Ventajas e Implementación de un sistema SIEM

Luis Miguel Jaso Marquina
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Telecomunicaciones (UOC, URV, UAB).

Director del TFM:
Marco Antonio Lozano Merino
Profesor Responsable de la Asignatura:
Víctor García Font

Junio 2018

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Ventajas e Implementación de un sistema SIEM*
Nombre del autor:	*Luis Miguel Jaso Marquina*
Nombre del consultor/a:	Marco Antonio Lozano Merino
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2018
Titulación:	*Máster Universitario* en Seguridad de las Tecnologías de la Información y de las Telecomunicaciones
Área del Trabajo Final:	*Trabajo Final de Máster*
Idioma del trabajo:	*Castellano*
Palabras clave	*Informática, seguridad, SIEM, HIDS, Elastic Stack*

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

La fuerte demanda por parte de las organizaciones en el contexto de seguridad informática, ha disparado el interés de las mismas por los sistemas SIEM. El presente trabajo muestra, por una parte, un enfoque teórico sobre lo que es un SIEM y sus sistemas más populares desarrollados, por otra, un enfoque práctico de la implementación de un sistema SIEM. Este sistema está compuesto por una serie de componentes basados en Open Source, en el que se describen sus funcionalidades y algunos casos de uso.

El sistema implementado se basa en la integración de Elastic Stack (Elasticsearch, Logstash, Kibana y beats) con otras tecnologías como Wazuh (HIDS), Search Guard y Sentinl.

Con el sistema SIEM implementado, se ha gestionado la seguridad en: sistemas finales, un cortafuegos, un servidor web y un servidor NAC. Todos ellos han sido monitorizados por un HIDS integrado en el SIEM (Wazuh). En el NAC y el cortafuegos han sido extraídos sus logs en crudo y tratados para integrarlos en nuestro SIEM, pudiendo realizar filtrados inteligentes en tiempo real o en modo forense. La seguridad de acceso al SIEM y la comunicación con los sensores se ha realizado a través de Search Guard, integrándose a la perfección con nuestro SIEM. Por ultimo, el sistema de alertas y reporting se basa en la solución open source Sentinl.

Con este trabajo se ha intentado demostrar que, a partir de los componentes anteriormente descritos, todos ellos Open Source, se puede desarrollar un

sistema SIEM que ofrezca unas funcionalidades básicas y necesarias para la gestión de la seguridad en una organización.

Abstract (in English, 250 words or less):

The strong demand on the part of organizations in the context of computer security, has triggered their interest in SIEM systems. The present work shows, on the one hand, a theoretical approach on what is a SIEM and the most popular systems SIEM and on the other, this work carries out a practical approach to the implementation of a SIEM system. This system is composed of a series of components based on Open Source, in which its functionalities and some use cases are described.

The implemented system is based on the integration of Elastic Stack (Elasticsearch, Logstash, Kibana and beats) with other technologies such as Wazuh (HIDS), Search Guard and Sentinl.

With the SIEM system implemented, security has been managed in: final systems, a firewall, a web server and a NAC server. All of them have been monitored by a HIDS integrated in the SIEM (Wazuh). Furthermore, In the NAC and in the firewall, their raw logs have been extracted and processed to integrate them into our SIEM, being able to perform intelligent filtering in real time or in forensic mode. The security of access to the SIEM and the communication with the sensors has been done through Search Guard, this integrates our SIEM perfectly. Finally, the alerting and reporting system is based on the open source Sentinl solution.

With this work we have tried to demonstrate that, from the previously described components, all of them Open Source, a SIEM system can be developed offering basic and necessary functionalities for security management in an organization.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

El Trabajo de Fin de Máster “Ventajas e implementación de un sistema SIEM” que pretendo desarrollar versará sobre un sistema de seguridad en la red, con distintos componentes, en el cual el SIEM será el elemento orquestador del sistema.

El trabajo combinará dos apartados principales:

- Apartado de Investigación: Fundamentos teóricos sobre los SIEM, características, capacidades, tipos de sensores, funcionalidades, integración con sensores (IPS, IDP, etc.), externalización del servicio SOC, necesidad del sistema en una organización). Se realizará una comparativa entre los diferentes sistemas SIEM más populares en la actualidad y finalizaremos eligiendo uno de ellos para poder implementarlo en la parte de desarrollo.
- Apartado de desarrollo: Se implementará un pequeño laboratorio (por medio de tecnología virtual) en el cual instalaremos el SIEM elegido y lo integraremos con diferentes tipos de sensores como pueden ser IPS/IDS, NAC, escáner, etc. Se realizarán casos de uso (pruebas) para posteriormente analizar el comportamiento del SIEM presentando un informe sobre las mismas. Se tratará de analizar todas las características del SIEM mediante pruebas. La memoria constará de un manual de instalación y configuración básica y casos de uso.

En este trabajo, la parte con más dedicación será la de desarrollo, ya que es la que tiene más complejidad y requiere de mayor esfuerzo.

1.2 Objetivos del Trabajo

Con la realización de este TFM pretendo desarrollas las siguientes competencias:

Objetivos Generales:

1. Capacidad de análisis y síntesis de la seguridad de un sistema.
2. Conocimiento de herramientas y tendencias tecnológicas del mercado de la seguridad informática.
3. Capacidad para seleccionar, aplicar e integrar los conocimientos técnicos y científicos adecuados para resolver problemas en entornos nuevos.
4. Capacidad de comunicar información tanto a público especializado como no especializado de modo claro y sin ambigüedades.
5. Capacidad para redactar documentación científica.
6. Capacidad de aprendizaje autónomo consultando información.
7. Capacidad para realizar, presentar y defender ante un tribunal universitario un ejercicio realizado individualmente consistente en un proyecto integral de seguridad de las tecnologías de la información y de las comunicaciones de naturaleza profesional.

Objetivos específicos:

1. Conocimiento del concepto de SIEM, sus capacidades y funcionalidades.
2. Conocimiento de los diferentes herramientas y tendencias tecnológicas del mercado de los sistemas de seguridad alrededor de un SIEM.
3. Capacidad para usar técnicas y contramedidas básicas de seguridad para la prevención de ataques.
4. Capacidad para identificar, evaluar y gestionar los principales riesgos del sistema en el entorno que se encuentra instalado el SIEM.
5. Capacidad para identificar las vulnerabilidades de privacidad de los sistemas y capacidad para protegerlos.
6. Conocimiento y utilización de herramientas para la administración y protección de redes, y la gestión de alertas de seguridad.
7. Capacidad para concebir, desplegar, organizar y gestionar redes de comunicaciones en contextos residenciales, empresariales o institucionales, responsabilizándose de la seguridad del sistema y la protección de los datos de los usuarios.
8. Capacidad para diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, detección y disuasión de ataques.
9. Conocimiento de los métodos para la adquisición y análisis de evidencias de un incidente de seguridad. Capacidad de usar el SIEM para la gestión y resolución de incidentes.
10. Conocimiento de las problemáticas de seguridad y algunas de sus posibles soluciones.

1.3 Enfoque y método seguido

Tal y como se expuso en un apartado anterior, el TFM tiene dos claros apartados. El correspondiente a “conocer el SIEM” de forma genérica y responde a las siguientes preguntas:

- ¿Qué es un SIEM?
- ¿Qué funcionalidades tiene?
- ¿Qué aporta a una organización?
- ¿Cuáles existen en el mercado en la actualidad?
- ¿Cómo se puede gestionar?
- ¿Ventajas?, ¿inconvenientes?
- ¿Cómo se relaciona con los demás elementos de seguridad de una red?
- ¿Qué SIEM conviene a nuestra organización?
- ….

Como se puede observar, este apartado es un trabajo de investigación/aprendizaje en el cual deberemos apoyarnos, fundamentalmente, en búsquedas en la web y bibliografía.
El otro apartado es el correspondiente a “saber hacer”, en definitiva, el trabajo práctico, la implementación del sistema con la herramienta SIEM. En este apartado abordaremos los siguientes puntos:

- Instalación del sistema.
- Configuración del mismo.

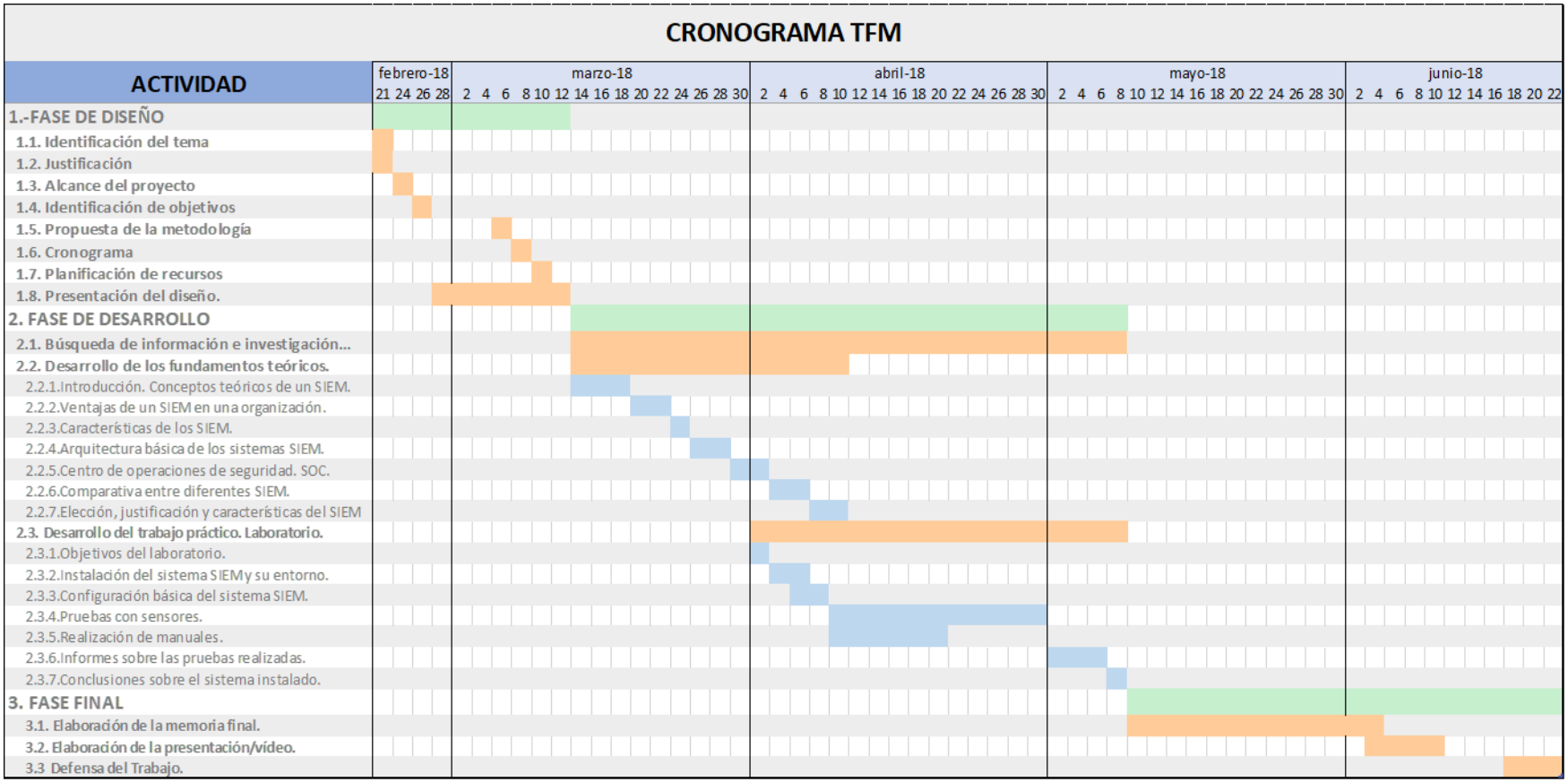
- Pruebas.
- Informes.

Todos estos puntos se realizarán de forma práctica en un entorno de laboratorio virtual. Será el laboratorio de pruebas.
Por último, se preparará un manual (puede ser un documento de texto o videotutorial, etc.) del funcionamiento del mismo.

1.4 Planificación del Trabajo

He realizado tres grupos para categorizar las tareas a realizar:

1. Fase de diseño
   - 1.1. Identificación del tema
   - 1.2. Justificación
   - 1.3. Alcance del proyecto
   - 1.4. Identificación de objetivos
   - 1.5. Propuesta de la metodología
   - 1.6. Cronograma
   - 1.7. Planificación de recursos
   - 1.8. Presentación del diseño.
2. Fase de desarrollo.
   - 2.1. Búsqueda de información e investigación sobre los SIEM y el sistema. Google. Bibliografía.
   - 2.2. Desarrollo de los fundamentos teóricos.
     - 2.2.1. Introducción. Conceptos teóricos de un SIEM.
     - 2.2.2. Ventajas de un SIEM en una organización.
     - 2.2.3. Características de los SIEM.
     - 2.2.4. Arquitectura básica de los sistemas SIEM. Sensores.
     - 2.2.5. Centro de operaciones de seguridad. SOC. Externalización.
     - 2.2.6. Comparativa entre diferentes SIEM.
     - 2.2.7. Elección, justificación y características del SIEM a implementar en la fase práctica.
   - 2.3. Desarrollo del trabajo práctico. Laboratorio con el sistema SIEM elegido en el punto anterior.
     - 2.3.1. Objetivos del laboratorio.
     - 2.3.2. Instalación del sistema SIEM y su entorno.
     - 2.3.3. Configuración básica del sistema SIEM.
     - 2.3.4. Pruebas con sensores como (IDS/IPS, escáneres, control de accesos, etc.). Alertas de ataques, logging, correlación de logs, informes, etc.
     - 2.3.5. Realización del manual de instalación y configuración.
     - 2.3.6. Informes sobre las pruebas realizadas.
     - 2.3.7. Conclusiones sobre el sistema instalado.
3. Fase final
   - 3.1. Elaboración de la memoria final del Trabajo de Fin de Máster
   - 3.2. Elaboración de la presentación/vídeo del Trabajo de Fin de Máster.
   - 3.3. Defensa del Trabajo de Fin de Máster.


CRONOGRAMA TFM
ACTIVIDAD
febrero-18
21 24 26 28
marzo-18
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30
abril-18
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30
mayo-18
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30
junio-18
2 4 6 8 10 12 14 16 18 20 22
1.-FASE DE DISEÑO
1.1. Identificación del tema
1.2. Justificación
1.3. Alcance del proyecto
1.4. Identificación de objetivos
1.5. Propuesta de la metodología
1.6. Cronograma
1.7. Planificación de recursos
1.8. Presentación del diseño.
2. FASE DE DESARROLLO
2.1. Búsqueda de información e investigación...
2.2. Desarrollo de los fundamentos teóricos.
2.2.1.Introducción. Conceptos teóricos de un SIEM.
2.2.2.Ventajas de un SIEM en una organización.
2.2.3.Características de los SIEM.
2.2.4.Arquitectura básica de los sistemas SIEM.
2.2.5.Centro de operaciones de seguridad. SOC.
2.2.6.Comparativa entre diferentes SIEM.
2.2.7.Elección, justificación y características del SIEM
2.3. Desarrollo del trabajo práctico. Laboratorio.
2.3.1.Objetivos del laboratorio.
2.3.2.Instalación del sistema SIEMy su entorno.
2.3.3.Configuración básica del sistema SIEM.
2.3.4.Pruebas con sensores.
2.3.5.Realización de manuales.
2.3.6.Informes sobre las pruebas realizadas.
2.3.7.Conclusiones sobre el sistema instalado.
3. FASE FINAL
3.1. Elaboración de la memoria final.
3.2. Elaboración de la presentación/vídeo.
3.3 Defensa del Trabajo.

1.5 Estado del arte

La seguridad de la red de una organización es un punto clave a considerar desde cualquier punto de vista. Hoy en día existen un sinfín de herramientas encargadas de gestionar la seguridad (firewalls, IDS, IPS, NAC, etc.), todas y cada una de ellas con su propia gestión particular y si unir esfuerzos entre ellas.

Los SIEM existentes en la actualidad integran la gestión de todas estas herramientas, gestionando la seguridad completa de la red en una interfaz común.

La mayoría de los SIEM existentes en el mercado, tienen características muy parecidas (control en tiempo real, recolección de logs, correlación de los mismos, sistemas de alertas, informes, etc.), lo que los puede diferenciar son: su adaptación al entorno donde deba operar, su licenciamiento (precio, licencia open source, etc.), su manejabilidad, la presentación de informes, la gestión forense, el análisis de riesgos, etc.

Lo sistemas SIEM nacen como la integración de dos tecnologías diferentes, que se integran en los últimos años:

- SEM. Gestión de Eventos de Seguridad. Se centraba en el seguimiento de alertas de seguridad en tiempo real generado por cortafuegos o IDS/IPS.
- SIM. Realizaba las mismas operaciones que SEM con la diferencia que la gestión no era en tiempo real, pudiendo recabar información pasada y generando informes en base a ella.

1.6 Recursos

Los recursos necesarios para la consecución del presente Trabajo Fin de Máster, grosso modo, serán:

- Buscadores de internet. Google, Bing, etc.
- Artículos y referencias bibliográficas sobre el presente trabajo.
- Laboratorio virtual. Host Windows 10. Sistema de virtualización - VirtualBox 5. Máquinas virtuales Ubuntu, CentOS 7, etc.
- Software SIEM elegido en la fase teórica.
- Sistema de grabación de vídeo. Nimbus y Lightworks 14.
- Editor de textos Microsoft Word 2016. Hoja de cálculo Excel 2016.
- Generador de diagramas de flujo y software – Microsoft Visio.

2. Fundamentos teóricos

Cada vez resulta más complicado hacer frente a los ataques que ocurren en las redes informáticas, los sistemas SIEM ayudan a los administradores de red a automatizar este trabajo para posibilitar una gestión de la seguridad de la red más eficiente.

La demanda de sistemas SIEM en las organizaciones es una constante durante los últimos años. Tal y como indica Forecast, en "Information Security, Worldwide, 2015-2021, 3Q17 Update", las ventas de tecnología SIEM crecieron de 2001 billones de dólares en el año 2015, a 2167 billones de dólares en el año 2016.

Hoy en día la gestión y el tratamiento de las amenazas es uno de los aspectos más importantes a considerar por parte de las organizaciones modernas, dedicando los recursos necesarios para poder responder a cualquier incidente de seguridad que surja. Los sistemas SIEM actúan como un repositorio registrando eventos de red relacionados con la seguridad, usados para monitorizar, identificar, documentar e incluso responder a dichos incidentes de seguridad.

Algunos de los incidentes de seguridad son claros y su identificación podría ser sencilla, pero una gran parte de los incidentes de seguridad, aunque puedan ser obvios, se esconden detrás de la gran cantidad de eventos por segundo que se producen en la red de una organización, y que sin un sistema SIEM serían completamente inadvertidos. Los sistemas SIEM son usados para monitorizar, identificar, documentar e incluso para responder a incidentes de seguridad.[1-Introducción]

Una de las grandes propiedades de un sistema SIEM es la reducción de falsas alertas, frecuentemente producidas, por ejemplo, a través de sistemas de detección de intrusiones (IDS). La reducción de falsas alertas viene de la mano de la filtración y correlación de eventos de seguridad producidas por el SIEM, discriminando con precisión aquellas situaciones que los sensores las catalogan de incidentes de seguridad sin realmente serlo. [1-Introducción]

2.1 Conceptos teóricos de un SIEM. Características

El acrónimo SIEM procede de la frase "Security Information and Event Management" (Administrador de Eventos e Información de la Seguridad) y se atribuye a Gartner Amrit Williams y Nicolett Marcos.

Los sistemas SIEM surgen de la convergencia de dos tecnologías diferentes [1-Introducción]:

- SEM (Administrador de Eventos de Seguridad). Procesa y monitoriza eventos de seguridad en tiempo real, generados en diferentes sensores (FW, IDS, NAC, etc.), los correlaciona y es capaz de generar alertas al usuario.

- SIM (Administrador de Información de Seguridad). Almacena todos los eventos generados por los sensores conectados al mismo, pero a diferencia de los SEM, el procesamiento de estos eventos se centra en el análisis histórico, posibilitando análisis forense, monitorización y realización de informes.

Los sistemas SIEM combinan las capacidades de estas dos tecnologías proporcionando la siguiente colección de servicios:

- Recolección y gestión de logs. Los sistemas SIEM capacidad de adquirir datos de diversas fuentes, particularmente las más importantes o críticas (FW, IDS, Servidores, Aplicaciones, etc.) y almacenarlos en una base de datos centralizada. Esta base de datos inicialmente realiza un análisis sintáctico del dato, normalizándolo, ya que los distintos sensores (elementos fuente) envían el dato en diferentes formatos. Hay que tener presente que estos sensores normalmente son de naturalezas muy diversas (equipos con diferentes sistemas operativos, sistemas de infraestructura de red como switches, routers, cortafuegos, sistemas de detección de intrusos, etc.). Seguidamente el SIEM, normalmente, almacena todos los datos normalizados, los organiza y les aplica una política de retención para satisfacer los requerimientos de la organización o regulaciones vigentes. Estos datos también son utilizados en tiempo real, para analizar la salud y seguridad de estos sensores y equipos que se encuentran en nuestra organización proporcionando datos al SIEM.
- Cumplimiento de las regulaciones vigentes de la seguridad de la información. Todos los sucesos generados desde los sistemas que están siendo recolectados como logs, pueden ser analizados bajo filtros y reglas para auditar y validar el cumplimento de los requerimientos impuestos por la organización en su política de seguridad y satisfacer estos requisitos de seguridad exigibles y los asociados a las regulaciones vigentes.
- Capacidad forense. Posibilidad de analizar los datos y alertas para determinar el origen de las incidencias de seguridad y hacer frente a las mismas.
- Agregación y correlación de eventos de seguridad en tiempo real. El SIEM establece relaciones entre diferentes sucesos, estudiando la frecuencia de los sucesos, el horario de los mismos, etc., para establecer la veracidad del incidente (eliminar falsos positivos) y poder unir todos estos sucesos y verlos como un único incidente, lo cual ayuda a su tratamiento. El motor de correlación puede considerar otros eventos diferentes al investigado para proporcionar una fotografía más completa de la verdadera causa del problema.
- Capacidad de respuesta. Acciones reactivas. Una vez que el SIEM es capaz de identificar el incidente de seguridad tras recolectar y adecuar los logs y correlacionarlos para estar seguro de que el incidente es cierto, algunos SIEM cuentan con la capacidad de reaccionar automáticamente frente a dichos incidentes tratando de mitigar el problema. Por ejemplo, una vez confirmada la causa del problema podríamos apagar la boca del switch desde donde se genera el problema, si es posible y adecuado, o filtrar el acceso a esa IP determinada desde donde se origina el incidente, etc.

