UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE UPV INGENIEROS DE TELECOMUNICACIÓN

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE EVENTOS DE SEGURIDAD DE UNA EMPRESA DE TAMAÑO MEDIO

Ignacio Ramírez Tomas

Tutor: Antonio León Fernández

Cotutor: Alfonso Fernández Martín

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2017-18

Valencia, 11 de septiembre de 2018

Agradecimientos

Para la realización de este trabajo final de grado agradezco al señor Alfonso Fernández Martín, el cual fue mi cotutor y contó conmigo para la realización y puesta en marcha de este proyecto. Agradezco también a mis compañeros de TI de la compañía por permitirme y ayudarme a desarrollar este proyecto con los activos de la compañía.

También me gustaría agradecer a todas las personas y amigos que me han ayudado y dirigido en este proyecto. Sin ellos no habría sido posible.

Muchas gracias a todos.

Resumen

Ante los problemas de seguridad y ataques cibernéticos sufridos por las empresas, se necesita tener conocimiento, detección y corrección de dichos eventos de seguridad y actuar rápidamente. El objetivo es tener visibilidad de las amenazas de distintos proveedores y mantener la infraestructura computacional limpia de intrusos. Surge la necesidad de contratar un sistema de seguridad, pero, teniendo en cuenta la viabilidad en cuanto a valor y coste se refiere, ya que se trata de una empresa de tamaño medio/pequeño, se debe analizar diferentes soluciones de mercado para hacer posible su aplicación. Analizaremos y compararemos las herramientas SIEM más viables dentro de las posibilidades de la empresa. La herramienta SIEM se trata de un software de seguridad el cual permite, a través de un único panel de control, detectar y gestionar cualquier evento que afecte a la infraestructura de la propia red, pudiendo con ello solucionar el problema.

Resum

Davant els problemes de seguretat i atacs cibernètics patits per les empreses, es necessita tindre coneixement, detecció i correcció d'aquest esdeveniments de seguretat i actuar ràpidament. L'objectiu es tindre visibilitat de les amenaces dels diferents proveïdors i mantenir la infraestructura computacional neta d'intrusos. Sorgeix la necessitat de contractar un sistema de seguretat, però, tenint en comte la viabilitat en quant a valor i cost es refereix, ja que es tracta de una empresa d'una mida mitja/petita, es deu d'analitzar les diferents solucions de mercat per a fer possible la seua aplicació. Analitzarem i compararem les ferramentes SIEM més factibles dins de les possibilitats de l'empresa. La ferramenta SIEM es tracta de un software de seguretat el qual permet, a traves d'un únic panell de control, detectar i gestionar qualsevol esdeveniment que afecte a la infraestructura de la pròpia ret, solucionant així el problema.

Abstract

In the face of security problems and cyber-attacks against companies, it is necessary to have knowledge, detection and correction of such security events and act quickly. The company's aim is to have visibility of threats from different suppliers and keep the computing infrastructure clear of intruders. The need to contract a security system arises, but, considering the feasibility in terms of value and cost, since it is a medium/small size company, different market solutions must be analysed to make possible its application. We will analyse and compare the most viable SIEM tools within the possibilities of the company. The SIEM tool is security software that allows, through a single control panel, to detect and manage any event that affects the infrastructure of the network itself, which can solve the problem.

Índice

Lista de tablas

Lista de gráficas

Capítulo 1. Introducción y objetivos

1.1 Contexto y justificación

Ante los problemas de seguridad y ataques cibernéticos sufridos por las empresas, se necesita tener conocimiento, detección y corrección de dichos eventos de seguridad y actuar rápidamente.

La mayoría de sistemas dejan archivos de registro denominados comúnmente logs con el objetivo de mantener informados a sus administradores. Pero, analizar dichos logs en ocasiones requiere de mucho tiempo por parte de los responsables de la seguridad de la información que en ocasiones no llega a ser relevante. Frente a esta situación, aparece la necesidad de implementar una herramienta capaz de unificar todos los logs y correlacionarlos para su posterior análisis. Dicha herramienta se denomina SIEM.

¿Qué es SIEM?

Las siglas **SIEM** significan **S**ecurity **I**nformation & **E**vent **M**anagement. La palabra SIEM consta de la combinación de dos palabras, SIM y SEM. SIM significa Security Información Management. Se encarga de recabar información de los eventos en la red y almacenarla para un futuro análisis. SEM significa Security Event Management. Se encarga de identificar eventos de seguridad en la red en tiempo real y así ejecutar acciones defensivas rápidamente.

Las características que podemos obtener de la herramienta son, análisis, monitorización y gestión de incidentes en tiempo real, gestión de logs y eventos, flexibilidad y sinergia, cumplimiento y representación gráfica de las amenazas detectadas junto a una alarma programada.

En los siguientes puntos analizaremos y compararemos las herramientas SIEM más viables dentro de las posibilidades de una empresa de tamaño medio o pequeño.

1.2 Objetivo

Diseñar, implementar, administrar y evaluar un sistema de administración de seguridad para la información y gestor de eventos centralizado de logs, que permita la creación de cuadros de mando para una rápida actuación frente a una violación de los tres principios de la seguridad de la información, confidencialidad, integridad y disponibilidad. Con el fin de aplicar acciones restrictivas frente a las amenazas de seguridad.

Con la implementación de dicho sistema conseguiremos mantener la red limpia de intrusos.

1.3 Organización de la memoria

La memoria consta de 5 capítulos. Empezando por el capítulo 1, se introduce el tema del proyecto. En el capítulo 2, se muestra el diagrama temporal que se ha seguido durante meses. Estructurando las tareas realizadas durante el trabajo, recordando que se trata de un diagrama meramente orientativo. En el capítulo 3, se analizará el desarrollo para llevar a cabo el proyecto, así como un estudio comparativo y el por qué elegir una herramienta u otra. En el capítulo 4, se muestra la obtención de resultados, así como imágenes adjuntas del software empleado. Finalmente, en el capítulo 5, se hace una conclusión sobre los objetivos cumplidos, las garantías que nos ofrece la utilización de este software junto a su fiabilidad y las carencias que puede llegar a tener. También se comentan las posibles líneas futuras que presenta dicho trabajo.

Capítulo 2. Metodología

2.1 Realización del proyecto

Decididos los motivos los cuales se debe aplicar un software de detección y actuación para actividades maliciosas en la red, se procedió a desarrollar un calendario orientativo para poder asignar las tareas.

En primer lugar, se buscó información relacionada sobre las amenazas que queríamos analizar y filtrar. También se recopilo información respecto a cómo actuar al detectar una amenaza. Con esto, se pudo determinar que se necesitaba de un software especializado en dichos eventos.

En segundo lugar, surgía el problema de la viabilidad económica del proyecto, puesto que se trata de una empresa de tamaño medio/pequeño y los recursos son limitados. Se debía evaluar diferentes soluciones de mercado para poder hacer posible su aplicación.

Por último, se elige la opción más viable y factible para la empresa. Con esto se contrata una licencia de uso del software y se ejecutan las pruebas, tanto de filtrado como de actuación ante eventos en la red. Obteniendo así diferentes informes de eventos y actuando al respecto en tiempo real.

2.2 Distribución de tareas

a. Proceso de documentación y formación. En esta primera tarea, se realizó una búsqueda de información acerca de conceptos relacionados con el proyecto a realizar y recibí formación por parte del señor Ricardo Rodríguez, compañero de infraestructura.
b. Análisis de las herramientas existentes en el mercado. Se realizó una búsqueda y comparación de las diferentes compañías que ofrecen el software a implementar para la red de la empresa.
c. Diseño de casos de uso. Se decide entre los expertos y el jefe de proyecto de la compañía que máquinas serán auditadas con la herramienta elegida.
d. Implementación de la herramienta. Una vez manejada la herramienta y conociendo gran parte de sus posibilidades, se decidió implementar el software en la infraestructura de red de la empresa.
e. Pruebas y ajustes realizados. Con la implementación realizada, se realizaron simulaciones de ataques contra la infraestructura de red, poniendo a prueba la herramienta y ver todo su potencial.
f. Desarrollo de la memoria y realización de la presentación. Se realizó la redacción de la memoria comentando en la misma, los objetivos, el desarrollo y las conclusiones junto a las previsiones de futuro para dicha herramienta y el sector de la ciberseguridad en general. Para finalizar el proyecto, se hizo la presentación para la defensa del trabajo frente a un tribunal y concluir así el Trabajo Final de Grado.

2.3 Diagrama temporal

En el siguiente diagrama temporal (**Tabla 1**) se muestra las diferentes tareas detallas con anterioridad. Este diagrama representa las semanas pasadas entre el mes de Febrero y Agosto de 2018. Marcando así, el mes que se iniciaron las tareas para la realización del trabajo y el último mes que se finalizaron las tareas.

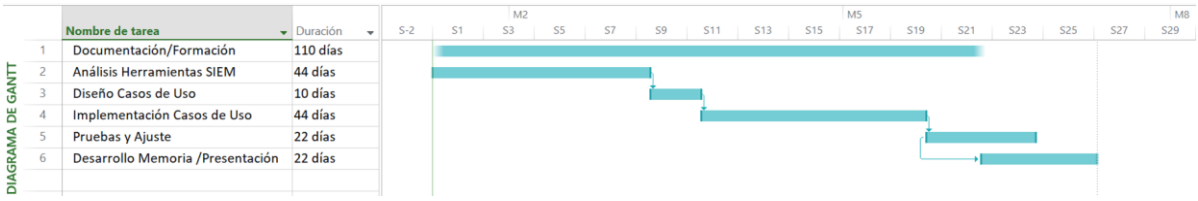


Tabla 1: Diagrama de Gantt

Capítulo 3. Desarrollo

3.1 Análisis de mercado

En el mercado actual hay diversas soluciones al respecto, pero no todas son factibles y rentables para una empresa de tamaño medio/pequeño. Antes de tomar una decisión tenemos que evaluar si vale la pena implementar un sistema de gestión de eventos como SIEM. Las principales ventajas que se pueden obtener tras la implementación son: Obtención de informes y auditorías de cumplimiento, priorización de amenazas, acceso a soporte técnico y rápida actuación.

Entre las distintas opciones están: IBM QRadar SIEM, Solar Winds, Alert Logic o Alien Vault USM, entre otros. Sin embargo, tienen un precio muy elevado.

Por lo que hay que buscar otras opciones más económicas. Opciones implementando software como el del fabricante Fortinet, FortiSIEM. Herramienta que proporciona visibilidad de las amenazas en un único panel de control e implementa soluciones de ciberseguridad. En la siguiente tabla se compararán algunas de las diferentes herramientas en cuanto a fortalezas, debilidades, oportunidades y amenazas se refieren.

Herramienta SIEM	Fortaleza	Debilidad	Oportunidades	Amenaza
Alien Vault USM	SIEM integrado, VM, detección de amenazas en todas las plataformas de la red.	Nueva implementación en la nube. No está muy probado.	Fuerte competencia en materia de precios.	Otras compañías intentan conseguir el todo-en-uno que tiene esta compañía.
SolarWinds LEM	Log asequible y Event Manager (LEM) desplegado.	LEM no tiene una opción de servicio.	Muchos de los clientes tienen más de un producto de SolarWinds.	Detección administrada y servicios de respuesta.
Alert Logic	Primera herramienta en implementar el SIEM en la nube como servicio.	No ofrecen la posibilidad de tener el servidor físico en la empresa.	Buen enfoque en la nube, nube híbrida y datos de los dispositivos del centro.	Grandes proveedores de SIEM cambian su enfoque a los mercados medianos.
AWN Cyber-SOC	Primer innovador en detección de amenazas administradas.	Falta de mercado específico de SIEM e informes de cumplimiento.	Posibilidad de escalar los productos si el cliente amplía su negocio.	Detección en el extremo y respuesta. SIEM como servicio.

Event Tracker 9	Análisis de amenazas predictivo y monitoreo.	SIEM co-administrado, dificultades para los equipos de IT.	Diseñado para las empresas que no tiene una infraestructura grande.	Plataformas que manejan big data y requieren de soporte.
UEBA	Intuitivo, herramientas efectivas.	Alto coste para el producto XM que es todo en uno.	UEBA, es un SIEM con características y un servicio al cliente específico.	SIEM no es un factor en el manejo de eventos.
FortiSIEM	Rápida integración con los servicios, correlación de eventos SOC/NOC, escalabilidad en la arquitectura.	Sistema bastante nuevo, con dificultades para su implementación.	Funciones más allá de un SIEM. Muchos usuarios tienen más productos de este fabricante. FortiSIEM API.	Alta competitividad en el sector del SIEM por su precio.

Tabla 2: Comparativa herramienta software

3.2 Posibles soluciones

A continuación se compararán las diferentes capacidades que tienen algunas de las herramientas analizadas y comparadas en el punto **3.1**. Se elegirá la mejor opción para la empresa.

