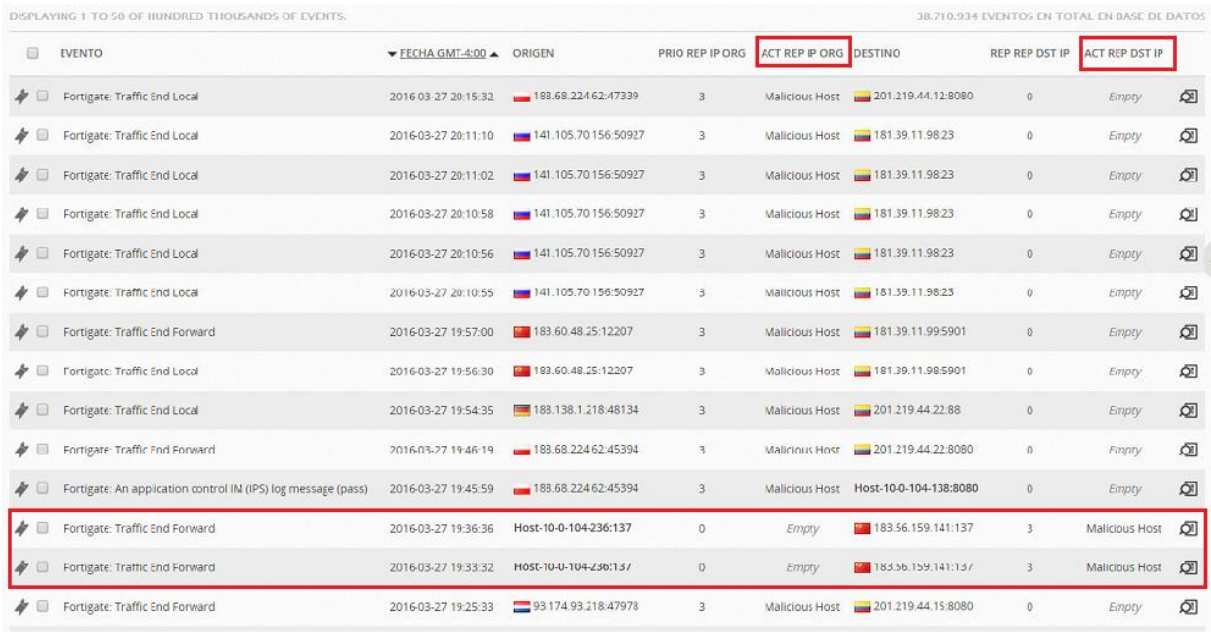


Figura 155. Opciones de filtros para los eventos SIEM de la herramienta

Por ejemplo se filtró por **OTX IP reputation** y se seleccionó la opción **malicius host – médium severity** y se obtuvo todos los eventos de este tipo, en la Figura 156 se presenta la pantalla que se despliega al escoger este tipo de filtro.



DISPLAYING 1 TO 50 OF HUNDRED THOUSANDS OF EVENTS. 38.710.934 EVENTOS EN TOTAL EN BASE DE DATOS

EVENTO	FECHA GMT-4:00	ORIGEN	PRIO REP IP ORG	ACT REP IP ORG	DESTINO	REP REP DST IP	ACT REP DST IP
Fortigate: Traffic End Local	2016-03-27 20:15:32	188.68.224.62:47339	3	Malicious Host	201.219.44.12:8080	0	Empty
Fortigate: Traffic End Local	2016-03-27 20:11:10	141.105.70.156:50927	3	Malicious Host	181.39.11.98:23	0	Empty
Fortigate: Traffic End Local	2016-03-27 20:11:02	141.105.70.156:50927	3	Malicious Host	181.39.11.98:23	0	Empty
Fortigate: Traffic End Local	2016-03-27 20:10:58	141.105.70.156:50927	3	Malicious Host	181.39.11.98:23	0	Empty
Fortigate: Traffic End Local	2016-03-27 20:10:56	141.105.70.156:50927	3	Malicious Host	181.39.11.98:23	0	Empty
Fortigate: Traffic End Local	2016-03-27 20:10:55	141.105.70.156:50927	3	Malicious Host	181.39.11.98:23	0	Empty
Fortigate: Traffic End Forward	2016-03-27 19:57:00	183.60.48.25:12207	3	Malicious Host	181.39.11.99:5901	0	Empty
Fortigate: Traffic End Local	2016-03-27 19:56:30	183.60.48.25:12207	3	Malicious Host	181.39.11.98:5901	0	Empty
Fortigate: Traffic End Local	2016-03-27 19:54:35	183.138.1.218:48134	3	Malicious Host	201.219.44.22:88	0	Empty
Fortigate: Traffic End Forward	2016-03-27 19:46:19	188.68.224.62:45394	3	Malicious Host	201.219.44.22:8080	0	Empty
Fortigate: An application control IM (IPS) log message (pass)	2016-03-27 19:45:59	188.68.224.62:45394	3	Malicious Host	Host-10-0-104-138:8080	0	Empty
Fortigate: Traffic End Forward	2016-03-27 19:36:36	Host-10-0-104-236:137	0	Empty	183.56.159.141:137	3	Malicious Host
Fortigate: Traffic End Forward	2016-03-27 19:33:32	Host-10-0-104-236:137	0	Empty	183.56.159.141:137	3	Malicious Host
Fortigate: Traffic End Forward	2016-03-27 19:25:33	93.174.93.218:47978	3	Malicious Host	201.219.44.15:8080	0	Empty

Figura 156. Detalles de eventos con filtro OTX reputation: malicius host – médium severity

En esta figura se puede observar algunos hosts que son considerados maliciosos y que pueden continuar atacando a la red por lo que se bloqueó sus IPS de origen. También se obtuvo eventos cuando se filtró por **scanning host – médium severity** y se obtuvieron algunas IPS de origen provenientes de China que están intentando hacer escaneo a la red del MINTEL, en la Figura 157 se presenta los resultados obtenidos al realizar el filtro indicado.

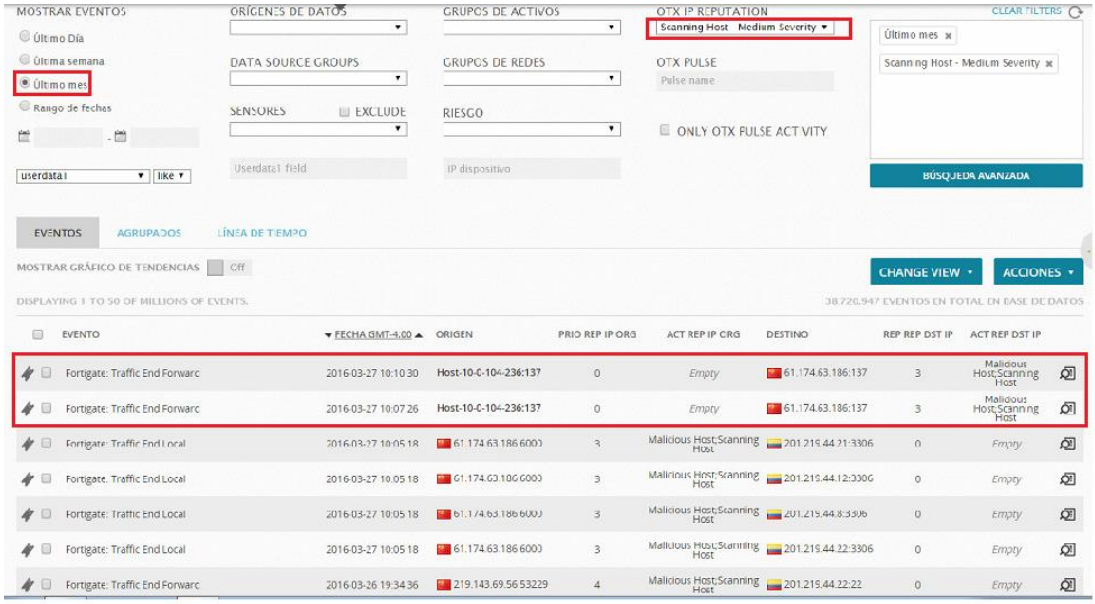


Figura 157. Detalles de eventos con filtro OTX reputation: scanning host – médium severity

Otro ataque que se pudo observar en la red del MINTEL es el **spamming**, es decir el enviar mensajes electrónicos (spam, habitualmente de tipo comercial) no solicitados y en cantidades masivas, se puede observar que los servidores comprometidos en este ataque son el 10.0.104.60 y 10.0.104.32 desde IP´s de Estados Unidos. En la Figura 158 se visualiza los resultados al realizar este filtro.

