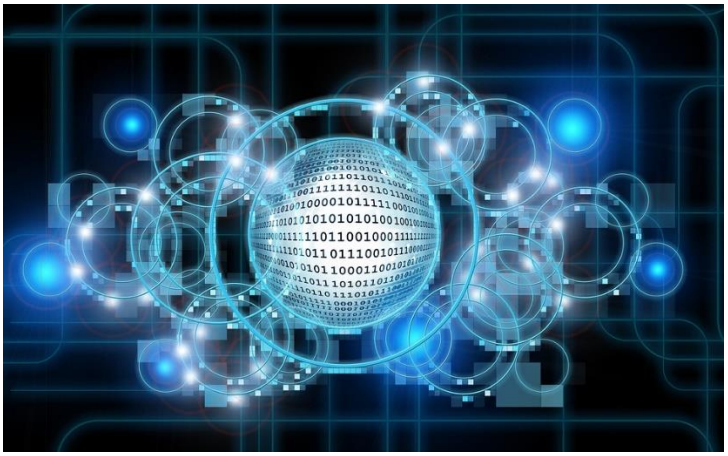
**Fundamentos de SIEM, *Security Information and Event Management***

Las herramientas SIEM, ofrecen un análisis en tiempo real para eventos de seguridad generados en gran medida por la infraestructura de los sistemas de información.



https://cdn.pixabay.com/photo/2018/05/30/08/43/binary-3441010_960_720.jpg

## 1. Conceptos

Los SIEM se convierten en estrategias de ciberseguridad muy importante en la gestión de eventos, ya que recopilan los datos de *logs* que facilitan los análisis forenses para determinar las causas que pueden generar eventos o incidentes de seguridad digital. Asimismo, permiten mantener la seguridad en los *logs* que pueden servir como evidencia de cumplimiento de requisitos legales en procesos de auditoría.

A continuación, se describen algunos conceptos básicos que fundamentan los SIEM.

- **Recolección de *Logs***

  Consisten en la recopilación de *logs* de manera planificada, ordenada y cronológica, de diversos dispositivos o elementos de una red, que permite a los administradores de sistemas, equipos de seguridad y auditores de sistemas, entender los sucesos digitales que garantizan o ponen en riesgo los principios de seguridad de la información (Confidencialidad, Integridad y disponibilidad). La recolección de *logs* también es importante para tener evidencia digital ante casos de investigación judicial.

- **Eventos de Ciberseguridad**

  Se puede considerar un evento de ciberseguridad, a la ocurrencia identificada del estado de un sistema, servicio o red que indica una posible violación de la seguridad digital, o un suceso previamente desconocido que puede ser importante para la seguridad digital. Dentro de un SIEM, un evento se considera como el objeto de análisis, por tanto, los eventos deben ser

registrados aplicando el concepto de *log*, de tal manera que se pueda almacenar la mayor cantidad de datos relevantes del evento de ciberseguridad.

Los eventos deben ser documentados o registrados considerando los eventos o sucesos relacionados con:

- Accesos de usuario y administradores en aplicaciones, servicios y sistemas.
- Mecanismos de autenticación e identificación.
- Accesos y comportamientos de la red.
- Accesos remotos e inalámbricos.
- Cambios en la configuración de aplicaciones, servicios y sistemas.
- Cambios en los usuarios, accesos y perfiles.
- Cambios en las funcionalidades de los sistemas de seguridad digital.
- Accesos a registros de sistemas, aplicaciones y servicios
- Consumo de recursos.

- **Gestión de la información de seguridad - *SIM, Security Information Management***

  El SIEM realiza la centralización y administración de *logs*, el reporte de logs, y el reporte de cumplimiento, enfocado en monitoreo tradicional de infraestructura TI y no propiamente en seguridad digital.

  "Es la práctica de recopilar, supervisar y analizar datos relacionados con la seguridad de los registros informáticos. Un sistema de gestión de la información de seguridad (SIMS) automatiza esa práctica. La información de seguridad incluye datos de registro generados a partir de numerosas fuentes, incluido el *software* antivirus, los sistemas de detección de intrusiones (IDS), los sistemas de prevención de intrusiones (IPS), los SIEM, temas de archivos, los cortafuegos, los enrutadores, los servidores y los conmutadores."

  Traducido de searchsecurity.techtarget.com (2009).