Capacidad	FortiSIEM	UEBA	Alien Vault USM	IBM Q-Radar
CMDB a tiempo real	✓	✗	✗	✗
Integración externa de Ticketing	✓	✗	Limitado	Limitado
Única consola	✓	✗	✗	✗
Rápida y simple escalabilidad	✓	✗	✗	Parcial
Análisis distribuido	✓	✗	✗	✗
Multi-Tenancy	✓	Limitado	Limitado	✓

Tabla 3: Capacidad herramientas

Lo que hace a FortiSIEM diferente a otros SIEM del mercado es que reúne funcionalidades SOC y NOC en una misma plataforma. Normalmente las empresas necesitan plataformas de gestión de red (NOC) y plataformas de correlación de logs para la seguridad (SOC), pero estas herramientas trabajan aisladas. Aun siendo una herramienta que unifica SOC+NOC, es posible crear perfiles de acceso para que el personal de comunicaciones explote la parte NOC y el de seguridad la parte SOC, pero que existan reglas de correlación que aprovechen la información de los dispositivos de seguridad, de red y de los sistemas.

Una vez analizadas las necesidades de la empresa y el presupuesto para implementar este tipo de software se elige la opción FortiSIEM, del fabricante Fortinet. Con un coste por la

contratación de la licencia de unos 4700€ anuales con los debidos descuentos aplicados. Se trata de un precio bajo respecto a los fabricantes comparados anteriormente.

Con la contratación de dicha licencia obtenemos tanto un sistema SIEM como una base de conocimiento para gestionar las amenazas detectadas. Esta base de conocimiento consta de unas reglas predefinidas editables que explicaremos más adelante en el punto **3.3.5**. Además va a contar con la experiencia de los laboratorios de investigación de amenazas de Fortinet. FortiGuard labs cuenta con +300 investigadores, que no solo cuentan con sus propios descubrimientos, además existen alianzas de terceros (p.e. ciberthreat alliance, etc), la inteligencia colectiva de millones de sondas en internet (FG, sandbox..) y todo ello redunda en una información de inteligencia de amenazas (malware, reputación IP, botnet...) sin igual que se aplica en FortiSIEM para alertarnos de cualquier comportamiento anómalo no sólo en los equipamientos de seguridad, también en los de red, sistemas, almacenamiento....

3.3 Funcionalidad FortiSIEM

3.3.1 Capacidades

Recolección de datos: La herramienta FortiSIEM debe tener total visibilidad frente a firewalls, bases de datos, sistemas operativos, servidores, switches, sistemas de control de acceso, entre otras. Toda la infraestructura mencionada tiene similares funciones de registro y alertas pero varía un poco el formato, el protocolo o la información que proporcionan. Algunos componentes son capaces de conectarse directamente con el FortiSIEM, con un protocolo estándar, pero otros no, por lo que hay que asignarle un protocolo de comunicación seguro entre ellos, como pueden ser el SSH, SMTP, Telnet, entre otros.

Indexación de datos: Una vez almacenados todos los datos recopilados en la fase anterior, correlacionamos todos estos. La indexación puede hacerse de dos formas, mencionadas seguidamente en el punto **3.4**. Esta función puede llegar a presentar una serie de retos y complicaciones dependiendo del tamaño de la infraestructura y la cantidad de datos que se guardan.

Normalización de datos: Partiendo que cada dispositivo genera sus logs y no todos los dispositivos los genera con el mismo formato, pero si con una información muy similar, aplicamos la normalización a dichos datos y se extrae información que tienen los logs en común. Esta información se expresa en un formato coherente así permite una comparación directa entre diferentes eventos de seguridad.

Correlación de eventos: Función de vincular múltiples eventos de seguridad que por separado no resultarían una actividad inusual pero gracias a esta función, relaciona los eventos a través de múltiples sistemas ocasionados en un mismo momento. Para conseguir esta correlación de eventos hay que preestablecer unas reglas que indica los tipos de eventos que queremos percibir.

Muchas de estas reglas vienen predefinidas, pero se pueden crear reglas personalizadas adaptándolas a nuestras preocupaciones de seguridad. Se mostrará la creación y edición de reglas personalizadas más adelante, en el punto **3.5.3**.

Reportes: Dicha función es la parte más importante de la herramienta, ya que a partir de ella se tomarán medidas respecto a los eventos sucedidos. Estos reportes nos ayudan al cumplimiento normativo. Según el tipo de evento y su gravedad, el informe tendrá diferente aspecto. Personalizado con los diferentes tipos de reportes existentes en el FortiSIEM. Se mostrará la personalización más adelante, en el punto **3.5.2**.

Alertas: Gracias a la correlación de eventos podemos generar alertas para notificar a los administradores del sistema de una posible amenaza en el sistema. Esta notificación puede realizarse mediante un aviso por correo electrónico. Dicha configuración de avisos se mostrarán más adelante, en el punto **3.5.2**.

Análisis: Tiene la capacidad de buscar en el registro logs determinados aplicando unos filtros de búsqueda. Ya sean eventos anómalos o maliciosos. Gracias a la correlación de eventos y la normalización se pueden filtrar y analizar dichos eventos. Ahorrando mucho tiempo a los administradores del sistema para recopilar información. Este análisis se mostrará más adelante, en el punto **3.5.2**.

Consola de administración central o Dashboard: Dicha consola no se trata de una capacidad específica, pero cualquier centro de control que se precie necesita de un tablero de mando. Con dicho tablero se puede monitorizar en tiempo real todos los eventos que se están ejecutando. Entre otras funciones también está el análisis, manipulación de datos y generación de informes. Más adelante se mostrará el dashboard del FortiSIEM, punto **3.5.2**.

3.3.2 Beneficios

Gracias a la implementación del FortiSIEM conseguimos una serie de beneficios asociados como los siguientes:

- Permite una rápida detección y actuación al equipo de seguridad frente amenazas de malware y actividades sospechosas. Esto hace que el equipo sea más eficaz y así conseguir interceptar y abordar los eventos de seguridad en su comienzo, antes de que pueda afectar gravemente a la infraestructura empresarial.
- Gracias a las capacidades mencionadas anteriormente, punto **3.3.1**, se pueden desarrollar y entregar informes más completos a cargos superiores de infraestructura. Con FortiSIEM dicha generación de informes se puede gestionar en un par de horas, tarea que antes de su implementación podía llevar días. Gracias a esta simplicidad el administrador de seguridad puede dedicarse a otras labores con más prioridad y responsabilidad.
- FortiSIEM es el conjunto de varias herramientas como SIM, SEM, sistemas de análisis y administración de logs y sistemas de monitoreo. Con la unificación de todas estas herramientas en una conseguimos una reducción de presupuesto y costes computacionales. Permitiendo a la compañía ahorrar tiempo y dinero.
- Con la búsqueda de información a tiempo real, dispondremos de todos los informes detallados frente a una auditoría o investigación a la empresa.

3.3.3 Requisitos requeridos

Para la implementación del SIEM se requieren unos mínimos para que el sistema funcione en tiempo real y sin apenas retardos. Dependiendo del número de eventos por segundo (EPS) que se quieran analizar deberán cumplirse una serie de requisitos del sistema como los representados en la siguiente tabla:

EPS	Licencias	Host	Procesador	Memoria	Almacenamiento para datos de eventos (1 año)
1500	1	ESXi (4.0 o superior)	4 núcleos 3GHz	16Gb; 24Gb	3 TB
4500	1	ESXi (4.0 o superior)	4 núcleos 3GHz	16Gb; 24Gb	8 TB
7500	1 Super; 1 Worker	ESXi (4.0 o superior)	**Super:** 8 núcleos 3GHz; **Worker:** 4 núcleos 3GHz	**Super:** 24Gb; **Worker:** 16Gb	12 TB
10000	1 Super; 1 Worker	ESXi (4.0 o superior)	**Super:** 8 núcleos 3GHz; **Worker:** 4 núcleos 3GHz	**Super:** 24Gb; **Worker:** 16Gb	17 TB
20000	1 Super; 3 Workers	ESXi (4.0 o superior)	**Super:** 8 núcleos 3GHz; **Worker:** 4 núcleos 3GHz	**Super:** 24Gb; **Worker:** 16Gb	34 TB
30000	1 Super; 5 Workers	ESXi (4.0 o superior)	**Super:** 8 núcleos 3GHz; **Worker:** 4 núcleos 3GHz	**Super:** 24Gb; **Worker:** 16Gb	50 TB

Tabla 4: Requisitos FortiSIEM

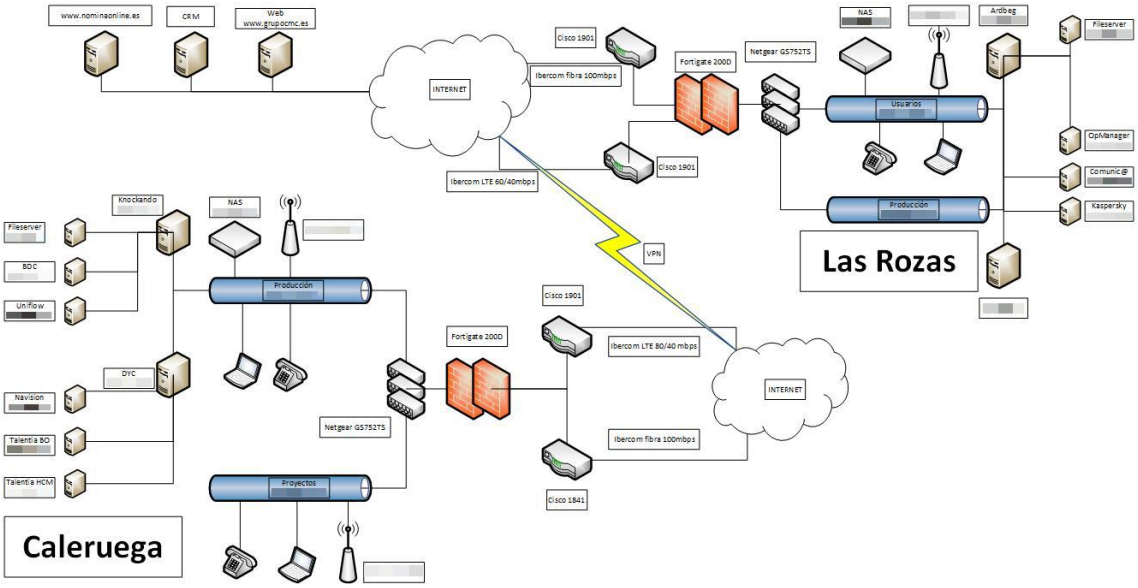
3.4 Arquitectura de soluciones

La tecnología SIEM une a las tecnologías de administración de logs consiguiendo así una gran variedad de datos de logs, retención eficiente, búsquedas entre los logs, indexación y reportes.

Antes de implementar la herramienta FortiSIEM debemos definir que servidores y elementos de la red serán analizados, teniendo en cuenta que dispositivos pueden ser más críticos. También se debe definir un administrador de ciberseguridad y analista encargado de la supervisión de los resultados.

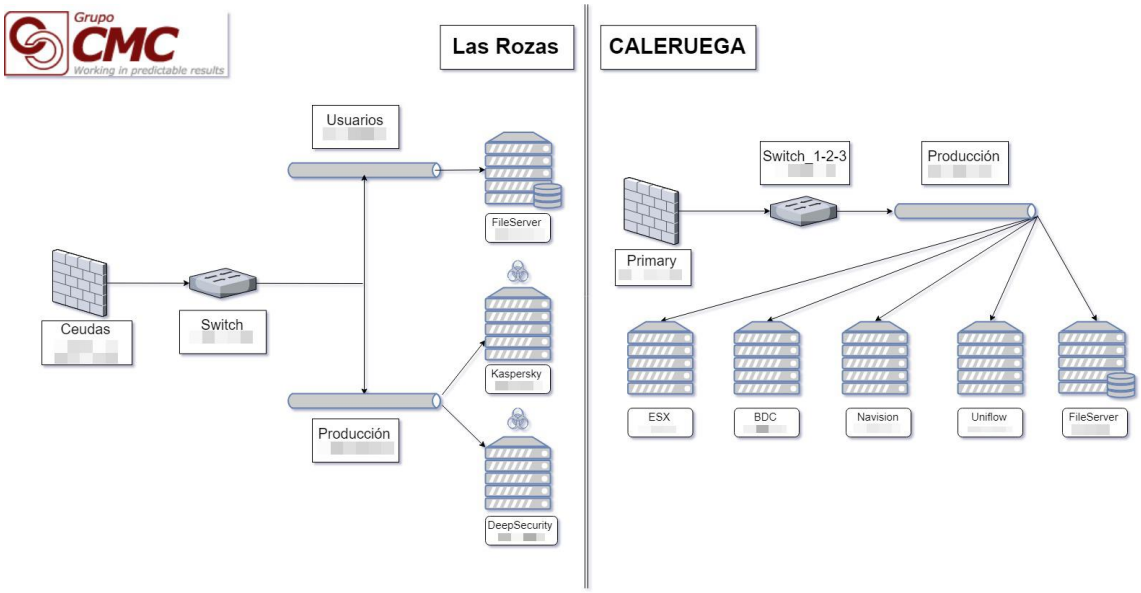
En la siguiente imagen podemos apreciar la arquitectura de la infraestructura que tiene desplegada la empresa Grupo CMC. Se muestran todas las máquinas que tiene, pero no todas están siendo auditadas por la herramienta FortiSIEM. Más adelante hablaremos como se añaden

máquinas a la herramienta seleccionada para así poder llevar un control riguroso sobre ellas, punto **3.5.2**.



Gráfica 1: Infraestructura Grupo CMC

A continuación se muestran las máquinas que estas siendo auditadas de todas que tiene grupo CMC.