- Seguridad en los equipos clientes. Los sistemas SIEM tienen la capacidad de monitorizar la salud y el estado de un equipo final. Por ejemplo, pueden monitorizar el estado de los recursos del sistema de un servidor, desktop u otros, los procesos que se están ejecutando, escanear sus vulnerabilidades, monitorizar el estado de sus antivirus, etc.
- Monitorización y alertas de seguridad. Los sistemas SIEM tienen la capacidad de visualizar, monitorizar y administrar todos los eventos de seguridad. Son capaces de analizar automáticamente todos los eventos y solamente notificar de aquellos que realmente son más relevantes. Se debe tener presente la gran cantidad de datos que proporcionan los sensores al sistema SIEM y esta debe ser capaz de alertar solamente de aquellos que sean realmente significativos, realmente se trata de "encontrar la aguja dentro del pajar"
- Presentación de Informes de seguridad. Capacidad de presentación de informes ejecutivos y técnicos.

2.2 Arquitectura de los sistemas SIEM [1-Capítulo 5]

Un SIEM representa una máquina compleja con múltiples partes que se pueden caracterizar desde un punto de vista tanto lógico como físico [1-78].

La siguiente figura ilustra la arquitectura lógica de un sistema SIEM, con las funcionalidades que puede albergar. No tienen por qué estar todas las funcionalidades descritas en todos los SIEM, algunos las integran todas y otros la mayoría de ellas.

Ilustración 1.-Arquitectura lógica del SIEM

Desde el punto de vista físico, el conjunto de piezas que forman el SIEM todavía es más evidente la independencia de las mismas, siendo el elemento SIEM el orquestador de todo el sistema integrado.

El SIEM se puede ver desde la perspectiva de un sistema gestor de logs, al cual se le van añadiendo capacidades en el ámbito de la seguridad de la información.

Primeramente, recolectamos los logs de aquellos dispositivos interesantes desde un punto de vista de la seguridad, añadimos la capacidad de análisis, filtrado y normalización de los mismos, preparamos unas reglas que nos alerten de los sucesos más importantes siempre y cuando cumplan unas condiciones que previamente se han implementado, almacenamos los logs con una política de retención adecuada e implementamos un sistema de visualización para monitorizar los datos almacenados en el SIEM.

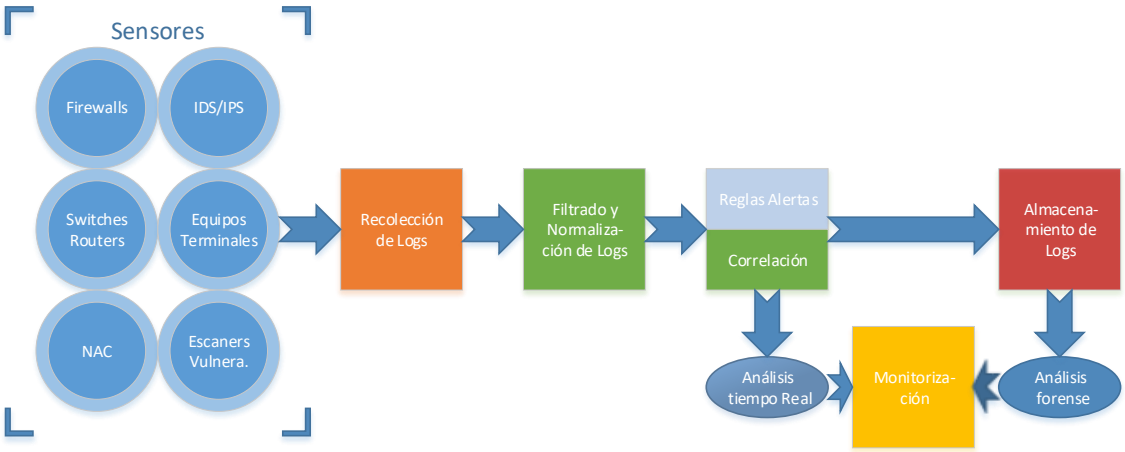


Ilustración 2.- Arquitectura física del SIEM. Adaptación de la figura [1-78]

Descripción de las partes físicas:

- Sensores: Son los equipos de seguridad que capturan la información, estos pueden ser: routers, switches, servidores, NACs, IDS/IPS, firewalls e incluso aplicaciones como Nmap, OpenVAS, etc. Cualquier dispositivo que tenga que ver con la seguridad y sea capaz de generar registros (logs), debiera poder ser conectado al SIEM.
- Recolección de logs [1-81]: Es el procedimiento de traslado de los registros al SIEM, y fundamentalmente existen dos métodos dependiendo de quien se encarga la tarea de la recolección: el sensor "push method" o el SIEM "pull method". En el método "push", el sensor envía los registros hacia el SIEM por medio de algún método (syslog, beats, nxlog, etc) con total independencia del SIEM, en cambio en el método "pull" es necesario que el SIEM inicie la conexión para poder recoger los registros generados en el sensor. Por ejemplo, en el método "push", el SIEM podría leer los registros de los sensores cuando fuese necesario.
- Filtrado y normalización de logs [1-83]: Los registros provenientes de diferentes sensores y por supuesto de distinta naturaleza, adoptan un formato que depende del mismo sensor y este formato normalmente es muy diferente para cada tipo de sensor. El SIEM debe normalizar todos los formatos diferentes llegados de los distintos sensores para facilitar su lectura y permitir formatos estándar para la posterior correlación de eventos. La forma unificada en el formato de logs facilita la creación de reglas de correlación.
- Reglas de alertas-correlación [1-85]: El SIEM debe tener la capacidad de generar alertas vía visualización, mensajería, etc. de todos aquellos

incidentes que hacen saltar las reglas de seguridad establecidas en el mismo. Además, para evitar falsos positivos y no generar alertas falsas que harían desviar nuestra atención y trabajar en vano, las alertas deben estar generadas por la asociación de diferentes incidentes, incluso provenientes de diferentes sensores, que aseguran la veracidad de la misma. Por ejemplo, un fallo de autenticación desde una máquina contra un servidor puede deberse a un error humano y el SIEM no debiera disparar ninguna alerta, pero si ese fallo se produce desde la misma máquina con una frecuencia de 100 veces por segundo, debiéramos pensar que puede ser un ataque de fuerza bruta y el sistema SIEM debiera alertar del mismo.

- Almacenamiento de logs [1-89]: Para trabajar con grandes volúmenes de registros y poder aplicarles una buena política de retención, necesitamos de un bien dimensionado almacén, que podría resultar una base de datos como Oracle Database, MySQL, Microsoft SQL, etc., ficheros de texto como por ejemplo archivos JSON o ficheros binarios. Dependiendo del volumen de registros almacenados puede ser interesante, para mejorar el rendimiento de almacenamiento y búsqueda, el utilizar varios nodos de almacenamiento formando clusters.
- Monitorización [1-90]: La fase final en la arquitectura del SIEM es la monitorización. Una vez se han recogido y procesado todos los registros se necesita poder acceder a la información guardada (análisis forense), normalmente con búsquedas inteligentes, también deben presentarse informes, gráficos, etc. que nos ofrezca una idea del estado actual del sistema o el más cercano. La capa de monitorización del SIEM hace que podamos visualizar en un único lugar el estado de todos los sensores conectados al mismo. Por último, la capa de monitorización nos facilita el poder desarrollar las reglas que extraen información de los eventos que se están procesando.

2.3 Centro de operaciones de seguridad. SOC. [5]

Un Centro de Operaciones de Seguridad (SOC), es un equipo de personas que continuamente están monitorizando las redes, vulnerabilidades en equipos, intrusiones, o cualquier síntoma de actividad anómala, desarrollando las respuestas apropiadas a estos incidentes, dentro de una organización. El tamaño de este equipo dependerá del tamaño de la organización a supervisar.

Este grupo de personas puede pertenecer a la organización “SOC interno”, puede ser un servicio externalizado o incluso mixto. Las razones principales por las que una organización delega la gestión de la seguridad en servicios externos suelen ser debidas, a una posible escasez de recursos técnicos y humanos que impiden hacer frente a las crecientes demandas de protección de datos, sistemas y aplicaciones contra amenazas cada vez más sofisticadas, además de asegurar el cumplimiento normativo.

Su principal misión es conseguir una mejor detección de incidentes de seguridad, investigar todo lo que sucede en nuestra red a nivel de seguridad y responder a debilidades e incidentes que existan o surjan en una organización. Además, un SOC envía informes a la organización al cual gestiona la seguridad informática

para que no tenga ningún problema en el cumplimiento de auditorías de seguridad y cumplimiento de la regulación vigente.

Un SOC debe recolectar y analizar datos relevantes de seguridad de varias fuentes diferentes como IDS, firewalls, aplicaciones de software, DNS, etc. Esta fotografía encaja a la perfección con el uso de sistemas SIEM, para poder extraer todos estos registros de diferentes sistemas y aplicar reglas para generar las alertas correspondientes en caso de incidentes de seguridad señalables. Debido a esto, el SOC, normalmente se apoya en un sistema SIEM para lograr sus objetivos.

Frecuentemente los SOCs utilizan fuentes de información de terceras partes para poder integrarlas con los sistemas SIEM de esta manera se obtiene un análisis más preciso del incidente. Estas terceras partes pueden ser bases de datos de amenazas, donde ya han sido analizadas anteriormente y proporcionan importante información veraz, que podría ser de gran ayuda para los SOC a la hora de gestionar los incidentes.

El proceso podría ser a la inversa, de tal manera que, amenazas desconocidas captadas por el SIEM del SOC, podrían ser enviadas a estos sistemas externos para que las analicen. Estos sistemas analizarán las amenazas, las evaluarán, decidirán su gravedad, y proporcionarán una respuesta al SOC sobre las mismas. En base a esta respuesta el SOC deberá tomar una decisión sobre el incidente dependiendo de su gravedad y además, el sistema externo añadirá esta amenaza en sus bases de datos indicando la gravedad o inocuidad de la misma para posteriores usos en todas las organizaciones que se apoyen en este sistema externo.

Los grandes SOCs suelen utilizar un sistema de tres niveles para manejar las alertas de seguridad generadas por un sistema SIEM. En las grandes organizaciones estos niveles son ocupados por personas diferentes, en cambio en organizaciones menores el personal del SOC puede pertenecer a varios niveles al mismo tiempo. Los niveles de un SOC son actúan de la siguiente manera:

- Nivel 1. Los analistas del nivel 1 se responsabilizan de monitorizar las alertas de seguridad en tiempo real y deciden si dichas alertas son reales y si son lo suficiente importantes para ser escaladas al Nivel 2, o por el contrario son tan insignificantes que deben ser cerradas inmediatamente sin realizar ninguna acción.
- Nivel 2. Los analistas del nivel 2 examinan con minuciosidad las alertas recibidas por el nivel 1 y las correlacionan con otras informaciones para comprobar si el incidente de seguridad ha ocurrido y determinan las posibles actuaciones tras el mismo. Una parte del trabajo consiste en evaluar el potencial impacto proporcionado por el incidente sobre los recursos de la organización, determinando el alcance del incidente, cual es el impacto sobre la organización, si el incidente debe ser priorizado o no, etc.
- Nivel 3. Los analistas del nivel 3, son personal experimentado en seguridad cuyas responsabilidades son:

- de manera proactiva identificar y rastrear actividad inusual y amenazas sobre la red y extinguirlas antes de que las alertas del SIEM actúen.
- Trabajar con los analistas del nivel 2 cuando una amenaza se ha detectado o ha provocado un incidente.

Como se puede apreciar, un sistema SIEM opera como la herramienta más importante dentro de un Centro de Operaciones de Seguridad.

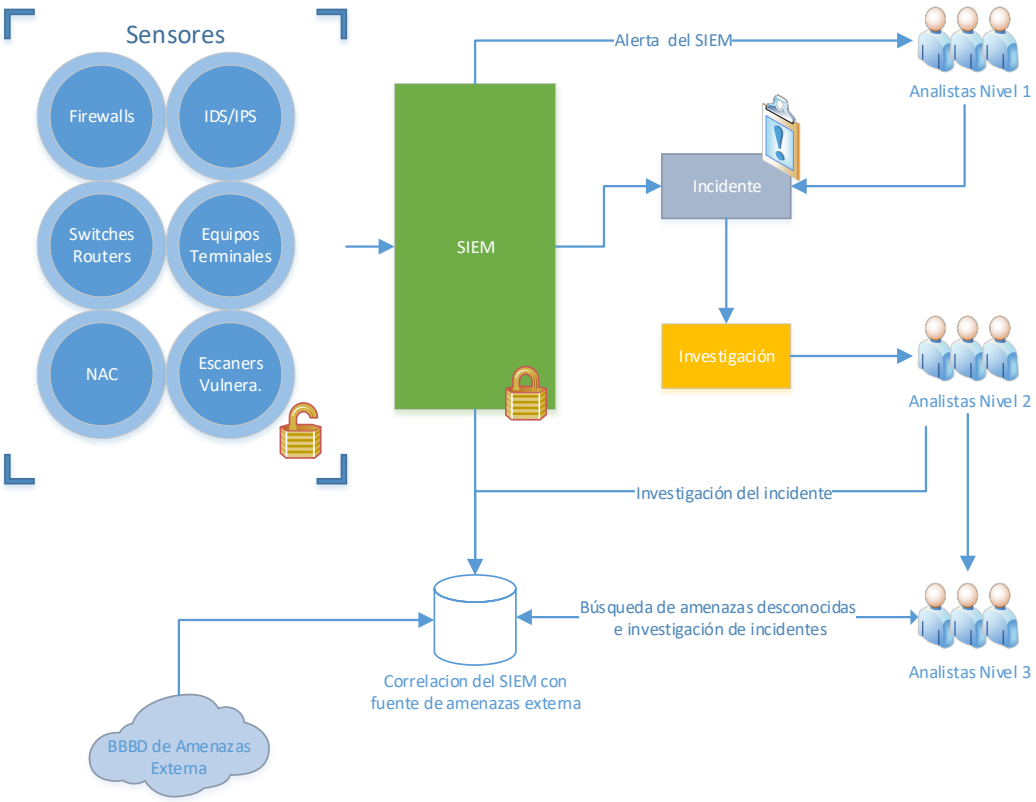


Ilustración 3.- Workflow de un SOC

2.4 Comparativa entre diferentes SIEM

La elección de un sistema SIEM es bastante complicado, básicamente depende de aquellas características que se necesiten controlar, los casos de uso necesarios.

Las organizaciones suelen adquirir SIEM sobrecargados, con todas las características y funcionalidades posibles, muchas veces anunciadas con "cantos y sirenas" por parte de los vendedores y que no se adecuan a las necesidades de la organización. De hecho, todas estas características añaden complejidad a un producto que, por su naturaleza, ya es bastante complejo en sus modelos más básicos.

Con lo cual, la elección de un SIEM deberá cubrir las necesidades y expectativas de la organización, se amoldará al tamaño adecuado de la misma en cuanto a recursos (rendimiento, almacenamiento, etc.), se deberá integrar de la mejor manera en la infraestructura existente, deberá tener un buscador de registros ágil y flexible, su sistema de visualización y generación de informes mostrando información en tiempo real, alertas e informes adecuados a la organización (ejecutivos, para auditorías, etc.) y por último se deberá considerar el precio del mismo.

En el mercado existen una variedad de sistemas SIEM, los más populares son prácticamente en toda su totalidad de pago, solamente unos pocos son open source y con características limitadas.

Para realizar la comparativa de sistemas SIEM nos basaremos en los sistemas más populares [4], y lo primero que vamos a mostrar es el Cuadrante Mágico de Gatner para los sistemas SIEM, publicado el 4 de diciembre de 2017.[2]

Ilustración 4.- Cuadrante mágico de Gatner para SIEM. Diciembre 2017

En el anterior cuadrante se puede observar que los sistemas SIEM líderes son QRadar (IBM), Splunk, LogRhythm y McAfee ESM, que también son los más populares unidos a AlientVault, ArcSight y RSA.

En la siguiente comparativa, se añadirá un nuevo producto Open Source como es ELK que, aunque por sí mismo no es un SIEM, añadiéndole plugins y configuraciones, puede llegar a tener similares características. [2][3][4].

QRadar

QRadar es un SIEM de la empresa IBM, con componentes adicionales como gestión de logs, monitorización de la red, gestión de vulnerabilidades y gestión de riesgos.

Ventajas	Inconvenientes
Se adapta a medianas y grandes organizaciones.	No integra monitorización de clientes finales (SO) (endpoints), necesita plugins de terceros.
Arquitectura flexible que soporta varios entornos. Solución disponible como física o virtual, centralizada o distribuida, también puede ser "on cloud" o cogestionada con partners de IBM QRadar.	Buen motor de búsqueda, aunque competidores como Splunk y LogRhythm lo mejoran.
Posibilidad de conectar al SIEM seguridad de terceros.	La herramienta de respuesta a incidentes (IBM Resilient) no es nativa y debe conectarse a través de la herramienta de conexión de terceros.
Buen sistema de monitorización en tiempo real e históricos.	El licenciamiento es confuso y complejo.

Splunk

Splunk está compuesto por dos componentes, la solución Enterprise (el sistema SIEM) y dos soluciones añadidas premium (Enterprise Security que analiza casos de uso y Splunk User Behavior Analytics- UBA que mejora el análisis de las consultas realizadas en la versión enterprise).

Ventajas	Inconvenientes
El SIEM con el añadido (UBA) presenta un magnífico motor de búsqueda. Podría ser el mejor junto con LogRhythm.	Elevado precio de licenciamiento.
Es un producto apreciado por los clientes.	Splunk no ofrece una versión Appliance, se debe instalar sobre hardware soportado.
Gran parque de empresas asociadas que facilita la implementación en las organizaciones.	
Puede convivir con otros sistemas, utilizando otros casos de uso, facilitando el camino para los equipos de seguridad que buscan agregar una solución SIEM a su entorno donde la infraestructura central y las fuentes de registro de eventos ya están en funcionamiento.	

LogRhythm

LogRhythm consta de varios componentes que pueden funcionar de manera conjunta sobre un appliance o de manera distribuida.

Ventajas	Inconvenientes
Es una plataforma sólida y escalable desde un solo dispositivo hasta arquitecturas de n niveles.	Difícil integración con soluciones de terceros. APIs menos abiertas a terceros que sus competidores.
Poderosa interfaz de usuario que proporciona una sólida experiencia de monitorización en tiempo real.	Dificultad de escalado para soportar volúmenes de eventos muy altos.
Integra actividades de respuesta automática y manual frente a incidentes de seguridad	
Muy adecuado para entornos ICS/SCADA	
Buen modelo de implementación y soporte a través del servicio de implementación central.	

Enterprise Security Manager – ESM

ESM es el SIEM de McAfee, con una interfaz de usuario basada en web, análisis de base de datos de eventos, capacidad de realización de informes y administración de forma centralizada otros componentes que se pueden añadir a la solución.

Ventajas	Inconvenientes
Licenciamiento simplificado para las diferentes opciones, tanto físicas como virtuales.	Peor capacidad de análisis avanzado, en comparación con otros competidores.
Se integran nativamente con otros productos McAffe.	Menor capacidad de automatización y acciones de respuesta que sus competidores.
Adecuado para entornos ICS/SCADA.	Débiles ofertas de formación en el producto. Preocupación por parte de los clientes.
Mejoría progresiva en la satisfacción del cliente, con respecto al producto.	

AlientVault

AlienVault se presenta en el mercado con dos ofertas diferentes, Unified Security Management (USM) se trata de un appliance (físico o virtual) y USM Anywhere que es una solución SaaS en la nube.

Ventajas	Inconvenientes
Incluyen capacidades de seguridad integradas, como detección de activos, IDS, escáneres de vulnerabilidades, etc.	Importantes diferencias entre las capacidades de los dos productos ofertados (appliance y la nube).
Precio del producto menor en comparación con sus competidores.	El flujo de trabajo basado en roles, la integración de tickets, el soporte para múltiples feeds de inteligencia en amenazas y capacidades de análisis avanzadas, están por detrás de los otros competidores
Tipo de licenciamiento sencillo, flexible y fácil de entender.	Orientado a pequeñas y medianas organizaciones.
Tiene un producto Open Source (OSSIM), con capacidades limitadas.	

ArcSight

ArcSight Enterprise Security Manager (ESM) es el componente principal del SIEM de Micro Focus. ESM proporciona análisis y monitorización en tiempo real, búsqueda, informes, administración de casos y flujo de trabajo.

Ventajas	Inconvenientes
Muy utilizados en SOC grandes y complejos.	Momento crítico para el producto después de ser comprado por Micro Focus. Posibilidad de descontinuación o modificaciones importantes en el mismo.
Personalización de conectores que permite la normalización de una amplia gama de fuentes de logs de seguridad.	Problemas con la complejidad y costos de su licenciamiento.
Muy flexible para la admisión de diferentes casos de uso y muy orientado al cumplimiento de políticas de seguridad y regulaciones vigentes.	Se están produciendo cambios con la introducción de nuevos módulos que pueden dar como resultado duplicación de datos.
La API permite extensas integraciones en entornos SOC.	

RSA

RSA NetWitness Suite, es un producto de Dell, enfocado en la detección de amenazas en tiempo real, respuesta a incidentes, análisis forense y casos de uso de amenazas aprovechando la captura de paquetes completos de red, eventos de seguridad y datos de registro, NetFlow y telemetría desde los puntos finales.

Ventajas	Inconvenientes
Arquitectura flexible que se extiende desde un solo dispositivo hasta implementaciones complejas.	Interfaz de usuario básica en comparación con sus competidores. RSA indica que este aspecto se mejorará con la siguiente versión.
Solución adecuada para implementación de un SOC.	Baja capacidad de administración de incidentes. Los clientes suelen necesitar comprar un añadido.
Solución única para detección de amenazas y monitorización, investigación y respuesta a eventos de seguridad	Capacidades de automatización y orquestación limitadas.

Elastic Stack

Elastic Stack es un conjunto de paquetes que funcionan de forma conjunta, la mayoría de ellas open source. Está compuesto por el motor de búsqueda, un colector de datos, agentes para endpoints, un sistema de visualización X-pack (no open source), que es un combinado de herramientas con diferentes funciones como alertas, seguridad, reportes, monitoreo, etc.

En un principio Elastic Stack es un potente gestor de eventos, pero debido a su flexibilidad se puede acercar a un sistema SIEM de altas capacidades.

Ventajas	Inconvenientes
La mayoría de sus componentes son open source.	En su forma básica no es un SIEM.
Es modular, se instalan los componentes que se necesiten.	Algún componente interesante todavía no es open source, como X-pack. Se anuncia su liberación en breve.
Tiene un potente motor de búsqueda (Elastic Search).	Nada está automatizado, hay que hacerlo uno mismo.
Tiene agentes que pueden ser instalados en servidores o desktops.	No tiene soporte, a no ser que se adquiera el producto licenciado por alguna empresa como logz.io
Se pueden conectar varios productos de terceros.	
Gartner lo presenta como una alternativa elegida por un conjunto de organizaciones debido a los altos precios que supone adquirir un SIEM y la complejidad de sacarle el rendimiento del conjunto de funcionalidades por las que se ha pagado	

Cualquiera de los productos anteriormente evaluados son candidatos fuertes para el uso empresarial, todos tienen buenos recolectores de eventos, aunque algunos productos no tengan agentes para integrar de forma nativa a los endpoints como Splunk, ESM de McAfee y AlientVault. Todos excepto Elastic Stack tienen feeds de inteligencia de amenazas y todos tienen un potente motor de búsqueda de eventos, destacando a Elastic Stack, Splunk y LogRhythm. Todos vienen preparados para el cumplimiento de políticas de seguridad y regulaciones vigentes, exceptuando Elastic Search que se debería implementar.