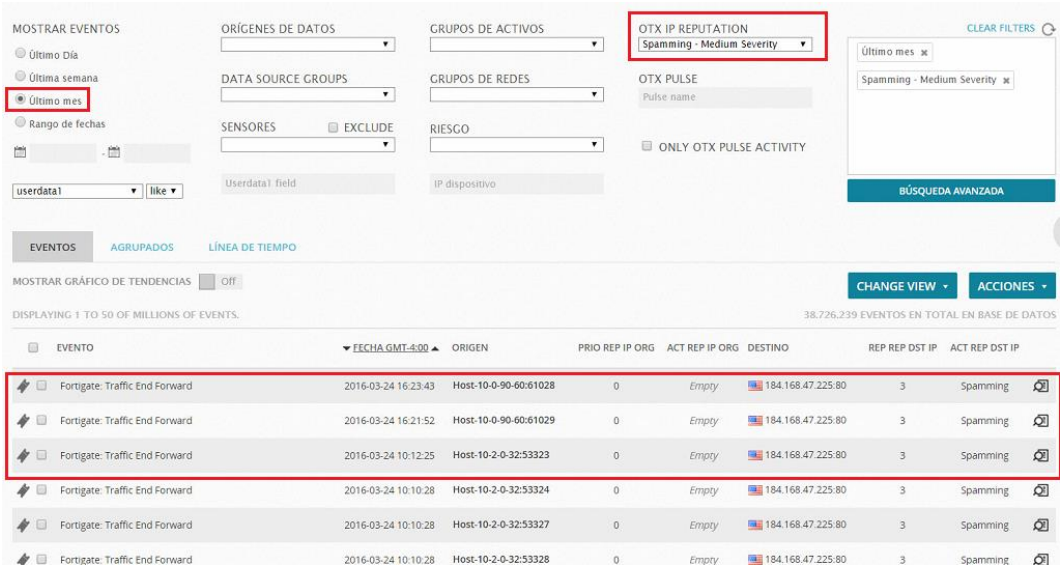


Figura 158. Detalles de eventos con filtro OTX reputation: spammig – médium severity

Bajo la misma pestaña de **análisis** también se encuentran la opción de tickets generados por la herramienta, en donde se pueden encontrar: prioridades para el ticket, el usuario a quien se le asignó el ticket y el estado del mismo, es decir si ha sido atendido o no todavía. En la Figura 159 se presenta la pantalla de tickets abiertos que no han sido atendidos.

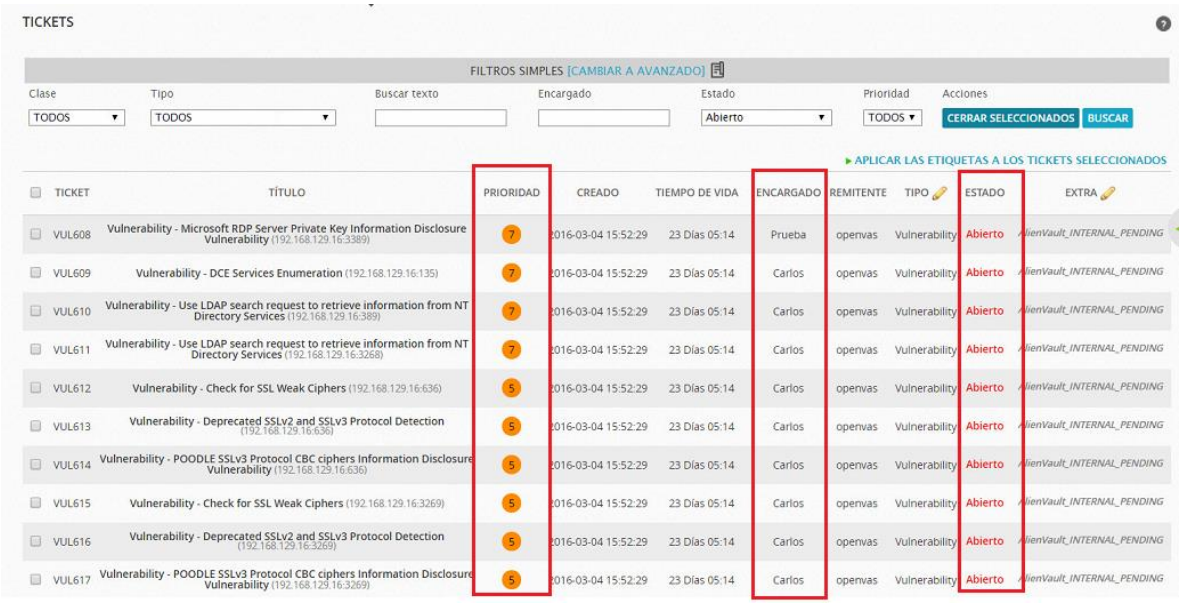


Figura 159. Detalles de tickets abiertos por la herramienta, con prioridad, encargado y estado

Al dar clic en cualquiera de los tickets abiertos se despliega otra pantalla en donde se obtienen los datos indicados anteriormente, siendo lo más importante en la mayoría de los casos es que se encuentra la solución para el evento de seguridad asignado, con esto la persona a la cual se le asignó el ticket puede remediar el hueco de seguridad detectado, lo cual ayuda significativamente al personal y sobre todo se ejecutará una solución rápida de la vulnerabilidad o ataque. En la Figura 160 se presenta la pantalla donde se indica el detalle de uno de los tickets abiertos con prioridad 7.

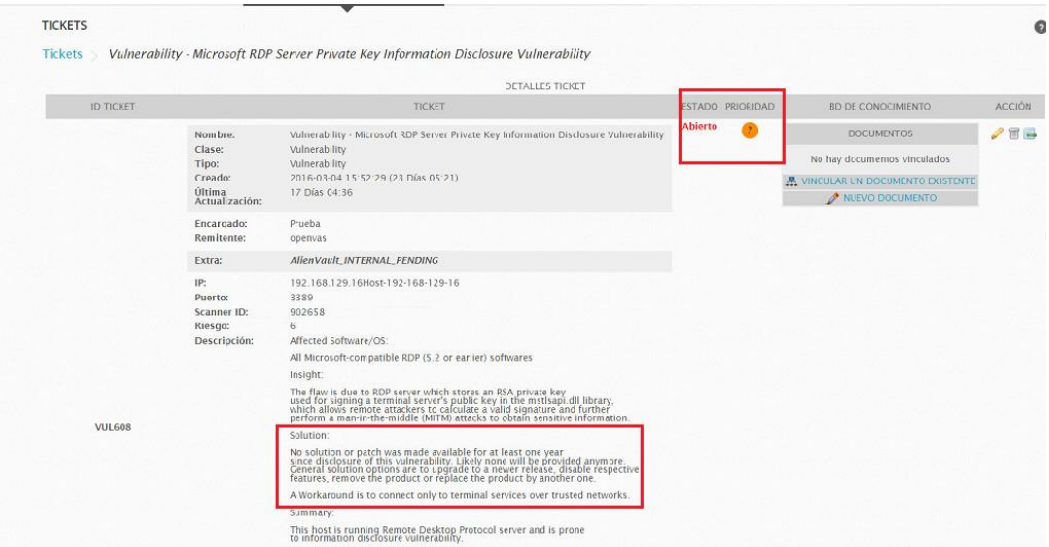


Figura 160. Pantalla detalle de un ticket de una vulnerabilidad de Microsoft de un equipo

Por último otro de los tableros usados para evaluar temas de seguridad en la red del MINTEL, fue el panel top 10 de host con virus detectado como se indica en la Figura 161, ahí se puede observar que el equipo cuya IP es 10.0.30.52 tiene casi 30 virus detectados, siguiéndole el equipo con IP 10.0.70.58, por lo que se dio atención inmediata a estos equipos y se procedió a desinfectarlos.

