Ventajas e Implementación de un sistema SIEM

Àngel Rigau Pedraza

Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones.

M1.749 - TFM - Seguridad empresarial

Jorge Chinea López
Victor Garcia Font

4 de Junio de 2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Ventajas e Implementación de un sistema SIEM*
Nombre del autor:	*Àngel Rigau Pedraza*
Nombre del consultor/a:	*Jorge Chinea López*
Nombre del PRA:	*Victor Garcia Font*
Fecha de entrega (mm/aaaa):	06/2019
Titulación::	*Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones.*
Área del Trabajo Final:	*M1.749 - TFM - Seguridad empresarial*
Idioma del trabajo:	*Español*
Palabras clave	*Máximo 3 palabras clave, validadas por el director del trabajo (dadas por los estudiantes o en base a listados, tesauros, etc.)*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

En las empresas cada vez hay más sistemas y más complejos, que interactuan entre ellos y en sistemas de terceros, como servicios en la nube, proveedores o clientes. Todos esos sistemas generan logs, que generalmente o no se analizan, o se hace solo una vez a ocurrido algún problema. En ese contexto es donde tiene sentido la utilización de un SIEM (Security Information and Event Management) en las corporaciones, para agrupar los logs y generar alertas de seguridad en tiempo real.

En el proyecto se analiza los diferentes productos que hay en el mercado. Para ello se ha puesto en contactos con diferentes fabricantes de productos para hacer una demostración del producto y tener un presupuesto. Una vez echo eso, se implementa una solución en el entorno real de la compañía, cumpliendo las restricciones marcadas por esta.

La solución elegida finalmente es Wazuh, que se adaptará a un subconjunto de sistemas de la empresa (Electrónica de red, controladores del dominio windows y servidor SFTP) para realizar una prueba de concepto, para poder ser evaluada por la dirección de IT, si finalmente se implementa o no.

Abstract (in English, 250 words or less):

In companies there are more and more complex systems that interact between them and in third party systems, such as cloud services, suppliers or customers. All of these systems generate logs, which are generally either not analysed, or only done once a problem has occurred. In this context is where it makes sense to use a SIEM (Security Information and Event Management) in corporations, to group the logs and generate security alerts in real time.

The project analyzes the different products on the market. In order to do this, it has contacted different product manufacturers in order to demonstrate the product and have a budget. Once that is done, a solution is implemented in the real environment of the company, complying with the restrictions set by the company.

The solution finally chosen is Wazuh, which will be adapted to a subset of the company's systems (network devices, Windows domain controllers and SFTP server) to perform a proof of concept, to be evaluated by the IT management, whether it is finally implemented or not.

Índice

Lista de Figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

Actualmente, las empresas están cada vez mas expuestas a ataques. Estos se han convertido en un negocio que mueve cada vez más dinero y es mas profesionalizado. En las empresas cada vez hay más sistemas y más complejos, que interactuan entre ellos y en sistemas de terceros, como servicios en la nube, proveedores o clientes.

Todo eso hace que cada vez haya mas ataques y esos sean mas difíciles de detectar, por lo que se hace necesario recopilar toda la información de los diferentes sistemas de la empresa, para poder detectar los diferentes ataques y analizar los problemas de forma transversal. En ese contexto es donde tiene sentido la utilización de un SIEM (Security Information and Event Management) en las corporaciones.

Así pues, se propone evaluar las ventajas e implementación de un sistema SIEM para la detección de amenazas en una empresa real, que ahora no tenga ningún sistema centralizado de recolección de logs y eventos.
Por lo que cuando se detecta algún problema se tiene que ir revisando los logs de los diferentes sistemas, lo que conlleva mucho tiempo y en caso de tener un problema de seguridad, eso podría ser crítico.
Así con la implementación del SIEM se pretende tener una visión global de los logs de los diferentes sistemas de la empresa y poder correlacionarlos de forma ágil.

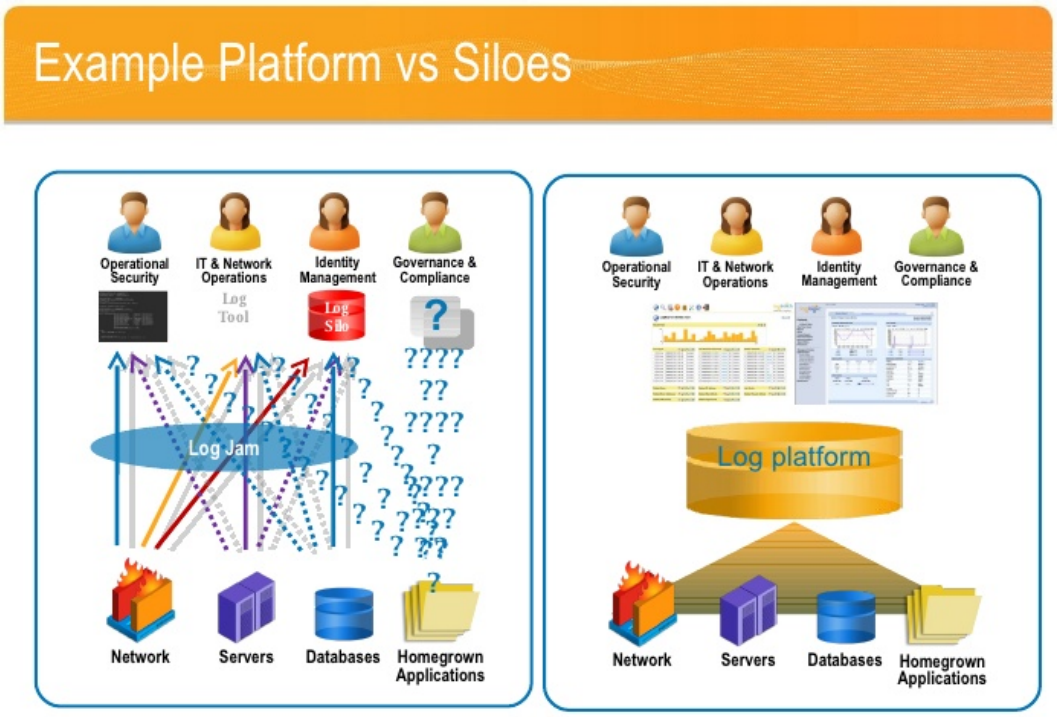


Figura 1: Gestión de logs vs Silos de logs

1.2 Objetivos del Trabajo

Los objetivos generales que se han marcado para el trabajo son los siguientes:

- Comprender como funcionan y que tipos de SIEM hay para poder valorar que se adapta mejor en cada situación
- Analizar los diferentes sistemas para valora que información aporta valor y cuál no.
- Tener capacidad para seleccionar entre diferentes productos, para adaptarlos en una situación concreta
- Ser capaz de diseñar e implementar un SIEM en un entorno real
- Mejorar las capacidades de gestión de proyectos

1.3 Enfoque y método seguido

El proyecto se basa en la evaluación de diferentes productos comerciales para implementar el SIEM. Una vez elegido el producto, se va a implementar una prueba piloto en un entorno real per valorar el desempeño de este y ver si es útil para la empresa.

Para hacer se va a seguir la metodología siguiente:

- Identificar las ventajas y justificación de la implementación de un SIEM en la empresa
    - Teoría de la gestión de Logs y SIEMs
    - Ventajas en la empresa
- Diseño del SIEM
    - Definición del entorno
    - Identificación de los logs necesarios
- Estudio de las diferentes alternativas para implementar un SIEM que se ajuste a los requerimientos de la empresa.
- Selección y justificación de la solución que se ajuste mas.
- Implementación de una prueba piloto en maquinas virtuales para probar y valorar la solución elegida.
- Conclusiones y trabajo futuro

1.4 Planificación del Trabajo

La planificación del trabajo se ha echo teniendo en cuenta las horas del TFM (300) para distribuir los trabajos.

El coste en horas de cada una de las tareas es el siguiente

Planificación

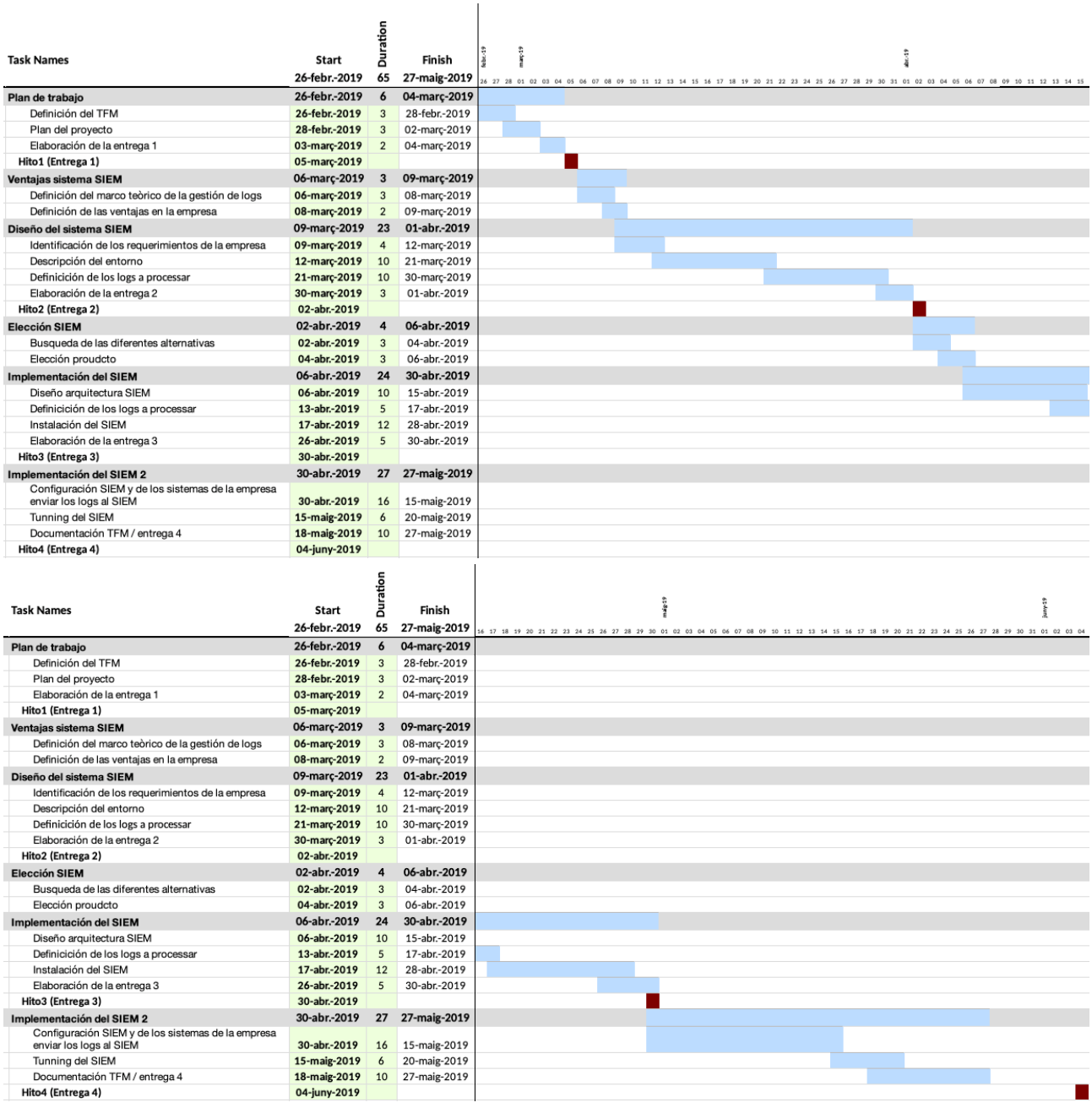
Hitos	Tareas	Tiempo (Horas)
	Plan de trabajo	**20**
	Definición del TFM	10
	Plan del proyecto	6
	Elaboración de la entrega 1	4
Hito 1 - 05/03/2019		
	Ventajas sistema SIEM	**15**
	Definición del marco teòrico de la gestión de logs	8
	Definición de las ventajas en la empresa	7
	Diseño del sistema SIEM	**80**
	Identificación de los requerimientos de la empresa	10
	Descripción del entorno	30
	Definición de los logs a procesar	30
	Elaboración de la entrega 2	10
Hito 2 - 02/04/2019		
	Elección SIEM	**15**
	Busqueda de las diferentes alternativas	10
	Elección proudcto	5
	Implementación del SIEM	**80**
	Diseño arquitectura SIEM	25
	Creación infrastructura virtual	10
	Instalación del SIEM	35
	Elaboración de la entrega 3	10
Hito 3 - 30/04/2019		
	Implementación del SIEM 2	**90**
	Configuración SIEM y de los sistemas de la empresa enviar los logs al SIEM	50
	Tunning del SIEM	10

Hitos	Tareas	Tiempo (Horas)
	Documentación TFM / entrega 4	30
Hito 4 - 04/06/2019		

Figura 2: Tabla de planificación

I pasando las tareas a días, nos resulta el siguiente plan de trabajo:

En nuestro caso no se ha tenido en cuenta festivos y vacaciones, ya que se cuentan con ellos para la elaboración del TFM.