Algunos productos como AlientVault no son recomendables para organizaciones muy grandes.

Una máxima en la mayoría de estos productos es su coste, y la mayoría de empresas se decantan no tanto por el más adecuado para su organización si no por el más adecuado con el precio que se está dispuesto a pagar. Hay que significar que la compra de un sistema SIEM no tiene un retorno directo de la inversión y la amortización solo es evaluada en negativo. Es decir, cuando existe un incidente y el hecho de no haber adquirido uno de estos sistemas supone unas considerables pérdidas económicas en la empresa.

Para finalizar podemos determinar que, cada organización debe realizar su propia evaluación, teniendo en cuenta no solamente los puntos fuertes y débiles presentados en este trabajo u otros lugares, si no todos los demás aspectos del SIEM que puedan ser importantes para la organización. Debido a que cada implementación SIEM debe abordar un conjunto único de fuentes de registro y debe admitir diferentes combinaciones de requisitos de informes de cumplimiento, entre otras variaciones, el mejor sistema SIEM para una organización puede no ser adecuado para ninguna otra organización.

2.5 Elección, justificación y características del SIEM a implementar en la fase práctica.

Una vez evaluado algunos de los más populares sistemas SIEM existentes en nuestro mercado, lo más sencillo y a la vez lo más complicado debido a su alto precio, sería decantarnos por cualquiera de los productos anteriormente citados.

Debido a que el sistema Elastic Stack es open source en la mayor parte de sus componentes y, debido a su modularidad aquellos componentes que no son open source pueden ser reemplazados por otros con las mismas funcionalidades que si lo son. Además, la transformación de un gestor de logs, como es Elastic Stack, a un sistema SIEM puede servir de ayuda a la hora de implementar o simplemente valorar la implementación del mismo a otras organizaciones, he optado por elegir el sistema Elastic Stack como sistema SIEM a implementar en mi trabajo.

En un principio solo se usará software open source para la consecución del trabajo. Así que todos aquellos componentes de Elastic Stack que no sean open source serán descartados y reemplazados por otros. En este momento solamente el paquete X-pack de Elastic Stack no es open source, con lo cual deberá ser sustituido por otro u otros que otorguen las mismas funcionalidades, en concreto Sentinl.

Debido a que Elastic Search es un potente gestor de logs con un impresionante poder de monitorización a través de Kibana, se deberá añadir algún paquete de terceros para cubrir algunas de las necesidades importantes de un SIEM, como por ejemplo alertas, informes, correlación, etc.

3.-Desarrollo del trabajo práctico

3.1.- Laboratorio. Objetivos.

El laboratorio se ha realizado desde un PC Windows 10 Educacional, con una memoria de 8GB de RAM como maquina host de la virtualización. La virtualización se ha realizado mediante el entorno Oracle VirtualBox 5.2.8.

El objetivo del laboratorio es intentar implementar un SIEM a través del componente principal Elastic Stack, añadiéndole aplicaciones de seguridad y otros componentes para que su funcionalidad vaya más allá de un gestor de logs.

Junto a la implementación, se presentan unos casos de uso, que perfectamente pueden ser ampliados en una continuación del presente Trabajo Fin de Máster.

El laboratorio está compuesto por los siguientes componentes (servidores):

- Estación de trabajo W10.
  - Metricbeat.
  - Agente IDS.
- Estación de Trabajo Linux.
  - Metricbeat.
  - Agente IDS.
- Servidor SIEM
  - Sistema operativo Linux CentOS 7.
  - Elastic Stack (Elasticsearch, Logstash, kibana, beats)
  - Safe Search
  - IDS/IPS Wazuh
- Cortafuegos
  - Servidor CentOS 7 (Iptables).
  - Agente IDS.
  - Filebeats
- Servidor Web
  - CentOS 7 (Apache 2).
  - Agente IDS.
  - Metricbeat
- Servidor Radius
  - CentOS 7 (Freeradius 3).
  - Agente IDS.
  - Filebeat

Todo el laboratorio, exceptuando la máquina Windows 10, son máquinas virtuales independientes tal y como muestra el esquema físico de red.

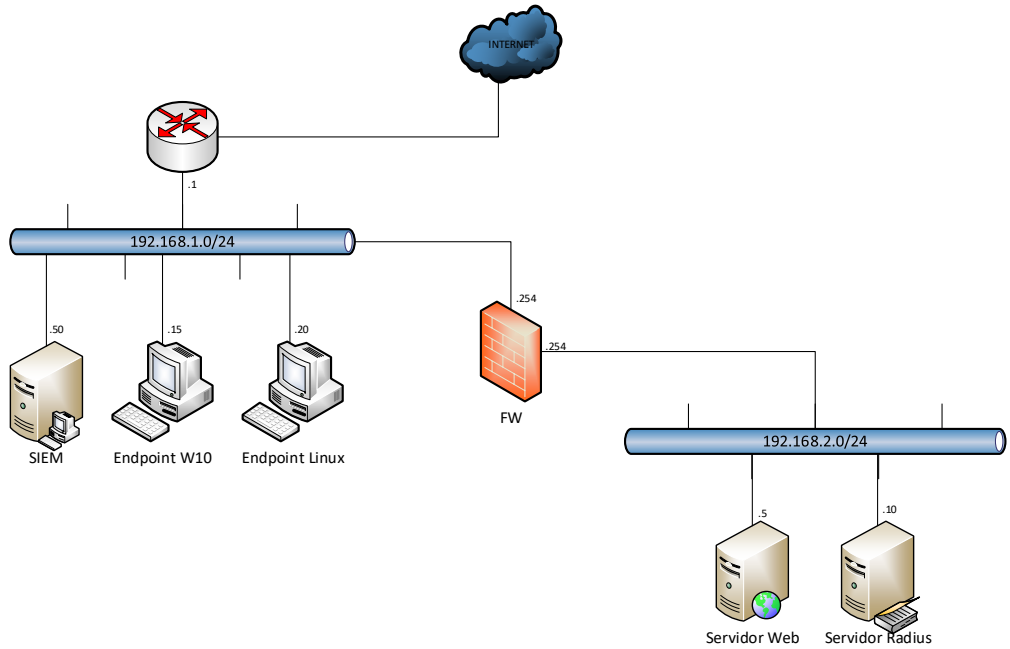


Ilustración 5.-Esquema de red del laboratorio.

El servidor SIEM consta de Elastic Stack con algunos plugins (Safe search) y el IDS/IPS Wazuh que es un fork de OSSEC HIDS, y se integra perfectamente con Elastic Stack.

La siguiente figura muestra el esquema lógico del laboratorio, con las aplicaciones y agentes instalados en cada servidor.

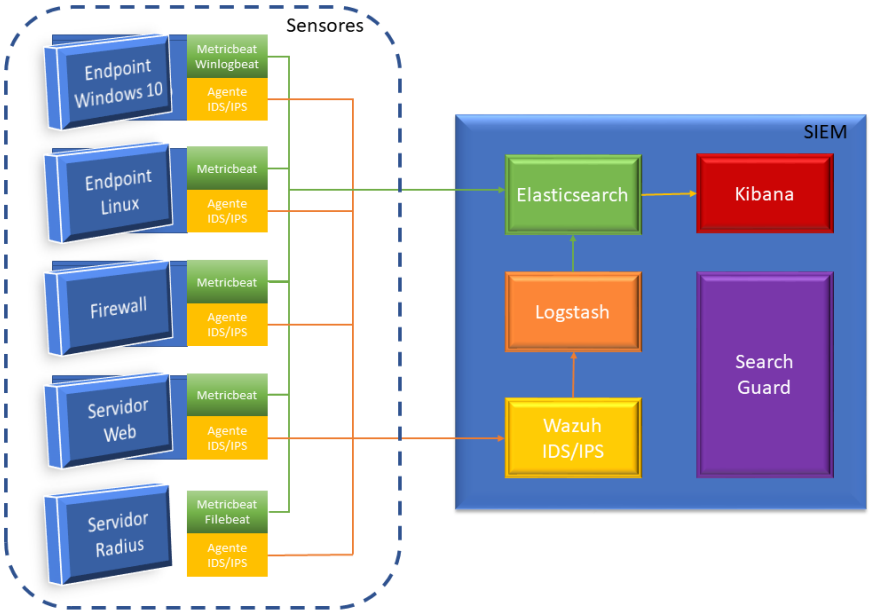


Ilustración 6.-Esquema lógico del laboratorio.

3.2.- Instalación de Elastic Stack y su entorno [6]

3.2.1.- Instalación y configuración de Elasticsearch. [6-Elasticsearch Reference]

En primer lugar, instalamos el repositorio para CentOS 7 de Elastic Stack tal y como muestra la figura.

```
[root@siem ~]# cat > /etc/yum.repos.d/elasticsearch.repo <<\EOF
[elasticsearch-6.x]
name=Elasticsearch repository for 6.x packages
baseurl=https://artifacts.elastic.co/packages/6.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF
[root@siem ~]#
```

Ilustración 7.- Instalación del repositorio de Elastic Stack.

Seguidamente instalamos Elasticsearch.

```
[root@siem ~]# yum install elasticsearch
```

Es necesario tener el java jdk instalado.

```
[root@siem ~]# yum install java-1.8.0-openjdk
```

Activamos en el arranque el servicio, para que se inicie automáticamente cuando arranca el servidor.

```
[root@siem ~]# systemctl daemon-reload
[root@siem ~]# systemctl enable elasticsearch.service
```

Por último, iniciamos elasticsearch.

```
[root@siem ~]# systemctl start elasticsearch.service
```

Y comprobamos que el arranque del servicio ha sido correcto.

```
[root@siem ~]# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: active (running) since sáb 2018-04-14 11:14:06 CEST; 21s ago
     Docs: http://www.elastic.co
 Main PID: 11092 (java)
   CGroup: /system.slice/elasticsearch.service
           └─11092 /bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=

abr 14 11:14:06 siem.uoc.edu systemd[1]: Started Elasticsearch.
abr 14 11:14:06 siem.uoc.edu systemd[1]: Starting Elasticsearch...
abr 14 11:14:06 siem.uoc.edu elasticsearch[11092]: OpenJDK 64-Bit Server VM warning: If the number of
Hint: Some lines were ellipsized, use -l to show in full.
[root@siem ~]#
```

Ilustración 8.- Esto del servicio elasticsearch.

También existe la posibilidad que elasticsearch funcione correctamente, accediendo a través del protocolo “http” contra el puerto “9200”.

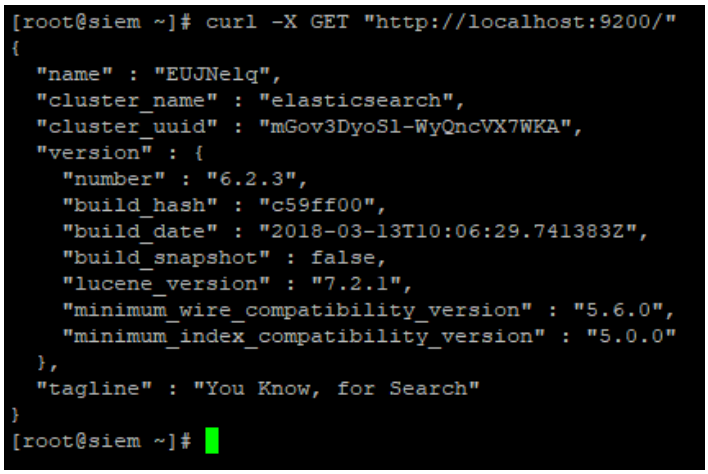


Ilustración 9.- Acceso http a elasticsearch.

En la figura anterior se puede apreciar la versión de elasticsearch y otros parámetros.

Una vez instalado elasticsearch es necesario realizar algún cambio en su configuración en el fichero *"/etc/elasticsearch/elasticsearch.yml"*

Concretamente en el apartado *network,* será necesario cambiar la variable *network.host* con la IP de la máquina donde se encuentra elasticsearch. Así podremos llamarla desde otras ubicaciones.

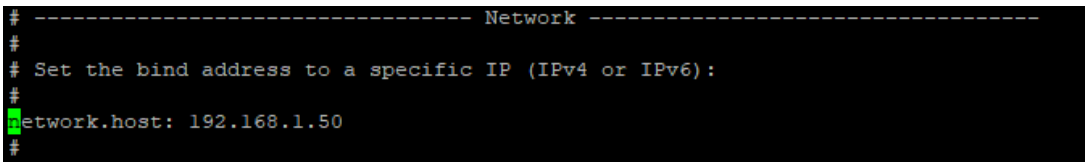


Ilustración 10.-Introducción de la IP del servidor para que se pueda llamar a elasticsearch desde otras ubicaciones.

Seguidamente se puede apreciar que se puede llamar a elasticsearch a través de la IP del servidor, tal y como muestra la siguiente figura.

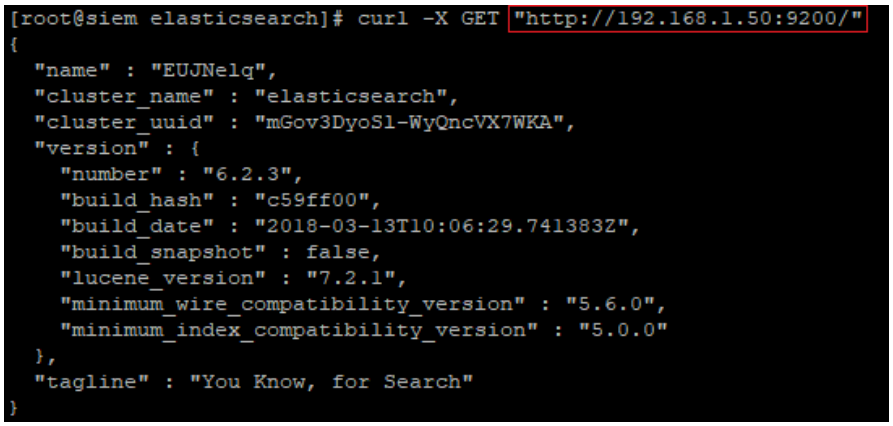


Ilustración 11.-Llamada a elasticsearch a través de la IP del servidor SIEM.

3.2.2.-Instalación de Kibana. [6-Kibana Reference]

Como ya hemos configurado el repositorio de Elastic Stack para instalar elasticsearch, directamente se instala kibana en el servidor por medio de la herramienta *"yum".*

```
[root@siem /]# yum install kibana
```

Activamos en el arranque el servicio kibana, para que se inicie automáticamente cuando arranca el servidor.

```
[root@siem /]# systemctl daemon-reload
[root@siem /]# systemctl enable kibana.service
```

En el fichero de configuración de kibana *"/etc/kibana/kibana.yml"* será necesario cambiar la dirección de elasticsearch a la IP del servidor SIEM. En nuestro caso 192.168.1.50

```
# The URL of the Elasticsearch instance to use for all your queries.
elasticsearch.url: "http://192.168.1.50:9200"
```

Y fijaremos la dirección 192.168.1.50 como IP de llamada a kibana, para poder ser accedido desde otras ubicaciones.

```
# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "192.168.1.50"
```

Una vez configurado Kibana iniciaremos el servicio.

```
[root@siem /]# systemctl start kibana.service
```

Al igual que se realizó con elasticsearch, es conveniente comprobar que el servicio Kibana arrancó correctamente.

```
[root@siem kibana]# systemctl status kibana.service
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disabled)
   Active: active (running) since sáb 2018-04-14 11:55:10 CEST; 41s ago
 Main PID: 18580 (node)
   CGroup: /system.slice/kibana.service
           └─18580 /usr/share/kibana/bin/../node/bin/node --no-warnings /usr/share/kibana/bin/../src/cli -c /etc/kibana/kibana.yml

abr 14 11:55:10 siem.uoc.edu systemd[1]: Started Kibana.
abr 14 11:55:10 siem.uoc.edu systemd[1]: Starting Kibana...
abr 14 11:55:13 siem.uoc.edu kibana[18580]: {"type":"log","@timestamp":"2018-04-14T09:55:13Z","tags":["status","plugin:kibana@6.2.3","
abr 14 11:55:13 siem.uoc.edu kibana[18580]: {"type":"log","@timestamp":"2018-04-14T09:55:13Z","tags":["status","plugin:elasticsearch@6.
abr 14 11:55:14 siem.uoc.edu kibana[18580]: {"type":"log","@timestamp":"2018-04-14T09:55:14Z","tags":["status","plugin:timelion@6.2.3",
abr 14 11:55:14 siem.uoc.edu kibana[18580]: {"type":"log","@timestamp":"2018-04-14T09:55:14Z","tags":["status","plugin:console@6.2.3","
abr 14 11:55:14 siem.uoc.edu kibana[18580]: {"type":"log","@timestamp":"2018-04-14T09:55:14Z","tags":["status","plugin:metrics@6.2.3","
abr 14 11:55:14 siem.uoc.edu kibana[18580]: {"type":"log","@timestamp":"2018-04-14T09:55:14Z","tags":["listening","info"],"pid":18580,"
abr 14 11:55:14 siem.uoc.edu kibana[18580]: {"type":"log","@timestamp":"2018-04-14T09:55:14Z","tags":["status","plugin:elasticsearch@6.
Hint: Some lines were ellipsized, use -l to show in full.
[root@siem kibana]#
```

Es obligatorio permitir el acceso, desde el firewall del SIEM, para poder acceder a kibana desde cualquier ubicación. El servicio Kibana escucha en el puerto 5601

```
[root@siem /]# firewall-cmd --zone=public --add-port=5601/tcp
success
[root@siem /]# firewall-cmd --zone=public --permanent --add-port=5601/tcp
success
[root@siem /]#
```

Por medio de un navegador web se podrá acceder mediante la url http://192.168.1.50:5601 a la web de Kibana, tal y como muestra la siguiente figura.

Ilustración 12.-Aplicación web de Kibana.

Con la instalación de Elasticsearch y Kibana ya tenemos en funcionamiento un gestor de logs. Claramente este gestor de logs no tiene ningun registro, ya que no se le ha conectado ninguna fuente de datos. Sin embargo el proposito de este trabajo va un poco mas allá de solamente implementar un gestor de datos y debe de proporcionarsele otras capacidades para que se asemeje a un SIEM.

3.3.-Seguridad del SIEM. Search Guard. [8]

Tal y como se encuentra en estos momentos el SIEM (todavía gestor de logs), se observa que no existe ningun tipo de seguridad. El acceso a kibana es libre solo con conocer la url es accesible, además la conexión contra elasticsearch no es bajo ssl y también sin nombre de usuario y contraseña como Kibana.

Search Guard es un plugin de elasticsearch, que proporciona seguridad de acceso a Kibana, presentando un frontal web de acceso a kibana con una página que debemos introducir las credenciales. También proporciona seguridad a elasticsearch, obligando a acceder mediante ssl y con credenciales.

En el directorio *"/usr/share/elasticsearch/bin"* se encuentra el binario para instalar los plugings "elasticsearch-plugin"

```
[root@siem bin]# pwd
/usr/share/elasticsearch/bin
[root@siem bin]# ll
total 20
-rwxr-xr-x. 1 root root 1557 mar 13 11:08 elasticsearch
-rwxr-xr-x. 1 root root 2207 mar 13 11:08 elasticsearch-env
-rwxr-xr-x. 1 root root  239 mar 13 11:08 elasticsearch-keystore
-rwxr-xr-x. 1 root root  229 mar 13 11:08 elasticsearch-plugin
-rwxr-xr-x. 1 root root  242 mar 13 11:08 elasticsearch-translog
[root@siem bin]#
```

Ilustración 13.- Herramienta elasticsearch-plugin.

Desde el directorio *"usr/share/elasticsearch/bin"* será necesario escribir el siguiente comando, observando que la versión del plugin debe coincidir con la versión de elasticsearch. En este caso la versión de elasticsearch es la 6.2.3.

```
[root@siem elasticsearch]# bin/elasticsearch-plugin install -b com.floragunn:search-guard-6:6.2.3-22.0
```

Para instalar el plugin de search guard para Kibana debemos descargar la versión correcta de la siguiente dirección: https://search.maven.org/#search%7Cgav%7C1%7Cg%3A%22com.floragunn%22%20AND%20a%3A%22search-guard-kibana-plugin%22

Y elegir la versión correcta como en elasticsearch, en este caso la 6.2.3 como anteriormente indicamos.

Una vez obra en nuestro poder el plugin, se instala.

```
[root@siem kibana]# ./bin/kibana-plugin install file:///root/search-guard-kibana-plugin-6.2.3-11.zip
```

Una vez está instalado el plugin de Elasticsearch y Kibana, es necesario generar unos certificados para poder ejecutar search guard en producción. Para ello nos descargamos una herramienta de generación de certificados que nos ofrece el mismo search guard en la dirección https://search.maven.org/#search%7Cga%7C1%7Ca%3A%22search-guard-tlstool%22

En este caso se ha optado por descargar el paquete "search-guard-tlstool-1.1.tar" y se procede a su descomprensión.

```
[root@siem ~]#  tar -xvzf search-guard-tlstool-1.1.tar.gz
```

A partir de aquí con la herramienta generamos los certificados apoyándonos en el fichero de ejemplo "config/example.yml".

```
[root@siem ~]# tools/sgtlstool.sh -c ./config/example.yml -ca -crt
```

Con este comando se obtienen los certificados y un fichero donde están las líneas que son necesarios añadir al fichero de configuración de elasticsearch *"/etc/elasticsearch/elasticsearch.yml".*

```
[root@siem out]# ll
total 52
-rw-r--r--. 1 root root  472 abr 15 00:33 client-certificates.readme
-rw-r--r--. 1 root root 1801 abr 15 00:33 ljasomar.key
-rw-r--r--. 1 root root 2937 abr 15 00:33 ljasomar.pem
-rw-r--r--. 1 root root 1801 abr 15 00:33 luismi.key
-rw-r--r--. 1 root root 2937 abr 15 00:33 luismi.pem
-rw-r--r--. 1 root root 1222 abr 15 00:33 node1_elasticsearch_config_snippet.yml
-rw-r--r--. 1 root root 1801 abr 15 00:33 node1_http.key
-rw-r--r--. 1 root root 2973 abr 15 00:33 node1_http.pem
-rw-r--r--. 1 root root 1801 abr 15 00:33 node1.key
-rw-r--r--. 1 root root 2973 abr 15 00:33 node1.pem
-rw-r--r--. 1 root root 1801 abr 15 00:33 root-ca.key
-rw-r--r--. 1 root root 1363 abr 15 00:33 root-ca.pem
-rw-r--r--. 1 root root  309 abr 15 00:33 root-ca.readme
[root@siem out]# vi node1_elasticsearch_config_snippet.yml
[root@siem out]#
```

Ilustración 14.-Certificados y fichero de configuración para elasticsearch

```
searchguard.ssl.transport.pemcert_filepath: node1.pem
searchguard.ssl.transport.pemkey_filepath: node1.key
searchguard.ssl.transport.pemkey_password: XYXWRCnat2zR
searchguard.ssl.transport.pemtrustedcas_filepath: root-ca.pem
searchguard.ssl.transport.enforce_hostname_verification: false
searchguard.ssl.transport.resolve_hostname: false
searchguard.ssl.http.enabled: true
searchguard.ssl.http.pemcert_filepath: node1_http.pem
searchguard.ssl.http.pemkey_filepath: node1_http.key
searchguard.ssl.http.pemkey_password: sHPpXvOhA3S6
searchguard.ssl.http.pemtrustedcas_filepath: root-ca.pem
searchguard.nodes_dn:
- CN=node1.luismi.com,OU=Ops,O=luismi Com\, Inc.,DC=luismi,DC=com
searchguard.authcz.admin_dn:
- CN=ljasomar.luismi.com,OU=Ops,O=luismi Com\, Inc.,DC=luismi,DC=com
~
```

Ilustración 15.-Líneas a añadir al fichero de configuración de elasticsearch.