- **Gestión de Eventos de Seguridad - SEM *(Security event management)***

  Es predecesor a los SIEM y pertenece al mundo de seguridad digital. Se refiere a herramientas de revisión y análisis de datos para centralizar el almacenamiento y la interpretación de registros o eventos generados por dispositivos o elementos de una red.

  El SIM realiza captura de eventos en los dispositivos de red, sistemas, servicios y aplicaciones, realizando correlacionamiento de *logs* y un monitoreo en tiempo real de eventos para la respuesta a eventos e incidentes de seguridad digital.

- **Gestión de Eventos e Información de Seguridad - *SIEM, Security Information and Event Management)***

  El SIEM agrupa las características o definiciones de SEM y SIM, por así decirlo una conjugación, en donde se aplican cada una de las bondades para gestionar los eventos e información de seguridad digital relacionados. En sí, los SIEM son una evolución de SEM y SIM, los cuales permiten detectar anomalías de la red, amenazas, fallos, comportamientos de los usuarios, activos en la red, vulnerabilidades, probar la seguridad de los controles y el cumplimiento de regulaciones o estándares.
  Carvajal (2012).

## 2. Características

Los SIEM constan de datos de eventos de diversas fuentes de *logs*, una base de conocimiento o referencia para contrastar los eventos de los *logs*, reglas de cumplimiento.

- **Recolección de *logs***: función que se encarga de recolectar los *logs* de los dispositivos y elementos de la red sujetos de monitoreo, tales como Sistemas operativos, aplicaciones, bases de datos, dispositivos de red, entre otros.

- **Base de conocimiento**: consiste en una base de datos referente para determinar qué eventos son maliciosos con base en sucesos anteriores o pasados, la misma puede ser alimentada con nuevos eventos maliciosos detectados.

- **Reglas de cumplimiento**: se trata de reglas predefinidas y configurables para el cumplimiento de normas, regulaciones o estándares, como por ejemplo la ISO/IEC 27001.

- **Detección y Análisis**: realiza proceso de detección de eventos de logs con base en las fuentes o bases de conocimiento, generando salidas para la toma de acciones de respuesta. Genera información valiosa a partir de logs para análisis, informes y monitorización en tiempo real.

  El funcionamiento a nivel lógico de un SIEM está ordenado en capas de recolección, correlación y almacenamiento.

- **Recolección**: recolección de *logs* de forma activa (Consultas a Bases de datos, SCP, otros) y pasiva (Syslogs y agentes). En la recolección se deben configurar las fuentes de logs al sistema SIEM, y en los dispositivos de red se deben configurar el destino de logs que será el SIEM, para los sistemas operativos se pueden implementar agentes del SIEM.

- **Correlación**: consiste en la recepción de eventos, almacenamiento temporal, genera eventos correlacionados con base en los *logs* recolectados, dispara alarmas o notificaciones, y se pueden realizar búsquedas y análisis.

- **Almacenamiento**: se encarga de *backups* y control de datos considerando las regulaciones, leyes y/o normativas, determinado el tiempo de almacenado, la rotación y la accesibilidad. El almacenamiento facilita las búsquedas, consultas y reportes, la centralización de información de *logs*, y permite asegurar la integridad de los datos de los logs.

  Otras características importantes son el descubrimiento de vulnerabilidades, análisis y detección de anomalías de red, apoyo al cumplimiento normativo y centralización de reportes.

## 3. Aplicación

Para la aplicación de un SIEM dentro de una organización se debe definir el alcance de acuerdo con el contexto de la organización, y determinando los objetivos, presupuesto, entre otros detalles. Así entonces, considere los siguientes aspectos para la aplicación de un SIEM.

- **Definir objetivos y alcance**: según el contexto, necesidades y expectativas de la organización.

- **Cumplimiento**: establecer que normatividad se busca cumplir y que sistema SIEM es más adecuado.

- **Compatibilidad**: es importante determinar la compatibilidad en las fuentes de datos de los logs con el sistema SIEM que se quiere implementar. En este sentido se debe revisar si el SIEM que se pretende implementar es capaz de leer los logs de los sistemas operativos, aplicaciones y demás elementos de la red.