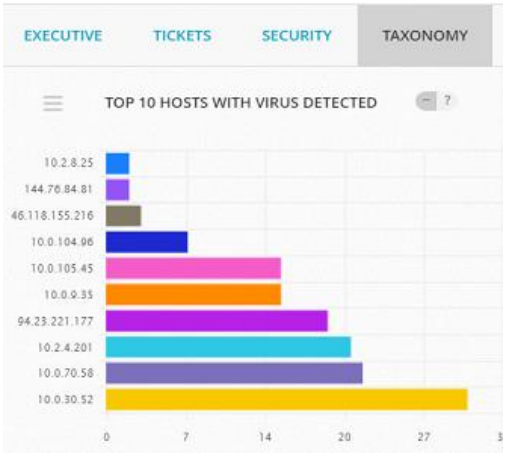


Figura 161. Panel gráfico del top 10 de equipos con virus detectados

5.4.3 Splunk

En Splunk existen pocos tipos de alertas que se pueden usar, cada tipo trabaja diferente con una búsqueda para desencadenar acciones de alarma. Se puede elegir un tipo de alerta dependiendo de qué evento se quiere realizar un seguimiento y también cuando se quiere saber algo sobre el mismo. Existen 3 tipos de alertas: alerta por resultado, alerta programada y alerta por ventanas continuas de tiempo.

La **alerta por resultado** notifica cuando una búsqueda en tiempo real devuelve un resultado que coincide con una condición creada. Por lo general, se especifica una condición de aceleración de modo que la alerta se dispara solo una vez durante un periodo de tiempo especificado, por ejemplo cada vez que se intenta ingresar en un equipo y se ingresa la contraseña fallidamente.

La **alerta programada** se utiliza para notificar cuando una búsqueda devuelve resultados programados que cumplen una condición específica, por ejemplo dar una alerta que funcione cada hora notificando cuando el número de errores 304 exceda en 50 cada hora en cierto servidor.

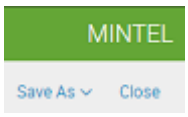
Por último la **alerta con ventanas continuas de tiempo** se usa para controlar los resultados de una búsqueda en tiempo real dentro de un intervalo de tiempo específico,

por ejemplo dar una alerta cuando un host no puede completar una transferencia de archivos por día a otro host.

Se creó un ejemplo de los dos primeros tipos de alertas que pueden tener aplicación sobre la infraestructura actual del MINTEL. Para el caso de alerta por resultado se va a monitorizar cuando el nivel de los logs que llegan a la herramienta desde los equipos agregados viene con error o warn o son críticos o son fatal, esto con el fin de alertar al administrador de infraestructura cuando algo está mal con la recepción de logs. El nivel de log con **warn** significa que la aplicación puede continuar trabajando pero tiene un comportamiento no apropiado, por ejemplo cuando hay muchos intentos de ingreso fallidos; en el nivel de **error** la aplicación puede continuar trabajando pero probablemente una parte de ella ya no funcione y por último el nivel **fatal** significa que la aplicación ya no trabaja, por ejemplo si la base de datos esta caída.

Para crear una **alarma por resultado**, primero se realiza la búsqueda de los eventos para los cuales sucederá la alerta, entonces en la pantalla de **search** se coloca la siguiente instrucción en lenguaje SPL:

```
index=_internal (log_level=ERROR OR log_level=WARN* OR log_level=FATAL OR log_level=CRITICAL) | stats
count as log_events
```

Después en la pestaña **save as** 

se selecciona la opción **alert** y aparecerá una pantalla como el de la Figura 162, donde se debe ingresar el nombre de la

alarma, en **alert type** para este caso se selecciona **real time** y en **trigger condition** se selecciona **Per-Result**

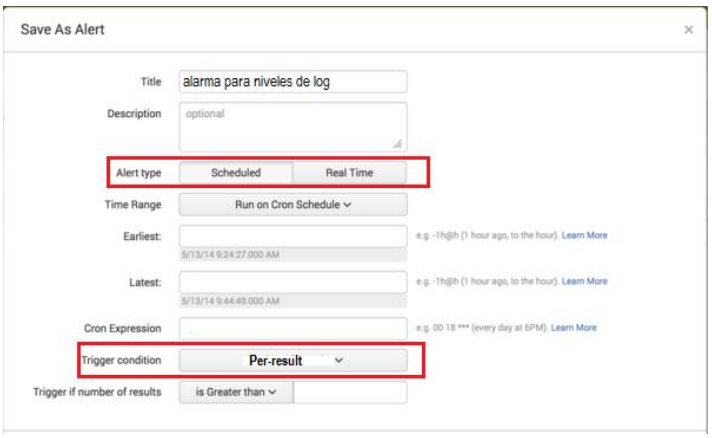


Figura 162. Pantalla de configuración de una alerta en Splunk

Para el segundo caso de **alerta programada**, se creó una alerta cuando existan más de 10 errores en un periodo de 24 horas en la plataforma Splunk. Para esto, en la sección de **search** se coloca la siguiente instrucción:

```
index=_internal " error " NOT debug source=*splunkd.log* earliest=-24h latest=now
```

Posteriormente se estableció los siguientes parámetros de la alerta como sigue

- Title: Errores en las últimas 24 horas
- Alert type: Scheluded
- Time range: Run every day
- Trigger condition: Number of results
- Trigeer when number of results: is greater than 5

Se puede configurar una alerta para enviar una notificación de correo electrónico a destinatarios específicos cuando la alerta se activa. Se configura la acción de notificación de correo electrónico para una alerta cuando se guarda la alerta desde la página de búsqueda. También se puede configurar la notificación por correo electrónico de la página Alertas y directamente de un comando de búsqueda.

Para configurar notificaciones por email cuando se graba una búsqueda como alerta, se lo realiza al momento de grabar la alarma seleccionando **send email** en la opción **when trigger** y ahí se despliega los datos para quien se enviará el mail y un mensaje de descripción con la acción a tomar. En la Figura 163 se presenta un ejemplo de envío de mail.

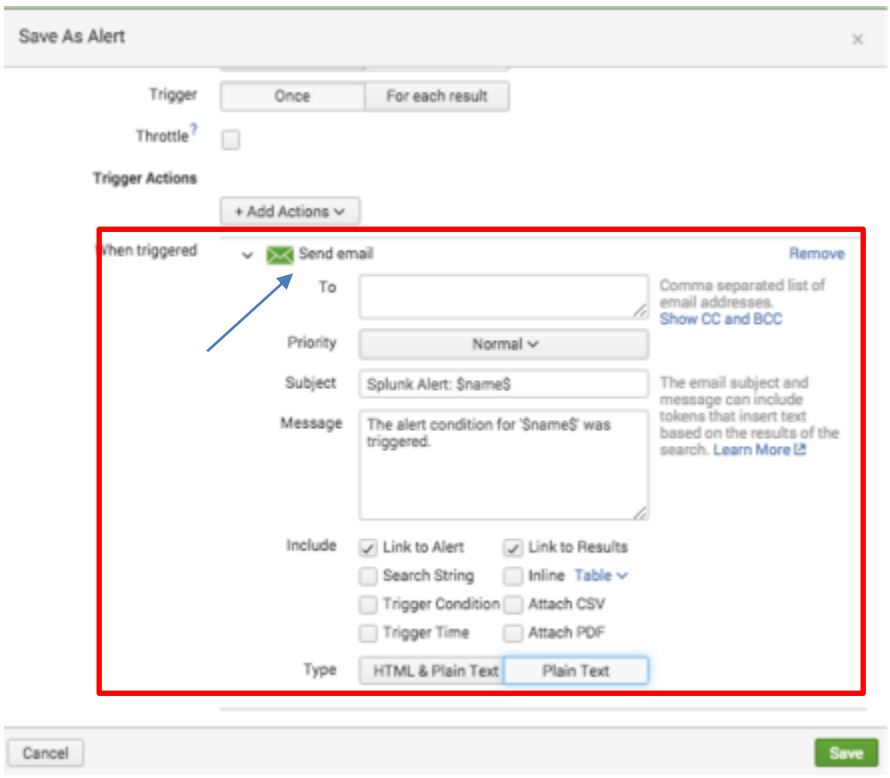


Figura 163. Pantalla de configuración para enviar un correo cuando suceda una alerta