Como se ha instalado la versión comunidad del plugin, también se debe añadir al fichero de configuración de elasticsearch la siguiente línea:

```
searchguard.ssl.http.pemtrustedcas_filepath: certs/root-ca.pem
searchguard.nodes_dn:
- CN=node1.luismi.com,OU=Ops,O=luismi Com\, Inc.,DC=luismi,DC=com
searchguard.authcz.admin_dn:
- CN=ljasomar.luismi.com,OU=Ops,O=luismi Com\, Inc.,DC=luismi,DC=com

searchguard.enterprise_modules_enabled: false
```

Ilustración 16.- Desactivación versión Enterprise de Search Guard

Seguidamente se generaran los usuarios necesarios para poder acceder a elasticsearch y kibana. Para ello accedemos al fichero "sg_internal_users.yml" situado en el directorio "/usr/share/elasticsearch/plugins/search-guard-6/sgconfig", como muestra la siguiente figura.

```
[root@siem sgconfig]# pwd
/usr/share/elasticsearch/plugins/search-guard-6/sgconfig
[root@siem sgconfig]# ll
total 44
-rw-r--r--. 1 root root 9499 abr 14 17:44 elasticsearch.yml.example
-rw-r--r--. 1 root root 2332 abr 14 17:44 sg_action_groups.yml
-rw-r--r--. 1 root root 9629 abr 14 17:44 sg_config.yml
-rw-r--r--. 1 root root 1144 abr 21 12:13 sg_internal_users.yml
-rw-r--r--. 1 root root  548 abr 14 17:44 sg_roles_mapping.yml
-rw-r--r--. 1 root root 6288 abr 21 10:39 sg_roles.yml
[root@siem sgconfig]#
```

Ilustración 17.Localización del fichero "sg_internal_users.yml"

Se necesitará editar el fichero y añadir los usuarios con los roles correspondientes. En este trabajo solo hemos editado el usuario admin, cambiándole la contraseña (generando el hash con la herramienta hash que se encuentra en el directorio "plugin/tool" y proporcionándole rol de admin.

```
# This is the internal user database
# The hash value is a bcrypt hash and can be generated with plugin/tools/hash.sh

admin:
  readonly: true
  hash: $2y$12$5oel9rCbxul8Ub3KMfwqLu4Oaf2TewtfkgzF5aZf.RI39fxmTjzTq
  roles:
  #  - readall
  #  - writeall
  #  - sg_own_index
  #  - sg_readall
     - admin
```

Ilustración 18.-Usuario admin en Search Guard

Se tienen que copiar los certificados, anteriormente generados, a una carpeta donde puedan ser leídos. En el presente trabajo se han copiado a la carpeta *"/usr/share/elasticsearch/certs*", como indica la siguiente figura. Los certificados importantes son la CA, y los correspondientes a "ljasomar.pem" y "ljasomar.key", ya que es un usuario registrado en elasticsearch en su configuración.

```
[root@siem certs]# pwd
/usr/share/elasticsearch/certs
[root@siem certs]# ll
total 52
-rw-r--r--. 1 root root  472 abr 15 00:33 client-certificates.readme
-rw-r--r--. 1 root root 1801 abr 15 00:33 ljasomar.key
-rw-r--r--. 1 root root 2937 abr 15 00:33 ljasomar.pem
-rw-r--r--. 1 root root 1801 abr 15 00:33 luismi.key
-rw-r--r--. 1 root root 2937 abr 15 00:33 luismi.pem
-rw-r--r--. 1 root root 1222 abr 15 00:33 node1_elasticsearch_config_snippet.yml
-rw-r--r--. 1 root root 1801 abr 15 00:33 node1_http.key
-rw-r--r--. 1 root root 2973 abr 15 00:33 node1_http.pem
-rw-r--r--. 1 root root 1801 abr 15 00:33 node1.key
-rw-r--r--. 1 root root 2973 abr 15 00:33 node1.pem
-rw-r--r--. 1 root root 1801 abr 15 00:33 root-ca.key
-rw-r--r--. 1 root root 1363 abr 15 00:33 root-ca.pem
-rw-r--r--. 1 root root  309 abr 15 00:33 root-ca.readme
[root@siem certs]#
```

Ilustración 19.-Certificados necesarios

Desde el directorio que indica la siguiente figura lanzamos la herramienta "sgadmin.sh" para que recoja los cambios realizados en el fichero "sg_internal_users.yml" y tengamos un usuario disponible en Search Guard que pueda administrar a Kibana y Elasticsearch.

```
[root@siem tools]# pwd
/usr/share/elasticsearch/plugins/search-guard-6/tools
[root@siem tools]# ll
total 36
-rw-r--r--. 1 root root   214 abr 14 17:44 hash.bat
-rwxr-xr-x. 1 root root   373 abr 14 17:44 hash.sh
-rw-r--r--. 1 root root 18994 abr 14 17:44 install_demo_configuration.sh
-rw-r--r--. 1 root root   282 abr 14 17:44 sgadmin.bat
-rwxr-xr-x. 1 root root   414 abr 14 17:44 sgadmin.sh
[root@siem tools]#
```

Ilustración 20.-Herramienta sgadmin.sh para generar usuarios y sus roles

En el comando será obligatorio indicar la CA, el certificado y key de uno de los usuarios existentes en la configuración de elasticsearch, con su contraseña. La contraseña del usuario ljasomar se encuentra en la carpeta donde están todos los certificados. Concretamente en el fichero "client-certificates.readme".

```
[root@siem tools]#  ./sgadmin.sh -cd ../sgconfig/ -h 192.168.1.50 -icl -nhnv
-cacert ../../../certs/root-ca.pem -cert ../../../certs/ljasomar.pem -key ../
../../certs/ljasomar.key -keypass KFGKGdmv06zm
```

Ilustración 21.- Comando para generar usuarios y roles en search guard.

```
Client certificates are used to authenticate REST clients against your authentication backend
Thus, the users represented by the client certificates must be also present in your authentic

See http://docs.search-guard.com/latest/client-certificate-auth for more on this topic.


CN=luismi.luismi.com,OU=Ops,O=luismi Com\, Inc.,DC=luismi,DC=com Password: vcDqsn8euJAq
CN=ljasomar.luismi.com,OU=Ops,O=luismi Com\, Inc.,DC=luismi,DC=com Password: KFGKGdmv06zm
```

Ilustración 22.-Credenciales del cliente ljasomar y luismi.

Ya está securizado Elastic Stack mediante el plugin Search Guard. Las siguientes figuras demuestran que el acceso a Elastic está securizado.

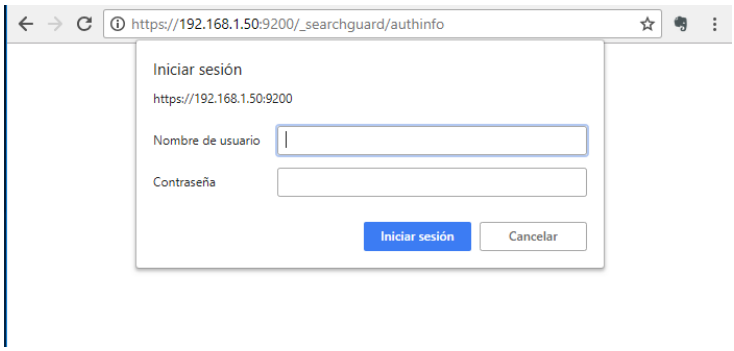


Ilustración 23.-Acceso a Elasticsearch obligatorio por https y con credenciales.

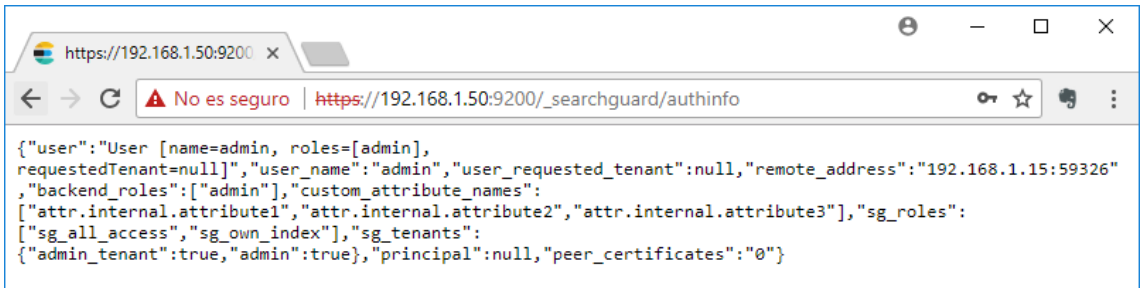
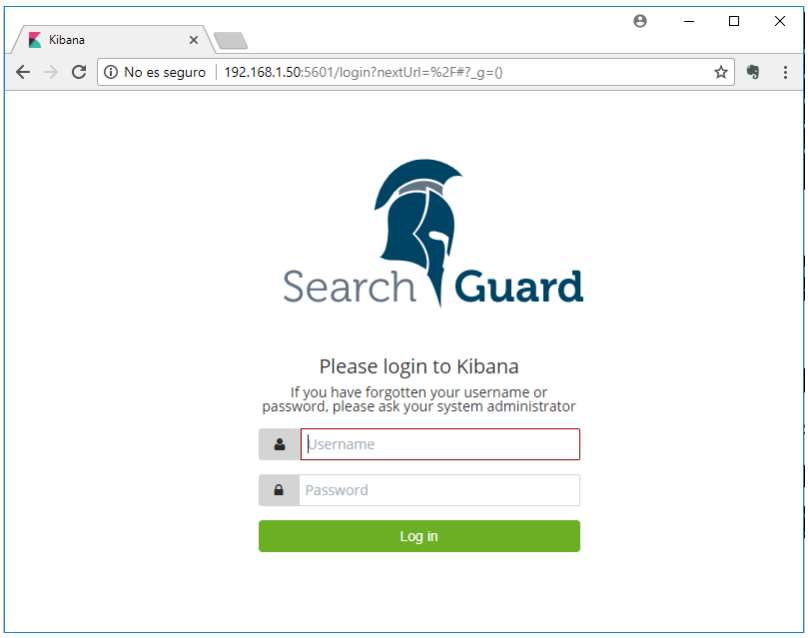


Ilustración 24.-Privilegios del usuario admin en Elasticsearch después de introducir credenciales.

La siguiente figura muestra que el acceso a Kibana ya no es libre, se necesitan introducir credenciales válidas.

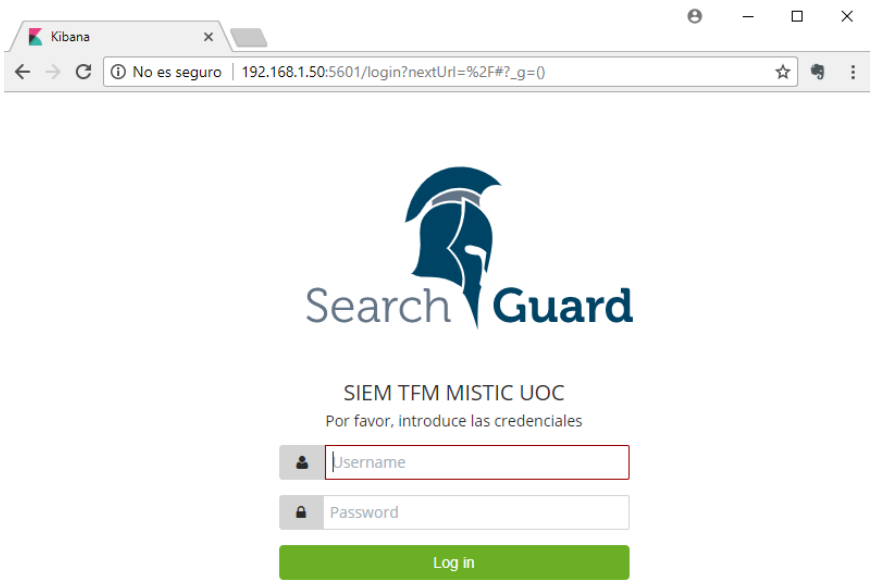


Si se desea, se puede cambiar el logo y los textos de la página de login que Search Guard proporciona para Kibana. En el fichero de configuración de Elasticsearch se pueden añadir líneas como las que muestra la ilustración 27.

Ilustración 25.-Acceso a Kibana securizado por Search Guard.

```
searchguard.basicauth.login.subtitle: "Por favor, introduce las credenciales"
searchguard.basicauth.login.title: "SIEM TFM MISTIC UOC"
```

Ilustración 26.-Personalización de la página de login de Kibana.



En la ilustración 27 se observa como el acceso a Kibana mediante Search Guard ha sido customizado colocando el nombre de la universidad y colocando la indicación de introducir las credenciales en castellano.

Ilustración 27.-Página de Login de Kibana personalizada.

Por último, es primordial colocar el servidor SIEM en hora, para que los logs estén adecuados al tiempo real.

```
[root@siem out]# yum install ntp
[root@siem out]# systemctl start ntpd.service
[root@siem out]# systemctl enable ntpd.service
```

3.4.- Instalación del HIDS/IPS – Wazuh [7]

Wazuh es un sistema de detección de intrusos open source (se trata de un fork de OSSEC), que realiza análisis de registro, FIM, detección de rootkits, alertas y respuesta activa (IPS). Wazuh se integra perfectamente con Elastic Stack y tiene plugins para poder utilizar otras interesantes aplicaciones, como “VirusTotal”, “OpenScap”, etc.

Para poder instalar el IDS/IPS Wazuh, se debe crear el repositorio de wazuh, como muestra la siguiente figura.

```
[root@siem out]# cat > /etc/yum.repos.d/wazuh.repo <<\EOF
> [wazuh_repo]
> gpgcheck=1
> gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
> enabled=1
> name=Wazuh repository
> baseurl=https://packages.wazuh.com/3.x/yum/
> protect=1
> EOF
```

Ilustración 28.- Creación del repositorio para wazuh.

Una vez creado el repositorio instalamos wazuh y comprobamos que su servicio funcione correctamente.

```
[root@siem out]# yum install wazuh-manager
```

```
[root@siem out]# systemctl status wazuh-manager
● wazuh-manager.service - SYSV: Starts and stops Wazuh (Host Intrusion Detection System)
   Loaded: loaded (/etc/rc.d/init.d/wazuh-manager; bad; vendor preset: disabled)
   Active: active (running) since lun 2018-04-16 22:47:42 CEST; 2min 3s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 23969 ExecStart=/etc/rc.d/init.d/wazuh-manager start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/wazuh-manager.service
           ├─23990 /var/ossec/bin/wazuh-db
           ├─24004 /var/ossec/bin/wazuh-modulesd
           ├─24013 /var/ossec/bin/ossec-execd
           ├─24018 /var/ossec/bin/ossec-analysisd
           ├─24024 /var/ossec/bin/ossec-syscheckd
           ├─24029 /var/ossec/bin/ossec-remoted
           ├─24043 /var/ossec/bin/ossec-logcollector
           └─24047 /var/ossec/bin/ossec-monitord

abr 16 22:47:38 siem.uoc.edu systemd[1]: Starting SYSV: Starts and stops Wazuh (Host Intrusion Detection System)...
abr 16 22:47:42 siem.uoc.edu wazuh-manager[23969]: Starting OSSEC: [  OK  ]
abr 16 22:47:42 siem.uoc.edu systemd[1]: Started SYSV: Starts and stops Wazuh (Host Intrusion Detection System).
[root@siem out]#
```

Ilustración 29.-Estado del servicio de wazuh-manager.

Es necesario instalar NodeJS para poder utilizar la API de Wazuh y para ello se configurará el repositorio y se instalará el paquete.

```
[root@siem ~]# curl --silent --location https://rpm.nodesource.com/setup_6.x | bash -
```

```
[root@siem ~]# yum install nodejs
```

Debe comprobarse que “Python” está instalado. Con comprobar la versión averiguaremos si está instalado. CentOS 7 trae instalada la versión 2.7.5 de Python, en su versión mínima de servidor.

```
[root@siem ~]# python --version
Python 2.7.5
```

Ilustración 30.- Versión de python.

Una vez sabemos está instalado Python, procedemos a instalar la API de wazuh.

```
[root@siem ~]# yum install wazuh-api
```

La siguiente figura muestra el correcto funcionamiento de wazuh-api.

```
[root@siem ~]# systemctl status wazuh-api
● wazuh-api.service - Wazuh API daemon
   Loaded: loaded (/etc/systemd/system/wazuh-api.service; enabled; vendor preset: disabled)
   Active: active (running) since mar 2018-04-17 03:34:25 CEST; 1min 58s ago
     Docs: http://wazuh-documentation.readthedocs.org/en/latest/ossec_api.html
 Main PID: 25519 (node)
   CGroup: /system.slice/wazuh-api.service
           └─25519 /bin/node /var/ossec/api/app.js

abr 17 03:34:25 siem.uoc.edu systemd[1]: Started Wazuh API daemon.
abr 17 03:34:25 siem.uoc.edu systemd[1]: Starting Wazuh API daemon...
```

Ilustración 31.-Estado de servicio API de wazuh.

Para integrar Elastic Stack con Wazuh, si las dos aplicaciones se están ejecutando en el mismo servidor será necesario instalar Logstash, que es un módulo de Elastic Stack.

```
[root@siem ~]# yum install logstash
```

En la url https://raw.githubusercontent.com/wazuh/wazuh/3.2/extensions/logstash/01-wazuh-local.conf disponemos de una configuración base de logstash, copiamos el fichero en *"/etc/logstash/conf.d/01-wazuh.conf"* y la editamos convenientemente.

```
# Fichero de configuración wazuh - logstash ssl
## Local Wazuh Manager - JSON file input
input {
    file {
        type => "wazuh-alerts"
        path => "/var/ossec/logs/alerts/alerts.json"
        codec => "json"
    }
}
filter {
    if [data][srcip] {
        mutate {
            add_field => [ "@src_ip", "%{[data][srcip]}" ]
        }
    }
    if [data][aws][sourceIPAddress] {
        mutate {
            add_field => [ "@src_ip", "%{[data][aws][sourceIPAddress]}" ]
        }
    }
}
filter {
    geoip {
        source => "@src_ip"
        target => "GeoLocation"
        fields => ["city_name", "continent_code", "country_code2", "country_name", "region_name", "location"]
    }
    date {
        match => ["timestamp", "ISO8601"]
        target => "@timestamp"
    }
    mutate {
        remove_field => [ "timestamp", "beat", "input_type", "tags", "count", "@version", "log", "offset", "type","@src_ip"]
    }
}
output {
    elasticsearch {
        hosts => ["192.168.1.50:9200"]
        user => admin
        password => Secret
        ssl => true
        ssl_certificate_verification => true
        cacert => "/usr/share/elasticsearch/certs/root-ca.pem"
        index => "wazuh-alerts-3.x-%{+YYYY.MM.dd}"
        document_type => "wazuh"
    }
}
```

Ilustración 32.- Fichero de configuración de Logstash, para la integración con wazuh.

Al ser obligatorio conectar a Elasticsearch mediante SSL, el apartado "output" del fichero será necesario editarlo y dejarlo como muestra la figura anterior.

Es necesario añadir el usuario "logstash" al grupo "ossec", para que el usuario "logstash" tenga los privilegios adecuados.

```
[root@siem conf.d]# usermod -a -G ossec logstash
```

Posteriormente se habilita que el servicio Logstash se inicie automáticamente en el arranque del servidor SIEM y se arranca el servicio Logstash.

```
[root@siem ~]# systemctl daemon-reload
[root@siem ~]# systemctl enable logstash.service
```

```
[root@siem ~]# systemctl start logstash.service
```

Es necesario cargar una plantilla JSON que proporciona wazuh, para Elasticsearch. Primero es necesario descargarla y seguidamente cargarla en Elasticsearch. Es obligatorio proporcionar las credenciales de admin generadas con Search Guard, para poder cargar la plantilla en Elasticsearch.

```
[root@siem ~]#  curl https://raw.githubusercontent.com/wazuh/wazuh/3.2/extensions/elast
icsearch/wazuh-elastic6-template-alerts.json | curl -XPUT -u admin:XXXXX 'https://192.1
68.1.50:9200/_template/wazuh' -H 'Content-Type: application/json' -d @- -k
```

Ilustración 33.-Descargado y cargado de la plantilla JSON de Wazuh para Elasticsearch.

Se recomienda aumentar el heap de memoria límite Node.js, para evitar problemas de desborde de memoria cuando instalamos Wazuh App.

```
[root@siem ~]# export NODE_OPTIONS="--max-old-space-size=3072"
```

Una vez integrado Wazuh con Elasticsearch, queda integrarlo con Kibana. Para ello, instalamos el plugin de wazuh para Kibana (debe corresponder con la versión de Elastic Stack, en el presente trabajo 6.2.3).

```
[root@siem ~]# /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/w
azuhapp/wazuhapp-3.2.1_6.2.3.zip
```

Ilustración 34.-Plugin de Wazuh para Kibana.

Al acceder a Kibana, ahora tenemos integrado en el SIEM el control y reporting del IDS Wazuh, tal y como se aprecia en la siguiente figura. Para poder ser utilizado es primordial configurar la API de Wazuh, como muestra la figura. Las credenciales son las de admin, proporcionadas en apartados anteriores a Search Guard. El puerto debe ser el 55000.