Task Names	Start	Duration	Finish
	26-febr.-2019	65	27-maig-2019
Plan de trabajo	**26-febr.-2019**	**6**	**04-març-2019**
Definición del TFM	**26-febr.-2019**	3	28-febr.-2019
Plan del proyecto	**28-febr.-2019**	3	02-març-2019
Elaboración de la entrega 1	**03-març-2019**	2	04-març-2019
Hito1 (Entrega 1)	**05-març-2019**		
Ventajas sistema SIEM	**06-març-2019**	**3**	**09-març-2019**
Definición del marco teòrico de la gestión de logs	**06-març-2019**	3	08-març-2019
Definición de las ventajas en la empresa	**08-març-2019**	2	09-març-2019
Diseño del sistema SIEM	**09-març-2019**	**23**	**01-abr.-2019**
Identificación de los requerimientos de la empresa	**09-març-2019**	4	12-març-2019
Descripción del entorno	**12-març-2019**	10	21-març-2019
Definicición de los logs a processar	**21-març-2019**	10	30-març-2019
Elaboración de la entrega 2	**30-març-2019**	3	01-abr.-2019
Hito2 (Entrega 2)	**02-abr.-2019**		
Elección SIEM	**02-abr.-2019**	**4**	**06-abr.-2019**
Busqueda de las diferentes alternativas	**02-abr.-2019**	3	04-abr.-2019
Elección proudcto	**04-abr.-2019**	3	06-abr.-2019
Implementación del SIEM	**06-abr.-2019**	**24**	**30-abr.-2019**
Diseño arquitectura SIEM	**06-abr.-2019**	10	15-abr.-2019
Definicición de los logs a processar	**13-abr.-2019**	5	17-abr.-2019
Instalación del SIEM	**17-abr.-2019**	12	28-abr.-2019
Elaboración de la entrega 3	**26-abr.-2019**	5	30-abr.-2019
Hito3 (Entrega 3)	**30-abr.-2019**		
Implementación del SIEM 2	**30-abr.-2019**	**27**	**27-maig-2019**
Configuración SIEM y de los sistemas de la empresa enviar los logs al SIEM	**30-abr.-2019**	16	15-maig-2019
Tunning del SIEM	**15-maig-2019**	6	20-maig-2019
Documentación TFM / entrega 4	**18-maig-2019**	10	27-maig-2019
Hito4 (Entrega 4)	**04-juny-2019**		

Figura 3: Diagrama de Gantt de la planificación

2. Marco Teórico

2.1 Que es un log?

Un mensaje de log es un mensaje que genera un sistema, dispositivo, software, etc,.. en respuesta a un estimulo o evento. El estimulo o evento depende del sistema (firewall, router, sistema operativo,…) Estos se puede clasificar de la siguiente forma:

- Infomation: Mensaje de que algo benigno a ocurrido.
- Debug: Información extra del sistema, para ayudar en la detección de bugs.
- Warning: Información de que algo falta o se necessita en el sistema, pero no impacta en la operación normal.
- Error: Mensaje de que a ocurrido un error en el sistema.
- Alert: Significa que algo de interés a ocurrido.

2.2 Tipos de logs

2.2.1 Fuentes

- Endpoint: Es un dispositivo final con red, como un PC o móvil. Los Endpoint pueden generar diferentes logs de diferentes niveles: Hardware, Sistema Operativo, Middleware, base de datos y aplicaciones.
- Dispositivos de red: Proporcionan información crítica de los flujos de información de la red (destinos, origines, volúmenes, protocoles,…). Normalmente utilizan el formato syslog.
- Aplicaciones: Muchas aplicaciones generan logs. En windows muchas las podemos encontrar en los eventos de windows. En el caso de linux, los solemos encotrar en / var/log. Algunas aplicaciones empresariales (Mail, bases de datos,…), tienen sus propios repositorios de logs.
- Proxy: Los proxys tienen las peticiones de usuarios a aplicaciones de internet, com servicios en la nube o actualizaciones de software, por lo que es una fuente de información muy importante.

2.2.2 Ejemplos de formatos de logs

Evento de windows:

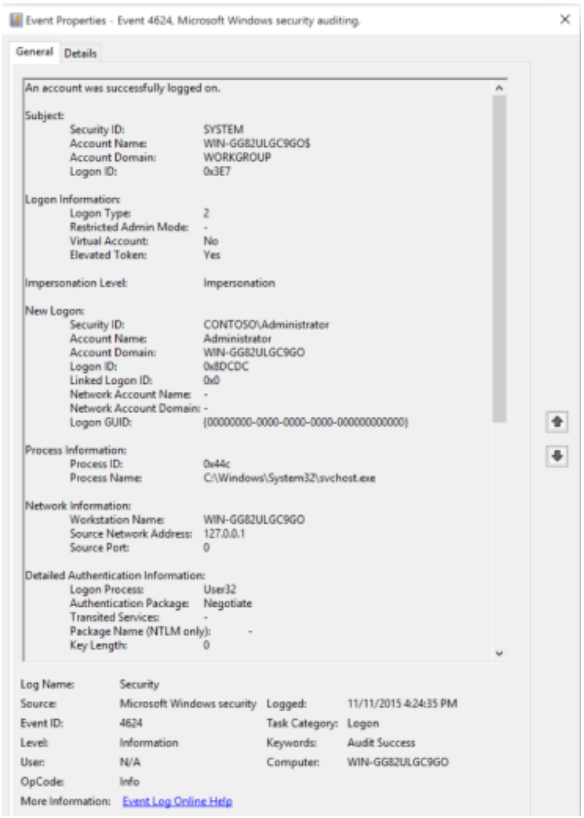


Figura 4: Ejemplo de evento de windows

XML:

Las nuevas versiones de windows, se puede consultar los eventos en formato xml, el qual se puede automatizar mejor.

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Guid="{9e814aad-3204-11d2-9a82-006008a86939}" />
<EventID>0</EventID>
<Version>3</Version>
<Level>0</Level>
<Task>0</Task>
<Opcode>1</Opcode>
<Keywords>0x0</Keywords>
<TimeCreated SystemTime="2009-07-14T16:27:43.441456400Z" />
<Correlation ActivityID="
{00000000-0000-0000-0000-000000000000}" />
<Execution ProcessID="2584" ThreadID="4324"
ProcessorID="1" KernelTime="90" UserTime="15" />
<Channel />
<Computer />
</System>
```

```
<EventData>
<Data Name="UniqueProcessKey">0xFFFFFA8005BBC950</Data>
<Data Name="ProcessId">0x1430</Data>
<Data Name="ParentId">0xA18</Data>
<Data Name="SessionId"> 1</Data>
<Data Name="ExitStatus">259</Data>
<Data Name="DirectoryTableBase">0x4E1D6000</Data>
<Data Name="UserSID">guest</Data>
<Data Name="ImageFileName">notepad.exe</Data>
<Data Name="CommandLine">notepad</Data>
</EventData>
<RenderingInfo Culture="en-US">
<Opcode>Start</Opcode>
<Provider>MSNT_SystemTrace</Provider>
<EventName xmlns=
"http://schemas.microsoft.com/win/2004/08/events/trace">
Process</EventName>
</RenderingInfo>
<ExtendedTracingInfo xmlns=
"http://schemas.microsoft.com/win/2004/08/events/trace">
<EventGuid>{3d6fa8d0-fe05-11d0-9dda-00c04fd7ba7c}</EventGuid>
</ExtendedTracingInfo>
</Event>
```

CSV (Comma-separated values):
Envío de información de log en formato de fichero de texto con valores separados en comas.

JSON:

Para intercambiar información de logs, muchos ssistemas utilizan JSON, como por ejemplo:

```
{% highlight javascript %} { “timestamp”: 1324830675.076, “status”:
“404”, “shortmessage”: “File does not exist: /var/www/no-such-file”,
“host”: “ord1.product.api0”, “facility”: “httpd”, “errno”: “ENOENT”,
“remotehost”: “50.57.61.4”, “remoteport”: “40100”, “path”: “/var/www/no-
such-file”, “uri”: “/no-such-file”, “level”: 4, “headers”: { “user-
agent”: “BadAgent/1.0”, “connection”: “close”, “accept”: ”/” }, “method”:
“GET”, “uniqueid”: “.rh-g2Tm.h-ord1.product.api0.r-
axAIO3bO.c-9210.ts-1324830675.v-24e946e” } {% endhighlight %}
```

CEF (Common Event Format):

Para una fácil integración se utiliza el formato de transporte de syslog (RFC 5424)

Formato CEF Base:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

Exemplo CEF Log:

```
Jan 18 11:07:53 dsmhost CEF:0|Trend Micro|Deep Security Manager|<DSM version>|600|Administrator
Signed In|4|suser=Master…
```

2.3 Ecosistema de Logs

El ecosistema es el conjunto de fuentes (dispositivos, hardware, …) que pueden generar logs. Para poder gestionarlos se tiene que habilitar el log, que nivel de información y enviarlo a un recolector de logs. La arquitectura mas simple seria:

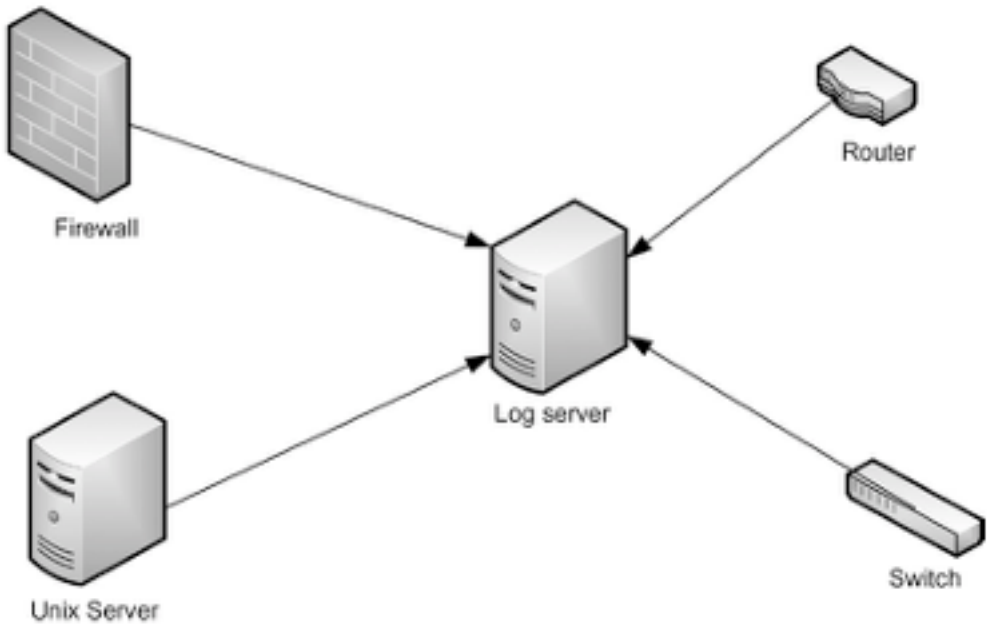


Figura 5: Ejemplo arquitectura sencilla de gestión de logs

Luego depende de las necesidades el servidor de logs, puede guardar-se en diferentes servidores (Separando el recolector del almacenamiento), usando incluso en la nube.

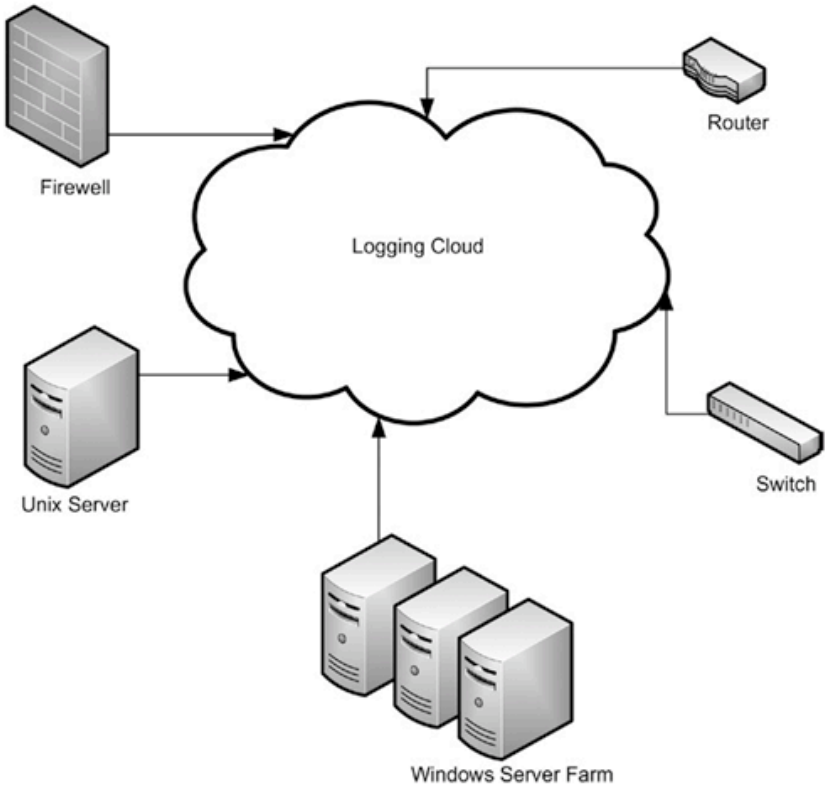


Figura 6: Ejemplo arquitectura de gestión de logs en la nube

Para poder centralizarlo es necesario que el log contenga la siguiente información básica:

- Timestamp: Fecha y tiempo en que se ha generado el log. Es importante remarcar que todos los sistemas deben tener la hora sincronizada para poder hacer el seguimiento.
- Source: Fuente o origen del log.
- Mensaje: Mensaje concreto del log.

2.4 Filtro, normalización y correlación

Si la fuente de Logs no lo permite, es necesario filtrar los Logs que se reciben de las fuentes para tener solamente la información que nos interesa, ya que se pueden generar muchos logs, es necesario solo gestionar los importantes.
El segundo paso es normalizarlo. Normalizar es coger el formato original del log, el cual puede ser muy diferente de una fuente a otra, convertirlo al mismo formato y extraer el máximo de información possible (Por ejemplo, IPs, transformar un codigo de error a la descripción, …)

Uno de la información que se debe sacar es la prioridad. Esta puede ser:

- Low: Informativo, por lo que no hace falte actuar en el mismo momento.
- Medium: Eventos que se tienen que revisar al cabo de poco tiempo, pero no de forma inminente.
- High: Eventos que requieren un intervención inmediata.

Un vez, tenemos el log normalizado hay que buscar una correlación entre logs. Esto típicamente se hace en base de reglas o estadísticamente. Una vez tenemos esta información, ya podemos, analizar, crear alertas o almacenar los logs.

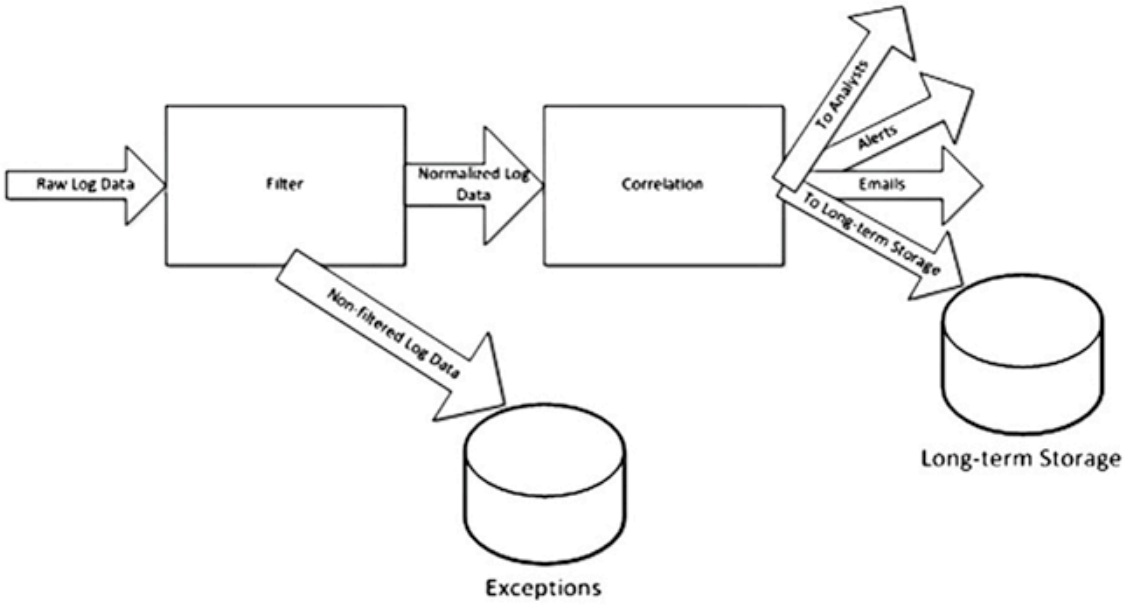


Figura 7: Proceso de filtro, normalización y correlación

2.5 SIEM (Security Information and Event Management)

El termino SIEM proviene de la mezcla de dos productos de software diferentes, Security Information Management (SIM) y Security Event Management (SEM).

Gartner define SIEM cómo la tecnología que soporta la detección y la respuesta a incidentes a través de la correlación de tiempo real y anàlisis de eventos históricos de una amplia variedad de eventos y fuentes de información.

2.5.1 Capacidades de un SIEM

- Agregación de datos: Soluciones para administración de logs desde muchas fuentes, incluyendo redes, seguridad, servidores, bases de datos, aplicaciones, proporcionando la capacidad de consolidar los datos monitoreados para ayudar a evitar la pérdida de los acontecimientos cruciales.

- Correlación: Busca los atributos comunes, y relaciona eventos en paquetes o incidentes. Esta tecnología proporciona la capacidad de realizar una variedad de técnicas de correlación para integrar diferentes fuentes, con el fin de convertir los datos en información. La correlación es típicamente una función de la parte de gestión de la seguridad en una solución SIEM completa.

- Alerta: El análisis automatizado de eventos correlacionados y la producción de alertas, para notificar a los destinatarios de los problemas inmediatamente. Una alerta puede ser un tablero de instrumentos, o enviarse a través de canales de terceros, tales como el correo electrónico.

- Dashboards: Herramientas para tomar los datos del evento y convertirlo en tablas informativas para ayudar a ver patrones o identificar una actividad que no está siguiendo un patrón estándar.

- Cumplimiento: Las aplicaciones SIEM se pueden emplear para automatizar la recopilación de datos y la elaboración de informes que se adapten a los procesos existentes de seguridad, gobernabilidad y auditoría.

- Retención: Emplea soluciones a largo plazo de almacenamiento de datos para facilitar la correlación de datos con el tiempo, y para proporcionar la retención necesaria para los requisitos de cumplimiento. Un largo plazo de retención de registros de datos es crítica en la investigación forense, ya que es poco probable que el descubrimiento de una violación de la red sea en el momento de la infracción se produzcan.

2.6 Ventajas en la empresa

La gran ventaja en las empresas es la detección temprana y respuesta rápida para mitigar amenazas. Los informes y la monitorización de Logs no son suficientes, las organizaciones necesitan tener la habilidad de detectar y responder a amenazas conocidas, desconocidas y avanzadas. Los SIEMs modernos pueden:

- Centralizar y agregar todos los eventos de seguridad relevantes y hacerlos disponibles para usarlos posteriormente
- Soporte de variedad de fuentes
- Añadir contexto a los eventos de seguridad
- Correlacionar y alertar
- Detectar amenazas avanzadas y desconocidas
- Crear perfil de comportamiento de la organización
- Poder investigar incidentes

En definitiva, para la empresa, no es solamente un servidor de logs, el cual se puede utilizar también para investigaciones forenses, sino que el SIEM puede tener otras ventajas como:

- Monitorización a tiempo real: Correlación de eventos en tiempo real para encontrr y parar las amenazas.
- Respuesta a incidentes: Ordena la diferente información para facilitar al equipo de IT, responder a un incidente y recuperase con el menor tiempo y coste.
- Monitorización de usuarios: Monitorizar los usuarios en su contexto puede ser esencial para encontrar brechas de seguridad y cumplir con algunos requerimientos.
- Inteligencia de amenazas: Ayuda a IT a reconocer comportamientos anómalos.
- Análisis avanzados: La inteligencia artificial ayuda en los análisis de toda la información.
- Detección de amenazas avanzadas: Da herramientas a los especialistas para monitorizar y analizar las amenazas y incidentes.
- Uso de librerías de casos: Para entender y responder a las amenazas en tiempo real.

3. Diseño del sistema SIEM

3.1 Identificación de los requerimientos de la empresa

La empresa en esos momento no tiene ningún servidor de logs, y a raíz de diferentes auditorias de seguridad y de la evolución de las amenazas se estima que se hace necesario un sistema centralizado de tratamiento de logs, así como añadir cierta inteligencia en el análisis de esos, para la detección de amenazas.

Para implementarlo se plantean tres diferentes etapas:

1a etapa:

En la primera etapa se requiere de recoger y analizar la información relacionada con:
- Electrónica de red (Switches, routers y Access Points)
- Autenticación de la red del protocolo 802.1x
- Firewall así como los accesos vía a VPN
- Autenticaciones a nivel de Active Directory (Controladores del dominio)

2a etapa:

Incorporación de los Logs de los sistemas:
- Logs y eventos de los servidores críticos
- Sistema de virtualizacion. Tanto software, hardware como almacenamiento
- Información de los antivirus y del sistema DLP (Data Lost Prevention)
- Logs y eventos de seguridad de las aplicaciones críticas.

3a etapa:

Recoger los Logs de el resto de sistemas:
- Servidores no críticos
- Ordenadores personales
- Aplicaciones no críticas

En el contexto de ese trabajo, se requiere hacer una prueba de concepto con un elemento de cada característica de la 1a etapa, para evaluar la solución SIEM. En caso de tener un feedback positivo, se procederá a la implementación completa de la 1a etapa, pero esto ya está fuera del ámbito de ese trabajo.

3.2 Descripción del entorno

La descripción del entorno de los sistemas afectados por la primera etapa de implementación es el siguiente:

Red:

La electrónica de red está compuesta por:
- 4 switches core (Cisco Nexus)
- 5 switches de Distribución Cisco
- 28 switches de acceso Cisco
- 14 Access points Cisco

Firewall:

- 2 Fortinet

Autentificación 802.1x:

- Toda la electrónica de red de acceso (Wired y wireless)
- Servidor RADIUS en el controlador del dominio (NPS)

Autentificación Active Directory:

- 2 Controladores del dominio Windows 2012R2
    - DHCP
    - DNS

Para la prueba de concepto se va utilizar la infraestructura de virtualización existente en la empresa. (VMWare vSphere)

3.3 Definición de los logs a procesar

Con el entorno anterior, primero estimamos la cantidad de logs que se procesarán:

Calculo EPS (Events per Second)

Tipo Dispositivo	Cantidad	EPS Unidad	EPS Total
Contraldor de Dominio Windows	2	15,075	30,15
Switches Core	4	1,1	4,4
Switches Distribución	5	1,1	5,5
Switches Acceso	28	1,1	30,8
Access Point	14	1,2	16,8
Firewall	2	289	578
TOTAL			**665,65**

Figura 8: Tabla de calculo de EPS

Ese calculo se ha realizado según los volúmenes medios de cantidad de logs según la industria.

Para evaluar la cantidad de logs, hemos de calcular el almacenamiento necesario. Esos cálculos se han realizado calculando una media por mensaje de 400 bytes y un ratio de compresión de 7:1.

Calculo Espacio

EPS	GB/Dia	GB/Mes	GB/Año
665,65	3,06	91,79	1.116,96

Figura 9: Tabla de calculo almacenamiento

4. Elección del SIEM

4.1 Búsqueda de las diferentes alternativas

4.1.1 Restricciones

Las restricciones que tiene la compañía son las siguientes:

- Tiene que ser un producto “on premise”, por política de la empresa, no se permite tener información en la nube.
- Se tiene que utilizar de forma virtual en la arquitectura existente.
- Se tiene que adecuar al presupuesto de la compañía.
- Tiene que tener gestión de logs.

4.1.2 Metodología

La metodología seguida para la búsqueda de diferentes alternativas es la siguiente:

- Búsqueda de Información

  Primero se ha buscado información de los diferentes productos, utilizando en primera estancia el cuadrante de Gartner (Anexo 1). I luego se han buscado alternativas, como las open source, que no aparecen en el informe de Gartner.

- Contacto proveedor

  Se ha contactado con los proveedores para pedir un presupuesto y a poder ser una pequeña presentación con demostración del producto.

- Valoración

  Se ha echo una valoración tanto cualitativa como económica de las diferentes soluciones.

4.1.3 Valoración cualitativa

Logpoint	
Pro	**Cons**
• Sencillo de utilizar. • UEBA incluido • Buena gestión almacenamiento • 400 Integraciones disponibles	• Sin soporte en español • Empresa pequeña

IBM QRadar	
Pro	**Cons**
• Alta integración con muchos diferentes sistemas • Capacidad de ampliación añadiendo monitoricación de red y escáner de vulnerabilidades • Actualización online de reglas para la detección de amenazas. • App Store con pluguins de diferentes fabricantes	• Pensado para grandes empresas

ManageEngine Log360	
Pro	**Cons**
• Sencillo de utilizar	• Características básicas • Pensado en integrarse con el resto de productos de ManageEngine

ArcSight	
Pro	**Cons**
• Potente modelo de reglas	• Poco intuitivo • Características básicas • Pensado para grandes empresas • SIEM que mas se reemplaza

LogRhythm	
Pro	**Cons**
• Fácil de utilizar • Todo integrado	• Pensado para grandes empresas

ELK + x-pack	
Pro	**Cons**
• Potente motor de búsqueda • Todo integrado en el mismo producto	• Pensado para ingerir grandes cantidades, por lo que está diseñado para grandes empresas.

OSSIM	
Pro	**Cons**
• Interficie agradable • Diferentes productos integrados (IDS, HDS,…)	• Sin actualizaciones de reglas • No almacena los logs para la gestión. • Adquirido por AT&T. Futuro incierto

SIEMonster	
Pro	**Cons**
• Diferentes productos integrados (IDS, HDS,…) • Precio competitivo i/o Gratuito	• Interfaces poco homogéneas • Gran cantidad de productos open source integrados, lo que se necesita conocimiento de cada uno de los subproductos. • Empresa de reciente creación • Poca documentación

ELK + Wazuh	
Pro	**Cons**
• Altamente configurable • Integrado en Kibana (ELK), interficie amigable	• Configuración no intuitiva • Sin seguridad integrada

EventTracker	
Pro	**Cons**
• Online support • Sencillo de utilizar	• Soporte solo en Inglés

AlienVault	
Pro	**Cons**
• Muy completo • Fácil de usar • IDS integrado	• Diseñado para grandes empresas • No se puede empezar solamente con una parte, ya que inspecciona la red y detecta a los dispositivos. • Adquirido por AT&T. Futuro incierto

SolarWinds Log & Event Manager	
Pro	**Cons**
• Muy completo • Fácil de usar • IDS integrado	• Pensado para trabajar con otros productos de SolarWinds

DNIF	
Pro	**Cons**
• Precio ajustado • Sencillo de utilizar	• Soporte solo des de la India (Inglés + Diferencia horaria) • Consola en la nube (provoca que el rendimiento se bajo)

Exabeam	
Pro	**Cons**
	• Pensado para grandes empresas • No me facilitaron un presupuesto ya que su producto no se ajusta a mis sistemas

Splunk	
Pro	**Cons**
	• Pensado para grandes empresas • No me facilitaron un presupuesto ya que su producto no se ajusta a mis sistemas

4.1.4 Valoración económica

Para poder comparar los diferentes productos, ya que algunos se tienen que comprar con licencia permanente y otros son de pago anual, se ha considerado un periodo de 5 años, ya que es el tiempo en que en la compañía se amortizan las inversiones en TI. También se especifica los tipos de licenciamiento.

Producto	Inversión inicial	Coste anual	Precio a los 5 años	Tipo Llicencia	Notas
Logpoint	3.000 €	13.600 €	71.000 €	100 Nodos	
Elastik Stack + x-pack	0 €	22.500 €	112.500 €	5Nodos Cluster = 25TB	
IBM QRadar	25.000 €	5.000 €	50.000 €	500 EPS	
Manage Engine Log360	0 €	4.618 €	23.090 €	50 Nodos	Con UEBA
Manage Engine Log360	8.978 €	0 €	8.978 €	50 Nodos	Sin UEBA
ArcSight	32.000 €	8.000 €	72.000 €	250 EPS	
LogRhytm	121.263 €	0 €	121.263 €	1000 EPS	
SolarWinds Log & Event Manager	0 €	6.350 €	31.750 €	50 Nodos	
OSSIM	0 €	0 €	0 €	-	Open source, sin Log management
SIEMonster SMB	0 €	6.000 €	30.000 €	200 Nodos / 13000 EPS	Open source + soporte + upgrades
SIEMonster Community	0 €	0 €	0 €	12000 Nodos / 25000 EPS	Open source
ELK + Wazuh	0 €	0 €	0 €	-	Open source
EventTracker SIEM	0 €	12.876 €	64.380 €	50 Nodes	
SureLog SIEM	0 €	42.000 €	210.000 €	5000 EPS	
AlienVault	10.500 €	3.500 €	24.500 €	75 Nodos / 1000EPS	1r any no Mant.
AlienVault	14.300 €	4.700 €	33.100 €	150 Nodos / 1000 EPS	1r any no Mant.
DNIF Comunity		900 €	4.500 €	200 GB/mes	extra GB 0.83$
DNIF Standard		3.600 €	18.000 €	200 GB/mes	Comunity + soporte (extra GB 1.66$)
DNIF Free		0 €	0 €	100 GB/mes	

Figura 10: Tabla comparativa SIEMs

4.2 Elección del producto

Después de la búsqueda de información, se puede ver que las soluciones SIEM del mercado son realmente caras, si tenemos en cuenta los requerimientos de la compañía, en especial la restricción de que no puede estar en la nube.

Así que nos decantamos por una solución open source.

Las soluciones finalistas son:

- SIEMonster
- ELK + Wazuh
- OSSIM

Finalmente nos decantamos por la solución ELK + Wazuh, ya que SIEMonster es muy complejo por la infraestructura que hay en la compañía y OSSIM no tiene gestión de los logs, que es un requerimiento de la compañía.

5. Implementación del SIEM

5.1 Diseño arquitectura

La arquitectura de Wazuh es la siguiente:

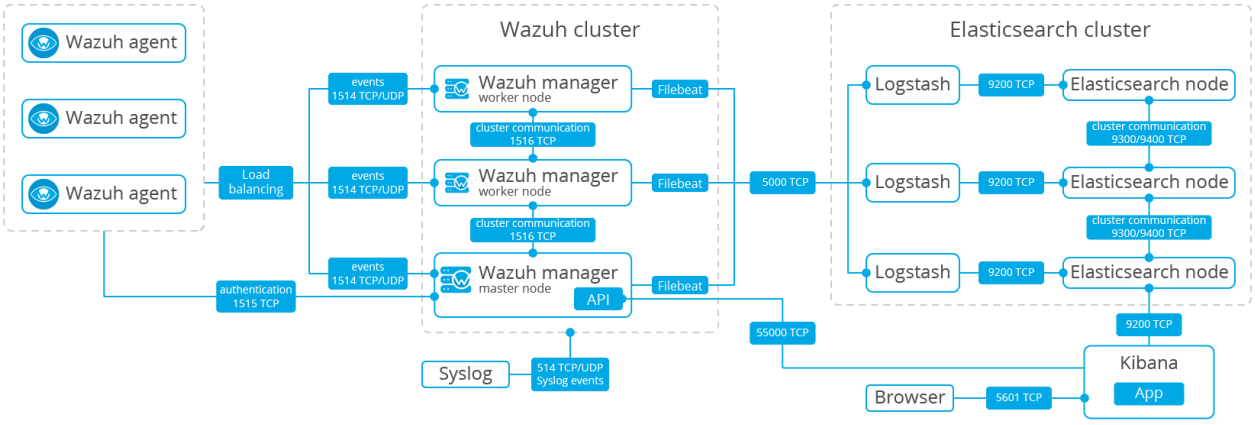


Figura 11: Arquitectura Wazuh

Debido a que se quiere implementar en una infraestructura pequeña, se decanta por la instalación en un solo host:

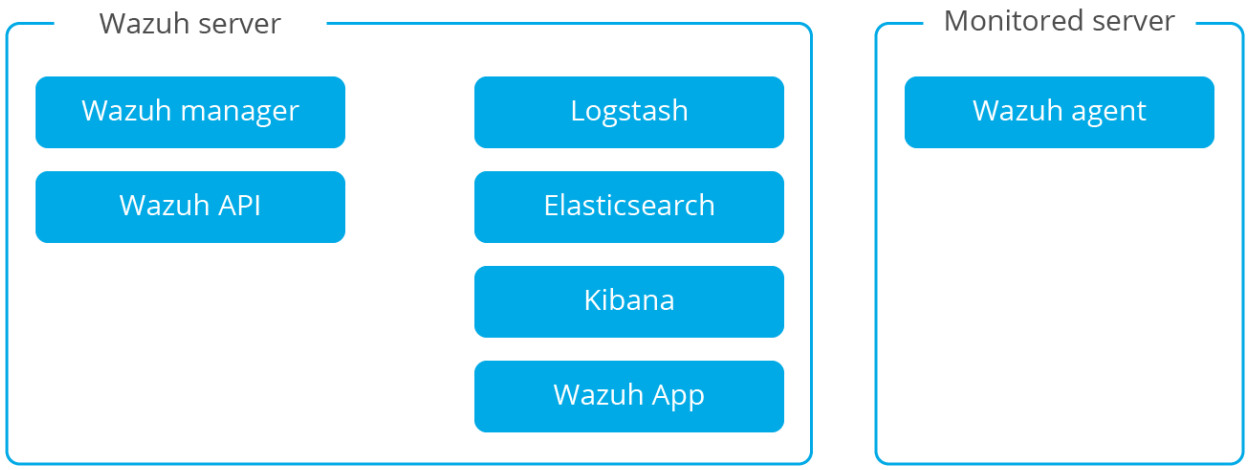


Figura 12: Arquitectura Wazuh en un solo host

5.1.1 Agentes

Para los dispositivos vamos a utilizar dos métodos de conexión:

- Syslog para los dispositivos de red
- Agente Wazuh para los servidores windows.

5.1.2 Seguridad

El servidor de ELK y el Wazuh no tienen control de la seguridad. Para darle esa capa de seguridad se utilizará Search Guard.

5.2 Creación infraestructura virtual e instalación

En el caso de single-host, Wazuh permite descargar un “appliance” con el siguiente software instalado:

- CentOS 7
- Wazuh 3.9.1
- Wazuh API 3.9.1
- Elasticsearch 7.1.0
- Filebeat 7.1.0
- Kibana 7.1.0
- Wazuh app 3.9.1-7.1.0

Se descarga el fichero OVA y se incorpora a la infraestructura virtual de la empresa:

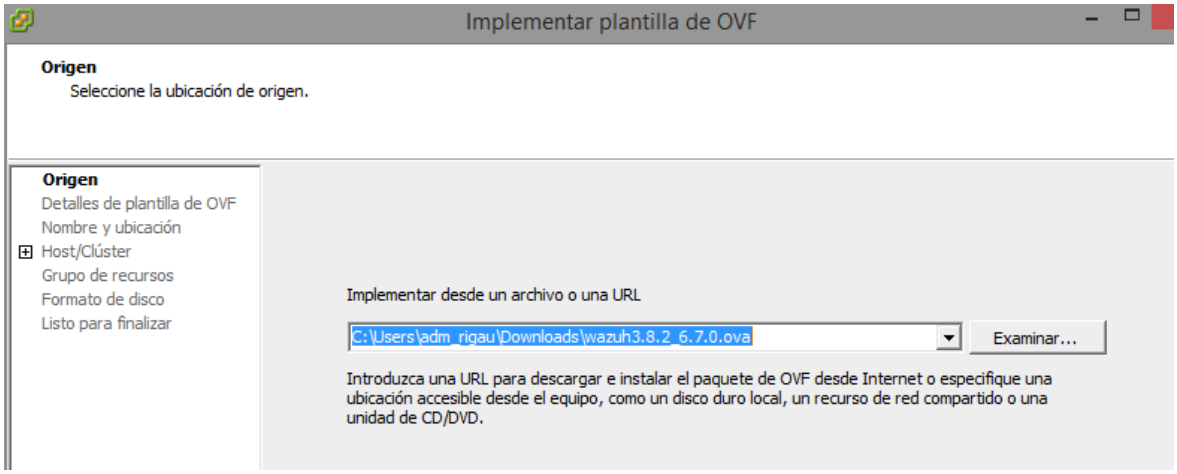


Figura 13: Implementación fichero OVA en VMWare vSphere

Una vez se ha añadido la maquina virtual a la infraestructura de la empresa, se enciende la maquina y se accede por la consola, para poder asignar una IP estática del rango de servidores.

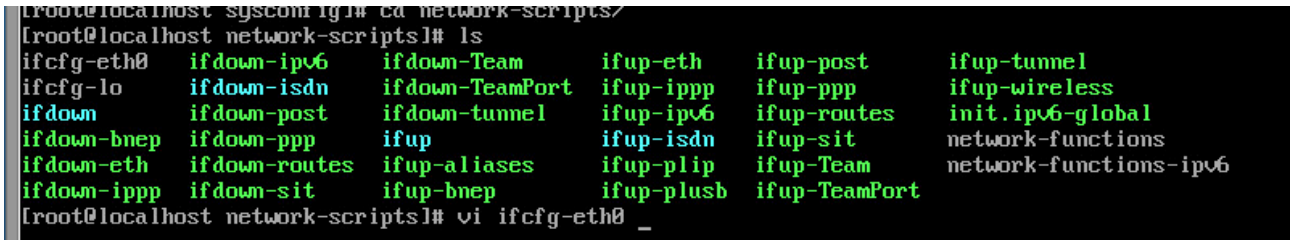


Figura 14: Ficheros modificación IP servidor wazuh

Para asegurar que se dipsone de la última actualización de todos los productos se actualiza:

```
yum update
```

Ahora ya se puede acceder a la consola web:

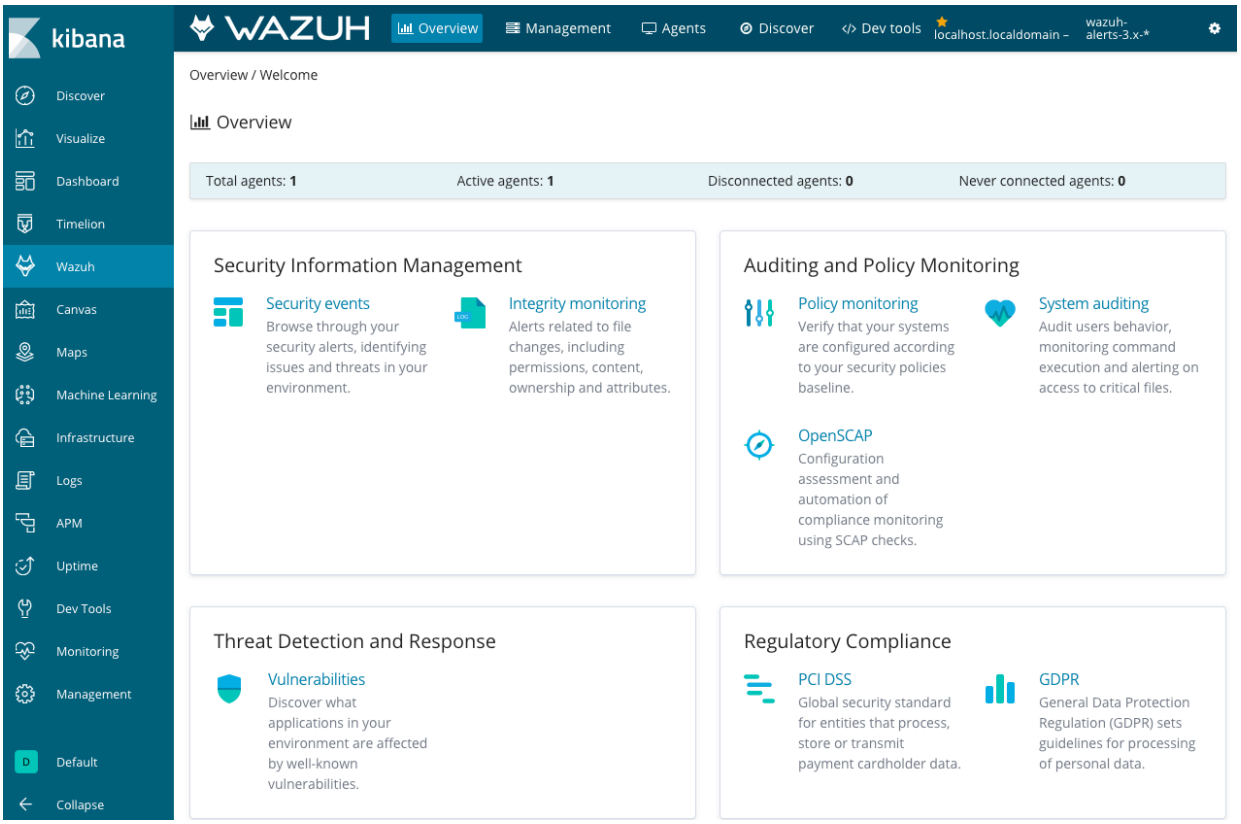


Figura 15: Consola web wazuh

5.3. Instalación Seguridad

Ahora se va a proceder a la instalación de Search Guard.

Primero, se tiene que aplicar la seguridad en el Logstash. Para hacer eso, primero se tiene que parar el servicio del Logstash