- **Activos Críticos**: *se deben considerar los activos de información críticos que requieren de la protección del SIEM, así entonces la solución SIEM a implementar se define con base a las necesidades de protección de dichos activos críticos.*

- **Presupuesto:** debe justificar la viabilidad financiera de los recursos de *hardware*, *software* y servicios de red necesarios para la implementación del SIEM conforme a los objetivos y alcance, destacando los beneficios para la compañía.

En la actualidad existen muchas soluciones SIEM y a veces resulta difícil elegir qué fabricante o marca de SIEM adquirir para implementar. Una de las formas de elegir una solución de SIEM es consultar los reportes de *Gartner* y específicamente sus denominados cuadrantes mágicos de *Gartner.*

Gartner, es una compañía de investigación y asesoramiento, principalmente en la investigación tecnológica. Gartner desarrolló una herramienta para saber sobre el liderazgo de la tecnología en el mercado a nivel mundial, la cual sirve como referente para elegir las soluciones y proveedores de tecnologías que más convienen.

- **Cuadrante mágico de Gartner**

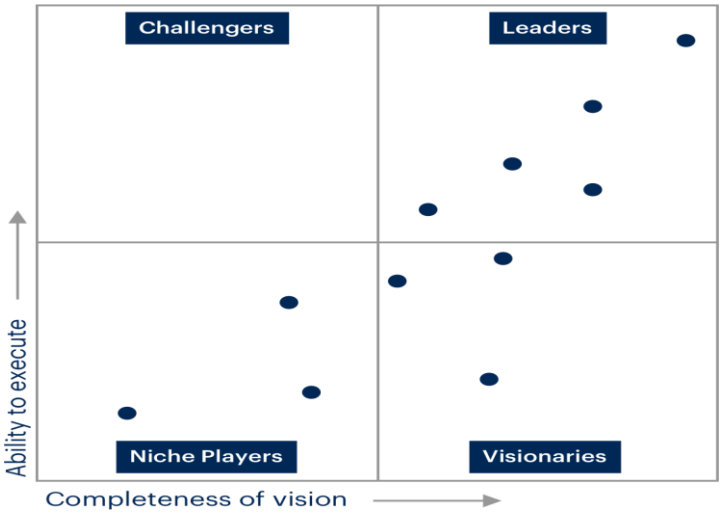
  Un Cuadrante Mágico proporciona un posicionamiento competitivo gráfico de cuatro tipos de proveedores de tecnología, en mercados donde el crecimiento es alto y la diferenciación de proveedores es distinta:

  - Los líderes se desempeñan bien en contra de su visión actual y están bien posicionados para el mañana.
  - Los visionarios entienden hacia dónde se dirige el mercado o tienen una visión para cambiar las reglas del mercado, pero aún no lo ejecutan bien.
  - Los jugadores de nicho se enfocan con éxito en un segmento pequeño, o están desenfocados y no superan en innovación ni superan a los demás.
  - Los retadores se desempeñan bien hoy en día o pueden dominar un gran segmento, pero no demuestran una comprensión de la dirección del mercado.

  *Traducido de Gartner (2021)*

**Figura 1**

*Cuadrante mágico de gartner*




Nota: https://emtemp.gcom.cloud/ngw/commonassets/images/build-graphics/mq-preview.png

A continuación, se muestra el Cuadrante mágico de *gartner* de las soluciones SIEM del año 2020

**Figura 2**

*Cuadrante mágico de gartner - SIEM 2020.*


Nota: https://panoramait.com/wp-content/uploads/2020/03/7mo.png

A continuación, se listan algunas soluciones SIEM:

- *Fusion SIEM*
- *IBM QRadar*
- *LogRhythm*
- *SolarWinds*
- *Splunk*
- *Elastic Security*
- *InsightsIDR*
- *Sumo Logic*
- *Graylog*
- *NetWitness*
- *AlienVault OSSIM (Open Source Security Information and Event Management)*

Para más detalles se recomienda visitar el recurso de *Pathak (2021)*, en la siguiente url https://geekflare.com/es/best-siem-solutions/

Todas las soluciones SIEM mantienen los conceptos y características similares, a continuación, se describe la solución *AlienVault OSSIM.*

- *AlienVault OSSIM (Open-Source Security Information and Event Management)*

“Una de las herramientas SIEM de código abierto más utilizadas: AlienVault OSSIM, es excelente para que los usuarios instalen la herramienta por sí mismos. Este software de gestión de eventos e información de seguridad proporciona un SIEM rico en funciones con correlación, normalización y recopilación de eventos.