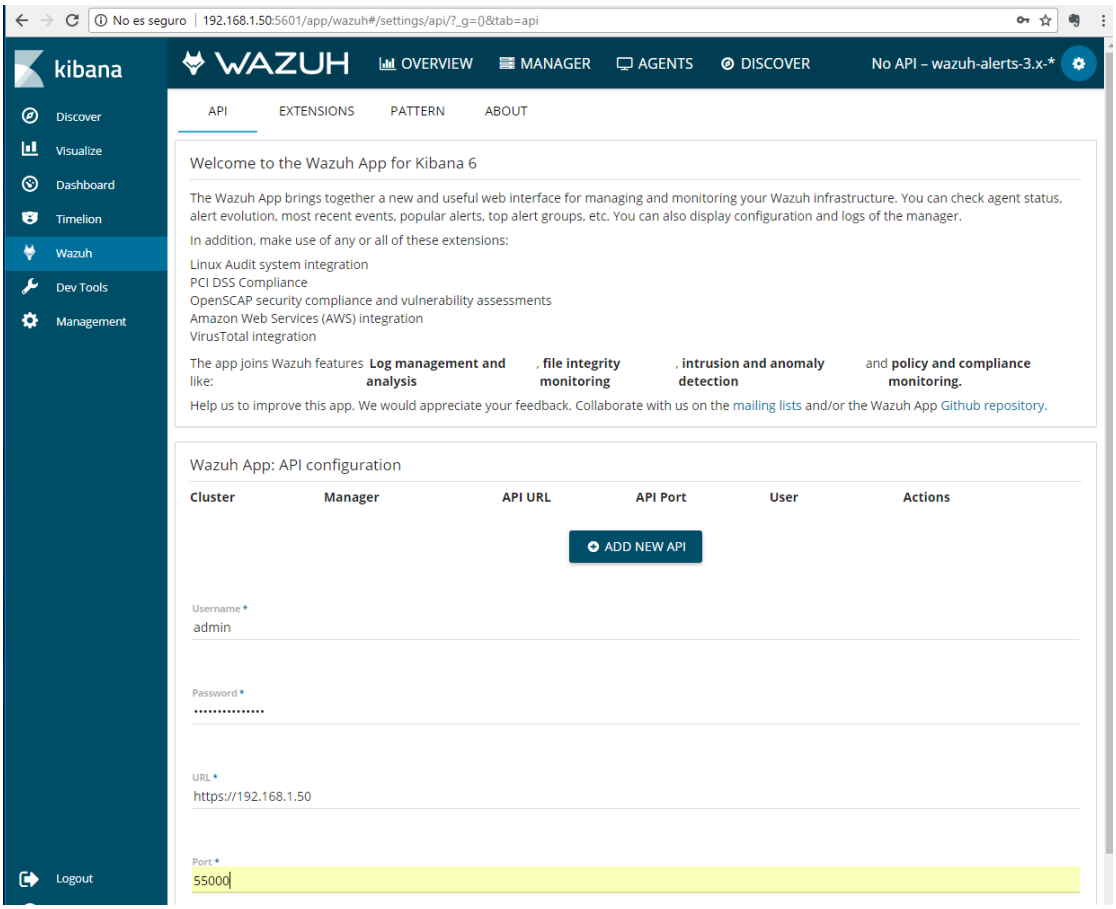


Ilustración 35.-Wazuh integrado en Kibana, mostrando la configuración de la API de Wazuh.

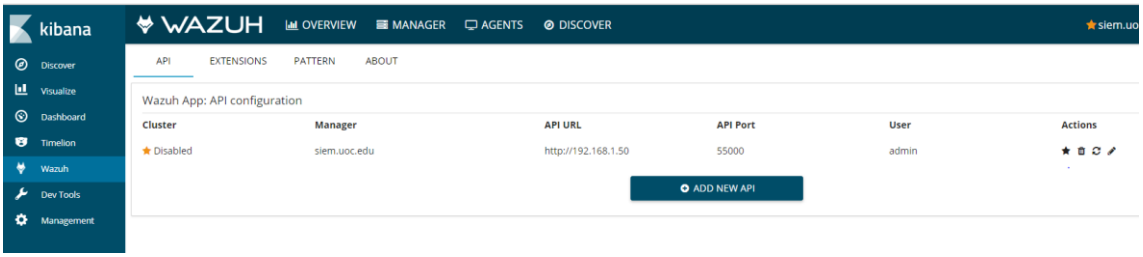


Ilustración 36.-API de Wazuh configurada e IDS listo para ser usado.

Ya está el IDS/IPS listo para ser usado, ahora debemos instalar los agentes en las máquinas que vamos a controlar.

Como las máquinas son externas al SIEM, para que este pueda recibir las alertas de las mismas es obligatorio abrir el puerto 1514/udp para la comunicación entre los agentes de las máquinas y el SIEM.

```
[root@siem etc]# firewall-cmd --zone=public --add-port=1514/udp
```

```
[root@siem etc]# firewall-cmd --permanent --zone=public --add-port=1514/udp
```

Los agentes de las máquinas (Sensores) para wazuh se instalan de igual forma, con lo cual en este trabajo mostraremos la instalación de uno de ellos. El agente donde se muestra la instalación será en el cortafuegos “fw.uoc.edu”.

Para la instalación del agente se descarga la última versión, acorde con el sistema operativo empleado y se instala. Para el cortafuegos descargaremos el paquete rpm de 64 bits.

```
[root@fw ~]# wget https://packages.wazuh.com/3.x/yum/wazuh-agent-3.2.1-1.x86_64.rpm
```

```
[root@fw ~]# yum localinstall wazuh-agent-3.2.1-1.x86_64.rpm
```

Posteriormente hay que registrar la máquina en el SIEM, a través de la herramienta “manage_agents” que proporciona wazuh, tal y como muestra la siguiente figura.

```
[root@siem ~]# /var/ossec/bin/manage_agents


****************************************
* Wazuh v3.2.1 Agent manager.          *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

Elegimos añadir un agente (A), y proporcionamos los datos del cortafuegos.

```
****************************************
* Wazuh v3.2.1 Agent manager.          *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: fw.uoc.edu
   * The IP Address of the new agent: 192.168.1.254
   * An ID for the new agent[002]:
Agent information:
   ID:002
   Name:fw.uoc.edu
   IP Address:192.168.1.254

Confirm adding it?(y/n): y
Agent added with ID 002.
```

Ilustración 37.- Registro de un agente en el SIEM.

Después de haber registrado el agente en el SIEM, es necesario trasladar la clave generada (Key) en el SIEM al agente de la máquina remota. En este caso el cortafuegos fw.ouc.edu.

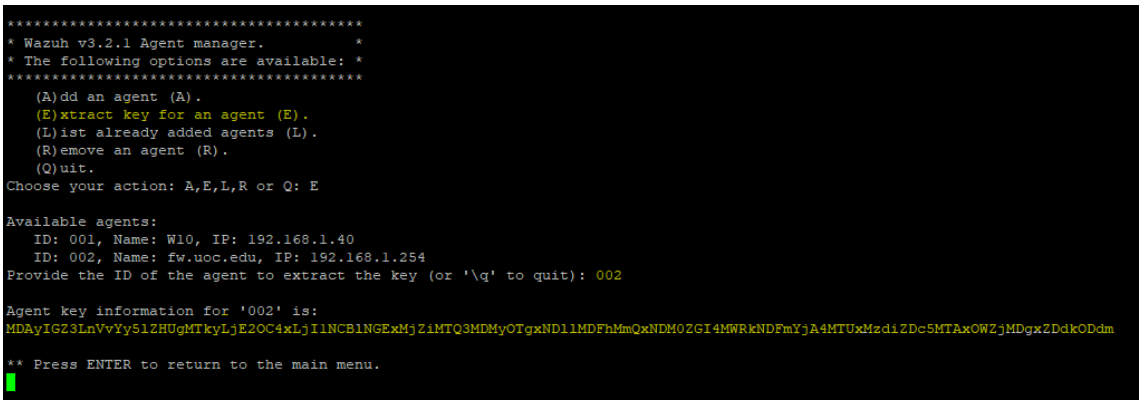


Ilustración 38.- Extracción de la clave, en el SIEM, de la máquina "fw.ouc.edu" para poder ser trasladado a la misma.

Ahora desde la máquina cliente, "fw.ouc.edu" se importa la clave copiada anteriormente y añadimos el agente. Con la herramienta "manage_agents", pero esta vez lanzada desde la máquina cliente.

Ilustración 39.-Importación de la clave del SIEM para fw.ouc.edu desde el cliente.

Ahora es necesario en el cliente, apuntar al servidor donde se encuentra el SIEM, mediante el fichero "/var/ossec/etc/ossec.conf". Se coloca la IP del SIEM.

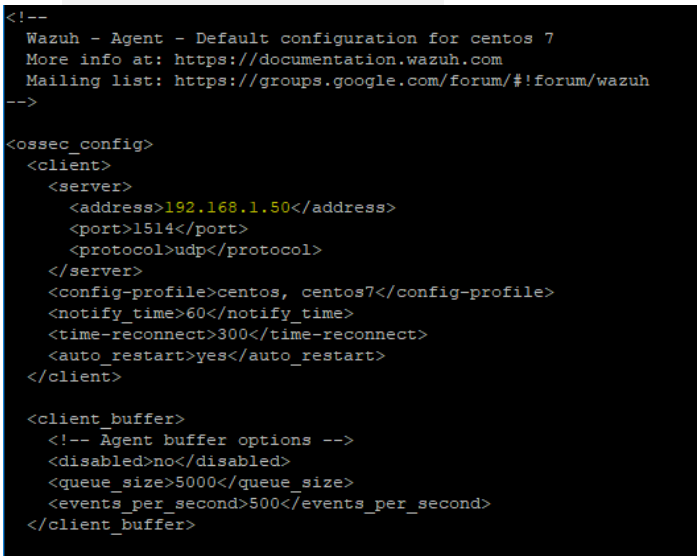


Ilustración 40.-Fichero ossec.conf en el cliente, apuntando hacia el SIEM (192.168.1.50).

Para finalizar, en el cliente arrancamos el servicio “ossec-control” y ya está registrado el cortafuegos “fw.uoc.edu” en el SIEM, más concretamente en el IDS Wazuh.

```
[root@fw etc]# /var/ossec/bin/ossec-control restart
ossec-logcollector not running ..
ossec-syscheckd not running ..
ossec-agentd not running ..
ossec-execd not running ..
wazuh-modulesd not running ..
Wazuh v3.2.1 Stopped
Starting Wazuh v3.2.1 (maintained by Wazuh Inc.)...
Started wazuh-modulesd...
Started ossec-execd...
2018/04/30 18:38:30 ossec-agentd: INFO: Using notify time: 60 and max time to reconnect: 300
Started ossec-agentd...
Started ossec-syscheckd...
Started ossec-logcollector...
Completed.
```

Ilustración 41.- Inicio del agente en el cliente fw.uoc.edu

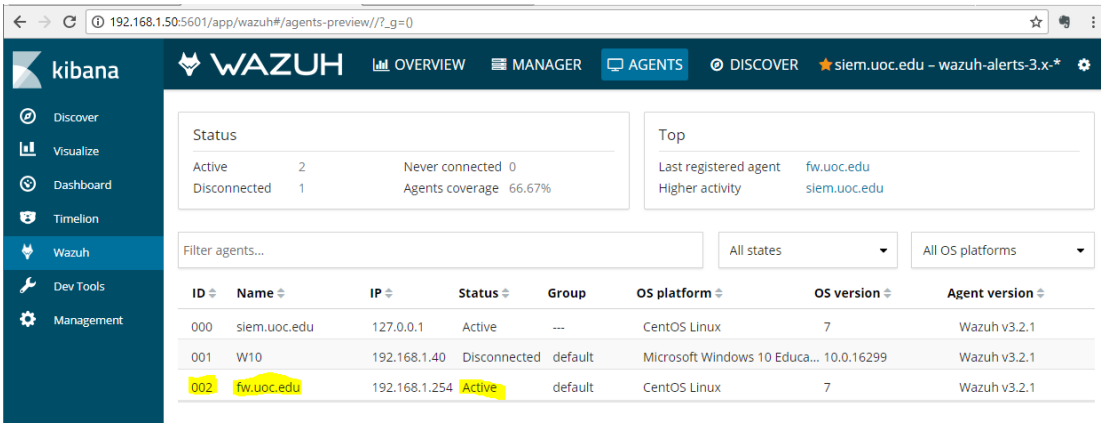


Ilustración 42. fw.uoc.edu registrado en Wazuh y activo.

Los demás clientes (servidor Web, Radius, Endpoint W10 y Endpoint Linux), se registrarán de igual forma.
Después de la instalación de los agentes en el SIEM, ya tenemos todas las máquinas controladas por el IDS.

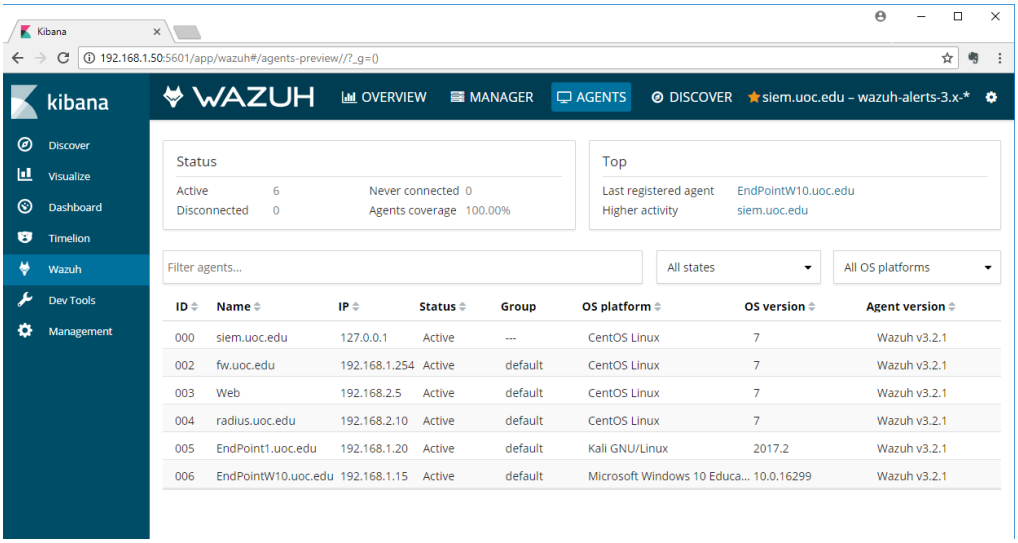


Ilustración 43.- Maquinas clientes controladas por el IDS Wazuh.

En estos momentos ya tenemos instalado el IDS con todos sus agentes en las máquinas clientes a inspeccionar. En la siguiente figura se muestra la vista principal, con un resumen de lo que está sucediendo en todos los equipos inspeccionados.

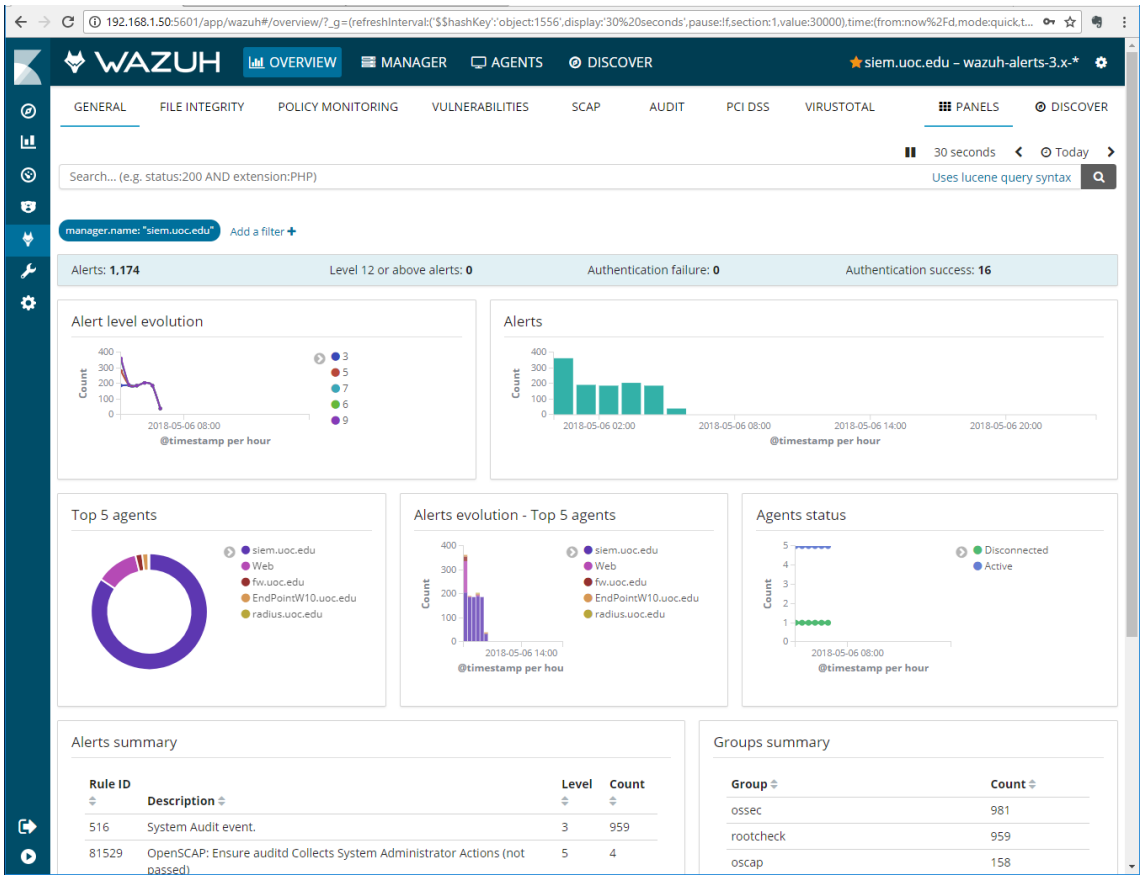


Ilustración 44.- Vista principal de eventos de seguridad en el conjunto de máquinas inspeccionadas.

3.5.- Instalación de beats. [6-Beats Platform Reference]

3.5.1.-Filebeat [6-Filebeat Reference]

El primer paso consiste desde la máquina cliente descargarse el beat correspondiente, como ejemplo para este trabajo se instalará en el servidor "radius.uoc.edu", con el objeto de poder enviar los logs de autenticación al SIEM. Para la recolección de logs genéricos proporcionados por un tercero, el beat apropiado es Filebeat.

```
[root@radius ~]# curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.2.3-x86_64.rpm
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 12.1M  100 12.1M    0     0  1934k      0  0:00:06  0:00:06 --:--:-- 2449k
[root@radius ~]#
```

Ilustración 45.-Descarga de Filebeat en radius.uoc.edu.

Posteriormente a la descarga, se instala Filebeat con yum o rpm.

```
[root@radius ~]# yum localinstall filebeat-6.2.3-x86_64.rpm
```

Una vez instalado Filebeat, es necesario configurarlo para que recoja el log que se le indique y lo envíe correctamente a elasticsearch. El fichero de configuración de Filebeat, se encuentra en "/etc/filebeat/filebeat.yml". Es suficiente con realizar unos cambios en el "prospector", indicándole de que log va a recoger los datos y adecuando la salida de Filebeat contra elasticsearch (la conexión es SSL).

Sera suficiente con activar el apartado log e indicar el fichero del cual filebeats enviará logs a elasticsearch. La siguiente figura muestra los cambios, recogiendo eventos de un fichero de radius llamado "linelog", donde se escriben todas las autenticaciones.

```
#========================== Filebeat prospectors =============================

filebeat.prospectors:

# Each - is a prospector. Most options can be set at the prospector level, so
# you can use different prospectors for various configurations.
# Below are the prospector specific configurations.

- type: log

  # Change to true to enable this prospector configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/radius/linelog
    #- c:\programdata\elasticsearch\logs\*
```

Ilustración 46.-Configuración en el apartado "prospectors" de filebeat.yml.

Después de este cambio se debe editar la sección "Elasticsearch output", para indicar a Filebeat como conectarse con Elastic search. Como elasticsearch solo admite conexiones SSL, previamente es necesario traer el certificado de la CA de Elasticsearch para referenciarlo. En el presente trabajo este certificado se ha copiado a la carpeta *"/etc/pki/out/root-ca-pem"*.

```
#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.1.50:9200"]

  # Optional protocol and basic auth credentials.
  protocol: "https"
  username: "admin"
  password: "XXXXXXXXX"
  ssl.certificate_authorities: "/etc/pki/out/root-ca.pem"
```

Ilustración 47.-Configuración para conectar Filebeat con elasticsearch vía SSL.

Por último, se levantará el servicio Filebeat y el log de radius será enviado en tiempo real a elasticsearch.