```
systemctl stop logstash
```

Despues se modifica el fichero */etc/logstash/conf.d/01-wazuh.conf* y se cambia la sección de output:

```
output {
    elasticsearch {
        hosts => ["localhost:9200"]
        index => "wazuh-alerts-3.x-%{+YYYY.MM.dd}"
        document_type => "wazuh"
     user => logstash
        password => logstash
        ssl => true
        ssl_certificate_verification => false
    }
}
```

I se vuelve a arrancar el servicio

```
systemctl restart logstash
```

Se tiene que asegurar de que no hay el x-pack habilitado en Elasticsearch, ya que eso entraría en conflicto con Search Guard. Para eso se tiene que mirar el fichero */etc/ elasticsearch/elasticsearch.yml* y se comprueba de que la opción esté deshabitada.

```
xpack.security.enabled: false
```

Ahora ya se puede instalar el plugin. Con las versiones que hay en el appliance, se instalará el plugin 6.7.1 y se hace con el siguiente comando:

```
/usr/share/elasticsearch/bin/elasticsearch-plugin install \
-b com.floragunn:search-guard-6:6.7.1-25.0
```

```
[root@wazuhmanager plugins]# /usr/share/elasticsearch/bin/elasticsearch-plugin install \
[> -b com.floragunn:search-guard-6:6.7.1-25.0
-> Downloading com.floragunn:search-guard-6:6.7.1-25.0 from maven central
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@     WARNING: plugin requires additional permissions     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
* java.io.FilePermission /proc/sys/net/core/somaxconn read
* java.lang.RuntimePermission accessClassInPackage.com.sun.jndi.ldap
* java.lang.RuntimePermission accessClassInPackage.sun.misc
* java.lang.RuntimePermission accessClassInPackage.sun.nio.ch
* java.lang.RuntimePermission accessClassInPackage.sun.security.x509
* java.lang.RuntimePermission accessDeclaredMembers
* java.lang.RuntimePermission accessUserInformation
* java.lang.RuntimePermission createClassLoader
* java.lang.RuntimePermission getClassLoader
* java.lang.RuntimePermission setContextClassLoader
* java.lang.RuntimePermission shutdownHooks
* java.lang.reflect.ReflectPermission suppressAccessChecks
* java.net.NetPermission getNetworkInformation
* java.net.NetPermission getProxySelector
* java.net.SocketPermission * connect,accept,resolve
* java.security.SecurityPermission getProperty.ssl.KeyManagerFactory.algorithm
* java.security.SecurityPermission insertProvider.BC
* java.security.SecurityPermission org.apache.xml.security.register
* java.security.SecurityPermission putProviderProperty.BC
* java.security.SecurityPermission setProperty.ocsp.enable
* java.util.PropertyPermission * read,write
* java.util.PropertyPermission org.apache.xml.security.ignoreLineBreaks write
* javax.security.auth.AuthPermission doAs
* javax.security.auth.AuthPermission modifyPrivateCredentials
* javax.security.auth.kerberos.ServicePermission * accept
See http://docs.oracle.com/javase/8/docs/technotes/guides/security/permissions.html
for descriptions of what these permissions allow and the associated risks.
-> Installed search-guard-6
[root@wazuhmanager plugins]#
```

Figura 16: Instalación Plugin Search Guard

Ahora se ejecuta el script de instalación demo.

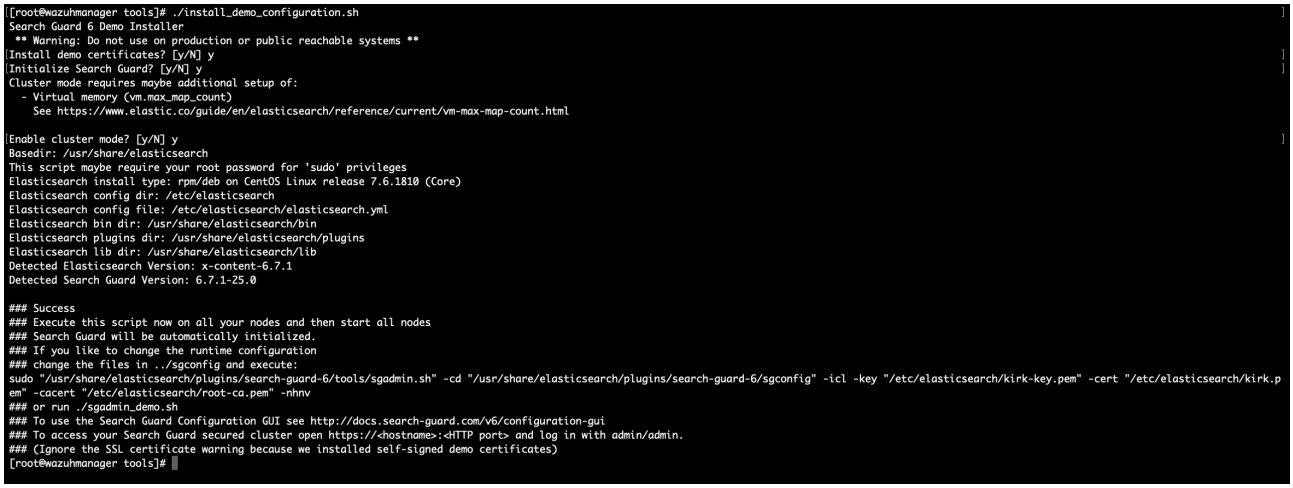


Figura 17: Script instalación demo de Search Guard

I se procede a reiniciar el servidor de Elasticsearch

Una vez instalado se tiene que añadir el indice que crea Wazuh en los roles de Logstash. Para ello, moficicamos el fichero */usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_roles.yml*

```
sg_logstash:
    cluster:
        - CLUSTER_MONITOR
        - CLUSTER_COMPOSITE_OPS
        - indices:admin/template/get
        - indices:admin/template/put
    indices:
        'logstash-*':
            '*':
                - CRUD
                - CREATE_INDEX
        '*beat*':
            '*':
                - CRUD
                - CREATE_INDEX
        'wazuh-alerts-3?x-*':
            '*':
                - CRUD
                - CREATE_INDEX
```

I se aplican los cambios

```
[root@wazuhmanager tools]# vi /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_roles.yml
[root@wazuhmanager tools]# /usr/share/elasticsearch/plugins/search-guard-6/tools/sgadmin.sh \
> -cd /usr/share/elasticsearch/plugins/search-guard-6/sgconfig -icl -key \
> /etc/elasticsearch/kirk-key.pem -cert /etc/elasticsearch/kirk.pem -cacert \
> /etc/elasticsearch/root-ca.pem -h localhost -nhnv
WARNING: JAVA_HOME not set, will use /usr/bin/java
Search Guard Admin v6
Will connect to localhost:9300 ... done
Elasticsearch Version: 6.7.1
Search Guard Version: 6.7.1-25.0
Connected as CN=kirk,OU=client,O=client,L=test,C=de
Contacting elasticsearch cluster 'elasticsearch' and wait for YELLOW clusterstate ...
Clustername: wazuh-cluster
Clusterstate: YELLOW
Number of nodes: 1
Number of data nodes: 1
searchguard index already exists, so we do not need to create one.
Populate config from /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/
Will update 'sg/config' with /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_config.yml
   SUCC: Configuration for 'config' created or updated
Will update 'sg/roles' with /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_roles.yml
   SUCC: Configuration for 'roles' created or updated
Will update 'sg/rolesmapping' with /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_roles_mapping.yml
   SUCC: Configuration for 'rolesmapping' created or updated
Will update 'sg/internalusers' with /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_internal_users.yml
   SUCC: Configuration for 'internalusers' created or updated
Will update 'sg/actiongroups' with /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_action_groups.yml
   SUCC: Configuration for 'actiongroups' created or updated
Done with success
[root@wazuhmanager tools]#
```

Figura 18: Aplicación cambios de Search Guard

Tal y como se ha echo anteriormente con elasticsearch, se tiene que cercionar de que la seguridad x-pack no está habilitada en Kibana, en el fichero */etc/kibana/kibana.yml*