Dentro de los tableros de control obtenidos con la herramienta el que más sirve para evaluar la seguridad de la red es el obtenido por el equipo Fortinet, en este se observa que por ejemplo en los últimos 30 días los ataques de severidad baja son los que más han sucedido con aproximadamente 500 ataques y para severidad alta o media no se llega más de los 50 ataques. Los servidores más atacados son: 10.0.104.238-página web con 500 ataques aproximadamente, de ahí le siguen los servidores 10.0.10.253- servidor de SGSI Infocentros y 10.0.104.92- servidor de correo electrónico con 250 ataques cada uno. Las IP´s de origen de los ataques son 40.121.148.157 desde Estados Unidos con casi 50 intentos y la 180.97.221.109 desde China con 40 intentos, por lo que se investigó estas direcciones y se detectó que son utilizadas para realizar ataques por lo que se procedió a bloquearlas en este equipo de seguridad. En la Figura 164 se presenta el tablero de control donde se presentan estos resultados

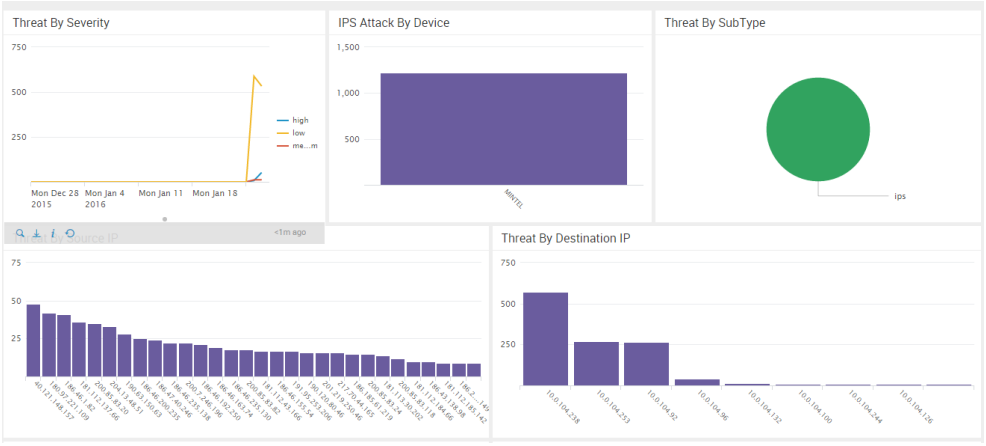
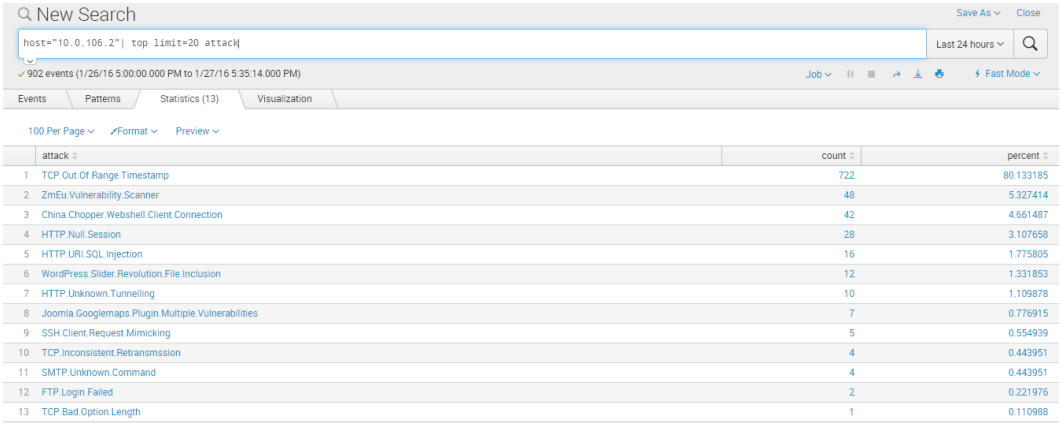


Figura 164. Tablero de control de ataques obtenidos para Fortinet

En el tablero de ataques contenidos por el Fortinet, se puede visualizar que el equipo está cumpliendo su función ya que ha contenido 722 ataques del tipo **TCP out of**

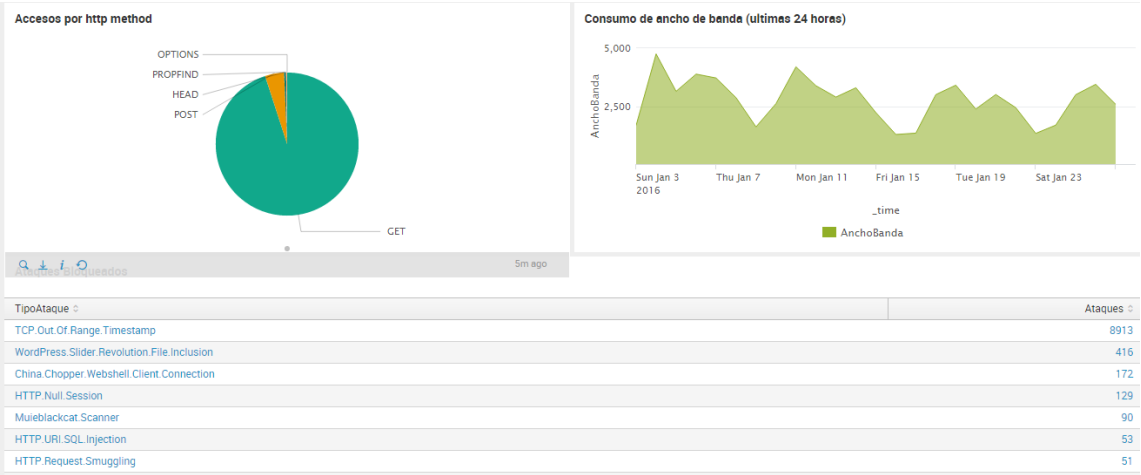
range Timestamp, el cual no representa un ataque muy grave y puede ser solucionado cambiando los parámetros de Timestamp de los servidores; otro ataque contenido fue el **ZmEu Vulnerability Scanner** con 80 veces, ZmEu hace un escaneo de vulnerabilidades en el ordenador en servidores web que esten abiertos para atacar a través del programa phpMyAdmin, también intenta averiguar las contraseñas de SSH a través de métodos de fuerza bruta y deja una persistente puerta trasera (backdoor) para futuros ataques. En la Figura 165 se presenta la lista de ataques contenido por Fortinet



	attack	count	percent
1	TCP.Out.Of.Range.Timestamp	722	80.133185
2	ZmEu.Vulnerability.Scanner	48	5.327414
3	China.Chopper.Webshell.Client.Connection	42	4.661487
4	HTTP.Null.Session	28	3.107658
5	HTTP.URI.SQL.Injection	16	1.775805
6	WordPress.Slider.Revolution.File.Inclusion	12	1.331853
7	HTTP.Unknown.Tunnelling	10	1.109878
8	Joomla.Googlemaps.Plugin.Multiple.Vulnerabilities	7	0.776915
9	SSH.Client.Request.Mimicking	5	0.554939
10	TCP.Inconsistent.Retransmssion	4	0.443951
11	SMTP.Unknown.Command	4	0.443951
12	FTP.Login.Failed	2	0.221976
13	TCP.Bad.Option.Length	1	0.110988

Figura 165. Listado de tipos de ataques contenidos por el equipo Fortinet

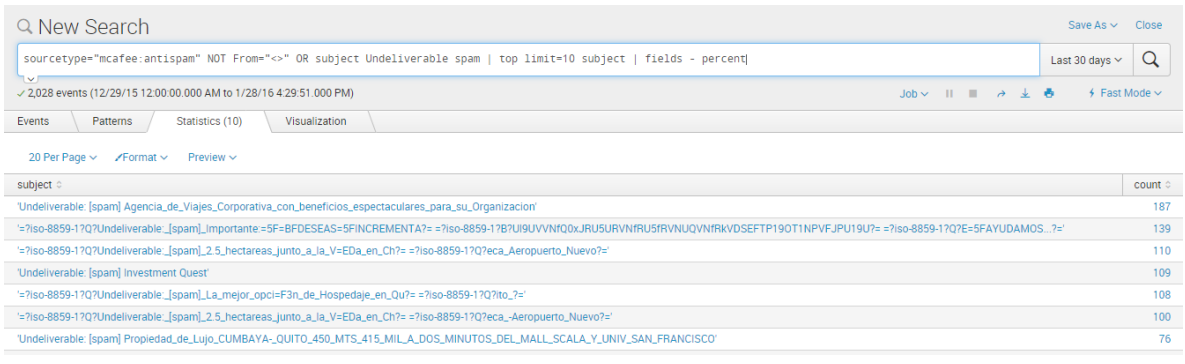
Dentro de los servidores que más ataques tienen es el de la página web, en la Figura 166 se presenta el detalle de los ataques que tiene esta página, siendo los del tipo **TCP Out Of Range, WordPress Slider Revolution y China Chopper WebShell** los ataques más comunes, lo que concuerda con lo obtenido por la herramienta Checkpoint