```
[root@radius filebeat]# systemctl start filebeat
```

Para monitorizar estos logs en el SIEM, se realizará a través de Kibana. Para esto es necesario crear el índice en Kibana y los logs podrán ser monitorizados.

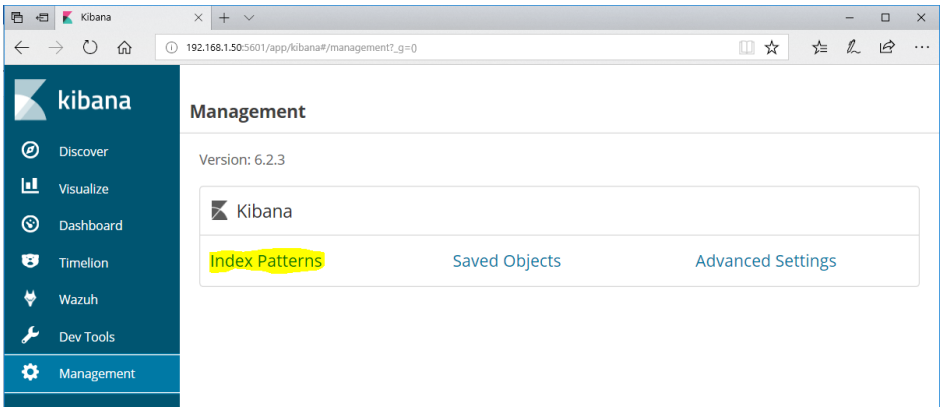


Ilustración 48.- Desde Management de Kibana se accede a Index Patterns.

Desde index Patterns crearemos un nuevo índice tal y como muestra la siguiente figura.

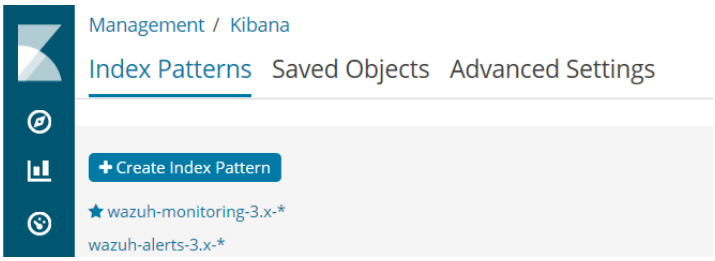


Ilustración 49.- Creación de un índice en Kibana para filebeat.

Seguidamente se asignará un nombre de índice que recoja todos aquellos documentos (registros) que comiencen con el patrón Filebeat-6.2.3-*.

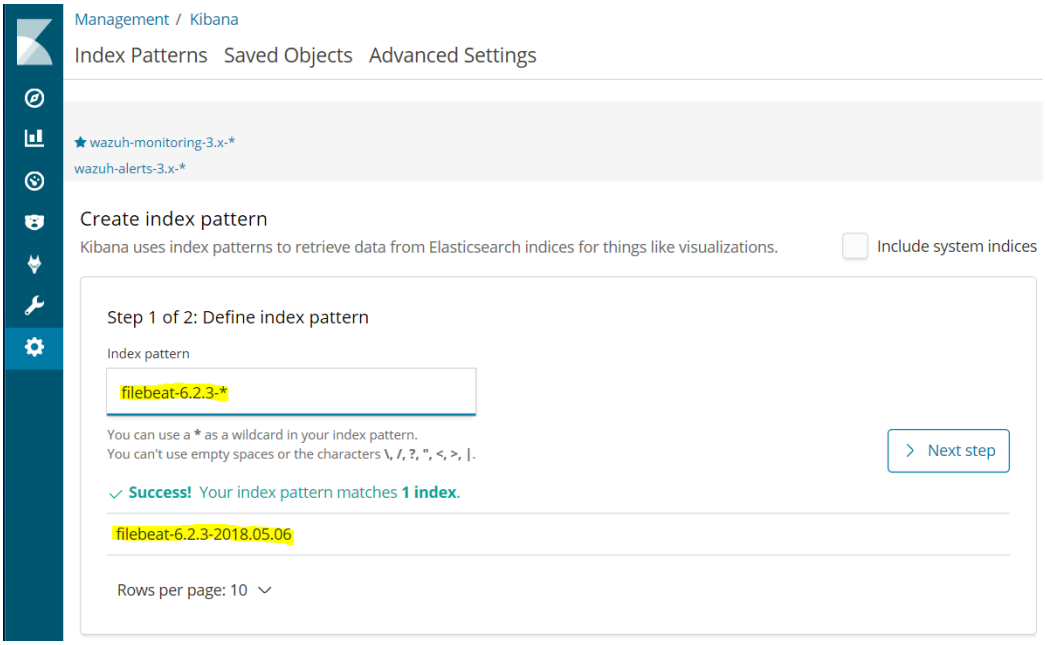


Ilustración 50.- Asignación de nombre de índice.

Se indica que el filtrado sea según la variable de “@timestamp” y se crea el índice.

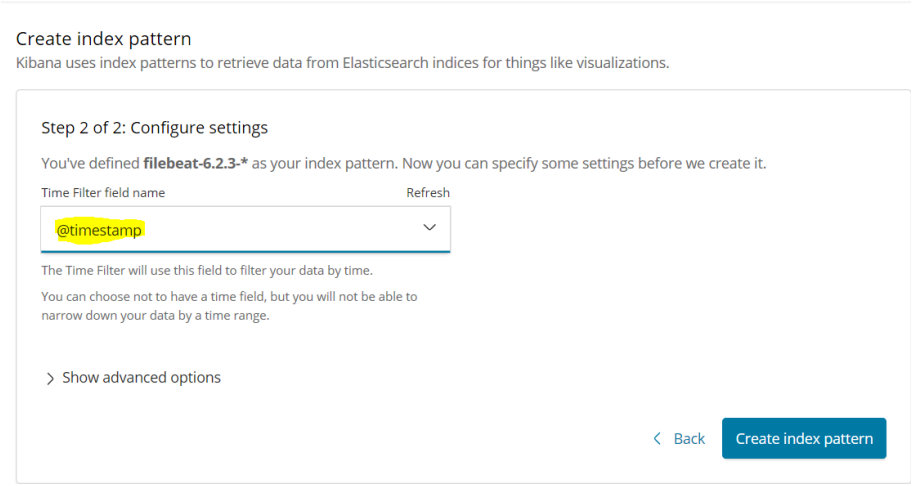


*Ilustración 51.-Creación del índice según el patrón filebeat-6.2.3-**

Posteriormente se mostrará el índice creado con los campos y sus características. En la siguiente figura se puede observar los campos que se le han enviado desde el log del radius (linelog).

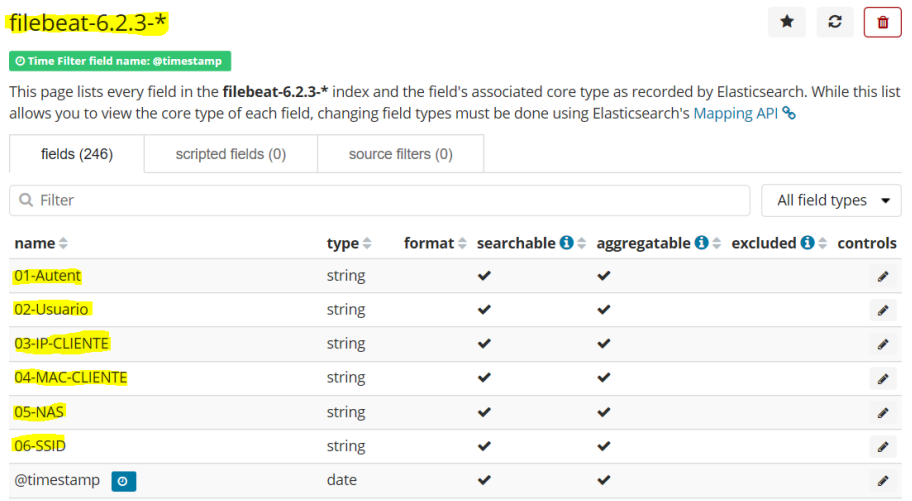


Ilustración 52.- Índice creado con los campos asignados.

Esta misma configuración se realizará con el cortafuegos para monitorizar las denegaciones producidas por el mismo.

3.5.2 Metricbeat [6-Metricbeat Reference]

Metricbeat es un agente de Elastic Stack que se instala en los servidores para recoger métricas del sistema operativo y de los servicios que se están ejecutando en el servidor. En este trabajo se instalará en el servidor Web, como ejemplo.

Se comienza descargando el agente de metricbeats para seguidamente instalarlo y configurarlo en la máquina cliente. En este caso en el servidor Web.

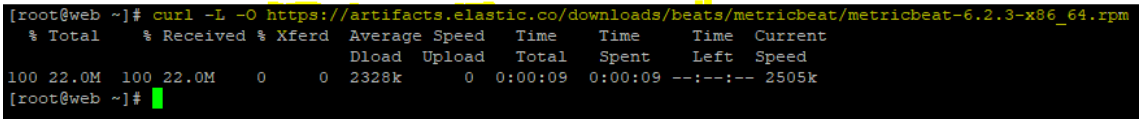


Ilustración 53.- Descarga de metricbeat 6.2.3.

Se instala metricbeat.

```
[root@web ~]# yum localinstall metricbeat-6.2.3-x86_64.rpm
```

Una vez instalado se procede a su configuración. El fichero de configuración se encuentra en *"/etc/metricbeat/metricbeat.yml*". Se configurará la sección de Kibana, para cargar automáticamente los dashboards que trae metricbeats.

```
#============================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "192.168.1.50:5601"
  username: "admin"
  password: "XXXXXXXXXX"
```

Ilustración 54.- Configuración para cargar los dashboard en Kibana.

Se necesita configurar la salida de Metricbeat para conectar por SSL con elasticsearch.

```
#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.1.50:9200"]

  # Optional protocol and basic auth credentials.
  protocol: "https"
  username: "admin"
  password: "XXXXXXXX"
  ssl.certificate_authorities: "/etc/pki/out/root-ca.pem"
```

Ilustración 55.- Configuración para conectar con elasticsearch por SSL.

Para finalizar con la configuración activaremos los módulos correspondientes a "Apache" y "MySQL", para que se recojan las métricas de estos servicios, además de la métrica del sistema que ya está activada por defecto. Desde la carpeta "/etc/metricbeat/modules.d", bastará con renombrar el módulo de *"****.yml.disable*" a *"****.yml*" para cualquier módulo que queramos activar.

```
[root@web modules.d]# pwd
/etc/metricbeat/modules.d
[root@web modules.d]# mv apache.yml.disabled apache.yml
[root@web modules.d]# mv mysql.yml.disabled mysql.yml
[root@web modules.d]#
```

Ilustración 56.- Activación de los módulos apache y MySQL.

Con el comando "*Metricbeat setup –dashboards*" cargaremos los dashboards en Kibana.

```
[root@web metricbeat]# metricbeat setup --dashboards
Loaded dashboards
[root@web metricbeat]#
```

Ilustración 57. Comando de carga de los dashboards de metricbeat en Kibana.

Finalmente arrancaremos el servicio

```
[root@web modules.d]# systemctl start metricbeat
```

Una vez instalados los dashboards por metricbeat, la siguiente figura muestra los que se han dejado por su importancia (Apache, MySQL y System). Se ha dejado el dashboard de Windows, para monitorizar por Metricbeat el EndPoint W10.

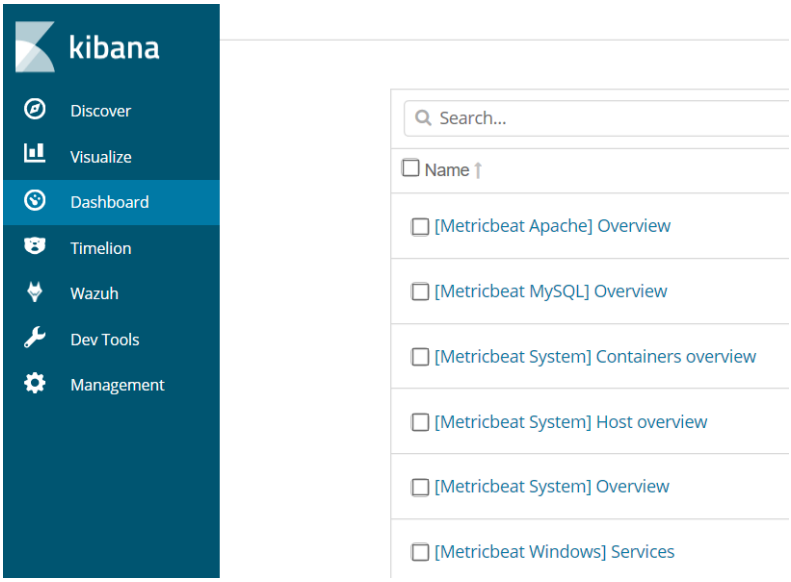


Ilustración 58.-Dashboards cargados en Kibana por metricbeats.

3.6.- Alertas. Sentinl.

Para conseguir un sistema de alertas totalmente integrado con Elastic Stack, se ha utilizado el plugin Sentinl 6. Este plugin proporciona funcionalidades de alertas, monitorización e informes.

Su instalación es similar a todas las instalaciones de los plugins de Elastic Stack. Una vez se está situado en el directorio donde se ejecutan los plugins de Kibana, ejecutamos la orden de descarga e instalación.

```
[root@siem bin]# pwd
/usr/share/kibana/bin
[root@siem bin]#
```

```
[root@siem bin]# ./kibana-plugin install https://github.com/sirensolutions/sentinl/releases/download/tag-6.2.3-3/sentinl-v6.2.3.zip
Attempting to transfer from https://github.com/sirensolutions/sentinl/releases/download/tag-6.2.3-3/sentinl-v6.2.3.zip
Transferring 7824286 bytes....................
Transfer complete
Retrieving metadata from plugin archive
Extracting plugin archive
Extraction complete
Optimizing and caching browser bundles...
Plugin installation complete
[root@siem bin]#
```

Ilustración 59.- Instalación del plugin Sentinl.

Una vez se ha instalado el plugin es necesario acceder al fichero de configuración de Kibana "/etc/kibana/kibana.yml" y añadir las líneas de código necesarias al final de este fichero, tal y como indica la siguiente figura. Posteriormente se reinicia el servicio de Kibana y ya estará integrada la funcionalidad de alertas y reporting "Sentinl" en Kibana.

```
# Configuracion sentinl
sentinl:
  es:
    host: '10.27.252.241'
    port: 9200
    # protocol: 'http'
    # results: 50
    # timefield: '@timestamp'
    # default_type: 'doc'
    # alarm_index: 'watcher_alarms'
    # alarm_type: 'sentinl-alarm'
  settings:
    email:
      active: true
      host: 'smtp.gmail.com'
      user: 'tu_mail@gmail.es'
      password: 'secreto'
      port: 465
      ssl: true
    report:
      active: true
      executable_path: '/usr/bin/chromium-brownser'
      timeout: 5000
      # authentication:
      #   enabled: true
      #   mode:
      #     searchguard: false
      #     xpack: false
      #     basic: false
      #     custom: true
      #   custom:
      #     username_input_selector: '#username'
      #     password_input_selector: '#password'
      #     login_btn_selector: '#login-btn'
      # file:
      #   pdf:
      #     format: 'A4'
      #     landscape: true
      #   screenshot:
      #     width: 1280
      #     height: 900
    pushapps:
      active: false
      api_key: '<pushapps API Key>'
```

Ilustración 61.-Código de configuración para Sentinl en Kibana

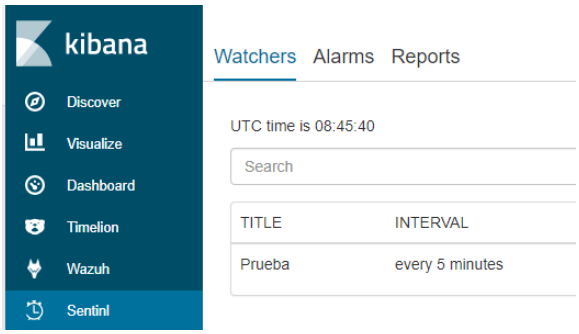


Ilustración 60.- Sentinl integrado en Kibana.

3.7.-Pruebas con sensores. Casos de uso

3.7.1- Wazuh IDS/IPS [7-User manual]

Wazuh es un IDS/IPS que se integra magníficamente con Elastic Stack. En el presente trabajo solo se estudiará la parte de IDS debido a la carga del trabajo. Las actuaciones post-alertas es un módulo que tiene wazuh y entre otras cosas

puede provocar la denegación de servicio a un recurso en función de la severidad de la alerta. Por ejemplo, a través de iptables.

3.7.1.1-Vista general del IDS/IPS

Wazuh tiene una vista general donde muestra el resumen de la evolución de las alertas de seguridad, el número de alertas recibidas, el número de alertas severas, el número de autenticaciones exitosas en un determinado tiempo.

Además, presenta tableros con la evolución de las alertas, el número de alerta por agente, el estado de los mismos y por último un resumen de las alertas indicando el nivel de severidad y las veces que se ha disparado, y un resumen de los grupos de alertas. Todo esto se muestra en la siguiente figura (ilustración 62).

Se puede apreciar la vista general para todos los agentes o también se puede ver esta vista resumen, para cada uno de los agentes individualmente. De hecho, todas las vistas de wazuh pueden hacer referencia a todos los agentes en global o podemos focalizar a cada agente individualmente como muestra la ilustración 63.

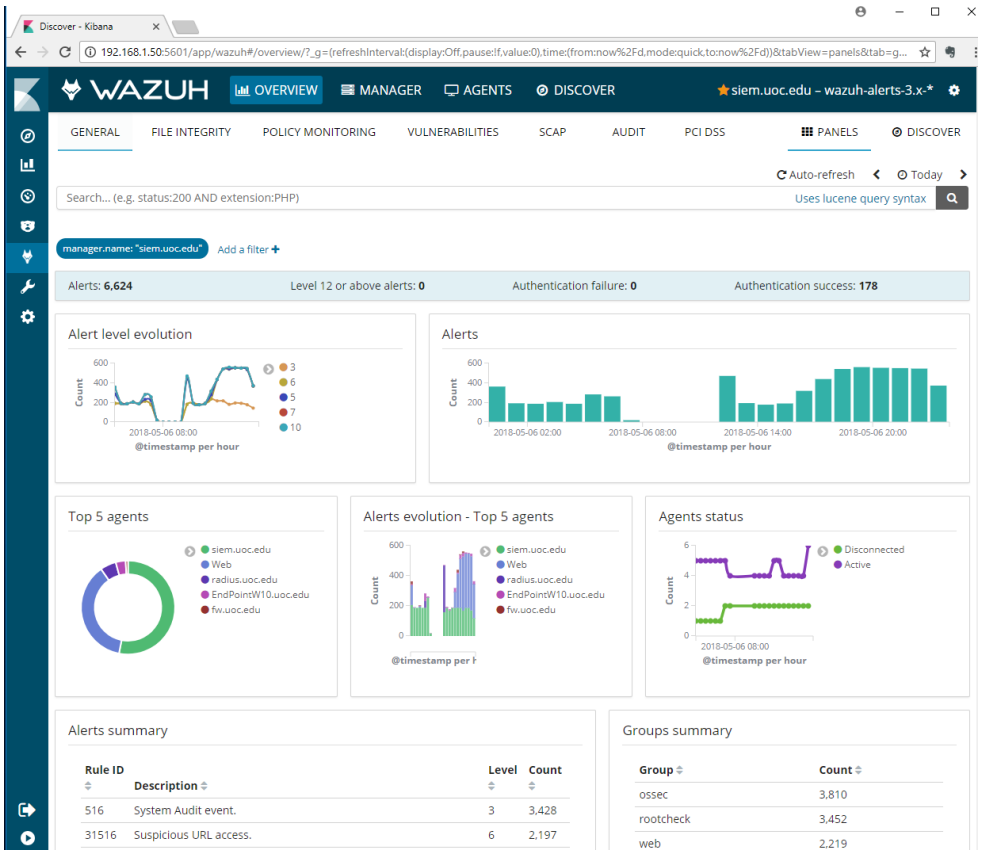


Ilustración 62.- Vista general (resumen) de todos los agentes

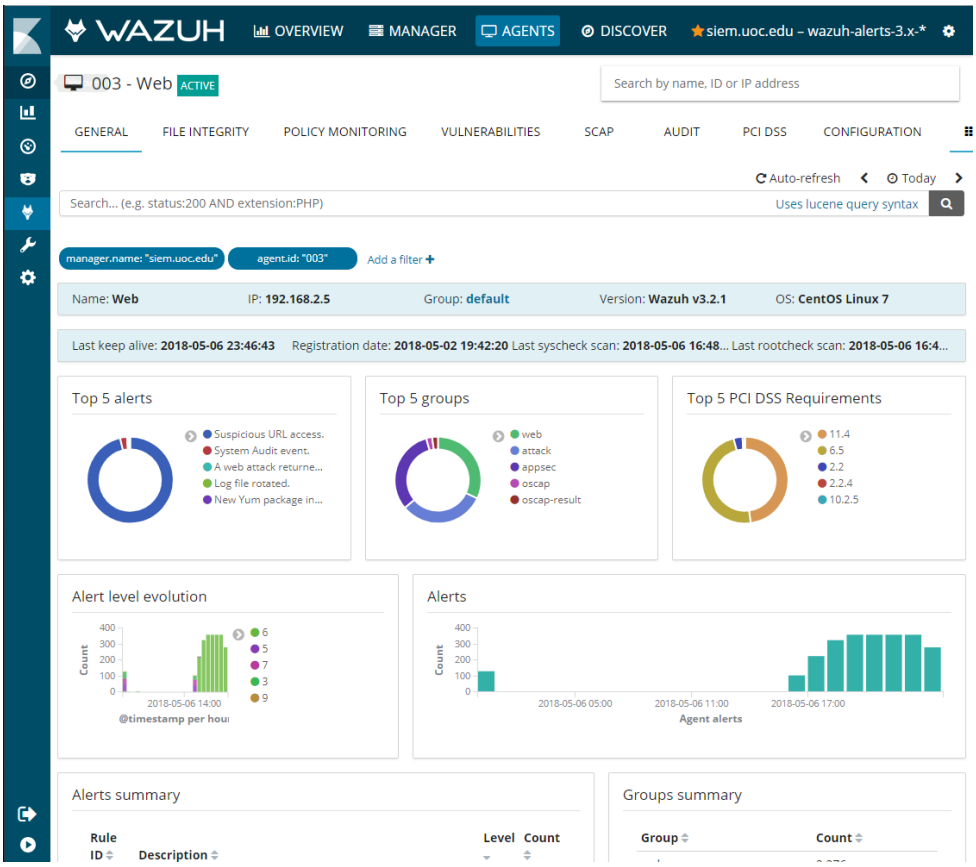


Ilustración 63.- Vista general del agente Web.

3.7.1.2-FIM. Monitorización de la integridad de ficheros

Wazhu tiene un escáner (syscheck) que comprueba periódicamente si los ficheros, de unos determinados directorios elegidos en la configuración, han sido creados, borrados o modificados. Estos directorios pueden ser analizados cada cierto tiempo, con una periodicidad ajustada por el administrador o comprobados en tiempo real.

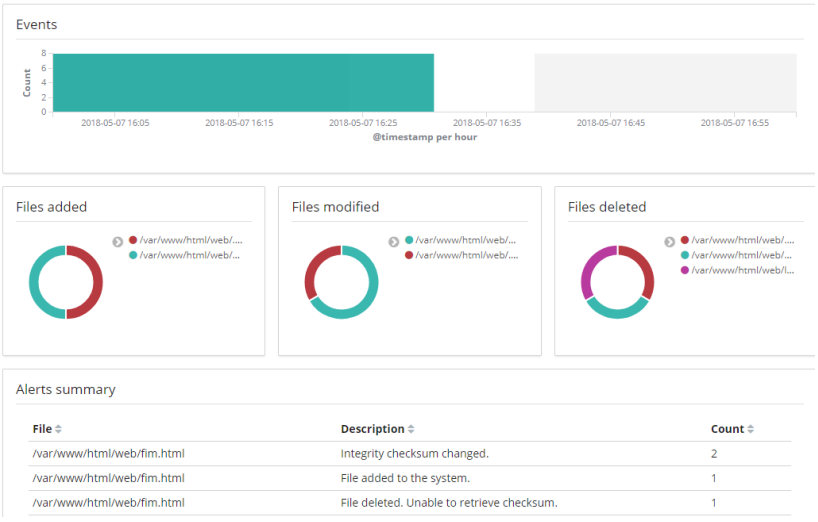


Ilustración 64.-Monitorización FIM en servidor Web.

El la figura 64, se observa la creación, modificación y posterior borrado del fichero "fim.html" en el directorio "/var/www/html/web" que está configurado para alertar en tiempo real y la siguiente figura el SIEM muestra los cambios realizados en dicho fichero.

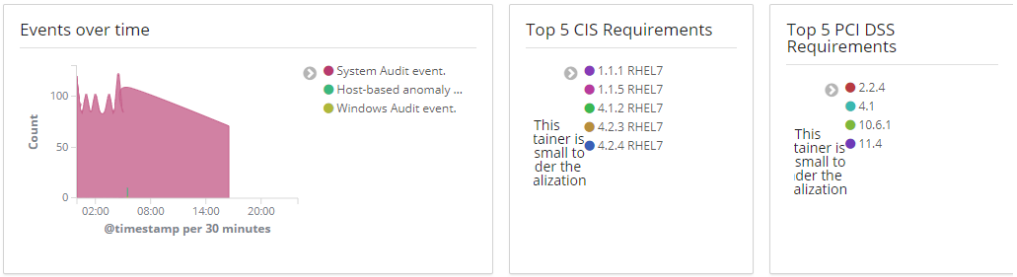
Existe una app en wazuh, que mediante una "api" se puede conectar el FIM con la aplicación en la nube "Virustotal", que además de monitorizar el cambio del

fichero, tras el mismo lo examinaría para comprobar que no se han introducido virus.

3.7.1.3-Monitorización de políticas de seguridad. Auditoría de equipos.

Policy monitoring realiza una auditoria de las políticas de seguridad de los distintos servidores e indica las debilidades que deben ser corregidas según el sistema CIS para el sistema operativo de cada servidor.

En la siguiente figura se puede observar que varios servidores no cumplen con los requerimientos del CIS e indican que apartado incumplen. Por ejemplo, se observa que en el Servidor web no está activada la herramienta de seguridad SELinux y que en varios servidores se permite más de 4 errores de accesos mediante SSH, etc.



Alerts summary

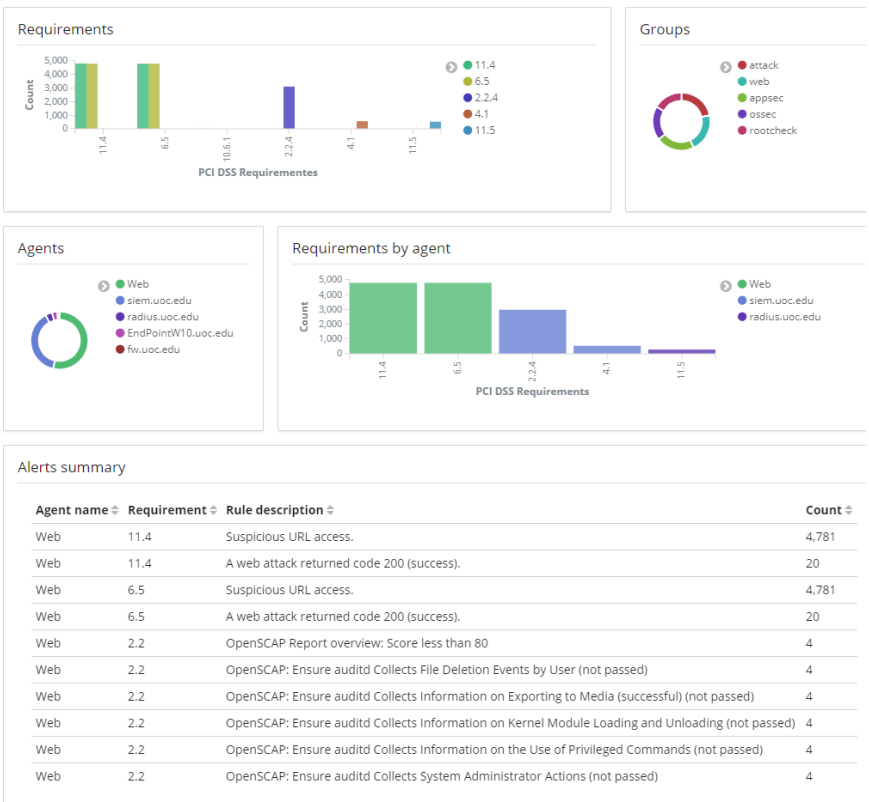
Agent	Description	Control	Count
siem.uoc.edu	System Audit event.	CIS - RHEL7 - 6.2.5 - SSH Configuration - Set SSH MaxAuthTries to 4 or Less	69
Web	System Audit event.	CIS - RHEL7 - 6.2.5 - SSH Configuration - Set SSH MaxAuthTries to 4 or Less	2
fw.uoc.edu	System Audit event.	CIS - RHEL7 - 6.2.5 - SSH Configuration - Set SSH MaxAuthTries to 4 or Less	1
Web	System Audit event.	CIS - RHEL7 - 1.4.2 - SELinux not set to enforcing	2
fw.uoc.edu	System Audit event.	CIS - RHEL7 - 4.1.1 - Network parameters - IP Forwarding enabled	1
siem.uoc.edu	System Audit event.	CIS - RHEL7 - 4.1.2 - Network parameters - IP send redirects enabled	69
Web	System Audit event.	CIS - RHEL7 - 4.1.2 - Network parameters - IP send redirects enabled	2
fw.uoc.edu	System Audit event.	CIS - RHEL7 - 4.1.2 - Network parameters - IP send redirects enabled	1
siem.uoc.edu	System Audit event.	CIS - RHEL7 - 4.2.2 - Network parameters - ICMP redirects accepted	69
Web	System Audit event.	CIS - RHEL7 - 4.2.2 - Network parameters - ICMP redirects accepted	2

Ilustración 65.- Auditoria de todos los servidores conectados.

Ilustración 66.- Grafico de incumplimientos de política de seguridad en las máquinas monitorizadas.

La figura anterior presenta un gráfico de todos los equipos monitorizados por el SIEM, con el número de alertas por incumplimiento del estándar CIS.

La siguiente figura muestra un resumen de alertas del servidor Web. Se puede apreciar en la segunda línea del resumen de alertas, que la web ha sido atacada exitosamente.



Agent name	Requirement	Rule description	Count
Web	11.4	Suspicious URL access.	4,781
Web	11.4	A web attack returned code 200 (success).	20
Web	6.5	Suspicious URL access.	4,781
Web	6.5	A web attack returned code 200 (success).	20
Web	2.2	OpenSCAP Report overview: Score less than 80	4
Web	2.2	OpenSCAP: Ensure auditd Collects File Deletion Events by User (not passed)	4
Web	2.2	OpenSCAP: Ensure auditd Collects Information on Exporting to Media (successful) (not passed)	4
Web	2.2	OpenSCAP: Ensure auditd Collects Information on Kernel Module Loading and Unloading (not passed)	4
Web	2.2	OpenSCAP: Ensure auditd Collects Information on the Use of Privileged Commands (not passed)	4
Web	2.2	OpenSCAP: Ensure auditd Collects System Administrator Actions (not passed)	4

Ilustración 67.-Resumen de alertas y problemas en la auditoría.

3.7.1.4-Monitorización de virus. VirusTotal.

Wazuh tiene un sistema de integración de terceros para, por ejemplo, escanear ficheros con posible contenido malicioso (virus). Este es el caso de la integración con VirusTotal.

VirusTotal es una poderosa aplicación que consta de múltiples productos antivirus que son capaces de escanear recursos online.

Esta herramienta a través de su API y junto con la herramienta FIM del IDS Wazuh, realizan un escaneo de todos aquellos ficheros que han sido creados, modificados, en resumen, monitorizados por la herramienta FIM de Wazuh (syscheck). Una vez el sistema FIM detecta que un fichero ha sido modificado o creado en un directorio especificado, sube la firma del fichero a la aplicación online de VirusTotal y es escaneado por más de 60 antivirus online, ofreciendo un resultado fiable del fichero analizado. El resultado se pasa a wazuh y se muestra en la interfaz de Kibana.

Para integrar VirusTotal con Wazuh, basta con añadir el código mostrado en la ilustración 65 al fichero "/var/ossec/etc/ossec.conf" en el SIEM.