Gráfica 2: Máquinas auditadas

Todo esto se puede implementar de distintas formas, una de ellas es mediante un recolector central de logs. Esto significa que solo hay un servidor encargado de todas las tareas administrativas referentes a los logs que genera el SIEM. La ventaja principal que obtenemos aplicando este tipo de recolección de datos es, la facilidad de analizar el rendimiento del sistema y plantear continuamente posibles mejoras. Pero, también encontramos inconvenientes al realizar esta configuración, toda incidencia pasa por él, por lo tanto, si dicho servidor falla,

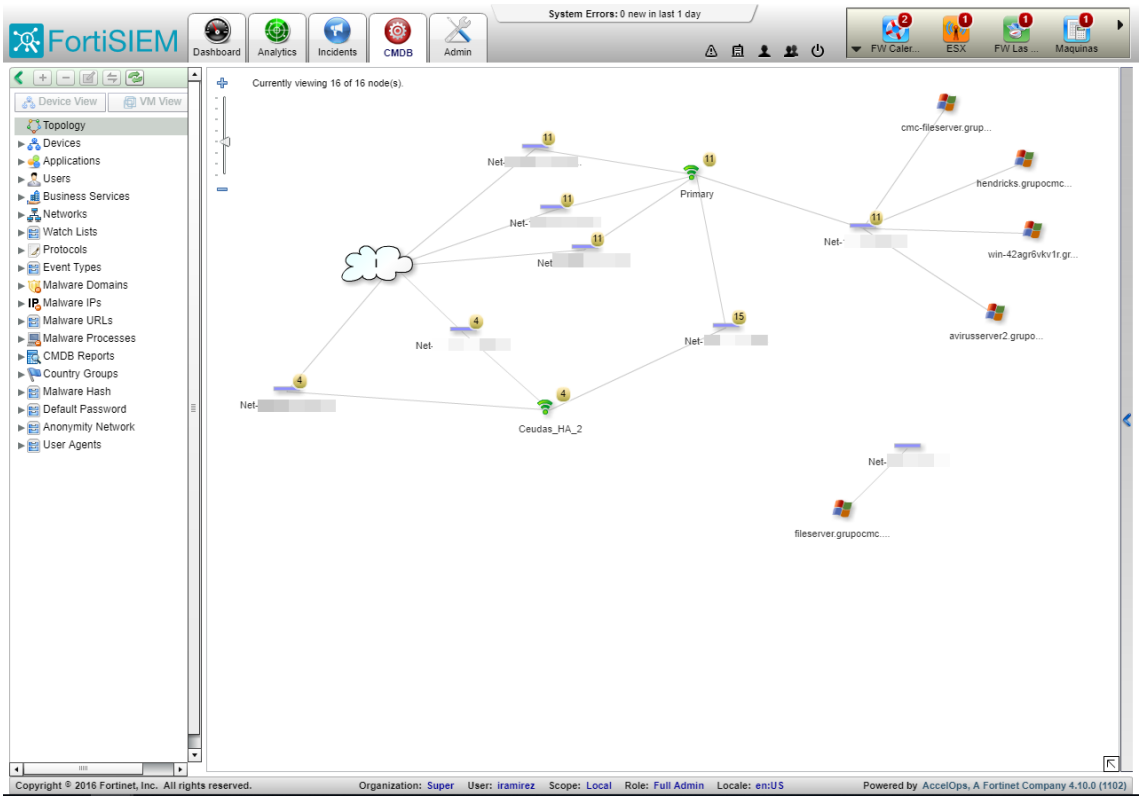
dejaría de coleccionar los logs y entonces no se retendría información durante ese periodo de indisponibilidad.

Otra posible opción para implementar varios recolectores de logs son los subrecolectores, así, mantenemos un recolector principal e instalamos recolectores secundarios en cada centro de operaciones. Con esto conseguiremos que si el servidor principal cayese no perderíamos los datos ya que disponemos de redundancia en la red para guardar los logs en diferentes servidores. Con dicha configuración también podemos especializar a cada agente con su unidad de trabajo y así que cada administrador gestione su servicio y los logs generados por el mismo.

3.5 Implementación

3.5.1 Alcance

Una vez decidido a que servidores o elementos de la red implementar FortiSIEM, pasamos a la práctica, aplicamos el FortiSIEM a la infraestructura de red. Podemos visualizar la siguiente tipología:



Gráfica 3: Topología de la red

Podemos ver la tipología implementada accediendo a la consola de FortiSIEM vía internet en la sección CMDB, Topology.

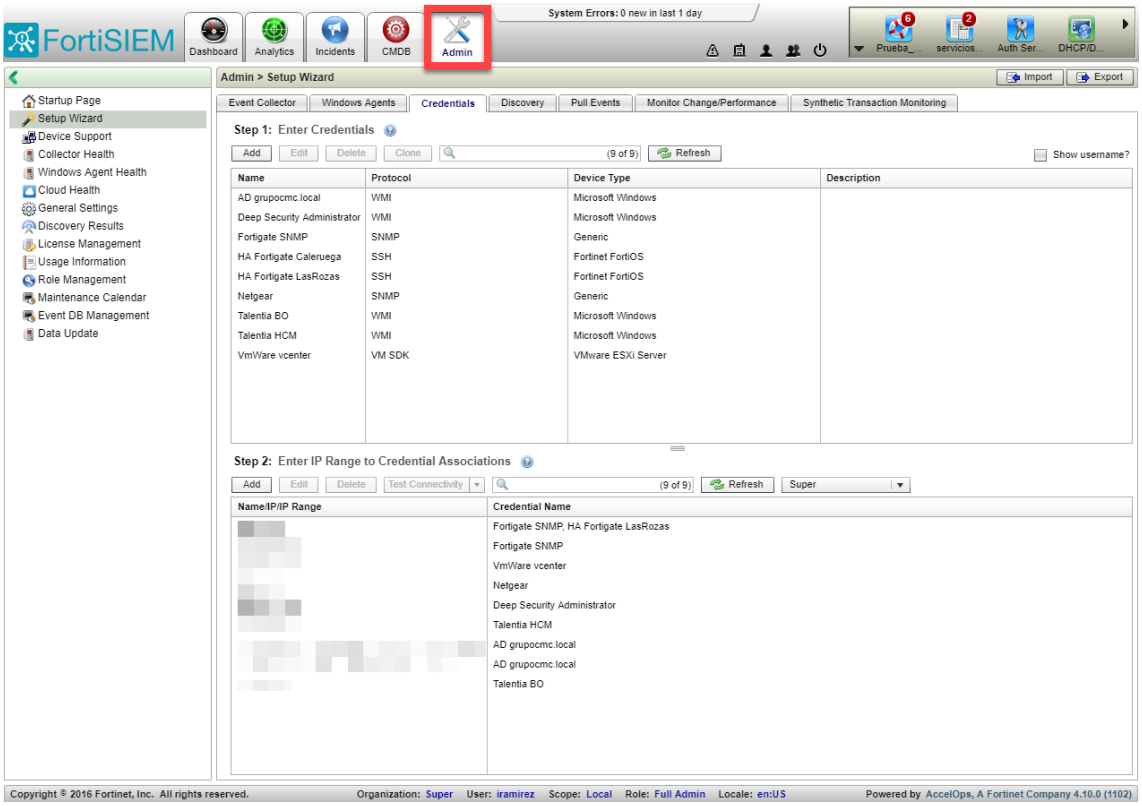
3.5.2 Pestañas

- **Admin**

En la pestaña Admin podemos encontrar diferentes pestañas para seleccionar y configurar nuestro sistema SIEM. Entre ellas destacan: Event Collector, Credentials, Discovery y Pull Events.

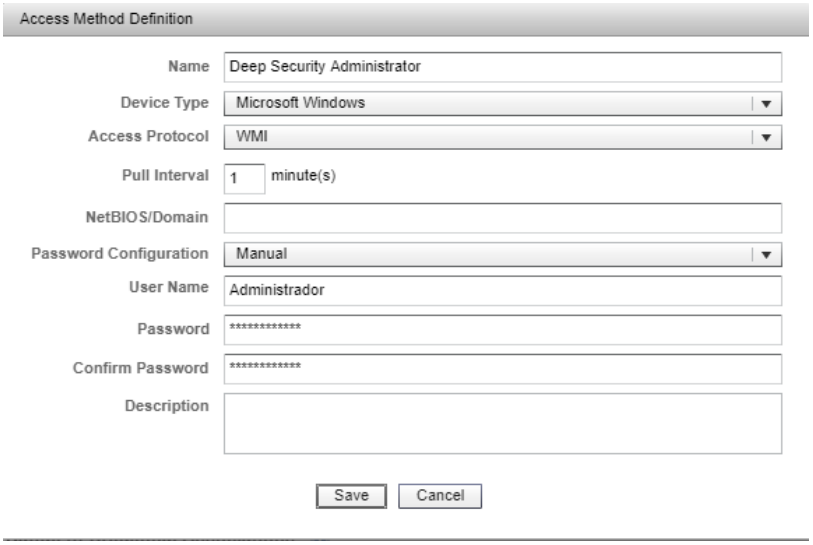
En la parte izquierda encontramos una serie de categorías donde obtendremos información relacionada con la licencia del FortiSIEM contratado.

En esta pestaña también podemos agregar nuevas máquinas para almacenar y gestionar los logs que generan.



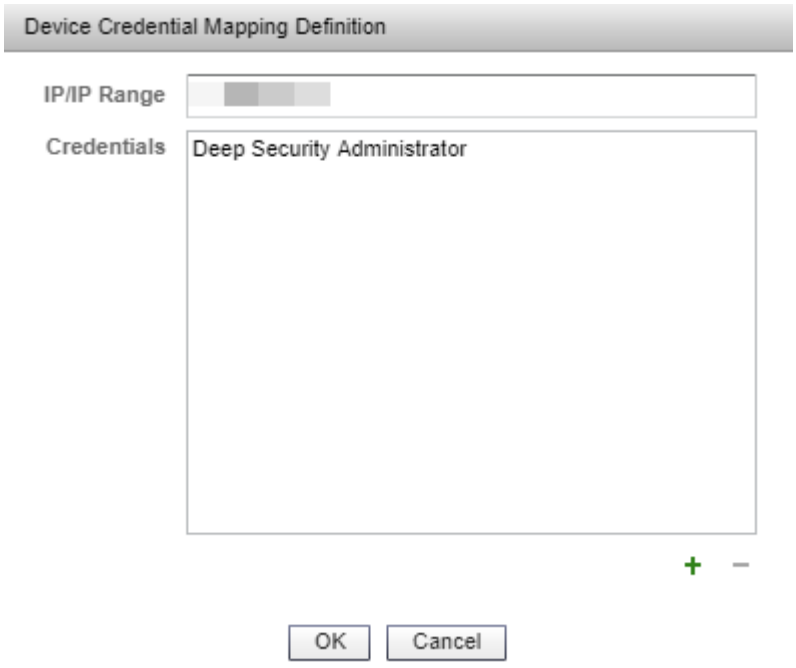
Gráfica 4: Pestaña Admin

En la categoría Setup Wizard, pestaña Credentials, en el step 1, tenemos que añadir el nombre de la máquina que queremos auditar con el fortiSIEM, el tipo de dispositivo, el protocolo de comunicación que usaran entre ellos y por último las credenciales para tener acceso a la máquina deseada.



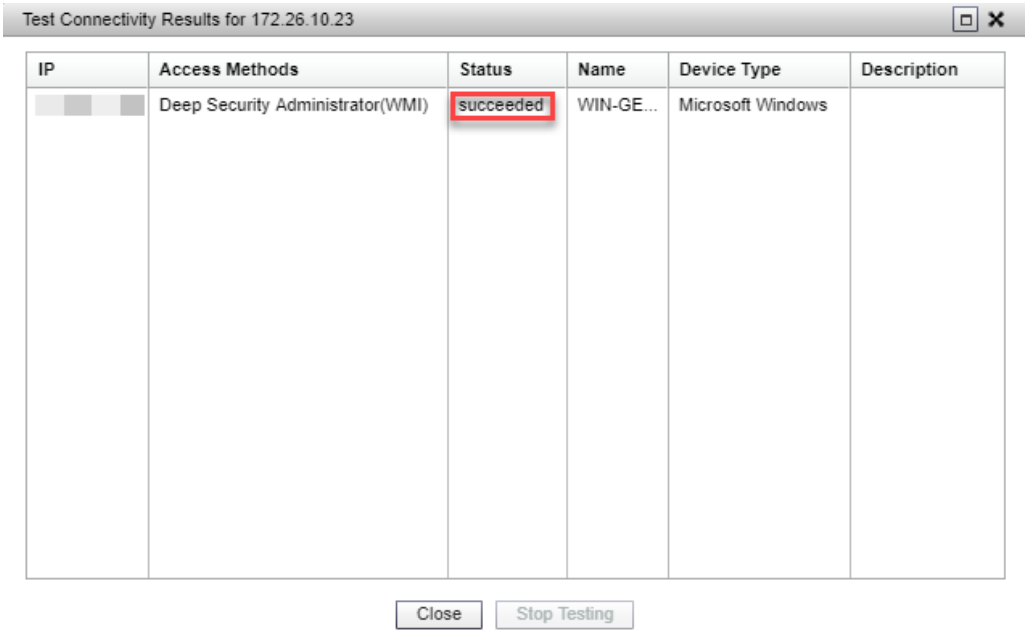
Gráfica 5: Step 1

Una vez creadas las credenciales para tener acceso a los dispositivos de red, pasamos al step 2. Este paso consiste en añadir la ip del dispositivo deseado y sus credenciales configuradas anteriormente en el step 1.