TipoAtaque	Ataques
TCP.Out.Of.Range.Timestamp	8913
WordPress.Slider.Revolution.File.Inclusion	416
China.Chopper.Webshell.Client.Connection	172
HTTP.Null.Session	129
Muieblackcat.Scanner	90
HTTP.URI.SQL.Injection	53
HTTP.Request.Smuggling	51

Figura 166. Detalle de cantidad de ataques por categoría para la página web del MINTEL

Por último una de las correlaciones creadas con Splunk para obtener el correo más recurrente del tipo Spam, se tienen datos en los cuales se puede analizar que el spam más recurrente en los últimos 30 días de análisis es de la Agencia de Viajes Corporativa con beneficios espectaculares con 187 veces, seguido por un spam de Deseas incrementar 5…, con 139 veces. En la Figura 167 se presenta el spam recurrente que está llegando a la institución.



subject	count
'Undeliverable: [spam] Agencia_de_Viajes_Corporativa_con_beneficios_espectaculares_para_su_Organizacion'	187
'=?iso-8859-1?Q?Undeliverable:_[spam]_Importante:=5F=BFDESEAS=5FINCREMENTA?= =?iso-8859-1?B?UI9UVVNfQ0xJRU5URVNfRU5fRVNUQVNfRkVDSEFTP19OT1NPVFJPU19U?= =?iso-8859-1?Q?E=5FAYUDAMOS...?='	139
'=?iso-8859-1?Q?Undeliverable:_[spam]_2.5_hectareas_junto_a_la_V=EDa_en_Ch?= =?iso-8859-1?Q?eca_Aeropuerto_Nuevo?='	110
'Undeliverable: [spam] Investment Quest'	109
'=?iso-8859-1?Q?Undeliverable:_[spam]_La_mejor_opci=F3n_de_Hospedaje_en_Qu?= =?iso-8859-1?Q?ito_?='	108
'=?iso-8859-1?Q?Undeliverable:_[spam]_2.5_hectareas_junto_a_la_V=EDa_en_Ch?= =?iso-8859-1?Q?eca_-Aeropuerto_Nuevo?='	100
'Undeliverable: [spam] Propiedad_de_Lujo_CUMBAYA-_QUITO_450_MTS_415_MIL_A_DOS_MINUTOS_DEL_MALL_SCALA_Y_UNIV_SAN_FRANCISCO'	76

Figura 167. Detalle de spam contenido por Fortinet

Todas estas fuentes fueron ingresadas en el software de antispam para que sean bloqueadas y no lleguen más a los correos de los funcionarios.

Cabe señalar que con Splunk no se pudo realizar mucho análisis en seguridades o vulnerabilidades más que lo indicado ya que la creación de las correlaciones para obtener eventos de seguridad no fue tan fácil como se indicó en el capítulo 5.2 y al no tener tableros de control por defecto, no tener mucha experticia en el lenguaje de programación SPL del aplicativo, no se tuvo mucha utilidad el analizar con Splunk los eventos de seguridad y vulnerabilidades de la infraestructura del MINTEL.

Como conclusión de la evaluación realizada se indica que la mayor cantidad de aportes en temas de seguridad lo da la herramienta USM ya que no se tiene mucho que configurar y la herramienta por si sola encuentra vulnerabilidades y ataques a la red. En términos de SIEM tanto USM como McAfee ESM ayudan mucho con las correlaciones automáticas que ya vienen incorporadas en las herramientas.

5.5 Comparación de las herramientas y selección

Desde un inicio las herramientas del tipo SIEM fueron creadas para proteger a las redes de datos frente a amenazas externas mediante el uso de correlaciones basadas en reglas unas predefinidas por los usuarios y otras definidas automáticamente por las herramientas en base a sus experiencias en análisis de seguridades. Pero con el paso del tiempo aparecieron nuevas regulaciones como por ejemplo la ISO 27000 o el PCI DSS lo cual obligó a nuevas evaluaciones y controles informáticos internos más estrictos. Por lo que para cumplir con estos nuevos requisitos las empresas se vieron en la necesidad de adoptar nuevas actividades como por ejemplo recopilar, analizar, elaborar informes y archivar los logs de los equipos y ya no solo detectar amenazas externas.

Es así que aparecieron los productos LEM (Log Management) para monitorizar las actividades de los usuarios más que para afrontar amenazas externas y con el paso del tiempo las empresas grandes con muchas sucursales se dieron cuenta que era necesario que convivan estos dos tipos de tecnología, el SIEM para correlacionar un conjunto de logs con el objetivo de destacar los eventos de seguridad más graves y el LEM para recopilar, generar informes y archivar gran cantidad de logs.

Con esta pequeña introducción, cabe indicar que al ser el MINTEL una empresa pública que no tiene sucursales y el número de usuarios no pasa los 350, no será

necesario tener una herramienta del tipo LEM y si una herramienta SIEM para detectar las amenazas a la cual está expuesto su infraestructura y poder correlacionarlas.

Para el análisis de que herramienta será la mejor para la infraestructura del MINTEL se tomarán en cuenta los siguientes parámetros: implementación y sus recursos en hardware, configuración, facilidad de uso, opciones de correlación y costo. Además se realizará una comparación de las características funcionales de las tres herramientas y ver cual tiene las mejores.

5.5.1 Recursos en hardware e implementación

Para analizar los recursos en hardware que necesita cada herramienta se realizará un cuadro comparativo del equipamiento necesario considerando que la implementación se la deberá realizar en servidores virtuales que se dispone en el MINTEL compatibles con VMWare. En la Figura 168 se presenta el cuadro comparativo de recursos en hardware.

Característica	Splunk	ESM-McAfee	USM-AlienVault
Procesador	8 cores	8 cores	8 cores
Memoria RAM(GB)	12	4 o más	8 o más
Disco Duro libre(GB)	300	250	500
Compatible con VMWare 5.X	SI	SI	SI
Sistema operativo	Windows server 2008 64 bits	Red Hat Linux	Debian

Figura 168. Cuadro comparativo de recursos de hardware de las herramientas analizadas.

En cuanto al hardware necesario para la implementación se puede observar que las tres herramientas necesitan 8 cores en su procesamiento, en memoria RAM la herramienta ESM es el que menor cantidad necesita al igual que en disco duro pero estas características dependerán directamente del número de eventos por segundo que se reciban en la red y el rendimiento de la red que se desea proteger, es decir mientras más activos se ingresen a la red los cuales generen más eventos por segundo estos recursos subirán considerablemente, por lo que en cuestiones de memoria y disco duro se concluye que cualquiera de las tres herramientas utilizarían la misma cantidad de memoria y disco para ingresar los mismos dispositivos de fuente de datos.

En cuanto a la implementación Splunk fue la más difícil de implementar ya que a pesar que la instalación del sistema operativo puede ser considerada la más fácil y en sí la instalación de la herramienta no fue difícil, pero en cambio es necesario instalar Splunk Forwarder en los equipos donde no se tenga un envió estándar de logs y esta instalación puede tomar más tiempo según el número de equipos a los cuales sea necesario instalarlo lo que en muchos casos involucrará tener conocimientos de Linux para los equipos que tienen este sistema operativo. La instalación de ESM y USM fue más sencilla ya que solo se cargaron las imágenes ISO de las herramientas y la adición de equipos o activos en ambos casos se lo realiza de una manera intuitiva por lo que fue mucho más sencilla que en Splunk. Para la recolección de los logs USM tiene una ventaja sobre ESM ya que como se explicó la herramienta reconoce muchos equipos de diferentes marcas ya que tienen almacenados en una base de datos y en caso de no existir se puede solicitar a AlienVault que se lo incluya y aún más si se tiene experiencia en programación se los puede crear.

Cabe señalar que las tres herramientas pueden ser administradas mediante un portal web lo que facilita su utilidad y uso.