```
<integration>
  <name>virustotal</name>
  <api_key>3393e                                                    :8be9f26476c47                    :66aa03f3</api_key>   <!-- Replace with your key -->
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>
```

Ilustración 68.- integración de VirusTotal al SIEM.

También es necesario indicar al SIEM, en el fichero anterior, el directorio o directorios donde residen los ficheros que son susceptibles de ser analizados en tiempo real.

```
<!-- Directories to check  (perform all possible verifications) -->
<directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes">/bin,/sbin,/boot</directories>
<directories check_all="yes" realtime="yes">/var/www/html/web</directories>
```

Ilustración 69.- Directorio a analizar en la zona syscheck del fichero "ossec.conf" del SIEM.

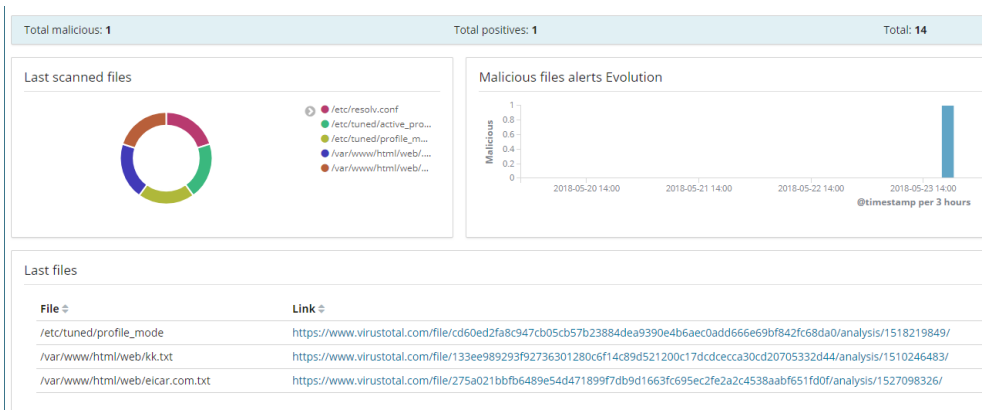


Ilustración 70.- Monitorización de virus, gusanos, troyanos, etc. a través de VirusTotal.

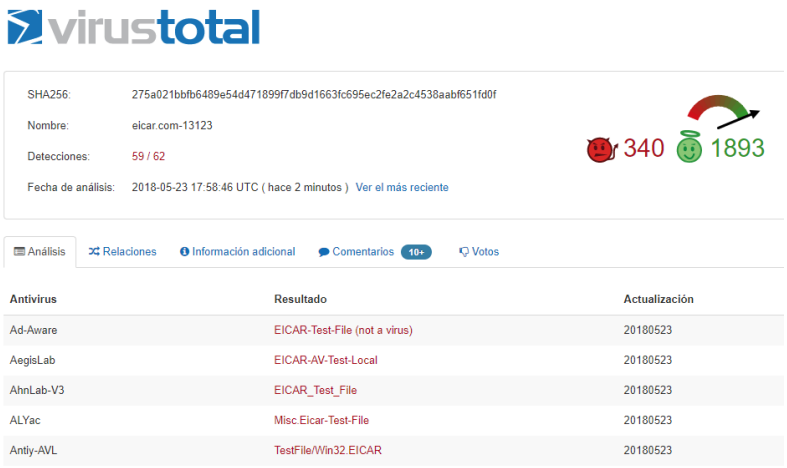


Ilustración 71.- Resultado del análisis del fichero eicar.com.txt, detectado por wazuh y analizado por VirusTotal.

3.7.2 Beats

3.7.2.1-Integración de logs de servidores con Elastic Stack. Filebeat

Mediante Filebeat trasladamos el log de autenticación de radius a Kibana y podemos monitorizar los accesos a el radius. La siguiente figura muestra la visualización de los accesos del Endpoint Windows contra el radius. Por medio de la herramienta RadTest realizamos las autenticaciones contra el radius.

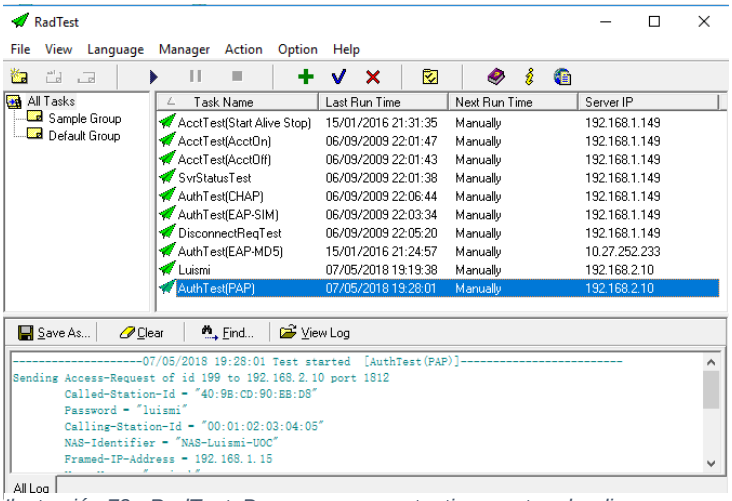


Ilustración 72.- RadTest. Programa para autenticar contra el radius.

En la siguiente figura se muestra la monitorización y el control de los accesos a la red, visualizando las conexiones contra “radius.uoc.edu”, ofreciéndose una información muy valiosa de que usuario está conectado no ha podido conectarse, la MAC de su equipo, su IP, etc. Se podría realizar un control exhaustivo de un usuario o su máquina, etc.

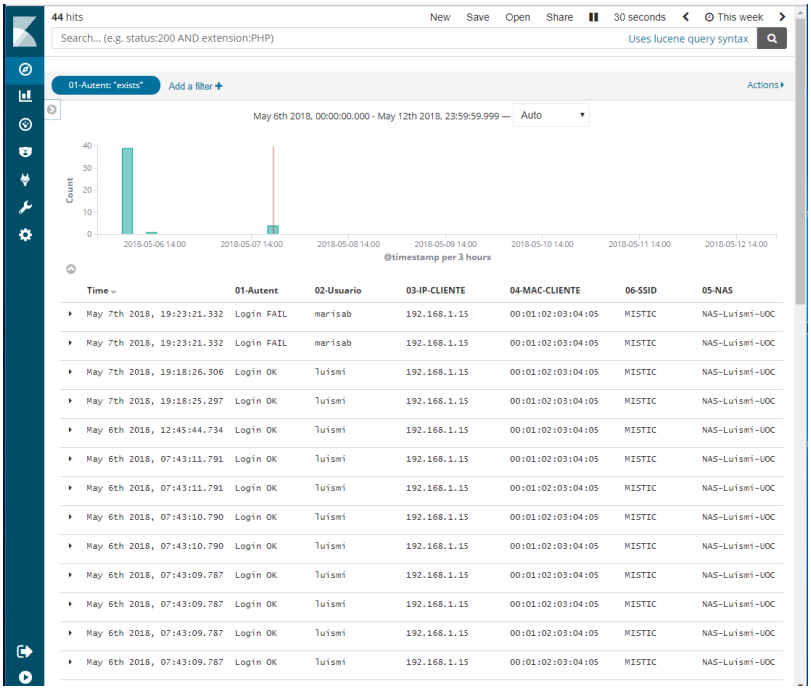


Ilustración 73.Monitorización de usuarios conectados al radius

Es posible el control del tráfico que pasa por el cortafuegos, proporcionando una información muy valiosa. Esta información consta del tráfico que fue permitido o no, la regla que actuó, quien genero el tráfico y contra quien, contra que puerto, si era udp o tcp, etc. El cortafuegos iptables, sin ninguna clase de monitorización en su instalación, pasa a ser completamente monitorizado en tiempo real o con búsquedas forenses, como cualquier otro cortafuegos comercial de alta gama, a través de sus logs generados en el script del mismo.

El procedimiento consiste en extraer los logs de cada regla de iptables y seguidamente con “nxlog” se convierte al formato adecuado en JSON. Anexo….

Elastic Stack permite filtrar la visualización por todos los campos mostrados en la monitorización, ventana de tiempo, IP de origen, de destino, puerto, protocolo, tráfico permitido o no, etc. La siguiente figura muestra esta información.

	json.Accion	json.Zona_Origen	json.IP_Origen	json.Zona_Destino	json.IP_Destino	json.Puerto_Destino	json.Protocolo	json.Regla
)71	Denegado	enp0s3	192.168.1.15	enp0s8	192.168.2.5		ICMP	Regla_Fin_Forw
)71	Denegado	enp0s3	192.168.1.1		224.0.0.1		2	Regla_Fin_Input
)69	Denegado	enp0s3	192.168.1.15	enp0s8	192.168.2.5		ICMP	Regla_Fin_Forw
)66	Denegado	enp0s3	192.168.1.15	enp0s8	192.168.2.5		ICMP	Regla_Fin_Forw
)66	Denegado	enp0s3	192.168.1.1		224.0.0.1		2	Regla_Fin_Input
)64	Denegado	enp0s3	192.168.1.15	enp0s8	192.168.2.5		ICMP	Regla_Fin_Forw
)62	Denegado	enp0s3	192.168.1.1		224.0.0.1		2	Regla_Fin_Input
)62	Denegado	enp0s3	192.168.1.15	enp0s8	192.168.2.5		ICMP	Regla_Fin_Forw
)58	permitido	enp0s8	192.168.2.5	enp0s3	216.58.210.163	80	TCP	Regla_9
)58	permitido	enp0s8	192.168.2.5	enp0s3	80.58.61.250	53	UDP	Regla_9
)58	permitido	enp0s8	192.168.2.5	enp0s3	80.58.61.250	53	UDP	Regla_9

Ilustración 74.- Monitorización del tráfico en el fw.

3.7.2.2-Monitorización del sistema de los equipos y sus procesos. Metricbeat

Con metricbeat es posible la monitorización de los servicios y el funcionamiento del sistema de un servidor o un endpoint. El servidor web está ejecutando “apache” y “mariadb”. A continuación, se muestra en las siguientes figuras el estado del servidor Web.

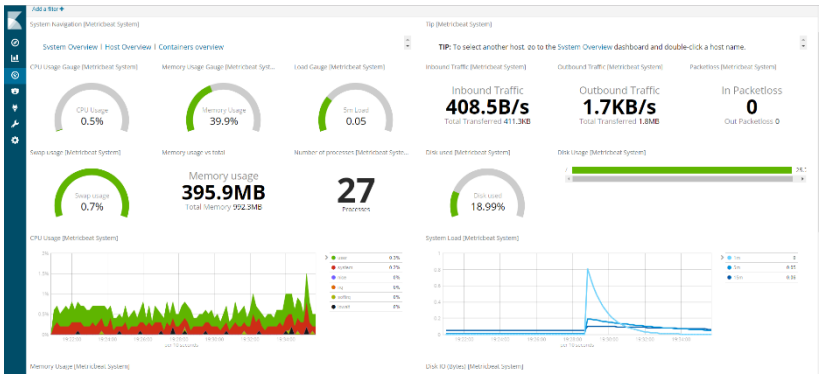


Ilustración 75.- Estado del sistema del servidor Web.

La figura 75, muestra el estado general del servidor web, monitorizando el uso de CPU, memoria RAM, carga del servidor, etc.

Si este servidor sufriera un ataque seguramente alguno de estos parámetros se vería fuertemente alterado y rápidamente se tendría constancia de un problema.

La ilustración 76, muestra con más detalle el estado del sistema del servidor web, mostrando los procesos (servicios) que se encuentran en ejecución y su balance de carga.

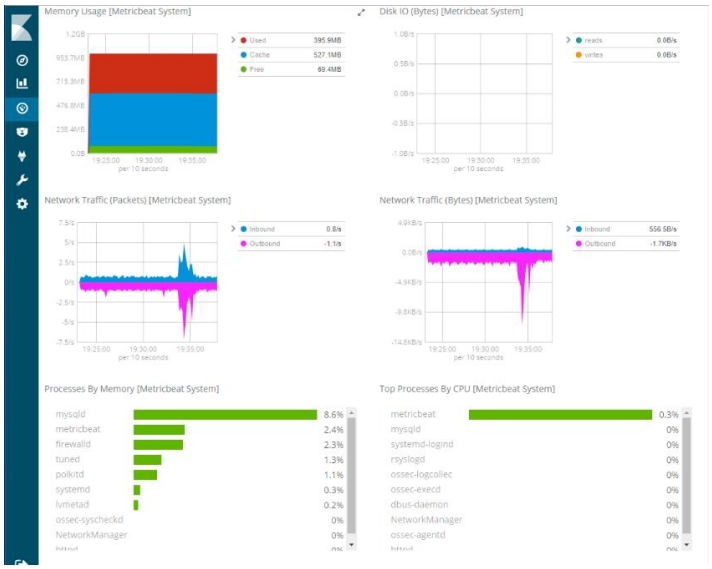
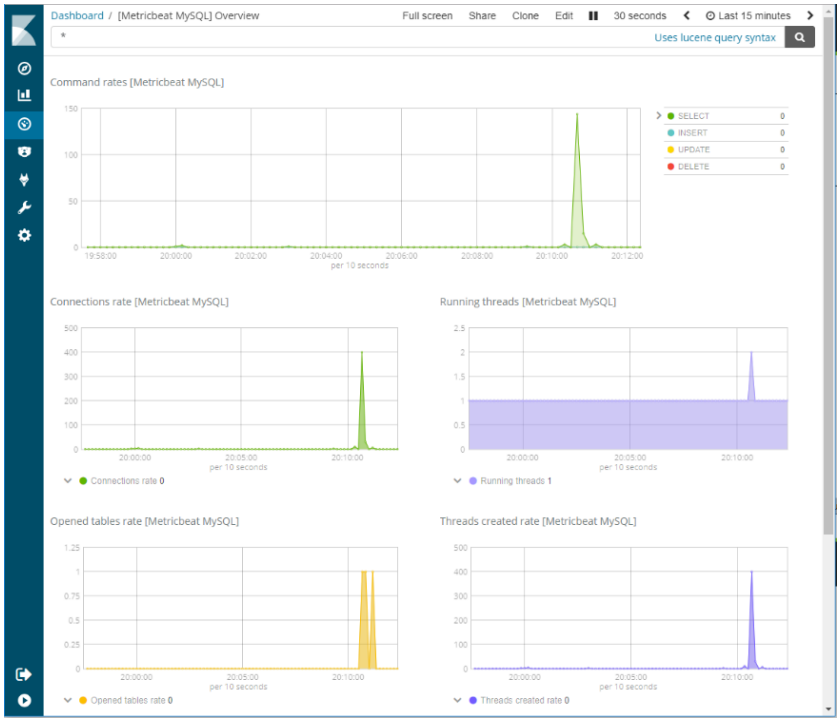


Ilustración 76.-Métricas del sistema del servidor web.



La figura 77, fija su atención en uno de los servicios mostrados en la ilustración anterior (MySQL), mostrando la velocidad de consultas, escrituras, número de conexiones, etc.

Ilustración 77.-Monitorización del servicio MySQL.

3.7.3- Alertas. Sentinl

Las alertas deben ser generadas a través del plugin Sentinl que tiene un wizard que nos ayuda a realizarlas. En primer lugar, se define la frecuencia con la que va a ser revisada la existencia de la alerta y su nombre según muestra la siguiente figura. En este caso es una alerta llamada prueba y se examinará cada 5 minutos.

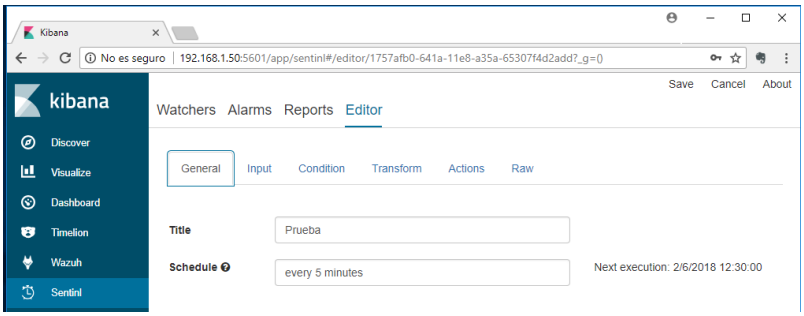


Ilustración 78.-Generación de la alerta.

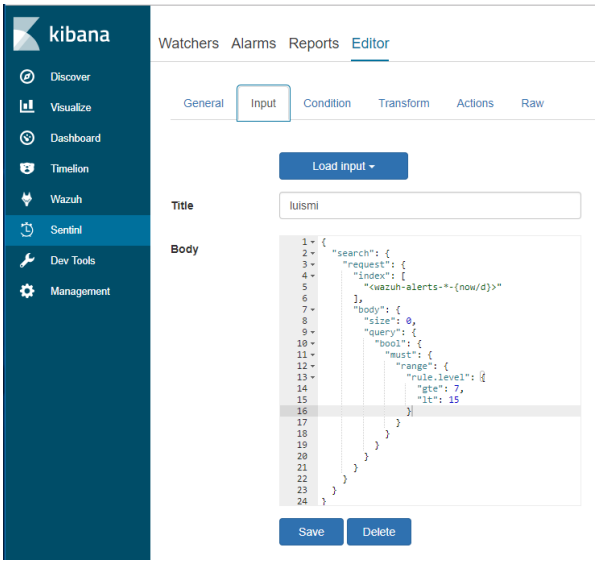


Ilustración 79.- Apartado Input de Sentinl.

Seguidamente se programa una consulta donde se indica el o los índices a examinar, el filtrado por alguno de los campos o el tiempo en el cual debe de centrarse la alerta. Figura 79.

El próximo paso es fijar la condición que hará que la alerta se dispare. Por ejemplo, que sucedan un número de eventos en un determinado tiempo. Figura 80.

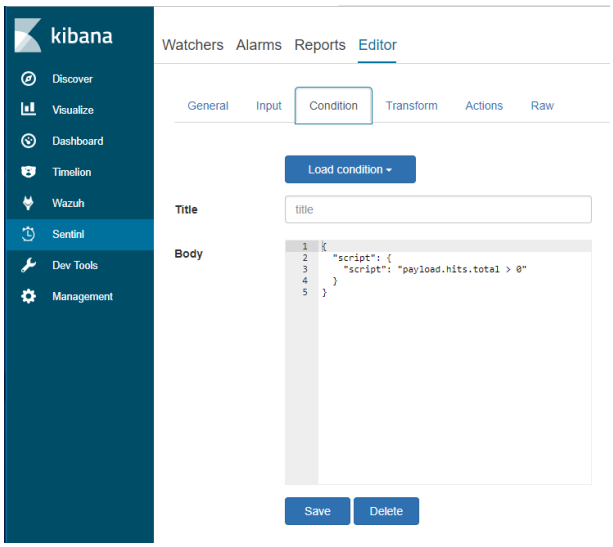


Ilustración 80.-Sección condición de Sentinl

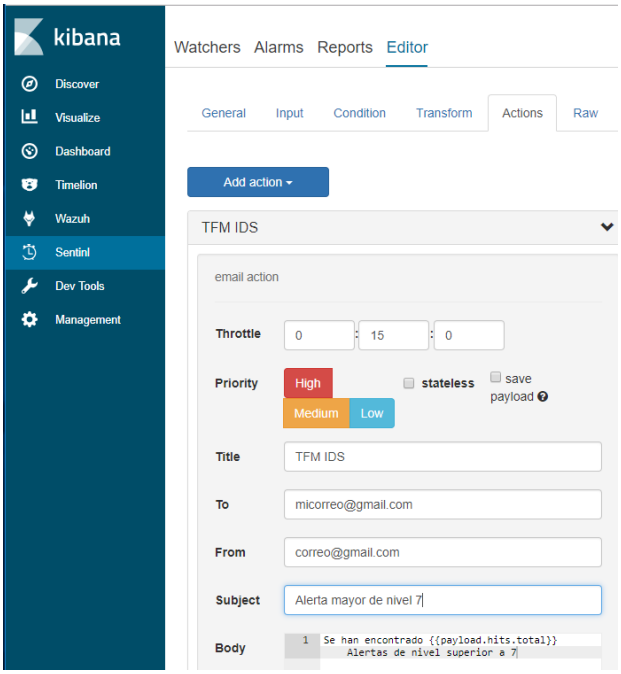


Ilustración 81.-Acción tras el disparo de la alerta.

Para finalizar se debe indicar la acción que se ejecutará cuando se dispare la alerta. Puede ser un simple aviso en el apartado de alertas del plugin de Sentinl, como se aprecia en la figura 82, un envió de correo electrónico, como indica la configuración en la ilustración 81 o incluso un informe en formato PDF o PNG.

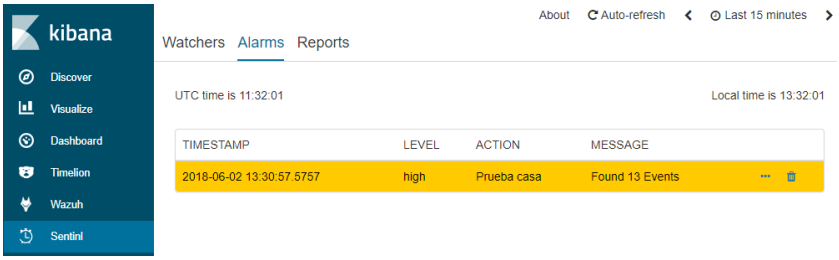


Ilustración 82.- Alerta mostrada por Sentinl

4. Conclusiones

Los sistemas SIEM son cada vez más usados en los entornos de seguridad de la información, no obstante, no están exentos de complejidad de manejo y costes económicos elevados, fundamentalmente a su precio en el mercado y la formación humana o la contratación de personal necesaria para su posterior manejo.

La idea de este TFM era conseguir una solución SIEM open source y dotar de unas aptitudes mínimas y necesarias para empezar a sacarle partido. De esta forma, se abaratan los costes de implementación del sistema al ser open source y supone un primer empujón en el manejo del mismo.

Es cierto que, en un principio cuando se planificó este trabajo, la idea del trabajo era un poco más ambiciosa. Además de lo aquí mostrado, los objetivos cubrían una parte de alertas a través de una herramienta open source como “sentinl”, que se integra perfectamente en Elastic Stack, pero debido a la carga de trabajo del TFM presentado no ha sido posible implementarlo.

Debido al párrafo anterior, no podría decir que el producto desarrollado alcanza la categoría de SIEM plenamente, pero si ofrece una solución utilizable que va mucho más allá de un simple gestor de logs y que, con toda seguridad, con un par de integraciones más alcanzaría la categoría de SIEM completamente.

Este trabajo perfectamente puede ser el inicio de otro trabajo donde las cotas a alcanzar sean mucho mayores, implementando un buen sistema de alertas, realizando reglas correlando diferentes fuentes, incluso realizando un manual de casos de uso y buenas prácticas, más desarrollado que el que consta en el presente trabajo.

Otros puntos por desarrollar podrían tener que ver con el rendimiento y recursos necesarios, para que este producto no solo funcione en un laboratorio, si no también en un entorno de trabajo real. Se podría aportar una guía de recursos necesarios de almacenamiento, computación, memoria, clusters de Elastic Stack, etc., para que el funcionamiento sea óptimo cuando la carga sobre el SIEM es más elevada.

La planificación del trabajo ha sido seguida fielmente y adecuada hasta bien entrado el trabajo en la fase de implementación. A partir de este punto se han utilizado más horas/días de los previstos debido a configuraciones incorrectas que ha habido que subsanar y debido a que la implementación del trabajo practico realmente necesitaba más horas de las planificadas. A pesar de estos inconvenientes se ha estado muy cerca de cumplir totalmente con lo planificado.

Por último, constatar que los 8GB de RAM usados en la máquina sobre la que se montó el laboratorio fueron insuficientes para albergar a 6 máquinas virtuales corriendo simultáneamente y fue necesario aumentar este valor hasta 16GB.

5. Glosario

API. Application Programming Interface. La interfaz de programación de aplicaciones, es un conjunto de subrutinas, funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

Amenaza. Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Auditoria. Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen unos criterios fijados.

BD. Base de datos.

CA. Certification Authority.

CIS. Center for Internet Security. Organización para la seguridad en internet.

Correlar. Proceso de comparar diferentes fuentes de información, obteniéndose de esta manera sentido a eventos que analizados por separado no la tendrían o pasaría desapercibida.

CSRF /XSRF. Cross Site Request Forgery. Falsificación de petición en sitios cruzados.

DMZ. Demilitarized Zone. Zona desmilitarizada.

DNS. Domain Name Service (o System). Servicio de nombres de dominio.

Escáner de vulnerabilidades. Programa que analiza un sistema buscando vulnerabilidades.

Evento de seguridad. Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad. [UNE-ISO/IEC 27000:2014].

FIM. Files Integration Monitoring.

Firewall (FW). Cortafuegos.

Gusano/Worm. Programa que está diseñado para copiarse y propagarse por sí mismo mediante mecanismos de red. No realizan infecciones a otros programas o ficheros.

HIDS. Sistema de detección de intrusos en un Host.

HTML. Hyper Text Markup Language.

HTTP. HyperText Transfer Protocol. Protocolo de transferencia de hipertexto, utilizado habitualmente en navegación web.

HTTPS. Secure Hyper Text Transfer Protocol.

ICS/SCADA. Sistemas de control industrial y supervisión de la adquisición de sus datos.

IDS. Intrusion Detection System. Sistema de Detección de Intrusiones. Sistema cuya finalidad es detectar las intrusiones que se han realizado o que están en curso.

Inyección SQL. Tipo de ataque a sitios web basados en bases de datos, pasándole código no autorizado.

IPS. Intrusion Prevention System. Sistema de Prevención de Intrusiones. Su función es prevenir los incidentes antes de que se produzcan.

JSON. Java Script Object Notation. Formato de texto ligero para el intercambio de datos.

Malware. Software de carácter malicioso cuyo objetivo principal es dañar o infiltrarse en un sistema.

NAC. Control Access Network. Sistema que controla el acceso a la red.

NAT. Network Address Translation. Conversión de una dirección IP de origen y/o

Destino.

Log. Un log es un registro de los eventos que ocurren dentro de los sistemas y redes de una organización. [NIST].

OWASP. Open Web Application Security Project.

Política de seguridad. Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos. [CNN-CERT].

Rootkit. Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema.

RPM. Red Hat Package Manager. Herramienta de administración de paquetería para GNU/Linux.

SIEM. Security Information and Event Management. Sistema que permite almacenar los registros (logs) de distintas fuentes de manera segura y correlarlos extrayendo información que podría pasar desapercibida si se analizan los distintos orígenes de información por separado.

SMTP. Simple Mail Transfer Protocol. Protocolo simple de transferencia de correo, utilizado para el envío de correo electrónico.

SNMP. Single Network Management Protocol. Protocolo estándar de Gestión de Red.

SOC. Security Operations Center. Centro de operaciones de seguridad.

SPAM. Correo basura. Información no solicitada, normalmente de carácter publicitario, que se puede recibir por diferentes medios como correo electrónico, foros etc.

SQL. Structured Query Language.

SSL. Secure Sockets Layer. Protocolo de cifra que permite el intercambio seguro de información entre dos extremos, predecesor de TLS.

TCP/IP. Transmission Control Protocol / Internet Protocol.

TLS. Transport Layer Security. Protocolo de cifra que permite el intercambio seguro de información entre dos extremos.

Troyano. código dañino con apariencia de un programa inofensivo que al ejecutarlo brinda al atacante acceso remoto al equipo infectado, normalmente instalando una puerta trasera (backdoor). [CCN-CERT].

UDP. User Datagram Protocol. Protocolo de datagramas de usuario.

URL. Uniform Resource Locator.

Virus. Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros. [CCN-STIC-430:2006].

VLAN. Virtual Local Area Network.

Vulnerabilidad. Debilidad que puede ser aprovechada por una amenaza.

WAF. Web Application Firewall. Cortafuegos de aplicación Web.

XML. eXtended Markup Language.

XSS. Cross Site Scripting. Secuencia de comandos en sitios cruzado.

6. Bibliografía

[1] David R. Miller, Shon Harris, Allen A. Harper, Stephen VanDyke, Chris Blask. (2011). Security Information and Event Management (SIEM) Implementation. New York: Mc Graw Hill.

[2] Kelly M. Kavanagh, Toby Bussa. (2017). Magic Quadrant for Security Information and Event Management. 26 de Febrero de 2018, de Gartner Sitio web: www.gatner.com. Visitado el 7 de abril de 2018.

[3] Karen Scarfone. (2018). Comparing the best SIEM systems on the market. Sitio web: https://searchsecurity.techtarget.com/feature/Comparing-the-best-SIEM-systems-on-the-market. Visitado el 5 de abril de 2018.

[4] Ben Canner. (2018). The Top 6 SIEM Vendors to Watch. Sitio web: https://solutionsreview.com/security-information-event-management/top-6-siem-vendors-watch-2018/. Visitado el 5 de abril de 2018.

[5] Micro Focus Enterprise Security Team, John P. Mello Jr, Jaikumar Vijayan, Paul Brettle. (2017). Security Information and Event Management (SIEM). Sitio web: https://learn.techbeacon.com/tracks/siem. Visitado el 5 de abril de 2018.

[6] Elastic Stack and Product Documentation (2018). Sitio web: https://www.elastic.co/guide/index.html. Visitado el 5 de abril de 2018. Visitado el 1 de mayo de 2018.

[7] Wazuh. Documentation Wazuh 3.x (2018). Sitio web: https://documentation.wazuh.com/current/index.html.Visitado el 5 de abril de 2018. Visitado el 1 de mayo de 2018.

[8] Search Guard. Search Guard 6 Documentation (2016-2017). Sitio web: https://documentation.wazuh.com/current/index.html.Visitado el 5 de abril de 2018. Visitado el 28 de abril de 2018.

7.Anexos

7.1.-Script del cortafuegos iptables “fw.sh”.