Gráfica 6: Step 2

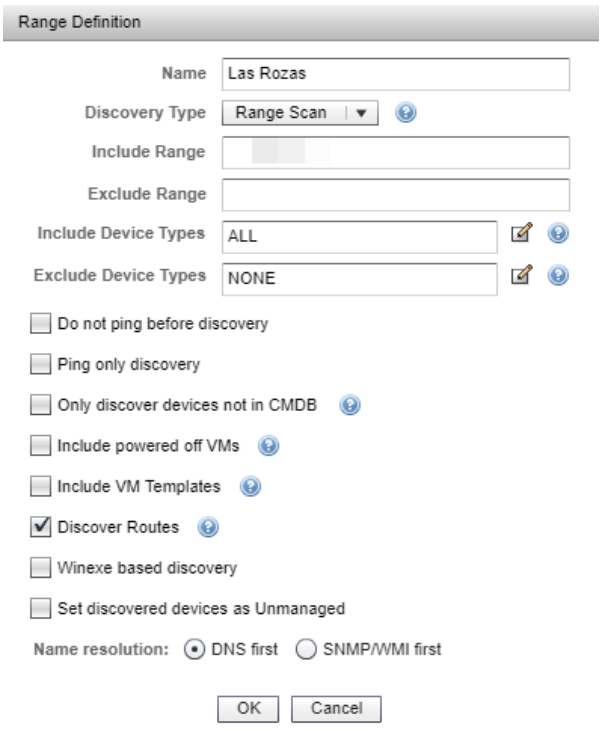
Acto seguido, pasamos a testear la conectividad entre el fortiSIEM y la máquina configurada.



Gráfica 7: Test conectividad

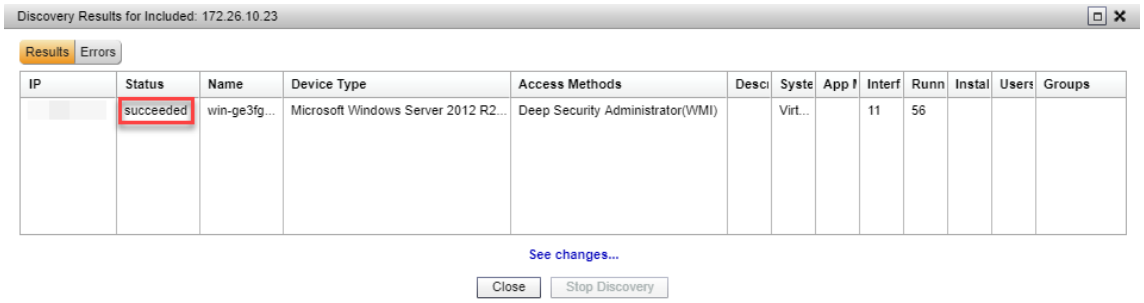
Como podemos ver en la gráfica 6, obtenemos una conectividad exitosa. Pero todavía no estamos auditando los eventos de la máquina en cuestión.

El último paso a seguir para conseguir auditar el dispositivo será abrir la pestaña Discovery y añadir un rango o una ip acorde a la máquina que se quiere tener los eventos.



Gráfica 8: Rango Ip

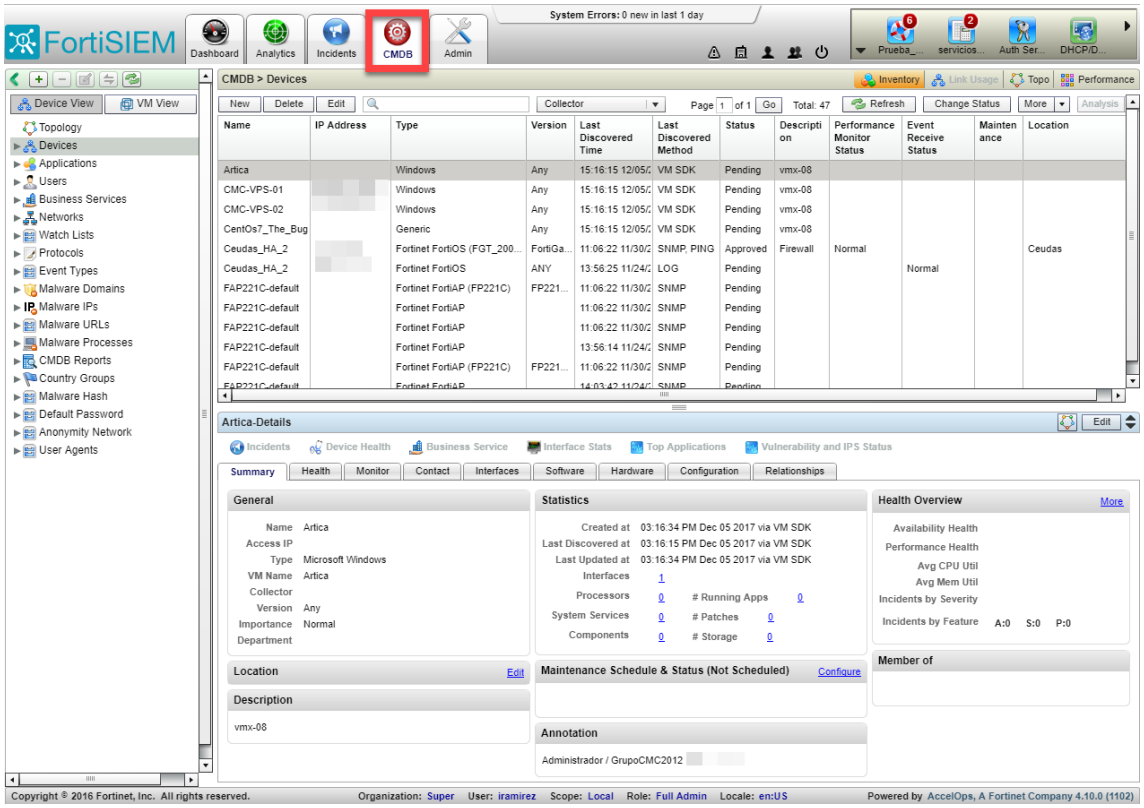
Una vez configurado, pulsamos en Discover y el fortiSIEM intentará conectarse con la máquina en cuestión. Si el resultado es exitoso, obtendremos unos resultados similares a los mostrados en la siguiente captura.



Gráfica 9: Discovery

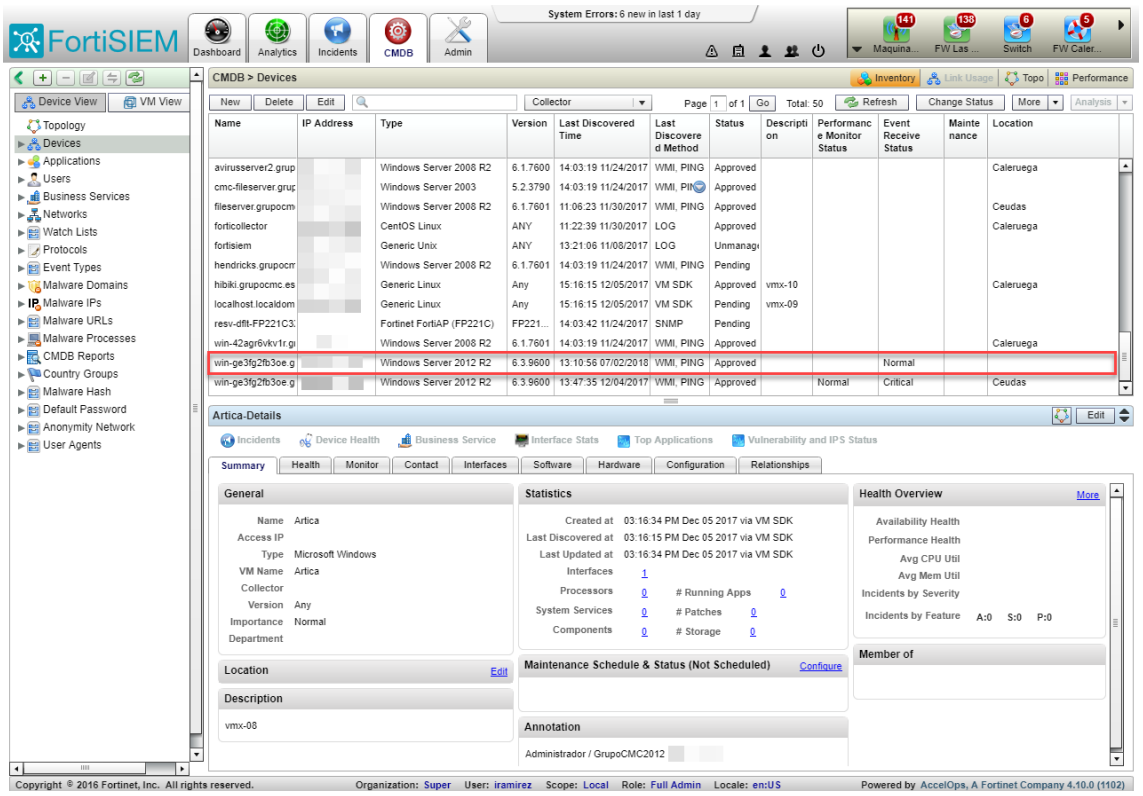
- **CMDB**

En la pestaña siguiente, a la izquierda de la analizada anteriormente, encontraremos el CMDB. Pestaña en la cual se puede apreciar la topología de la red, los dispositivos y los permisos que tienen los usuarios administradores en la herramienta FortiSIEM entre otras cosas.



Gráfica 10: Pestaña CMDB

En la categoría Devices, podemos apreciar todas las máquinas que están siendo auditadas por el fortiSIEM, entre ellas podemos ver la última incorporación que hemos realizado anteriormente.



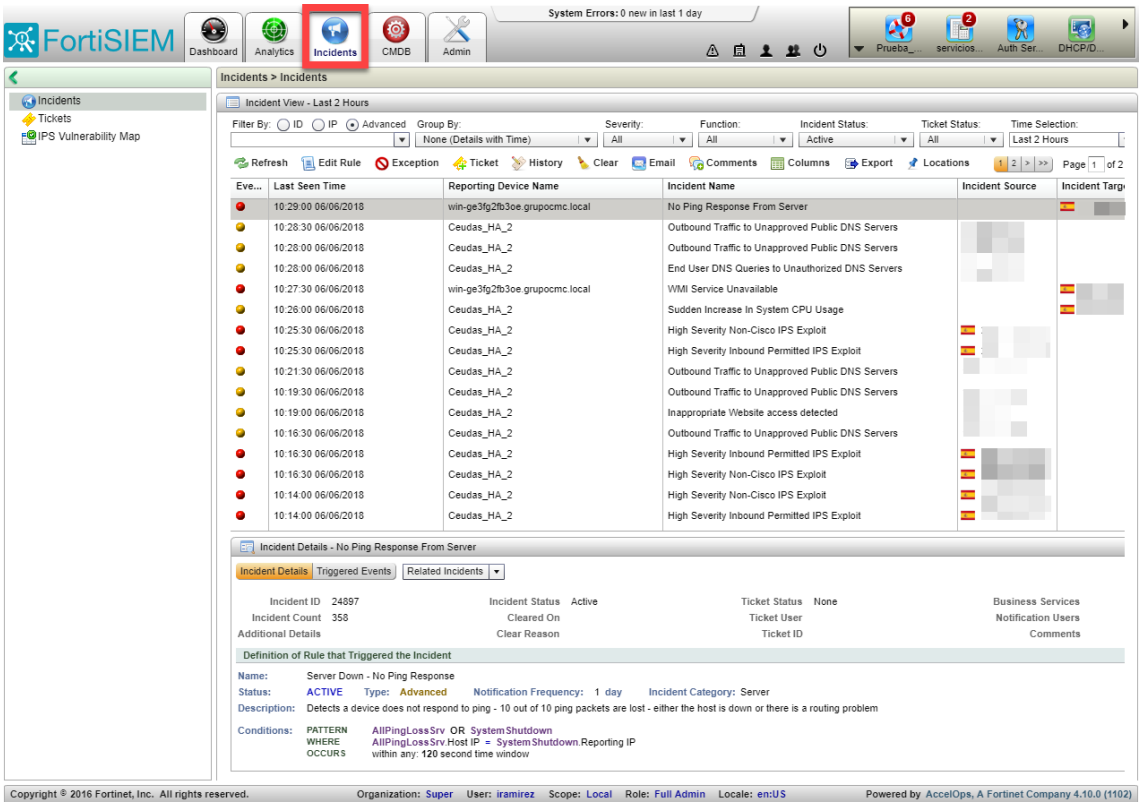
Gráfica 11: Devices

Como podemos apreciar, el estado de la máquina es aprobado, esto significa que el fortiSIEM está sincronizado correctamente y obtendremos los eventos del dispositivo en tiempo real.