5.5.2 Configuración:

La herramienta más difícil para configurar correlaciones de eventos fue Splunk ya que no se lo puede hacer de una manera intuitiva, se necesitó leer bien los manuales para poder añadir dispositivos, así como también la sintaxis de programación para realizar las

correlaciones utilizando el lenguaje SPL que se basa en comandos. Además se necesita conocer bien el estándar de los logs para poder entender cómo realizar una correcta correlación utilizando los datos que vienen en los registros. Cabe indicar que si se conoce bien este tipo de lenguaje y el entendimiento correcto de logs esta herramienta en realidad podría ser considerada bien útil y poderosa porque no tendría límites para la imaginación de los usuarios.

USM y ESM fueron herramientas más sencillas de configurar ya que se lo puede hacer de una manera intuitiva y sus mecanismos de correlación son más fáciles de aplicar y configurarlos.

Realizando otro tipo de análisis sobre configuración es que en Splunk existen solo tableros de control pre definidos o por defecto para equipos de la marca Fortinet, lo que ocasionaría que al no tener dentro de la infraestructura de la organización este tipo de equipo no se tendría ningún tablero por defecto. La creación de los mismos se basa en realizar búsquedas y con estos datos obtenidos en las búsquedas se los crea, lo que en las otras herramientas de análisis ya vienen tableros de control pre definidos con muchos paneles gráficos y con muchos datos para poder realizar un análisis preliminar básico en seguridad de la red, además que la adición o creación de nuevos tableros es mucho más sencilla. Al comparar USM y ESM para la creación de nuevos tableros de control se observa que ESM tiene una ventaja ya que su elaboración es sencilla pero en cambio

USM tiene muchas directivas de las cuales se podrían sacar nuevos tableros según las necesidades.

5.5.3 Correlación

Se puede decir que resulta complicado encontrar el equilibrio adecuado para la creación de nuevas reglas de correlación para descubrir los posibles ataques a los que estaban expuestos la red en las tres herramientas y además ver que estas reglas creadas no produzcan falsos positivos en alertas por lo que en cualquiera de las tres herramientas la creación de reglas de correlación fue complicado ya que se requiere realizar muchos ajustes y afinamientos en las mismas para llegar a una regla que en realidad sirva para detectar amenazas internas o externas. Por ejemplo en ESM se crearon algunas reglas pero nunca saltó ninguna alarma ya que los eventos pensados no sucedieron o no se correlacionaron, algo parecido sucedió en USM y en Splunk.

Además cabe señalar que al cambiar alguna fuente de datos de la red pueden afectar a las reglas creadas y una simple actualización de alguno de los dispositivos pueden crear falsas alertas.

La ventaja que tiene USM y ESM en este campo sobre Splunk es que por ejemplo en ESM ya viene incorporado un motor de correlación automático con algunas reglas de correlación por defecto, con lo cual no será necesario realizar ninguna configuración para la creación de reglas para amenazas básicas, al igual USM tienen ya informes propios de

la herramienta en los cuales se han aplicado ya reglas de correlación para ciertos aspectos de seguridad comunes que son de gran utilidad pero tiene una gran ventaja sobre ESM y es que tiene miles de reglas de correlación por defecto lo que no sucede con ESM ya que tiene capacidades de correlación muy básicas y pocas reglas ya creadas y ni que hablar de Splunk que tiene capacidades de correlación casi nulas y que se basan o pueden ser creadas de las experiencias de los usuarios ingresando búsquedas con lenguaje SPL.

Splunk en realidad no hace ninguna correlación, ya que no está diseñado para hacer eso. Sin embargo, puede ser utilizado para correlacionar eventos utilizando el lenguaje de búsqueda de Splunk. Se puede realizar una correlación manual mediante búsquedas por canalización, tablas de búsqueda, con guión de búsquedas, etc., pero de nuevo se necesita estar familiarizado con el lenguaje SPL como se indicó en el ítem 5.2.1.

5.5.4 Facilidad de uso

En general las soluciones de tipo SIEM generalmente son difíciles de usar ya que si se necesita tener ciertos conocimientos en temas de seguridad de la información. Del análisis de las herramientas seleccionadas para este caso de estudio, tanto USM como ESM son herramientas fáciles de usar ya que al leer los manuales de administración se pueden configurarlas y la gran ventaja es que como se indicó ya vienen incorporadas muchos tableros de control, reglas de correlación y herramientas para análisis de vulnerabilidades que son usadas inmediatamente por el usuario, una pequeña ventaja que

puede tener ESM sobre USM es que existen más documentación para leer en español en la página web lo que no sucede con USM que fue difícil de conseguir manuales aún en inglés.

El uso de Splunk no fue tan fácil ya que todo el ambiente SIEM de la herramienta se basa en la búsqueda de eventos en la red y si no se tiene sólidos conocimientos en identificar los datos que se obtienen será muy difícil llegar a obtener reglas de correlación que puedan ayudar en el tema de decisiones en seguridad de la información.

Adicional al analizar las bondades de uso que tiene la herramienta USM es que vienen incorporadas muchas herramientas para análisis de seguridad en una plataforma (por ejemplo IDS, SIEM) y eso sí es una gran ventaja sobre las otras ya que para que ESM cumpla con todo lo que viene incorporado en USM se necesita adquirir otros equipos que cumplan con estas funciones lo que involucra elevar los costos iniciales de instalación, con esto se puede concluir que si una herramienta ya viene con muchas instrumentos de seguridad incorporados en una sola plataforma y la cual funcione bien en ambientes pequeños como el MINTEL es un condicional muy importante en el análisis.

5.5.5 Costos

Las soluciones SIEM por lo general son caras y en la mayoría de casos solo pueden ser usados por empresas grandes y no por empresas medianas o pequeñas, los costos asociados a una implementación SIEM tradicional incluyen:

- Costos iniciales en el licenciamiento
- Costos para la implementación/optimización (afinamiento)
- Costos para la renovación de licencias, que en muchos caso vienen incluidos con soporte
- Integración de las fuentes de datos cuando no se manejan estándares en la recepción de logs
- Capacitación del personal

Por lo que encontrar una herramienta que a más de ser un SIEM pueda entregar otras funciones adicionales de seguridad sería de gran ayuda siempre y cuando el costo sea significativamente más bajo que adquirir esas herramientas para ejecutar temas extras de seguridad informática.

En la tabla 2 se entregan los valores para adquirir cada herramienta considerando solo costos de licenciamiento y capacitación, mismos que se obtuvieron de proveedores locales que son representantes de las marcas de las herramientas SIEM seleccionadas.

Tabla 2. Costos de licenciamiento y capacitación de las herramientas

Cantidad	Producto	Costo
1	Licenciamiento USM All in one por 1 año Estándar para 150 activos, incluye capacitación 1 persona con certificación del fabricante	$ 21.500,00
1	Splunk Enterprise Suscripción anual para 2 GigaByte/día, incluye cursos oficial de administración y de búsqueda y reportería	$ 13.500,00
1	Licenciamiento ESM All-in-one con las funciones: Gestión del SIEM, recolector de logs, gestión de logs (requiere almacenamiento externo tipo CIFS o NFS), incluye capacitación formal	$ 50.000,00

Además, adicional todas las empresas cotizaron el costo de instalación y afinamiento de la herramienta los cuales se indican a continuación:

Instalación USM:	$ 10.000,00
Instalación Splunk:	$ 8.500,00
Instalación ESM:	$ 12.000,00

Se observa que el costo es excesivo para la instalación y afinamiento, debido principalmente ya que hay casos sobre todo para infraestructuras grandes, que se demoran algunos meses hasta dejar completamente afinada la solución y con los

requerimientos que el cliente necesite. Para el caso del MINTEL no será necesario gastar en costos de instalación al no ser una infraestructura tan grande sino más bien con la experiencia que se tuvo en la instalación y configuración de las tres herramientas, se podrá profundizar con más detalle en la herramienta seleccionada y si gastar en cursos de capacitación.

Finalmente, se realizó un cuadro comparativo de las tres herramientas considerando ciertos parámetros y características que tienen los aplicativos de tipo SIEM, con el objeto de determinar que herramienta será la mejor que se acople a la red del MINTEL, el cual se presenta en la Figura 169.