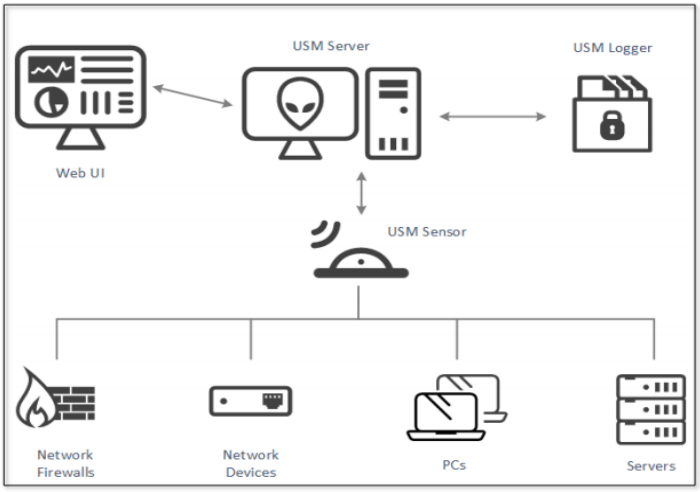
AlienVault OSSIM puede abordar muchas dificultades que encuentran los profesionales de la seguridad, como la detección de intrusiones, la evaluación de vulnerabilidades, el descubrimiento de activos, la correlación de ventilación y el monitoreo del comportamiento. Utiliza AlienVault Open Threat Exchange y le permite recibir datos en tiempo real sobre hosts maliciosos.”
Pathak (2021)

**Funcionalidades de seguridad**:

- *Inventario y descubrimiento de activos.*
- *Evaluación de vulnerabilidad.*
- *Detección de intrusiones.*
- *Monitoreo del comportamiento.*
- *Correlación de eventos siem.*
- *Soporte de la comunidad a través de foros de productos.*
- *Monitoreado por open threat exchange – OTX.*

**Figura 3**

*Arquitectura de AlienVault OSSIM*




Nota: https://cybersecurity.att.com/documentation/resources/pdf/usm-appliance-deployment-guide.pdf

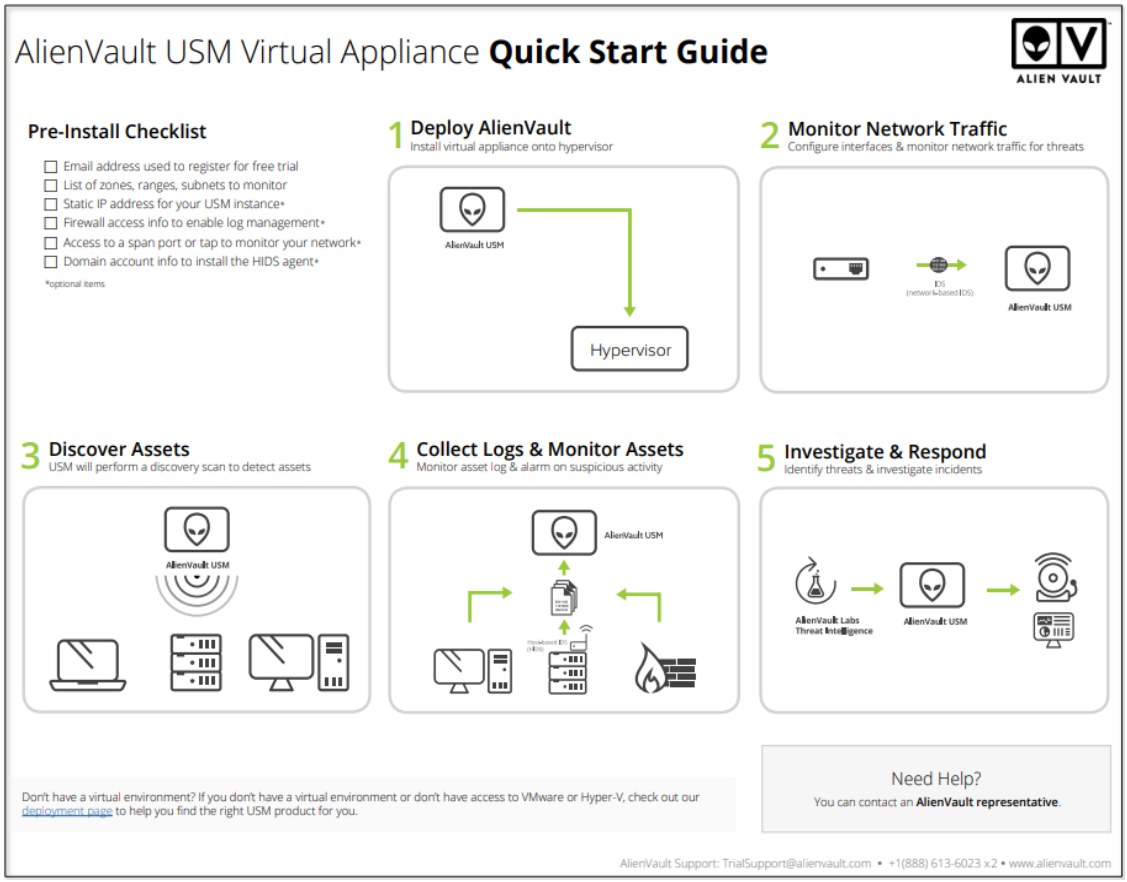
USM es igual a OSSIM, ya que USM es la versión comercial, pero manejan la misma arquitectura.