- **Incidents**

A continuación, en la pestaña contigua a la anterior, encontramos la de Incidents, pestaña en la cual podemos buscar eventos ocurridos en el sistema aplicando filtros como: ID, IP, Advanced, por grupo, por severidad, por función, estado del incidente, estado del ticket y que busque dentro de un determinado intervalo de tiempo. Una vez obtenemos el evento en cuestión, se puede mandar por email, añadir un comentario o exportar como archivo PDF o CSV.

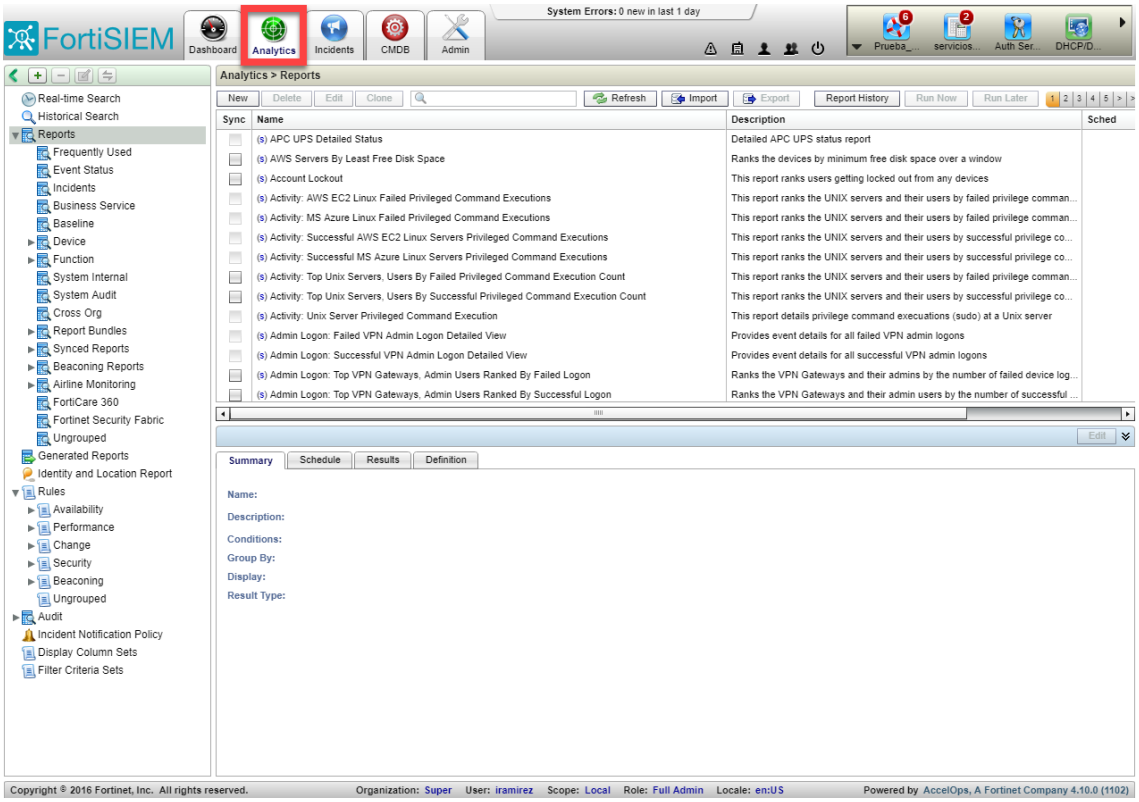
Estos incidentes se crean a partir de las reglas predefinidas en la pestaña siguiente, Analytics.



Gráfica 12: Pestaña Incidents

- **Analytics**

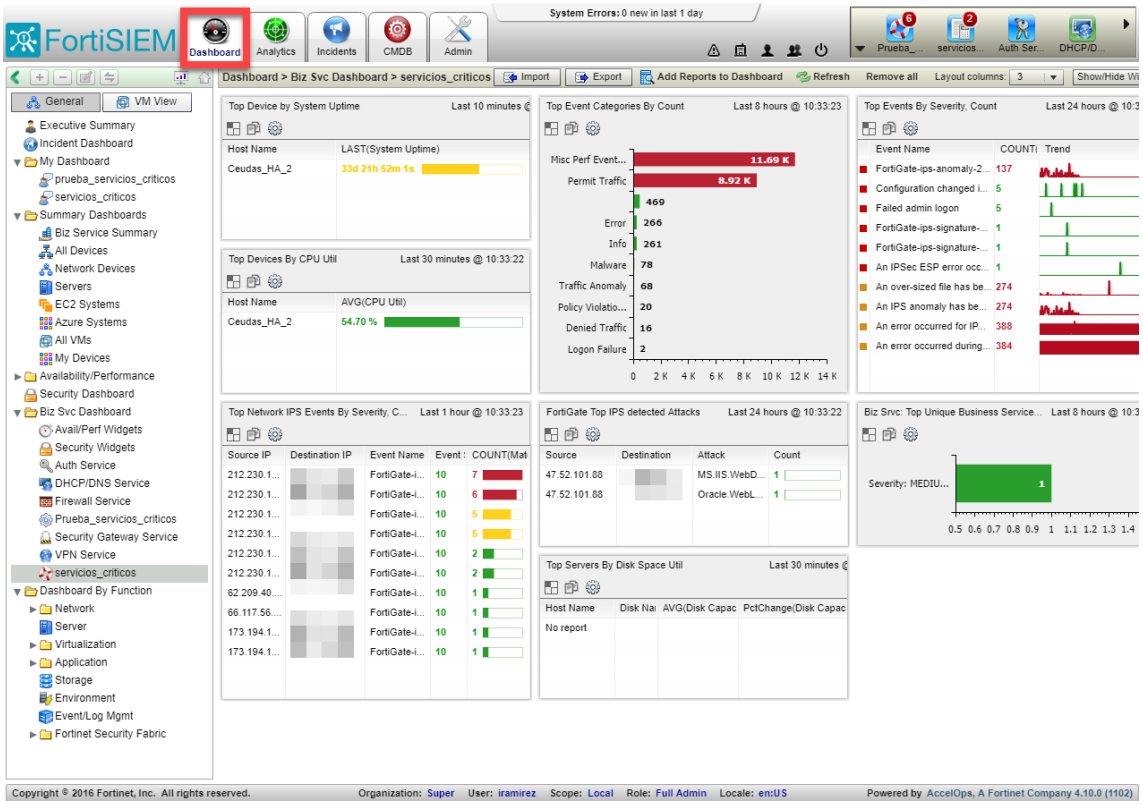
Es la pestaña siguiente a la de Incidents, en la cual podemos crear reportes de los eventos, habilitar o deshabilitar las reglas en las cuales se basa FortiSIEM para detectar eventos de amenazas, configurar auditorías a eventos y configurar las notificaciones mediante correo electrónico.



Gráfica 13: Pestaña Analytics

- **Dashboard**

Es la pestaña más a la izquierda de todas. Se pueden apreciar y configurar las vistas y gráficas de los eventos recopilados. Estas vistas ayudan al administrador de seguridad a detectar un evento anómalo en la red.



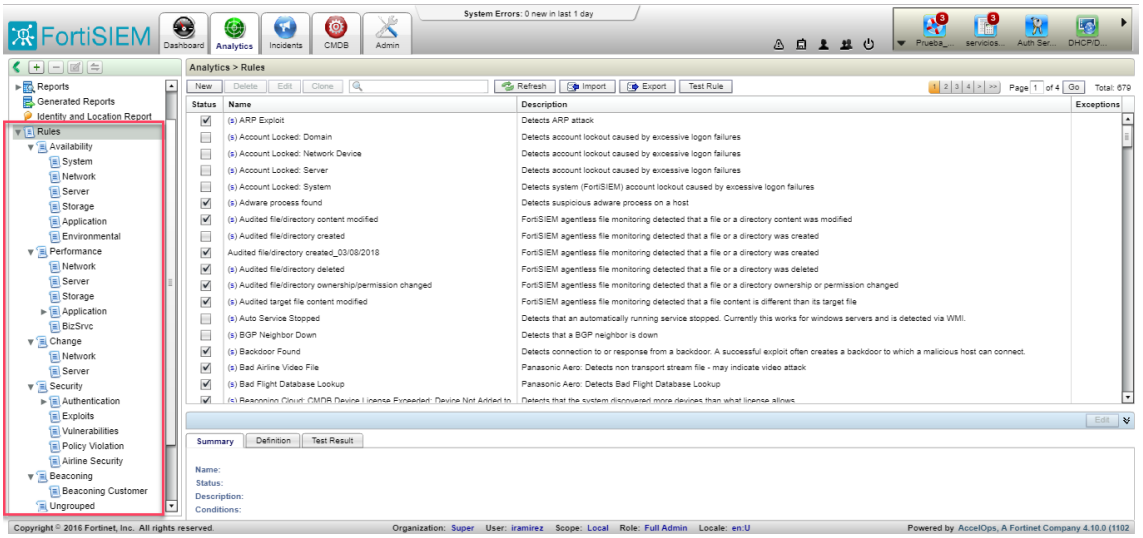
Gráfica 14: Pestaña Dashboard

3.5.3 Reglas

Una vez definidos los dispositivos a los que se les aplicará la herramienta FortiSIEM, debemos decidir que eventos queremos detectar para posteriormente analizar. Para realizar esta acción debemos aplicar una serie de reglas en la pestaña analytics de la consola de FortiSIEM.

Disponemos de los siguientes campos para filtrar los eventos:

- Availability
- Performance
- Change
- Security
- Beaconing
- Ungrouped

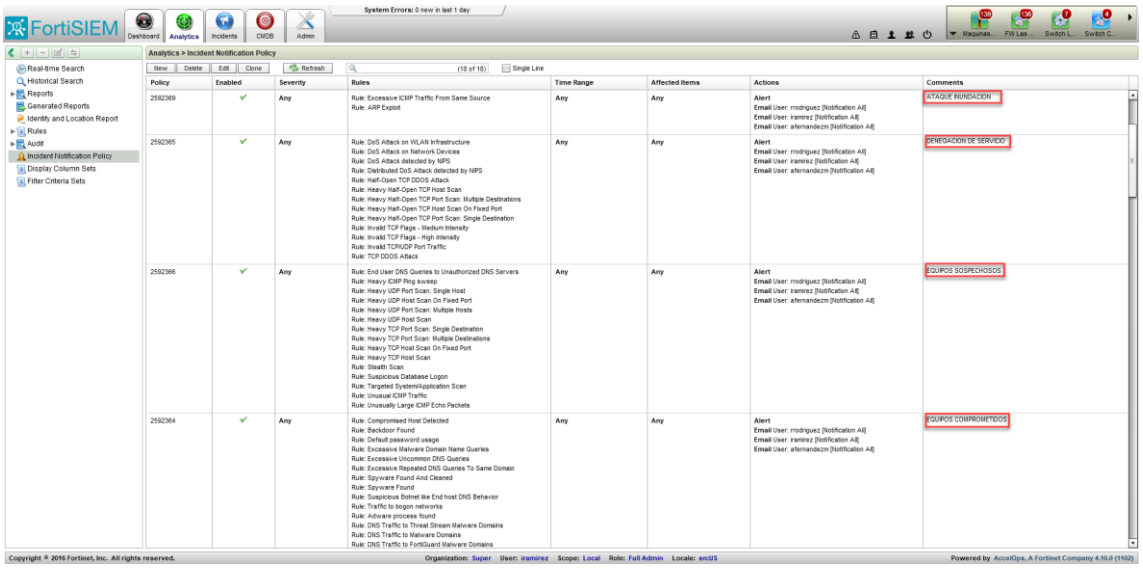


Gráfica 15: Reglas

Dependiendo del desplegable que se abra, se pueden obtener diferentes campos para así acotar más el filtrado con el uso de las reglas. Como por ejemplo, dentro de Availability, podemos encontrar los siguientes campos: System, Network, Server, Storage, Application y Environmental. Todas estas reglas vienen definidas por defecto, pero se tiene la posibilidad de editar cada una de ella adaptándolas a las necesidades propias.

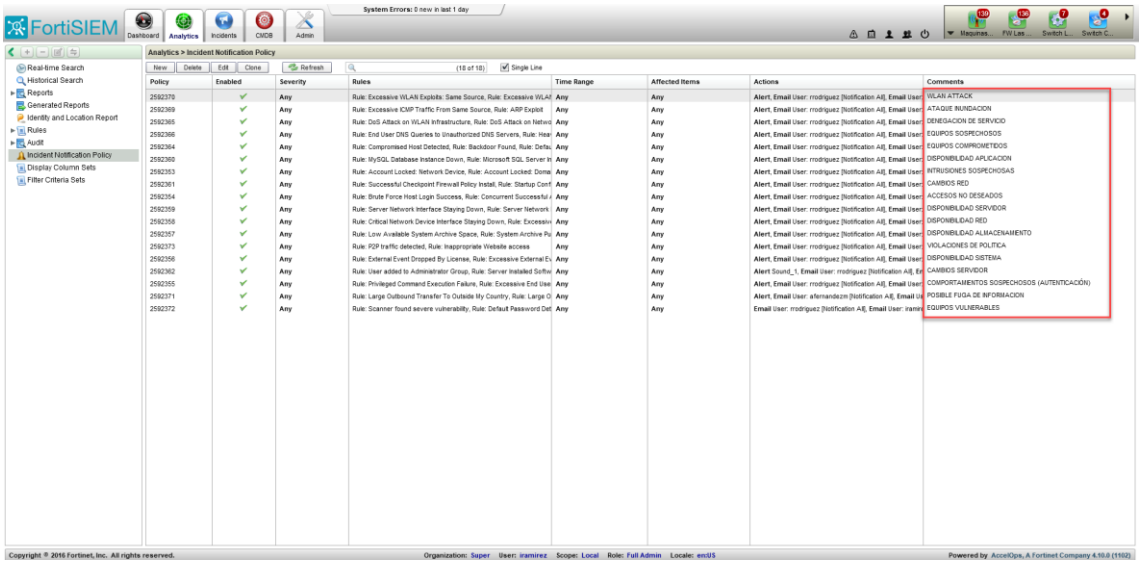
Una vez evaluadas y filtradas todas las reglas que se quieren aplicar para la auditoria en las máquinas, el comité de ciberseguridad de la empresa se dispone a crear las políticas de control y monitorización. Con dichas políticas se tendrá un mayor control y gobierno de la seguridad cibernética de la empresa dejando constancia de un registro de eventos y así poder hacer frente a una auditoria externa, como sería la de la ISO 27001.