Característica	**Splunk**	**USM**	**ESM**
Gestión de logs	✓	✓	✓
Normalización de logs	✓	✓	
Correlación de eventos automático		✓	✓
Tableros de control predefinidos		✓	✓
Inteligencia de seguridad	✓	✓	✓
Almacenamiento de logs	✓	✓	Necesita de módulo

Geo localización	✓	✓	✓
Detección de ataques externos/internos		✓	✓
Generación de informes	Básico	✓	✓
Generación de alertas	✓	✓	✓
Generación de alarmas		✓	✓
Generación de asignar casos		✓	
IDS incluido		✓	Necesita de módulo
Descubrimiento de fuentes o activos		✓	✓
Detección de amenazas		✓	✓
Análisis de vulnerabilidades		✓	Básico
Análisis de flujos de red		✓	
Disponibilidad de servicios de activos		✓	Básico
Integración de cualquier equipo		✓	
Líneas de tiempo para eventos en línea e históricos	✓	✓	✓
Redundancia			✓

Cumplimiento de estándares de seguridad		✓	✓
Identificación de sistemas infectados		✓	
Tiempo de configuración(* - ***/lento – rápido)	***	*	**
Costos de licenciamiento (* - ***/bajo – alto)	*	**	***
Soporte técnico (* - ***/bajo – alto)	**	*	***
Documentación (* - ***/bajo – alto)	**	*	***

Figura 169.Cuadro comparativo de características de las herramientas de análisis.

De los datos obtenidos del análisis realizado considerando los parámetros de evaluación enunciados anteriormente y del cuadro comparativo de la Figura 169, se concluye que la herramienta que puede ser de gran utilidad y que mejor se adapta para la pequeña infraestructura del MITEL es USM basado en lo siguiente:

- En una sola plataforma se encuentra un SIEM con más de 2000 directivas de correlación creadas, un IDS, escaneo de vulnerabilidades y realiza un monitoreo de consumo de la red mediante Netflow.
- Sencilla para implementar y configurar.

- En costos no es la mejor opción pero la poca diferencia de valor que existe con la siguiente herramienta que es Splunk hace que se pueda considerarla como la mejor alternativa.
- Integración de equipos para recepción de logs no complicada y en caso que no se encuentre un equipo dentro de la base de datos de dispositivos que ya vienen por defecto en la herramienta se puede mandar a crear en los laboratorios de AlienVault sin costo alguno, demorándose en la entrega de 1 a 2 semanas.
- Tableros de control de diferentes tipos en los cuales se encuentran gran cantidad de información sobre la seguridad de la red.
- Varios tipos de alertas por defecto.
- Muchos informes por defecto.
- Descubrimiento de activos automático y calendarizado

Finalmente dentro de este análisis cabe señalar que Splunk en costos parece ser la más económica pero mientras más eventos ingresen a la aplicación los costos irán incrementando ya que se licencia por eventos por día, además si no se realiza un buen curso de búsqueda y reportería será muy difícil poder conseguir resultados óptimos en seguridad con la herramienta. Pero al mismo tiempo y resultando un poco contradictorio a lo indicado anteriormente Splunk será de gran ayuda una vez que se tenga sólidos conocimientos en la reportería, lenguaje SPL y en el entendimiento de la información que se encuentran en los logs de los equipos, lo que hace que esta herramienta puede ser considerada poderosa ya que sin lugar a dudas Splunk es el mejor motor de búsqueda

para logs. ESM es una herramienta que tiene buenas prestaciones pero se debe adquirir otros equipos, sean como hardware o como máquinas virtuales, para que el sistema SIEM sea completo lo que encarece la solución.

Una vez seleccionada la herramienta de AlienVault y considerando que la situación económica actual del país es inestable y no se podrá contar con presupuesto en el sector público para implementar una plataforma del tipo SIEM, se plantea tener como solución alternativa para la infraestructura del MINTEL el poder usar la herramienta libre de esta marca, que es OSSIM , y aunque no tenga todas las bondades que presenta su contraparte comercial USM, puede ayudar a encontrar las vulnerabilidades de la red y usar las correlaciones básicas que tiene esta versión sin muchos reportes y tableros de control, ver las alertas y crear alarmas y casos, lo único que se tendría que analizar es el tema del soporte ya que el mismo es dado solo en los foros de la herramienta y si se desea tener un soporte especializado analizar la posibilidad de contratarlo.

6. Conclusiones y Recomendaciones

- Un sistema de Información de Seguridad y Administración de Eventos SIEM es de gran ayuda para detectar y alertar a los funcionarios encargados de la seguridad de una empresa en amenazas, ataques y vulnerabilidades que pueda tener la infraestructura a todo nivel empresarial, desde la más pequeña hasta la más grande, esto debido a que en la actualidad las organizaciones modernas centran sus actividades en el internet por lo que se encuentran más vulnerables a los ataques o tienen huecos de seguridad por donde facilmente pueden ingresar amenazas informáticas.
- Un SIEM es un sistema que administra bajo una misma plataforma todas las principales funciones de seguridad de una institución ya que al mismo llegan todos los eventos (logs) desde todos los dispositivos que conforman la red y los concentra y correlaciona según las necesidades que tenga la empresa y con esto no se administran muchos tableros de control por cada herramienta de seguridad que se utilice.
- No se puede realizar gestión de incidentes de seguridad de la información sin un sistema de correlación de eventos por lo que fue necesario que las herramientas que se analizaron en este caso de estudio cuenten con uno, además que para que

funcione lo indicado se deberá primero hacer una lista específica de dispositivos y priorizar la clase de logs que se recibirá de los mismos ya que al no recibir eventos de algún dispositivo no se podrá realizar correlaciones que pueden ayudar en mucho en el análisis de seguridad, por ejemplo en este caso de estudio al no poder envíar syslogs la version del antivirus de marca Eset que tiene la institución no se logró correlacionar algunos incidentes de seguridad que con certeza estan presentes en la red del MINTEL.

- A más de contar con herramientas informáticas de seguridad que ayudan grandemente en la admistración de la infraestructura, es necesario que la institución cuente con personal altamente especialiazado en las nuevas tecnologías de seguridad para gestionar de manera eficaz y ágil estos sistemas ya que en el MINTEL al no contar con este tipo de personal se tuvó que investigar mucho sobre temas de seguridad y entenderlos.
- Para elegir una herramienta del tipo SIEM que sea la más adecuada para la infraestructura de una institución hay que tener en cuenta algunos factores entre los que se destacan los siguientes: volumen de datos a adquirir, el uso que se le va a dar a la herramienta, que tan complejos son los equipos y sistemas de información que se tiene, el costo de la herramienta, la facilidad y que tan amigable es su administración. Solo realizando un análisis de estas variables se puede estar seguro de escoger con éxito un sistema SIEM para que brinde sus mejores bondades para la infraestructura de la empresa.

- La mejor manera para comparar productos del tipo SIEM es entendiendo completamente cual es el problema que se intenta resolver en temas de seguridad y ser entendido completamente por las personas de seguridad que administrarán la herramienta por lo que si el aplicativo no puede demostrar rapidamente para que va a ser usado, probablemente se seguirán buscando otros sistemas que si lo hagan, por ejemplo en este caso de estudio la herramienta SPLUNK puede ser la más importante de todas las analizadas pero por la forma en que toca realizar su programación y al no tener la suficiente experiencia en temas de eventos de seguridad no se la pudo usar en su total dimensión.
- Para la infraestructura del MINTEL se seleccionó la herramienta USM en su versión comercial ya que es la que brinda mejores características de seguridad para la pequeña infraestructura de la institución y no es necesario gastar demasiado dinero en este tipo de soluciones. Se la seleccionó en base a que: es muy fácil de usarla, tiene muchas reglas de correlación creadas, presenta muchos tableros de control de tipo ejecutivo en seguridades, entrega alarmas bajo cinco categorías cubriendo la mayor parte de sistemas de seguridad en una sola plataforma, tiene un IDS incorporado y entrega un detalle de todas las vulnerabilidades que estan presentes en la red de la institución, entre las principales.
- ESM de McAfee a pesar de tener casí todas las características de USM no se la seleccionó ya que se necesita muchos módulos o equipos adicionales para llegar a ejectur lo que USM realiza en una sola plataforma, pero se la puede considerar

para otro tipo de infraestructuras para grandes empresas donde se cuenta con suficiente dinero ya que además puede manejar grande cantidad de eventos y tiene un gran soporte a nivel mundial al ser distríbuido por INTEL.