```
#!/bin/bash
iptables -F
iptables -X

# Limpiamos la tabla de NAT
iptables -t nat -F
iptables -t nat -X

# Políticas del Cortafuegos
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP

#REGLAS INPUT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT

iptables -N Regla_1
iptables -A INPUT -i enp0s3 -s 192.168.1.15 -p tcp --dport 22 -m state --state NEW -j Regla_1
iptables -A Regla_1 -j LOG --log-level 4 --log-prefix " permitido "
iptables -A Regla_1 -j ACCEPT

iptables -A INPUT -j LOG --log-prefix " Denegado Regla_Fin_Input " --log-level 4

#REGLAS FORWARD
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -N Regla_2
iptables -A FORWARD -i enp0s3 -s 192.168.1.0/24 -p tcp --dport 80 -d 192.168.2.5 -m state --
state NEW -j Regla_2
iptables -A Regla_2 -j LOG --log-level 4 --log-prefix " permitido Regla_2 "
iptables -A Regla_2 -j ACCEPT

iptables -N Regla_3
iptables -A FORWARD -i enp0s3 -s 192.168.1.0/24 -p tcp --dport 443 -d 192.168.2.5 -m state --
state NEW -j Regla_3
iptables -A Regla_3 -j LOG --log-level 4 --log-prefix " permitido Regla_3 "
iptables -A Regla_3 -j ACCEPT

iptables -N Regla_4
iptables -A FORWARD -i enp0s3 -s 192.168.1.0/24 -p udp --dport 1812 -d 192.168.2.10 -m state --
state NEW -j Regla_4
iptables -A Regla_4 -j LOG --log-level 4 --log-prefix " permitido Regla_4 "
iptables -A Regla_4 -j ACCEPT

iptables -N Regla_5
iptables -A FORWARD -i enp0s3 -s 192.168.1.0/24 -p udp --dport 1813 -d 192.168.2.10 -m state --
state NEW -j Regla_5
iptables -A Regla_5 -j LOG --log-level 4 --log-prefix " permitido Regla_5 "
iptables -A Regla_5 -j ACCEPT

iptables -N Regla_6
iptables -A FORWARD -i enp0s3 -s 192.168.1.15 -p tcp --dport 22 -d 192.168.2.10 -m state --state
NEW -j Regla_6
iptables -A Regla_6 -j LOG --log-level 4 --log-prefix " permitido Regla_6 "
iptables -A Regla_6 -j ACCEPT

iptables -N Regla_7
iptables -A FORWARD -i enp0s3 -s 192.168.1.15 -p tcp --dport 22 -d 192.168.2.5 -m state --state
NEW -j Regla_7
iptables -A Regla_7 -j LOG --log-level 4 --log-prefix " permitido Regla_7 "
iptables -A Regla_7 -j ACCEPT

iptables -N Regla_8
iptables -A FORWARD -i enp0s3 -s 192.168.1.50 -d 192.168.2.0/24 -m state --state NEW -j Regla_8
iptables -A Regla_8 -j LOG --log-level 4 --log-prefix " permitido Regla_8"
```

```
iptables -A Regla_8 -j ACCEPT

iptables -N Regla_9
iptables -A FORWARD -i enp0s8 -s 192.168.2.0/24 -o enp0s3 -m state --state NEW -j Regla_9
iptables -A Regla_9 -j LOG --log-level 4 --log-prefix " permitido Regla_9 "
iptables -A Regla_9 -j ACCEPT

iptables -A FORWARD -j LOG --log-prefix " Denegado Regla_Fin_Forw " --log-level 4

iptables -t nat -N Regla_100
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o enp0s3 ! -d 192.168.1.0/24 -j Regla_100
iptables -t nat -A Regla_100 -j LOG --log-level 4 --log-prefix " Acceso_a_internet Regla_100 "
iptables -t nat -A Regla_100 -j MASQUERADE
```

7.2.-Fichero de configuración de nxlog "/etc/nxlog.conf" para convertir el log del cortafuegos a formato JSON.

```
## This is a sample configuration file. See the nxlog reference manual about the
## configuration options. It should be installed locally under
## /usr/share/doc/nxlog-ce/ and is also available online at
## http://nxlog.org/docs

########################################
# Global directives                    #
########################################
User nxlog
Group nxlog

LogFile /var/log/nxlog/nxlog.log
LogLevel INFO

########################################
# Modules                              #
########################################
<Extension _syslog>
    Module      xm_syslog
</Extension>

<Extension kvp>
    Module          xm_kvp
    KVPDelimiter    ' '
    KVDelimiter     =
    EscapeChar      \\
</Extension>

<Extension json>
    Module      xm_json
</Extension>

<Input in1>
    Module      im_file
    File        '/var/log/iptables.log'
    SavePos TRUE
    ReadFromLast TRUE
    <Exec>
        parse_syslog();
        if ( $Message =~ /^(\S+) (\S+) IN=(\S+) OUT=(\S+)? \
MAC=(\S+:\S+:\S+:\S+:\S+:\S+):(\S+:\S+:\S+:\S+:\S+:\S\S):08:00 SRC=(\S+) DST=(\S+) LEN=(\S+) \
TOS=(\S+) PREC=(\S+) TTL=(\S+) ID=(\S+) (\S+)? ?PROTO=(\S+) ?S?P?T?=?(\d+)? ?D?P?T?=?(\d+)? \
(.*)?$/ )
        {
                $Accion = $1;
                $Regla = $2;
                $Zona_Origen = $3;
                $Zona_Destino = $4;
                $MAC_DST = $5;
                $MAC_SRC=$6;
                $IP_Origen = $7;
                $IP_Destino = $8;
                $Longitud_Paquete = $9;
                $TOS = $10;
                $PREC = $11;
```

```
                $TTL=$12;
                $ID = $13;
                $FRAG = $14;
                $Protocolo = $15;
                $Puerto_Origen = $16;
                $Puerto_Destino = $17;
                $resto = $18;
        }

                delete($Hostname);
                delete($EventTime);
                delete($EventReceivedTime);
                delete($SourceModuleName);
                delete($SourceName);
                delete($SourceModuleType);
                delete($SyslogFacilityValue);
                delete($SyslogFacility);
                delete($SyslogFacilityUser);
                delete($SyslogSeverityValue);
                delete($SyslogSeverity);
                delete($SeverityValue);
                delete($Severity);
                delete($Message);
                to_json();
    </Exec>
</Input>

<Output fileout1>
    Module      om_file
    File        "/var/log/iptables"
</Output>

########################################
# Routes                               #
########################################
<Route 1>
    Path        in1 => fileout1
</Route>
```

7.3.-Configuración del fichero “linelog” en radius para extraer los logs relativos al cliente y NAS en la autenticación.

```
# -*- text -*-
#
#  $Id: c646da0a05cbdf6e984f79cea105de41de4b0528 $
#
#  The "linelog" module will log one line of text to a file.
#  Both the filename and the line of text are dynamically expanded.
#
#  We STRONGLY suggest that you do not use data from the
#  packet as part of the filename.
#
linelog {
        #
        #  The file where the logs will go.
        #
        #  If the filename is "syslog", then the log messages will
        #  go to syslog.
        filename = ${logdir}/linelog

        #
        #  Most file systems can handly nearly the full range of UTF-8
        #  characters.  Ones that can deal with a limited range should
        #  set this to "yes".
        #
        escape_filenames = no

        #
        #  The Unix-style permissions on the log file.
        #
        #  Depending on format string, the log file may contain secret or
```

```
        #  private information about users.  Keep the file permissions as
        #  restrictive as possible.
        permissions = 0600

        #  If logging via syslog, the severity can be set here.
        #  Defaults to info.
        #
        #  The default format string.
        format = "This is a log message for %{User-Name}"

        #  Reference the Packet-Type (Access-Accept, etc.)  If it doesn't
        #  exist, reference the "default" entry.
        reference = "messages.%{%{reply:Packet-Type}:-default}"

        #  The messages defined here are taken from the "reference"
        #  expansion, above.

        #Mensaje de autenticación convertido a formato JSON
        messages {
        Access-Accept = "{\"01-Autent\":\"Login OK\", \"02-Usuario\":\"%{User-Name}\", \"05-
NAS\":\"%{NAS-Identifier}\", \"04-MAC-CLIENTE\":\"%{Calling-Station-Id}\", \"03-IP-
CLIENTE\":\"%{Framed-IP-Address}\", \"06-SSID\":\"MISTIC\"}"

        Access-Reject = "{\"01-Autent\":\"Login FAIL\", \"02-Usuario\":\"%{User-Name}\", \"05-
NAS\":\"%{NAS-Identifier}\", \"04-MAC-CLIENTE\":\"%{Calling-Station-Id}\", \"03-IP-
CLIENTE\":\"%{Framed-IP-Address}\", \"06-SSID\":\"MISTIC\"}"
    }
}
```