En la siguiente imagen podemos apreciar la clasificación de algunas reglas en grupos de políticas, como serían las de: Ataque por inundación, denegación de servicio, equipos sospechosos, entre otros.



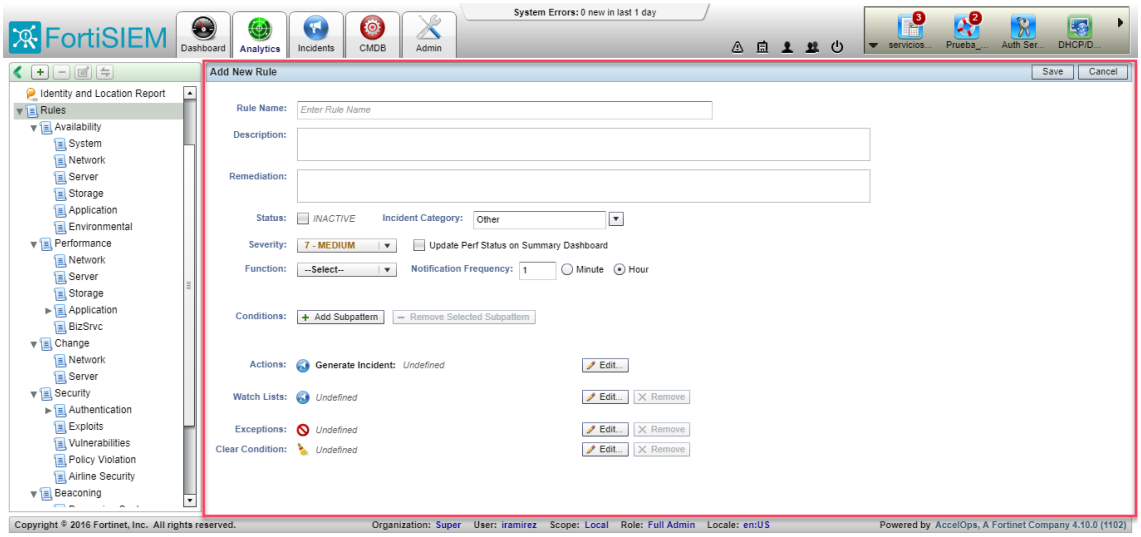
Gráfica 16: Grupos de políticas

A continuación, podemos ver todas las políticas creadas por el comité y el jefe de ciberseguridad de la empresa.



Gráfica 17: Políticas

También existe la posibilidad de crear reglas nuevas, éstas se guardarán en el desplegable Ungrouped. La creación de nuevas reglas requiere un conocimiento avanzado en seguridad y sistemas puesto que su realización no es trivial debido a los campos que se solicita rellenar. Como serían los siguientes:

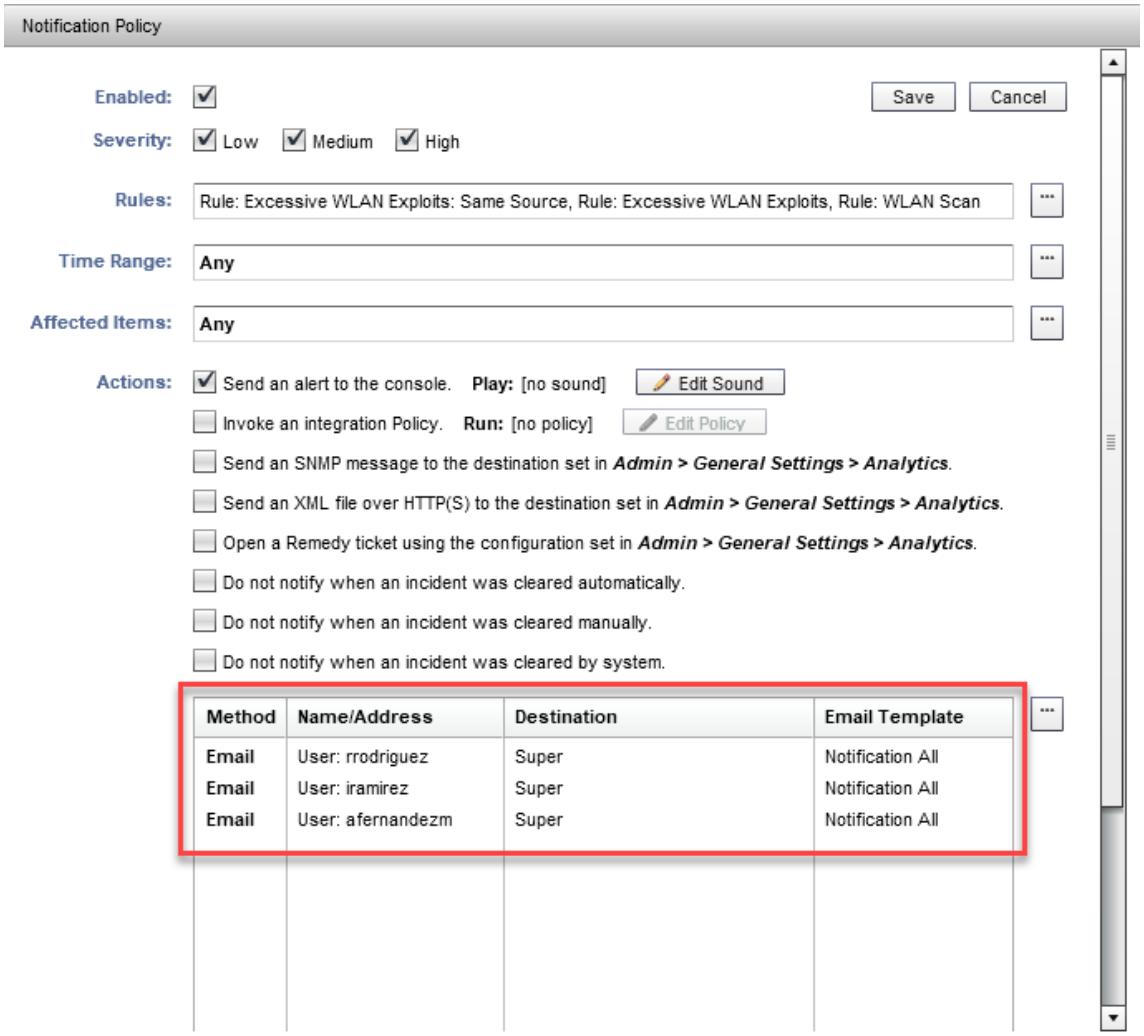


Gráfica 18: Añadir nueva regla

3.6 Notificaciones por correo

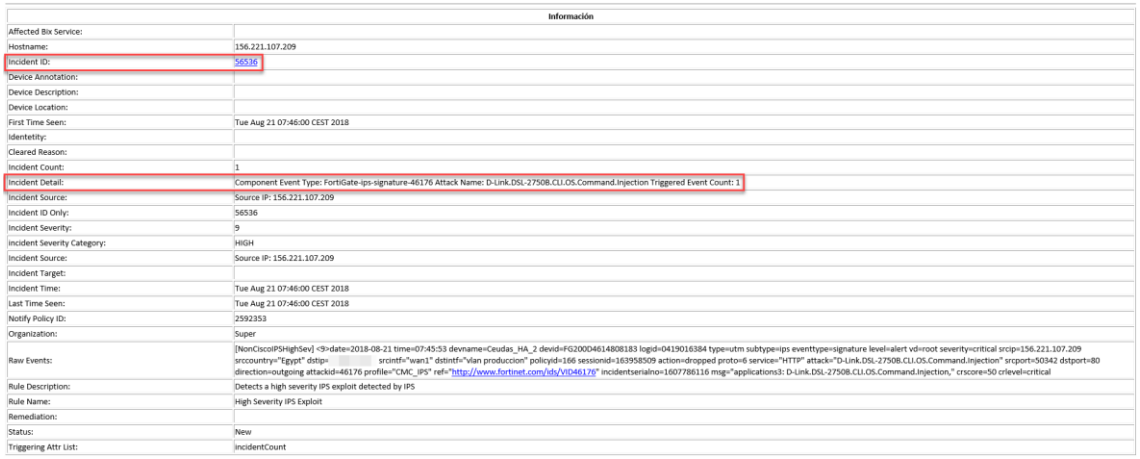
Una vez tenemos definidas todas las políticas que queremos que auditen los eventos, podemos configurar la herramienta fortiSIEM para ser notificados por correo electrónico o por SMS de todas las posibles violaciones del sistema.

Dentro del apartado Notification Policy podemos incluir los usuarios de correo que queremos que sean notificados. En este caso, como podemos observar en la siguiente imagen, hemos añadido tres cuentas de correo.



Gráfica 19: Notificación correo electrónico

El correo que se recibe en las tres cuentas tiene el siguiente formato:



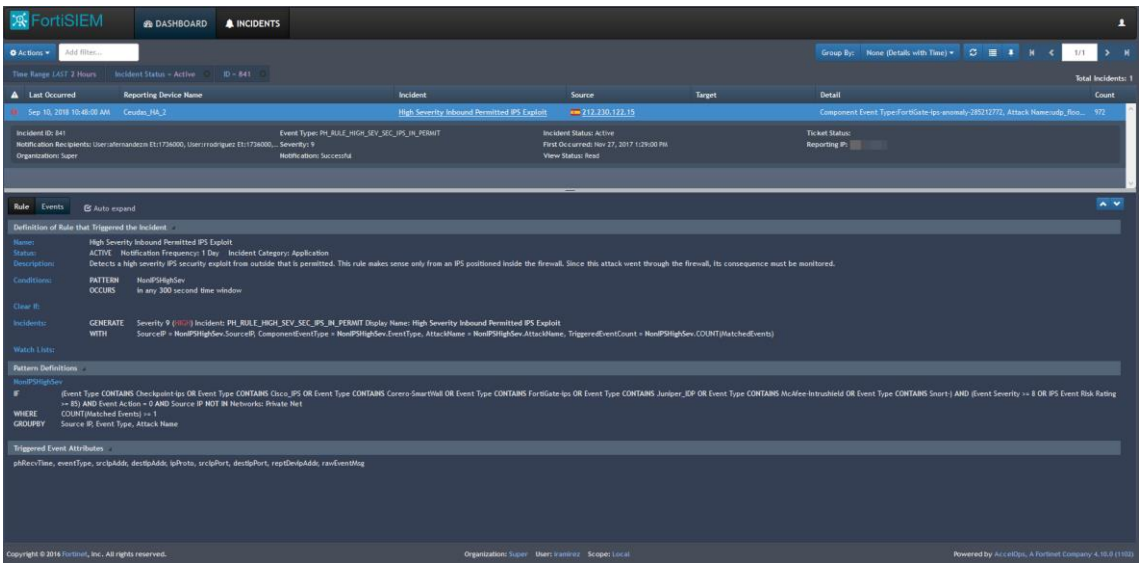
Información	
Affected Bix Service:	
Hostname:	156.221.107.209
Incident ID:	56536
Device Annotation:	
Device Description:	
Device Location:	
First Time Seen:	Tue Aug 21 07:46:00 CEST 2018
Identetity:	
Cleared Reason:	
Incident Count:	1
Incident Detail:	Component Event Type: FortiGate-ips-signature-46176 Attack Name: D-Link.DSL-2750B.CLI.OS.Command.Injection Triggered Event Count: 1
Incident Source:	Source IP: 156.221.107.209
Incident ID Only:	56536
Incident Severity:	9
incident Severity Category:	HIGH
Incident Source:	Source IP: 156.221.107.209
Incident Target:	
Incident Time:	Tue Aug 21 07:46:00 CEST 2018
Last Time Seen:	Tue Aug 21 07:46:00 CEST 2018
Notify Policy ID:	2592353
Organization:	Super
Raw Events:	[NonCiscoIPSHighSev] <9>date=2018-08-21 time=07:45:53 devname=Ceudas_HA_2 devid=FG200D4614808183 logid=0419016384 type=utm subtype=ips eventtype=signature level=alert vd=root severity=critical srcip=156.221.107.209 srccountry="Egypt" dstip= [redacted] srcintf="wan1" dstintf="vlan produccion" policyid=166 sessionid=163958509 action=dropped proto=6 service="HTTP" attack="D-Link.DSL-2750B.CLI.OS.Command.Injection" srcport=50342 dstport=80 direction=outgoing attackid=46176 profile="CMC_IPS" ref="http://www.fortinet.com/ids/VID46176" incidentserialno=1607786116 msg="applications3: D-Link.DSL-2750B.CLI.OS.Command.Injection," crscore=50 crlevel=critical
Rule Description:	Detects a high severity IPS exploit detected by IPS
Rule Name:	High Severity IPS Exploit
Remediation:	
Status:	New
Triggering Attr List:	incidentCount