- Los requerimientos de recursos en hardware que necesitan las herramientas del tipo SIEM depende directamente del número de eventos por segundo que enviarán todos los dispositivos que se deseen monitorizar y del rendimiento de la red que se desee proteger, para el análisis de este caso de estudio los requerimientos fueron los básicos pero si ya se desean ingresar más dispositivos seguramente tocará incrementar memoria RAM y almacenamiento para los logs que llegan.
- Se presentaron tableros de control al oficial de seguridad de la información indicándole los principales ataques, amenazas y vulnerabilidades a las que esta expuesta la red de la institución, quien indicó que esto ayudará de mucho para que las autoridades tomen conciencia de lo que esta sucediendo y se preste mayor atención a los temas de seguridad de la información que se están desarrollando en el MINTEL a través del Comité de Seguridad de la Información.
- Como experiencia propia, el tiempo que se demoro para la implementación, configuración, creación de tableros de control, alarmas y afinamiento de las herramientas seleccionadas dependió de cada una, siendo Splunk la que más tiempo requirió para ejecutar todas las tareas antes descritas, debido especialmente a que primero se tuvo que familiarizarse con el lenguaje SPL y logs

de los equipos, empleando un poco más de 3 semanas. Para ESM se demoró unas 3 semanas para dejar afinada la solución y por último para USM solo 2 semanas.

- Con los resultados obtenidos, se tomaron acciones de seguridad, como por ejemplo en el equipo de seguridad perimetral se bloqueo IPs que están realizando ataques continuos a la red, se mitigó algunas vulnerabiliades que se tienen en los servidores de la institución y se desinfectaron algunos equipos internos que tenían botnets y malwares que el antivirus institucional no los detectó.
- Como última conclusión se acota que la seguridad absoluta nunca existirá, siempre se estará propensos a tener nuevos ataques con tecnologías más avanzadas por lo que implementar una herramienta tipo SIEM ayudará en algo a mitigar huecos en la seguridad de la red, aunque a mi modo de ver la seguridad de una organización no se medirá por cuantas herramientas de seguridad se tienen implementadas sino que lo principal que se debe hacer es concientizar a los funcionarios de la institución en temas de seguridad, entregando políticas, procedimientos y controles sobre este tema los cuales deberán ser cumplidos por todo el personal caso contrario como se indica se seguirán teniendo muchos huecos de seguridad sin resolverse.
- Se recomienda instalar un sistema tipo SIEM para la seguridad de la red del MINTEL ya que al solo contar con un equipo de seguridad perimetral de tecnología un poco antigua el cual bloquea los ataques externos que se tienen a la red de la institución, se corre el riesgo de ser atacado sin “previo aviso” por lo que es importante y necesario tener una herramienta adicional para detectar las

posbiles amenazas y vulnerabilidades que tiene la red y además poder correlacionar eventos con el fin de evitarlos o si esto no es posible alertar para tomar las medidas necesarias de corrección en seguridad de la información. Además al implementar una herramienta tipo SIEM en el Ministerio se podrá cumplir con algunos controles e hitos para el Esquema Gubernamental de Seguridad de la Información –EGSI fase 1 y 2.

- Se recomienda que al no contar con recursos económicos al momento para realizar una inversíón de este tipo debido a la situación actual que vive el país, se utilice la versión gratuita de USM el cual es OSSIM, el mismo que difiere de su versión comercial en lo siguiente: el soporte en OSSIM viene dado por una comunidad en base a foros y vivencias propias de los usuarios, retención de logs solo para los eventos SIEM, 3 niveles de reportes y el desarrollo del número de reglas de correlación son realizadas por la comunidad y no son tantas como USM. A pesar de esto como la infraestructura del MINTEL no es grande se concluye que OSSIM puede acoplarse y prestará gran ayuda para detectar amenazas, ataques, vulterabiliades y con esto alertar cuando suceda algún evento de seguridad.
- Se recomienda al MINTEL contratar una persona que se encargue de la seguridad de la red de la institución ya que en la Dirección de Gestión Tecnológica no se tiene este tipo de especialista , mismo que este continuamente monitorizando y analizando los ataques y amenazas de la red y a su vez creando de ser el caso nuevas reglas de correlación que ayuden en el día a día en temas de seguridad de

la infraestructura que se dispone. A pesar que se tiene el Comité de Seguridad en la organización, es imposible que estas personas se encarguen de controlar la seguridad institucional si no más bien como se viene haciendo crear políticas y procedimientos de seguridad para los funcionarios pero teniendo como base la administración y análisis de eventos en seguridad de la información.

7. Bibliografía

[1] Romero Trejo, D. (2011). Security Information and Event Management. Obtenido de http://www.davidromerotrejo.com/2013/03/security-information-and-event.html

[2] Soto, J. (2015). Qué es un SIEM y porque implementar uno. Obtenido de http://www.jsitech.com/generales/que-es-un-siem-y-porque-deberias-implementar-uno

[3] Soto, J. (2015). OSSIM - Open Source Security Information Management . Obtenido de http://www.jsitech.com/seguridad/ossim-open-source-security-information-management/

[4] Kavanagh, K. M., & Rochford, O. (June de 2015). Magic Quadrant for Security Information and Event Management. Obtenido de http://www.gartner.com/technology/reprints.do?id=1-2JNVI05&ct=150720&st=sb

[5] Intel Corporation, (2015). Información de Seguridad y Administración de Eventos. Obtenido de http://www.mcafee.com/es/products/siem/index.aspx

[6] Ramos, L. (2013). Que es Splunk? Obtenido de https://prezi.com/wdcvyoo7wlsu/que-es-splunk/

[7] Splunk. (2012). La guía de inteligencia operativa de Splunk. Obtenido de https://www.splunk.com/web_assets/pdfs/secure/Splunk_Guide_to_Operational_Intelligence_es.pdf

[8] BytesChef. (10 de Mayo de 2013). Como configurar el forwarder universal de Splunk. Obtenido de http://byteschef.com/es/como-configurar-el-forwarder-universal-de-splunk/

[9] Intel, S. (2015). Guía de producto: McAfee Enterprise Security Manager 9.5.1. Santa Clara, California, USA.

8. Anexos

9. Glosario

AdHoc: Locución latina que significa literalmente “para esto”.

ANTIBOT: un bot es un software malicioso que permite a los cyber delincuentes para controlar de forma remota los ordenadores y ejecutar actividades ilegales, el antibot controla esto.

APPLIANCE: son equipos desarrollados específicamente para una utilidad en la red.

BBDD: Contracción usado para referirse a bases de datos.

HIDS: Host IDS.

IDS: Sistema de Detección de Intrusos, el IDS por sus siglas en inglés de Intrusion Detection System es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático en busca de intentos de comprometer la seguridad de dicho sistema.

IPS: Sistema de Prevención de Intrusos, es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

LDAP: Lightweight Directory Access Protocol, permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

LOG: es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema.

MEF: McAfee Event Forwarder, formato para recibir logs propio de McAfee.

NetFlow: es un protocolo de red desarrollado por Cisco Systems para recolectar información sobre tráfico IP.

OVF: Open Virtualization Format es un estándar abierto para empaquetar y distribuir servicios virtualizados o de manera más general software a ejecutar en máquinas virtuales.

PCI DSS: es un estándar de seguridad desarrollado por el consorcio Payment Card Industry Security Standards Council (PCI SSC) y su principal objetivo es reducir el fraude relacionado con las tarjetas de crédito y aumentar la seguridad de los datos almacenados en ellas.

Plugin: es un componente de software que muestra cierto contenido para el cual cierto programa no está diseñado.

SEM: Security Event Management, es el segmento de gestión de la seguridad que se ocupa del monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de la consola.

SIM: Security Incident Management, es el segmento que ofrece el almacenamiento a largo plazo, el análisis y la comunicación de los datos.

SPL: Search Processing Language, lenguaje utilizado por Splunk para realizar búsquedas y correlaciones.

SSH: Secure Shell, es un protocolo para acceder a máquinas remotas a través de una red.

SYSLOG: es un estándar para el envío de mensajes de registro en una red informática de tipo IP.

UTM: Gestión unificada de amenazas, es una sola solución de seguridad que ofrece varias funciones de seguridad en un solo punto en la red.