```
xpack.security.enabled: false
```

Ahora se instala el plugin para Kibana, que va a ser la misma versión que el plugin de elasticsearch, la 6.7.1

```
[root@wazuhmanager tools]# sudo -u kibana NODE_OPTIONS="--max-old-space-size=3072" /usr/share/kibana/bin/kibana-plugin install https://search.maven.org/remotecontent?filepath=com/floragunn/search-guard-kibana-plugin/6.5.4-17/search-guard-kibana-plugin-6.7.1-18.3.zip
Attempting to transfer from https://search.maven.org/remotecontent?filepath=com/floragunn/search-guard-kibana-plugin/6.5.4-17/search-guard-kibana-plugin-6.7.1-18.3.zip
Attempting to transfer from https://artifacts.elastic.co/downloads/kibana-plugins/https://search.maven.org/remotecontent?filepath=com/floragunn/search-guard-kibana-plugin/6.5.4-17/search-guard-kibana-plugin-6.7.1-18.3.zip/https://search.maven.org/remotecontent?filepath=com/floragunn/search-guard-kibana-plugin/6.5.4-17/search-guard-kibana-plugin-6.7.1-18.3.zip-6.7.1.zip
Plugin installation was unsuccessful due to error "No valid url specified."
[root@wazuhmanager tools]# sudo -u kibana NODE_OPTIONS="--max-old-space-size=3072" /usr/share/kibana/bin/kibana-plugin install https://search.maven.org/remotecontent?filepath=com/floragunn/search-guard-kibana-plugin/6.7.1-18.3/search-guard-kibana-plugin-6.7.1-18.3.zip
Attempting to transfer from https://search.maven.org/remotecontent?filepath=com/floragunn/search-guard-kibana-plugin/6.7.1-18.3/search-guard-kibana-plugin-6.7.1-18.3.zip
Transferring 1256411 bytes....................
Transfer complete
Retrieving metadata from plugin archive
Extracting plugin archive
Extraction complete
Optimizing and caching browser bundles...
Plugin installation complete
[root@wazuhmanager tools]#
```

Figura 19: Instalación de plugin de Search Guard en Kibana

Ahora se modifica el fichero de configuración */etc/kibana/kibana.yml*

```
# Elasticsearch URL
elasticsearch.url: "https://localhost:9200"

# Credentials
elasticsearch.username: "admin"
elasticsearch.password:       '

# Disable SSL verification because we use self-signed demo certificates
elasticsearch.ssl.verificationMode: none

# Whitelist the Search Guard Multi Tenancy Header
elasticsearch.requestHeadersWhitelist: [ "Authorization" , "sgtenant" ]
~
~
~
```

Figura 20: Modificación fichero kibana.yml

El siguiente paso es de habilitar la App de Wazuh para acceder a los indices. Para ello se crean los nuevos roles en el fichero */usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_roles.yml*

```
#Wazuh roles

sg_wazuh_admin:
  cluster:
    - indices:data/read/mget
    - indices:data/read/msearch
    - indices:data/read/search
    - indices:data/read/field_caps
    - CLUSTER_COMPOSITE_OPS
  indices:
    '?kiban*':
      '*':
        - MANAGE
        - INDEX
        - READ
        - DELETE
    '?wazuh':
      '*':
        - MANAGE
        - INDEX
        - READ
        - DELETE
    '?wazuh-version':
      '*':
        - MANAGE
        - INDEX
        - READ
        - DELETE

    'wazuh-alerts-3?x-*':
      '*':
        - indices:admin/mappings/fields/get
        - indices:admin/validate/query
        - indices:data/read/search
        - indices:data/read/msearch
        - indices:data/read/field_stats
        - indices:data/read/field_caps
        - READ
        - SEARCH

    'wazuh-monitoring*':
      '*':
        - indices:admin/mappings/fields/get
        - indices:admin/validate/query
        - indices:data/read/search
        - indices:data/read/msearch
        - indices:data/read/field_stats
        - indices:data/read/field_caps
        - READ
        - SEARCH
-- INSERT --
```

Figura 21: Creación de roles de Search Guard

Y se crea el hash del password de administración de wazuh

```
/usr/share/elasticsearch/plugins/search-guard-6/tools/hash.sh -p password
```

```
wazuhadmin:
  hash: $2y$12$iSjb0V50I8Ga5jK0DyvE..stOzJbUzNRq35CrqHj4ePuL51a9urF.
  roles:
    - wazuhadmin_role
~
~
```

Figura 22: Creación del hash del password de administración

Ahora se pone el rol en el fichero */usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_roles_mapping.yml*

```
sg_wazuh_admin:
  backendroles:
    - wazuhadmin_role
```

Figura 23: Crear nuevo role de administración

l se aplican los cambios realizados:

```
[root@wazuhmanager sgconfig]# vi sg_internal_users.yml
[root@wazuhmanager sgconfig]# vi sg_roles_mapping.yml
[root@wazuhmanager sgconfig]# /usr/share/elasticsearch/plugins/search-guard-6/tools/sgadmin.sh \
> -cd /usr/share/elasticsearch/plugins/search-guard-6/sgconfig -icl -key \
> /etc/elasticsearch/kirk-key.pem -cert /etc/elasticsearch/kirk.pem -cacert \
> /etc/elasticsearch/root-ca.pem -h localhost -nhnv
WARNING: JAVA_HOME not set, will use /usr/bin/java
Search Guard Admin v6
Will connect to localhost:9300 ... done
Elasticsearch Version: 6.7.1
Search Guard Version: 6.7.1-25.0
Connected as CN=kirk,OU=client,O=client,L=test,C=de
Contacting elasticsearch cluster 'elasticsearch' and wait for YELLOW clusterstate ...
Clustername: wazuh-cluster
Clusterstate: YELLOW
Number of nodes: 1
Number of data nodes: 1
searchguard index already exists, so we do not need to create one.
Populate config from /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/
Will update 'sg/config' with /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_config.yml
   SUCC: Configuration for 'config' created or updated
Will update 'sg/roles' with /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_roles.yml
   SUCC: Configuration for 'roles' created or updated
Will update 'sg/rolesmapping' with /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_roles_mapping.yml
   SUCC: Configuration for 'rolesmapping' created or updated
Will update 'sg/internalusers' with /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_internal_users.yml
   SUCC: Configuration for 'internalusers' created or updated
Will update 'sg/actiongroups' with /usr/share/elasticsearch/plugins/search-guard-6/sgconfig/sg_action_groups.yml
   SUCC: Configuration for 'actiongroups' created or updated
Done with success
[root@wazuhmanager sgconfig]#
```

Figura 24: Aplicación cambios de los roles de Search Guard

Y ya se tiene la seguridad aplicada:

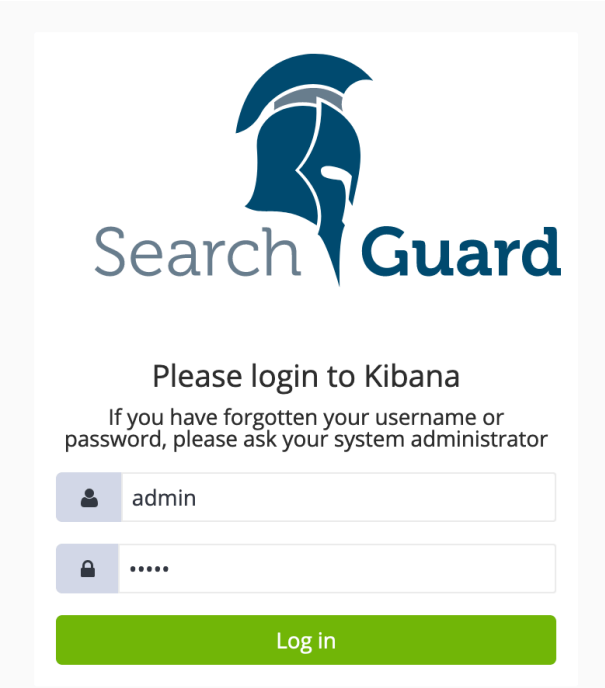


Figura 25: Login de Search Guard en Kibana

5.4. Instalación agentes windows Controladores del Dominio

Tal como se especifica, se instala el cliente a los dos controladores del dominio.

Para hacerlo se habilita la conexión del agente por password. Para eso modificamos el fichero */var/ossec/etc/ossec.conf*

```
<ossec_config>
  <auth>
    <disabled>no</disabled>
    <port>1515</port>
    <use_source_ip>no</use_source_ip>
    <force_insert>yes</force_insert>
    <force_time>0</force_time>
    <purge>yes</purge>
    <use_password>yes</use_password>
    <limit_maxagents>yes</limit_maxagents>
    <ciphers>HIGH:!ADH:!EXP:!MD5:!RC4:!3DES:!CAMELLIA:@STRENGTH</ciphers>
    <!-- <ssl_agent_ca></ssl_agent_ca> -->
    <ssl_verify_host>no</ssl_verify_host>
    <ssl_manager_cert>/var/ossec/etc/sslmanager.cert</ssl_manager_cert>
    <ssl_manager_key>/var/ossec/etc/sslmanager.key</ssl_manager_key>
    <ssl_auto_negotiate>no</ssl_auto_negotiate>
  </auth>
```

Figura 26: Fichero ossec.conf para permitir la conexión de agentes con password

I se crea el fichero authd.pass en el mismo directorio con el password. Ahora se reinicia el servidor con el comando:

```
/var/ossec/bin/ossec-control restart
```

Se descarga el cliente de windows y se instala en el servidor con el comando:

```
wazuh-agent-3.9.0-1.msi /q ADDRESS="x.x.x.x" AUTHD_SERVER="x.x.x.x"
PASSWORD="Password"
```

Y ya se puede ver el agente en la consola:

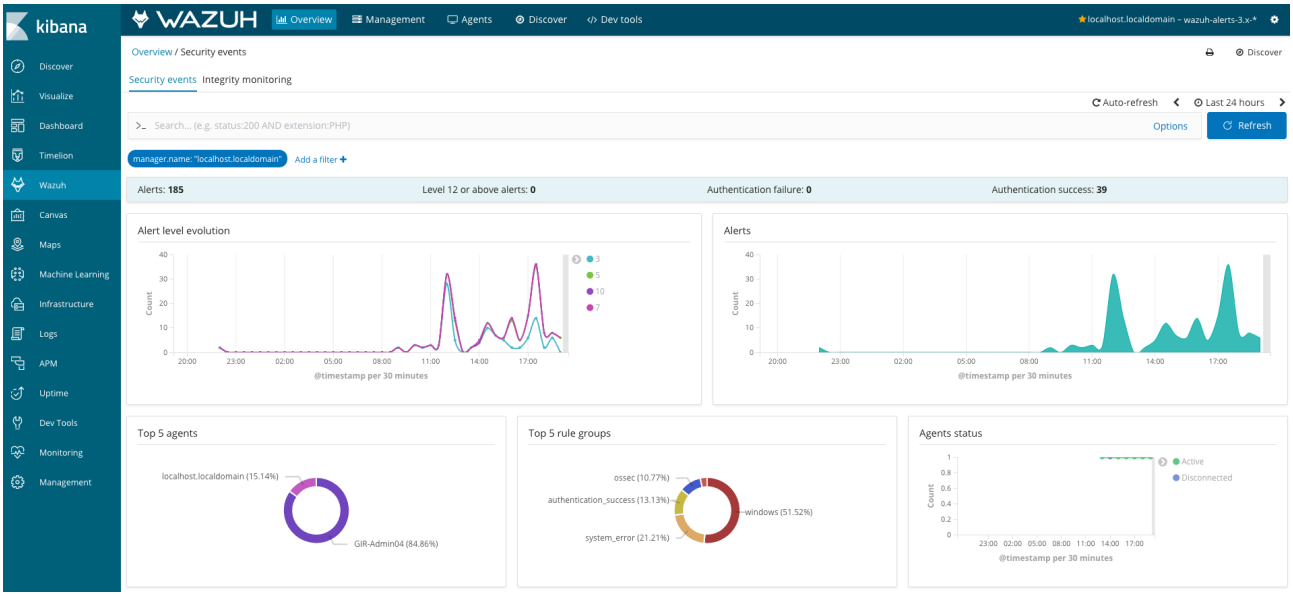


Figura 27: Consola web con el agente windows

5.5. Instalación agente windows en servidor SFTP

También se instala un agente a un servidor de SFTP, que tenemos en la DMZ. Para permitir la comunicación entre el manager y el agente se ha abierto el puerto 1515 para la autorización y el puerto 1514 para la comunicación del agente con el servidor.

Para obtener información sobre el uso del SFTP, lo que se ha echo es configurar el servidor SFTP, en nuestro caso BvSshServer, para que guarde la información en el registro de windows.

Una vez el servidor guarda la información en el registro, tenemos que procesarla correctamente para qué nos de alertas. En ese caso, se quiere registrar los fallos de autentificación. Para ello se tienen que crear reglas personalizadas.

Para hacerlo vamos al directorio */var/ossec/etc/rules* y editamos el fichero *local_rules.xml* y añadimos las siguiente regla:

```
<rule id="100002" level="0">
    <if_sid>60600,60601,60602</if_sid>
    <field name="win.system.providerName">^BvSshServer$</field>
    <description>Event BvSshServer</description>
```

```
</rule>
```

En ella, decimos que si se activan las reglas 60600 60601 i 60602 (que miran es si hay un nuevo evento de aplicación.), pues que esa se ejecute. I esta regla solo mira si el evento es generado por la aplicación BvSshServer.

Esa regla entra en conflicto con otra regla de Wazuh, 60675. Esta regla es la siguiente:

```
<rule id="60675" level="0">
    <if_sid>60600</if_sid>
    <field name="win.system.providerName">VSS</field>
    <description>Group of VSS events</description>
    <options>no_full_log</options>
  </rule>
```

Ya que esa regla se activa con todo proveedor que contenga las letras VSS. Para solucionar eso se cambia de la siguiente forma:

```
<rule id="60675" level="0">
    <if_sid>60600</if_sid>
    <field name="win.system.providerName">^VSS$</field>
    <description>Group of VSS events</description>
    <options>no_full_log</options>
  </rule>
```

Ahora hace falta generar las alertas en caso de fallo de autentificación. Para ello se ha creado 2 reglas mas:

```
<rule id="100003" level="3">
    <if_sid>100002</if_sid>
    <match>I_LOGON_AUTH_FAILED</match>
    <options>no_full_log</options>
    <description>LOGON_AUTH_FAILED Event BvSshServer</description>
    <group>authentication_failed</group>
</rule>
```

```
<rule id="100004" level="3">
    <if_sid>100002</if_sid>
    <match>SocketError</match>
    <options>no_full_log</options>
    <description>SocketError Event BvSshServer</description>
    <group>authentication_failed</group>
</rule>
```

Ahora se reinicia el servidor de reglas:

```
/var/ossec/bin/ossec-control restart
```

Y ya se puede ver que aparen las alertas en el dashboard:

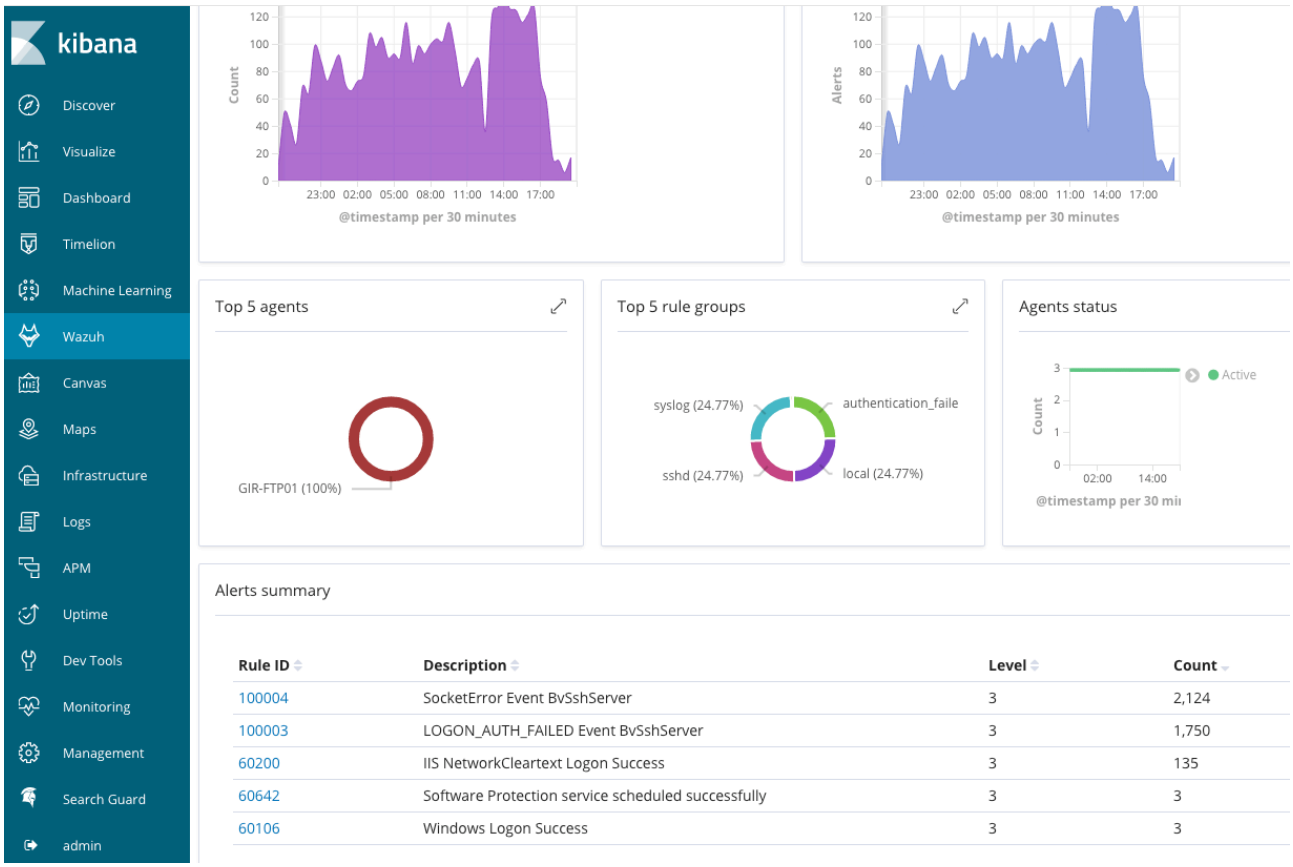


Figura 28: Consola web con el agente windows del servidor SFTP

5.6 Captura de logs utilizando servidor de syslog

Se modifica el fichero */var/ossec/etc/ossec.conf* y se habilita la captura de logs por syslog de las redes de servidores y electrónica de red.

```
    <remote>
        <connection>syslog</connection>
        <allowed-ips>x.x.x.x/21</allowed-ips>
        <allowed-ips>y.y.y.y/21</allowed-ips>
    </remote>
```

Para poder ver que logs llegan, y en que formato también se cambia el tag logall a yes:

```
<logall>yes</logall>
```

A partir de los formatos de logs y el uso del herramienta /var/ossec/bin/ossec-logtest se deduce que los logs de los dispositivos cisco se tienen que formatear utilizando los siguientes parámetros:

```
service timestamps debug datetime msec
service timestamps log datetime
no service sequence-numbers
no logging message-counter syslog
logging host zz.zz.zz.zz
no logging origin-id hostname
```

Aun así, los dispositivos cisco de la compañía no generan alertas, ya que están poniendo un espacio en blanco al principio. Para procesar eso correctamente se define un nuevo descodificador en el fichero */var/ossec/etc/decoders/local_decoder.xml*

```
<decoder name="cisco-ios">
  <prematch>^\p*\s\w+\s+\d*\s+\d+:\d+:\d+:\s+%</prematch>
</decoder>
```

```
<decoder name="cisco-ios-default">
  <parent>cisco-ios</parent>
  <regex>(%\w+-\d-\w+):</regex>
  <order>id</order>
</decoder>
```

Por defecto, las reglas de Wazuh no processan la autentificación 802.1x en los dispositivos Cisco. Una de las objetivos es monitorizar todos los fallos de autentificación de los dispositivos conectados a los switches. Para generar alertas de intentos de autentificación, se crea la siguiente regla:

```
  <rule id="100005" level="3">
    <if_sid>4715</if_sid>
    <id>^%DOT1X-5-FAIL</id>
    <description>Cisco IOS: Authentication failed for client.</
description>
    <group>authentication_failed</group>
  </rule>
```

Y ahora ya se pueden ver las alertas generadas por los dispositivos cisco, incluyendo las alertas de fallos de autentificación del protocolo 802.1x

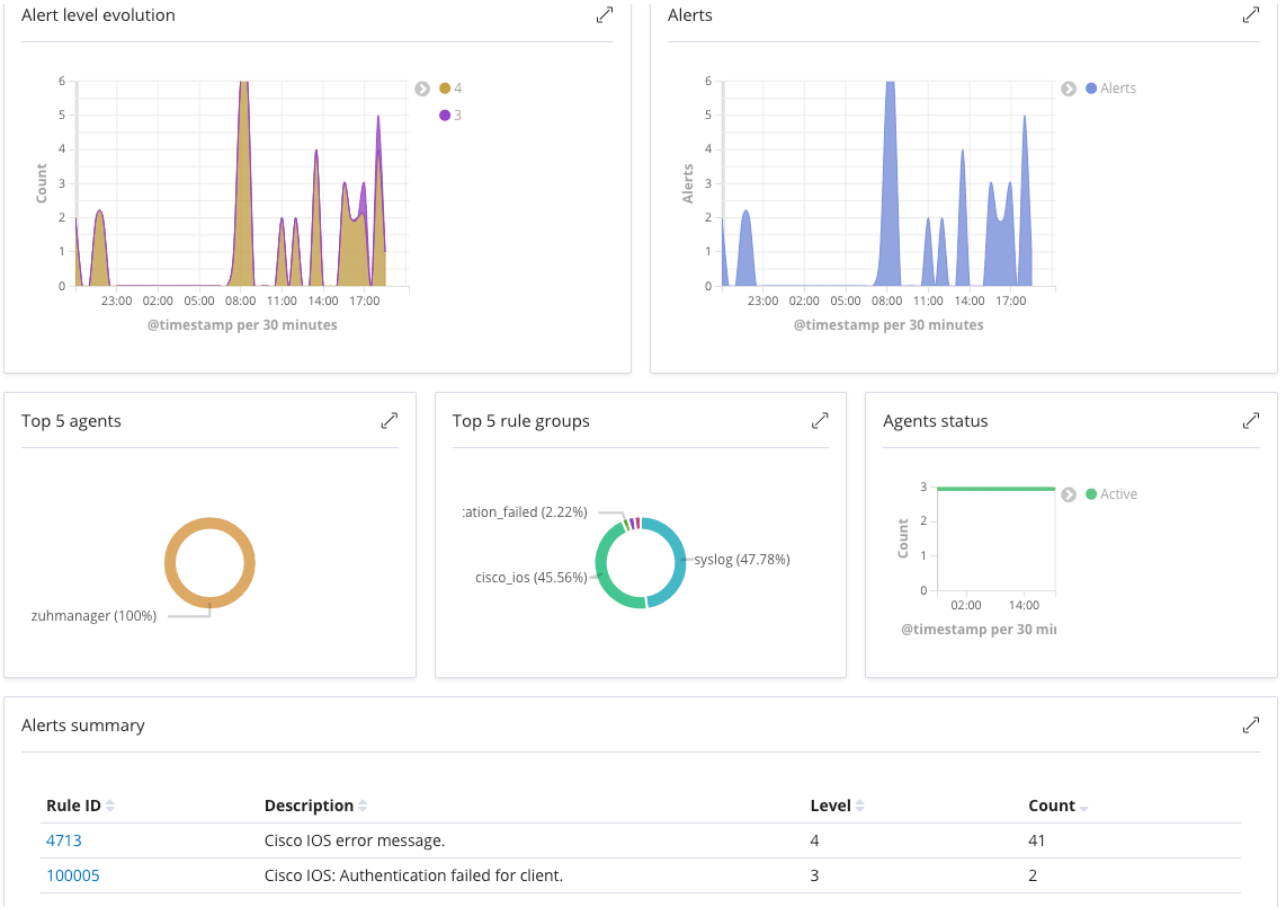


Figura 29: Consola web con las alertas de syslog

5.7 Dashboard Personalizado

Para gestionar los fallos de autenticación se decide crear un dashboard personalizado. Para ello, primero se tiene que crear diferente visualizaciones.

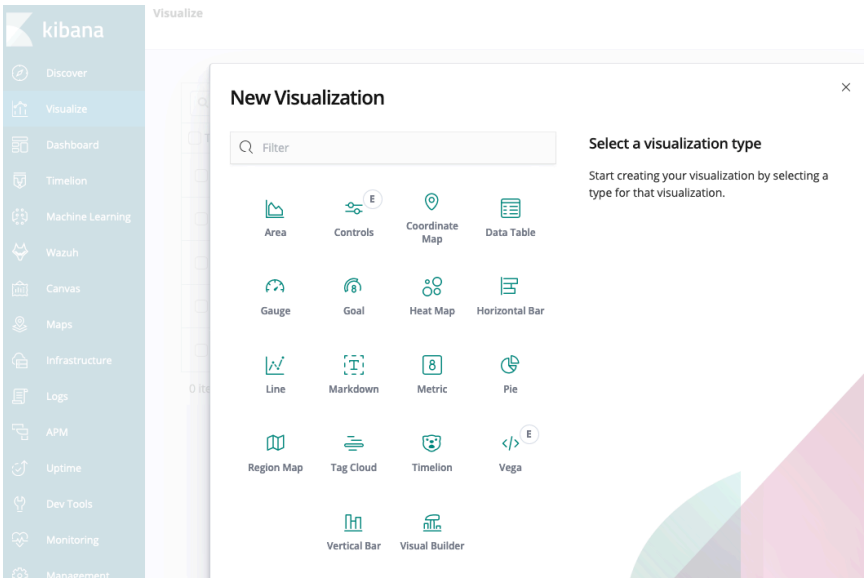


Figura 30: Crear nueva visualización

La primera visualización que se crea es para ver que dispositivos están creando mayor alertas. Para ello se crear un nuevo “tag cloud”. Para filtrar qsolamente los dispositivos creamos el siguiente filtro:

```
{
  "query": {
    "prefix": {
      "location": "10"
    }
  }
}
```

Y en los “Buckets” se agrega por “location”

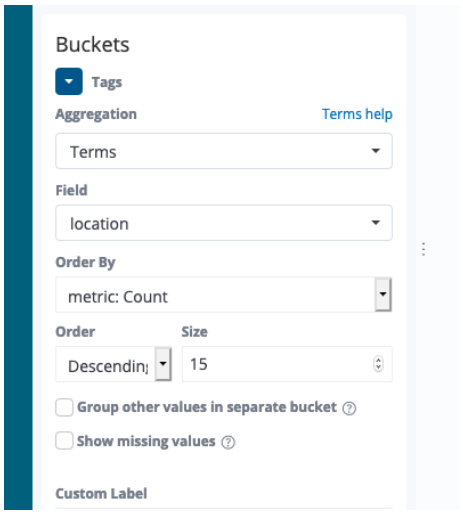
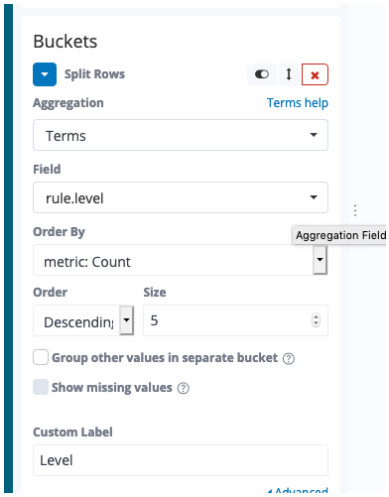


Figura 31: Buckets del Tag Cloud

Luego se crea una tabla de grupo de alertas, ordenadas por nivel. Para ello se crea un Bucket del nivel, ordenado de forma descendiente. También se añade la descripción



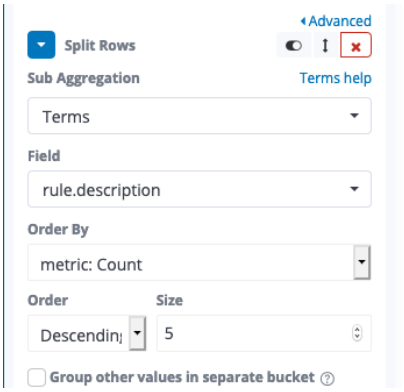


Figura 32: Buckets para la tabla de grupos de alertas

A continuación se crea otra tabla solamente con las alertas relacionadas con la autenticación. Para ello se crea un filtro donde el grupo de regla sea de fallo de autenticación.

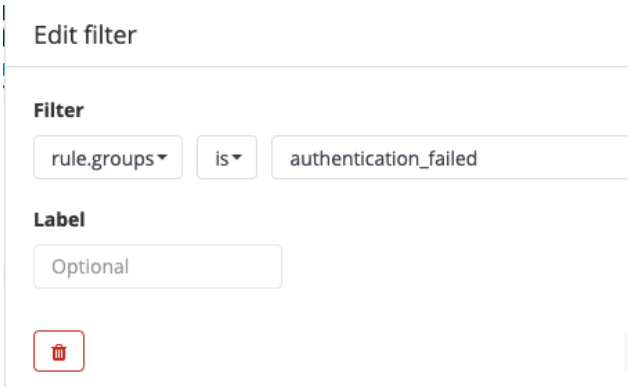


Figura 33: Filtro reglas de autenticación fallida.

I se añade el Bucket de descripción, como en la tabla anterior.

Finalmente se decide crear una gráfica para ver el numero de alertas de autenticación en el tiempo. Creamos una nueva visualización de gráfico de área. En la gráfica se utiliza el mismo filtro que en la visualización anterior y añadimos el Bucket en el eje X con el timestamp.

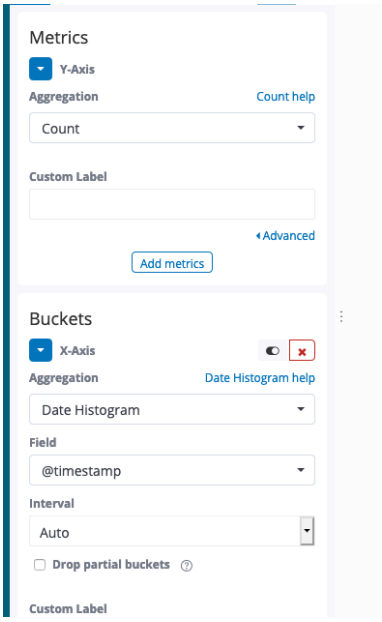


Figura 34: Definición ejes gráfica de autenticaciones fallidas.

Una vez se han definido las diferentes visualizaciones, ya se puede crear el dashboard con los elementos definidos:

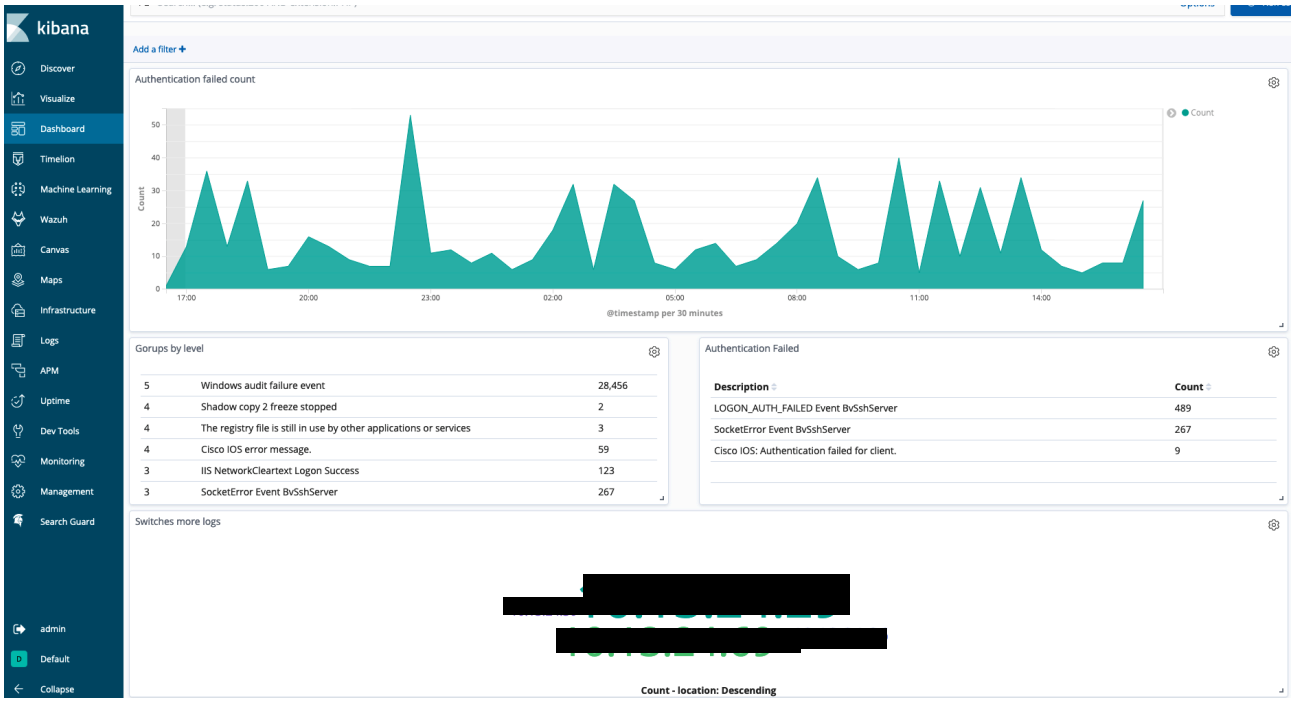


Figura 35: Dashboard personalizado.

6. Conclusiones

Después de la elaboración del TFM se pueden extraer diferentes conclusiones respecto a los sistemas SIEM.

La primera, es que hasta que no empiezas a analizar tu entorno, no te das cuenta de la cantidad de logs que se pueden generar en un entorno real y que sin un sistema SIEM no se pueden analizar ni sacar conclusiones.

Debido ha esa cantidad y diferentes fuentes de información, la complejidad de la normalización de los logs es grande, aunque muchos proveedores, si no los tienen predefinidos té los crean.

La última conclusión que se saca es que los sistemas SIEM del mercado, están orientados a grandes corporaciones o a SOCs externalizados, que gestiones diferentes empresas, por dos razones: La primera es que los precios no están al alcance de todas las organizaciones. La segunda es que las soluciones SIEM, no son un producto “Plug & play” ya que una vez lo tienes instalado, debes tener claro que te interesa monitorizar y analizar las diferentes alertas que genera el SIEM. Eso implica tener personal formado y capacitado y tiempo para hacerlo, lo que también es un gasto para las organizaciones. Sobretodo sí para reducir los costes del producto, se opta para soluciones open source.

Respecto a los objetivos iniciales, no se ha podido agregar los logs del firewall, debido a que en la empresa se ha cambiado de producto y ahora está gestionado des de la cede central. Debido ha eso se ha optado por analizar un servidor SFTP que está en nuestra DMZ.

La planificación inicial tampoco se ha cumplido el 100%, ya que el tiempo para valorar diferentes productos, contactar con los proveedores, hacer las demos y conseguir presupuestos consume mucho tiempo y puede llegar ha ser muy lento, pero tambien creo que es muy rico, ya que ves el enfoque de cada fabricante y te puedes ir haciendo a la idea de que te conviene en tu organización.

Como siguientes pasos se destacaría:
- Reorganización del departamento de IT para tener la formación para gestionar y analizar la solución SIEM
- Añadir y/o modificar reglas de correlación para detectar ataques de los sistemas propios.
- Seguir con las siguientes fases de incorporación de logs.
- Añadir un IDS he incorporar la información a nuestro SIEM.
- Utilizar herramientas de Machine Learning para crear patrones de comportamiento y ver conductas anormales.

7. Anexos

7.1 Anexo 1: Cuadrante de Gartner

Source: Gartner (December 2018)

8. Bibliografia

[1] Chuvakin, A., Phillips, C., & Schmidt, K. Logging and log management : The auitative guide to dealing with syslog, audit logs, events, alerts and other it 'noise'. Retrieved from https://ebookcentral.proquest.com, (2012).

[2] ArcSight. Common Event Format, Revision 16. ArcSight, Inc. (2010)

[3] https://www.ionos.es/digitalguide/online-marketing/analisis-web/el-log-el-archivo-de-registro-de-procesos-informaticos/

[4] Kelly Kavanagh, Toby Bussa, Gorka Sadowski. Magic Quadrant for Security Information and Event Management. Gartner (2018)

[5] Michael Starks, Open Source Log Management, Analysis and Intrusion Detection , Immutable Security (2009)

[6] David Swift, A Practical Application of SIM/SEM/SIEM Automating
Threat Identification, SANS Institute (2019)

[7] https://en.wikipedia.org/wiki/Security_information_and_event_management

[8] https://www.seguridadx.com/que-es-un-siem-que-es-prelude-siem/

[9] https://help.deepsecurity.trendmicro.com/Events-Alerts/syslog-parsing.html

[10] https://www.exabeam.com/siem-guide/what-is-siem/

[11] https://wazuh.com

[12] https://documentation.wazuh.com/current/index.html

[13] https://groups.google.com/forum/#!forum/wazuh

[14] https://groups.google.com/forum/#!forum/ossec-list