Gráfica 20: Correo electrónico

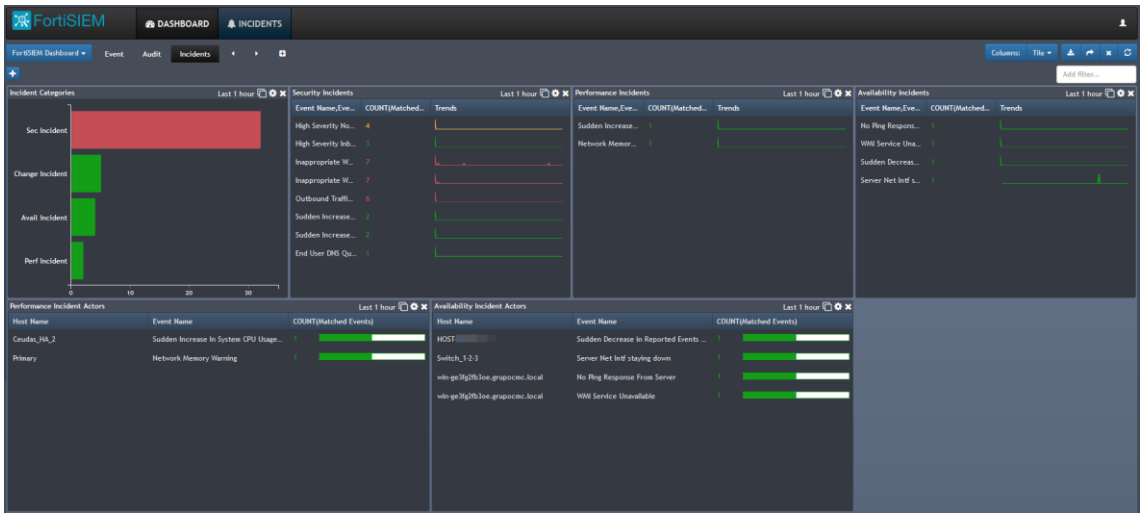
Gracias a estas notificaciones en tiempo real, no es necesario dedicar todo el tiempo a monitorizar el estado e incidencias de las máquinas, puesto que puedes configurar las notificaciones para que seas avisado de los eventos más críticos y así poder actuar en consecuencia.

3.7 Interfaz de incidencias

Una vez recibido la notificación por correo electrónico, se asigna un ID al evento en cuestión que ha hecho saltar la alerta. Si pinchamos en dicho ID, abriremos otro tipo de interfaz de monitorización que tiene el fortiSIEM. Este nuevo interfaz esta diseñado para poder ver con mayor detalle las incidencias como podemos apreciar en las siguientes imágenes.

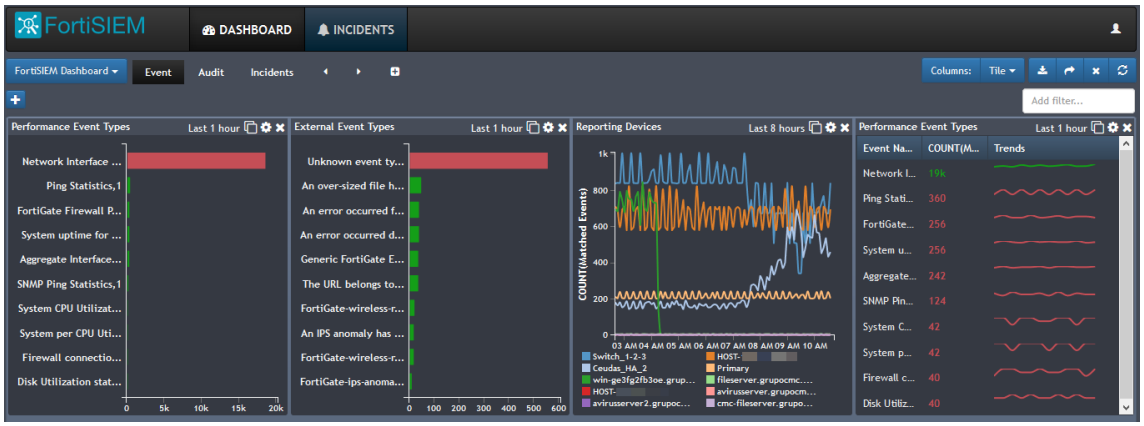


Gráfica 21: Incidencia en la nueva interfaz



Gráfica 22: Incidencias en tiempo real

En esta nueva interfaz también podemos monitorizar los eventos en tiempo real.



Gráfica 23: Eventos en tiempo real

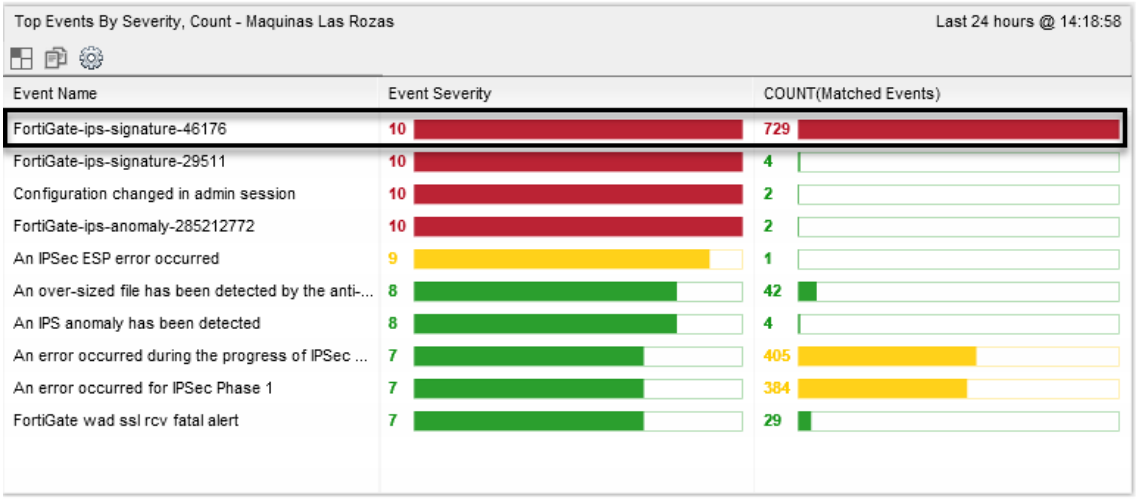
Aunque con esta interfaz podamos ver los eventos que suceden en nuestras máquinas en tiempo real, no es la herramienta más óptima para hacerlo, puesto que no tenemos tantas funciones como la analizada anteriormente. Por eso, esta interfaz se recomienda solo para ver y analizar los incidentes.

Capítulo 4. Resultados

4.1 Ataque exploit IPS

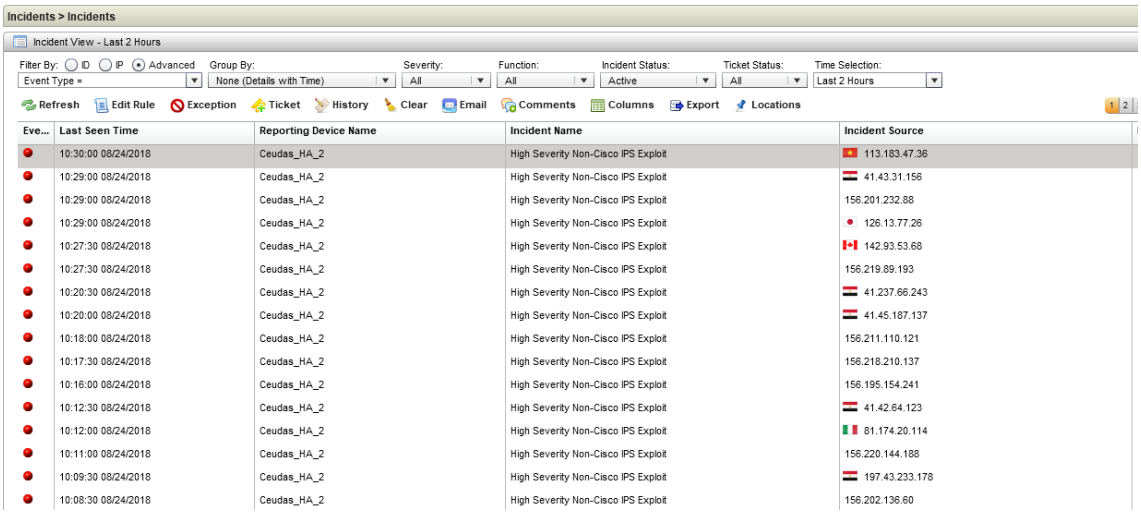
En el siguiente apartado pasaremos a analizar un ataque en tiempo real sobre la infraestructura de la empresa. Se trata de un ataque IPS, el cual intenta traspasar las medidas de seguridad cibernéticas que tiene la empresa para conseguir un comportamiento erróneo del sistema. Intentando así, obtener acceso de forma no autorizada al sistema, tomar el control o realizar una denegación del servicio.

La primera acción que se llevó a cabo fue la detección, gracias a la constante monitorización de las máquinas mediante el software FortiSIEM, nos dimos cuenta de que un evento extraño se estaba desarrollando. Como se observa en la siguiente imagen, en el dashboard aparecen muchos eventos con un nivel de criticidad alto.



Gráfica 24: Número de eventos

Por lo que acto seguido, el segundo paso a tomar es el de identificar que máquina está siendo la víctima del ataque. En la pestaña de incidents, podemos apreciar que el ataque está siendo bloqueado por el firewall de las Rozas (Ceudas_HA_2).



Incidents > Incidents

Incident View - Last 2 Hours

Filter By: ID IP Advanced Group By: Severity: Function: Incident Status: Ticket Status: Time Selection:

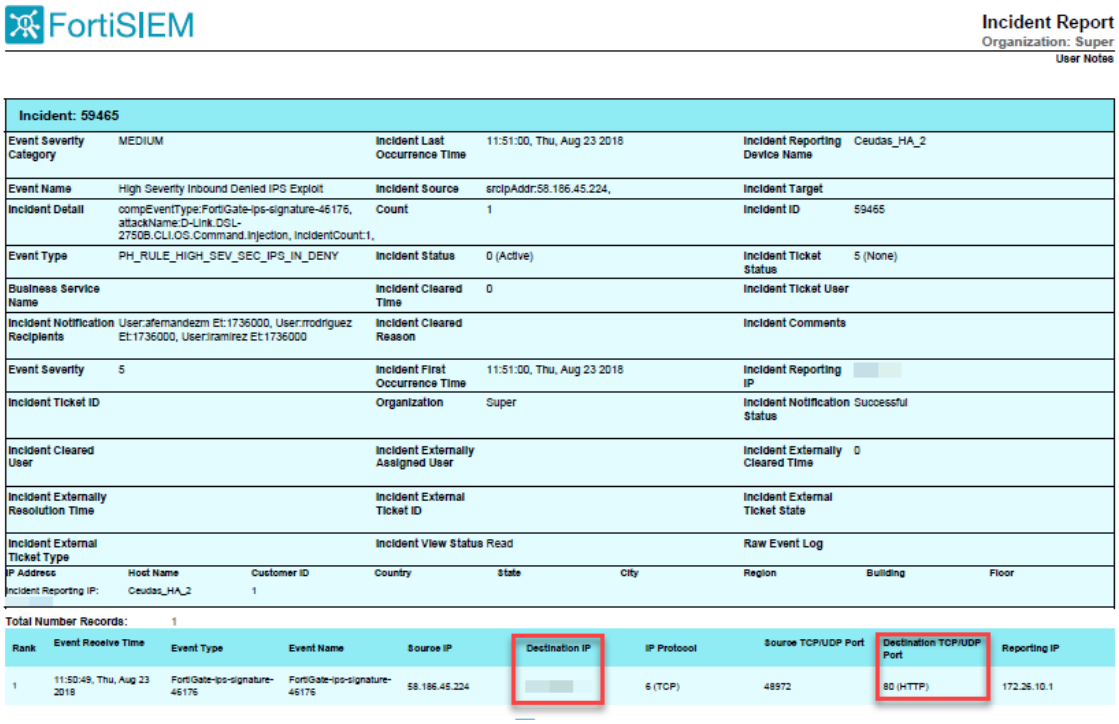
Event Type = None (Details with Time) All All Active All Last 2 Hours

Refresh Edit Rule Exception Ticket History Clear Email Comments Columns Export Locations

Eve...	Last Seen Time	Reporting Device Name	Incident Name	Incident Source
	10:30:00 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	113.183.47.36
	10:29:00 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	41.43.31.156
	10:29:00 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	156.201.232.88
	10:29:00 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	126.13.77.26
	10:27:30 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	142.93.53.68
	10:27:30 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	156.219.89.193
	10:20:30 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	41.237.66.243
	10:20:00 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	41.45.187.137
	10:18:00 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	156.211.110.121
	10:17:30 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	156.218.210.137
	10:16:00 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	156.195.154.241
	10:12:30 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	41.42.64.123
	10:12:00 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	81.174.20.114
	10:11:00 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	156.220.144.188
	10:09:30 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	197.43.233.178
	10:08:30 08/24/2018	Ceudas_HA_2	High Severity Non-Cisco IPS Exploit	156.202.136.60

Gráfica 25: Incidentes en las 2 últimas horas

Pero, si entramos más en detalle y solicitamos un informe de la incidencia obtenemos el siguiente log del incidente:



FortiSIEM

Incident Report
Organization: Super
User Notes

Incident: 59465

Event Severity Category	MEDIUM	Incident Last Occurrence Time	11:51:00, Thu, Aug 23 2018	Incident Reporting Device Name	Ceudas_HA_2
Event Name	High Severity Inbound Denied IPS Exploit	Incident Source	srcIpAddr:58.186.45.224,	Incident Target	
Incident Detail	compEventType:FortiGate-ips-signature-46176, attackName:D-Link.DSL-2750B.CLI.OS.Command.Injection, incidentCount:1,	Count	1	Incident ID	59465
Event Type	PH_RULE_HIGH_SEV_SEC_IPS_IN_DENY	Incident Status	0 (Active)	Incident Ticket Status	5 (None)
Business Service Name		Incident Cleared Time	0	Incident Ticket User	
Incident Notification Recipients	User:afernandezm Et:1736000, User:rodriguez Et:1736000, User:lramirez Et:1736000	Incident Cleared Reason		Incident Comments	
Event Severity	5	Incident First Occurrence Time	11:51:00, Thu, Aug 23 2018	Incident Reporting IP	
Incident Ticket ID		Organization	Super	Incident Notification Status	Successful
Incident Cleared User		Incident Externally Assigned User		Incident Externally Cleared Time	0
Incident Externally Resolution Time		Incident External Ticket ID		Incident External Ticket State	
Incident External Ticket Type		Incident View Status	Read	Raw Event Log	

IP Address	Host Name	Customer ID	Country	State	City	Region	Building	Floor
Incident Reporting IP:	Ceudas_HA_2	1						

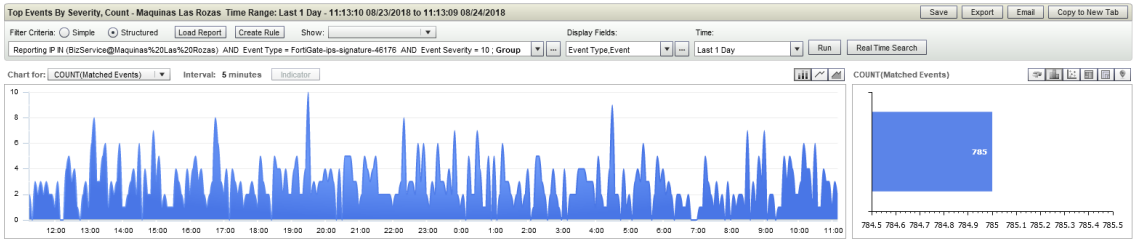
Total Number Records: 1

Rank	Event Receive Time	Event Type	Event Name	Source IP	Destination IP	IP Protocol	Source TCP/UDP Port	Destination TCP/UDP Port	Reporting IP
1	11:50:49, Thu, Aug 23 2018	FortiGate-ips-signature-46176	FortiGate-ips-signature-46176	58.186.45.224		6 (TCP)	48972	80 (HTTP)	172.26.10.1

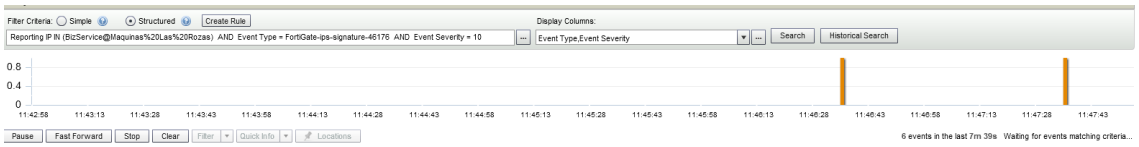
Gráfica 26: Log del incidente

Con esta información sabemos que la IP que intentan atacar, pero sin éxito es la xxx.xx.xx.xx por el puerto 80, pero que el firewall lo está evitando.

Si seguimos investigando dicho evento, podemos ver el número de veces que han intentado atacar la máquina durante el último día y los ataques que estamos recibiendo en tiempo real hacia esa misma IP.

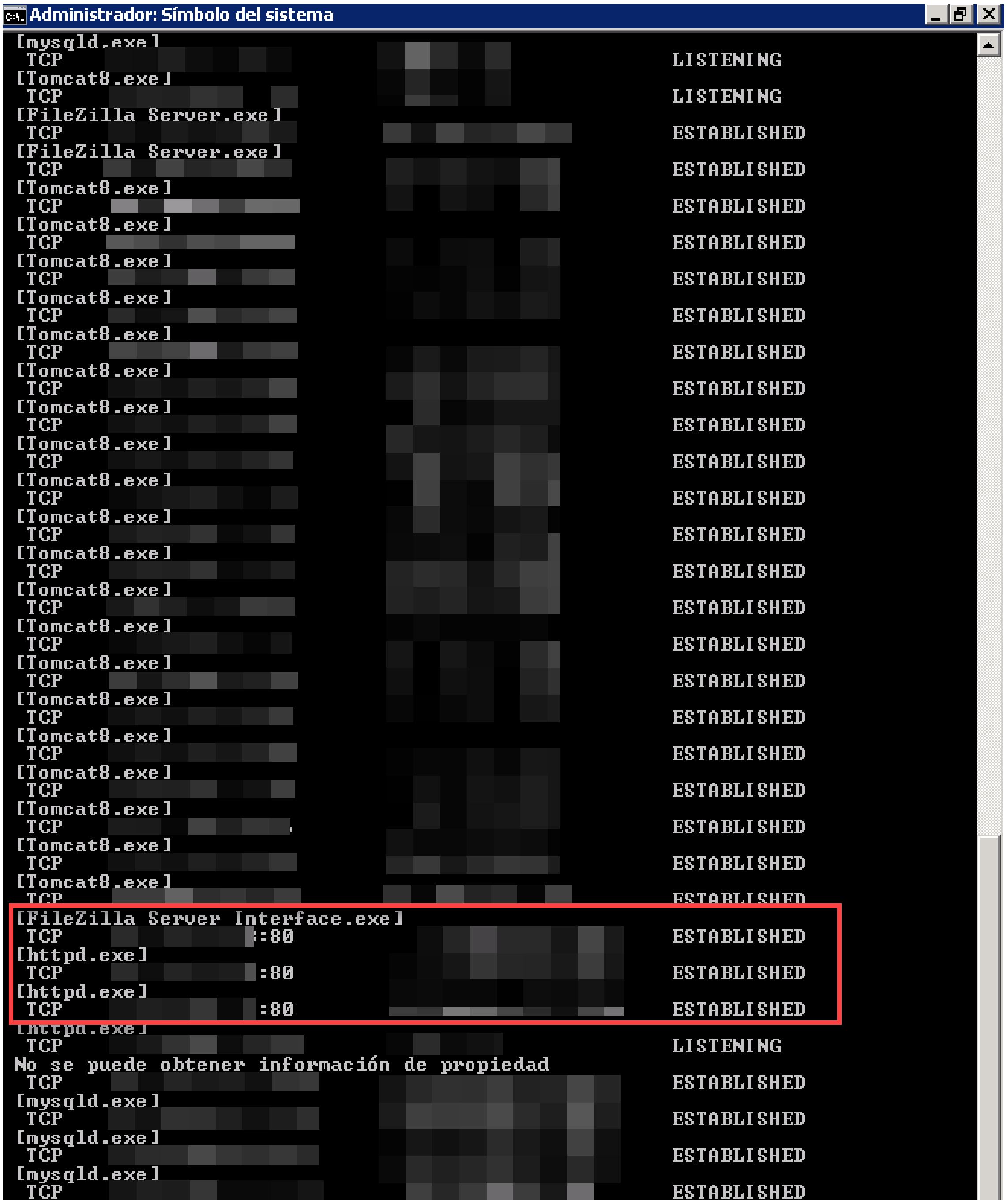


Gráfica 27: Histórico de eventos



Gráfica 28: Eventos en tiempo real

Una vez identificada la máquina, el siguiente paso a dar es ver que conexiones tiene dicha máquina por el puerto 80.

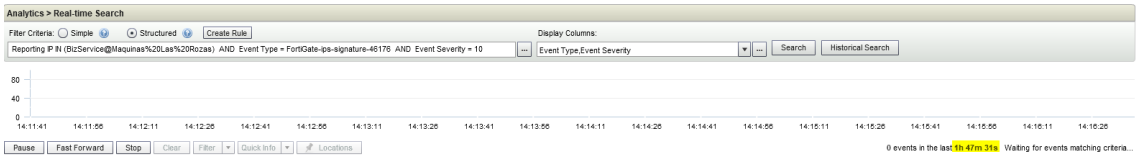


Gráfica 29: Conexiones

Las conexiones que podemos apreciar por el puerto 80 son el programa de transferencia de archivos (FileZilla) y una conexión de MySQL. Por lo que, como medida de contingencia se decide bloquear todas las conexiones por el puerto 80 hacia esa máquina. Es una solución parcial y rápida que se toma en tiempo real para prevenir males mayores y evitar que el ataque finalice con éxito. Más adelante se reunirán los expertos en ciberseguridad y tomarán una decisión de como impedir la intrusión. Pero por el momento, como medida temporal servirá.

Por último, pero no menos importante, se debe mantener un estado de alerta y monitorización sobre la máquina afectada para confirmar que el ataque haya finalizado.

Como se puede apreciar en la siguiente imagen, gracias a la monitorización en tiempo real podemos ver que, al cabo de 1 hora y 47 minutos, no se han vuelto a recibir eventos IPS.



Gráfica 30: Incidentes en tiempo real

Por lo que podemos concluir la incidencia dándola como solventada.

Capítulo 5. Conclusiones y líneas futuras

Las capacidades de Next Gen SIEM de FortiSIEM junto con la inteligencia de amenazas globales de FortiGuard Labs y los feeds de amenazas de terceros permitirán a las empresas beneficiarse de respuestas priorizadas y coordinadas e inteligencia de amenazas procesables a través de la red distribuida en una suscripción base.

FortSIEM detecta patrones de TI complejos en eventos y datos de gran volumen para dar sentido automáticamente a la complejidad, en tiempo real. El sistema se vuelve más inteligente a medida que se aprenden nuevos patrones, lo que le permite manejar automáticamente nuevos escenarios.

La seguridad ya no se trata solo de proteger la información, es fundamental para mantener la confianza con los clientes y proteger la marca y la reputación de la organización. Los incumplimientos hacen que los clientes migren sus negocios a otra parte, lo que resulta un impacto material y sustancialmente negativo para los resultados de una organización. Atraer a nuevos clientes se estima en siete veces más costoso que mantener a los clientes existentes. Todo esto se suma para explicar por qué más juntas se están involucrando en las decisiones de seguridad y por qué FortiSIEM debería ser una parte fundamental del ecosistema de seguridad de cualquier organización.

Bibliografía

[1] Página web del fabricante oficial del software. https://www.fortinet.com/products/siem/fortisiem.html [Online "Comprobada 7 de septiembre de 2018"].

[2] Documentación de la librería de Fortinet. https://docs.fortinet.com/fortisiem/admin-guides [Online "Comprobada 7 de septiembre de 2018"].

[3] Comparación entre productos. https://www.itcentralstation.com/products/comparisons/fortinet-fortisiem-accelops_vs_ibm-qradar [Online "Comprobada 7 de septiembre de 2018"].

[4] Guía de configuración del collector. https://docs.fortinet.com/d/fortisiem-500f-hardware-configuration-guide [Online "Comprobada 7 de septiembre de 2018"].

Anexo A

Valoración económica

SIEM tradicional: Estos productos se diseñaron para grandes centros de operaciones de seguridad. No obstante, las necesidades de cumplimiento crecieron, por lo que estos SIEM se vendieron a organizaciones que no tenían personal ni recursos para administrarlos. Estas licencias tienen unos costos muy altos desde unos 50.000 $.

SIEM evolucionado: Entraron en el mercado de SIEM muchas empresas de administración de registros y poco a poco incluyeron una funcionalidad similar al SIEM. El modelo de fijación de precios por lo general comienza en unos 20.000$ para la inclusión de las funcionalidades del SIEM. Incrementaron el costo con las funciones de los complementos.

FortiSIEM: Es el producto contratado por la empresa GrupoCMC, el valor de la licencia obtenida ronda los 18.000€/año sin descuentos aplicados. Una vez aplicados dichos descuentos el valor se reduce a unos 4.700€ anuales. Cabe destacar, que el precio de la licencia anual esta relacionada directamente con el número de máquinas que se quiera auditar y el total de eventos por segundo (EPS) unos 500. Cuantas más máquinas queramos analizar y más EPS, mayor será el precio que debemos pagar por dicha licencia. Con este precio no solo se contrata una licencia de SIEM sino que también se adquiere una base de conocimiento para detectar eventos de seguridad.