- **Instalación de OSSIM**

Para instalar *AlienVault* OSSIM se debe seguir la documentación oficial del fabricante *(AT&T)*, a continuación, se muestra un paso a paso rápido de cómo sería la instalación de OSSIM.

**Figura 4**

*Quick Start Guide Virtual Appliance*



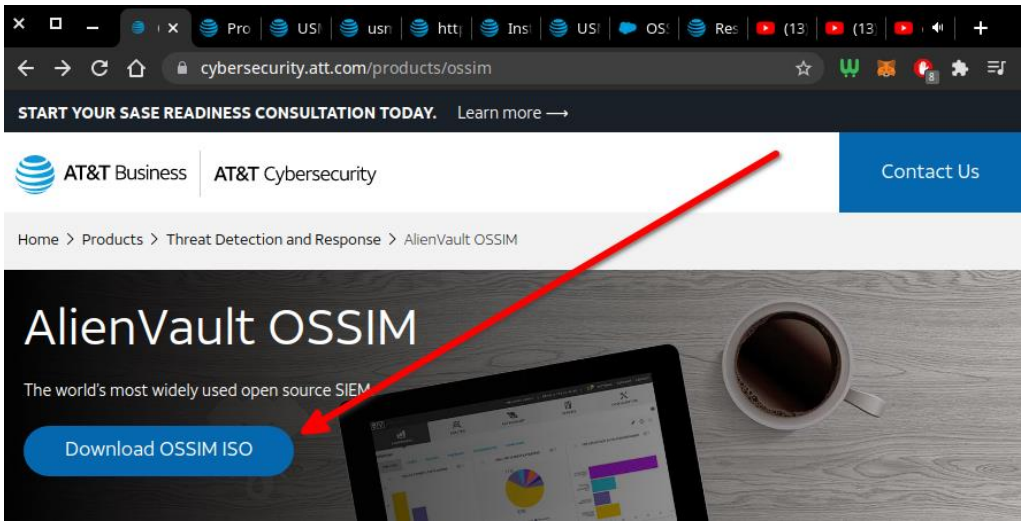

Nota: https://cybersecurity.att.com/documentation/resources/pdf/usm-appliance-quick-start-guide.pdf

Un *Virtual Appliance* es una máquina virtual preconfigurada que se despliega o instala en un entorno de servidores virtuales denominados hipervisores o en inglés *Hypervisor*. Existen varios hipervisores tales como VMware, Hyper-V, Citrix, Proxmox, ZenServe, VirtualBox. OSSIM es un sistema preconfigurado que se puede desplegar en un entorno físico o virtual.

Para descargar OSSIM se debe ir a la página oficial de por medio del siguiente enlace, https://cybersecurity.att.com/products/ossim, y hacer clic en el botón de descarga.

**Figura 5**

*Descargar AlienVault OSSIM*




Nota: https://cybersecurity.att.com/products/ossim

Para una mayor comprensión y detalles de cómo implementar OSSIM se recomienda seguir la guía de implementación oficial, por medio del siguiente enlace:

https://cybersecurity.att.com/documentation/resources/pdf/usm-appliance-deployment-guide.pdf

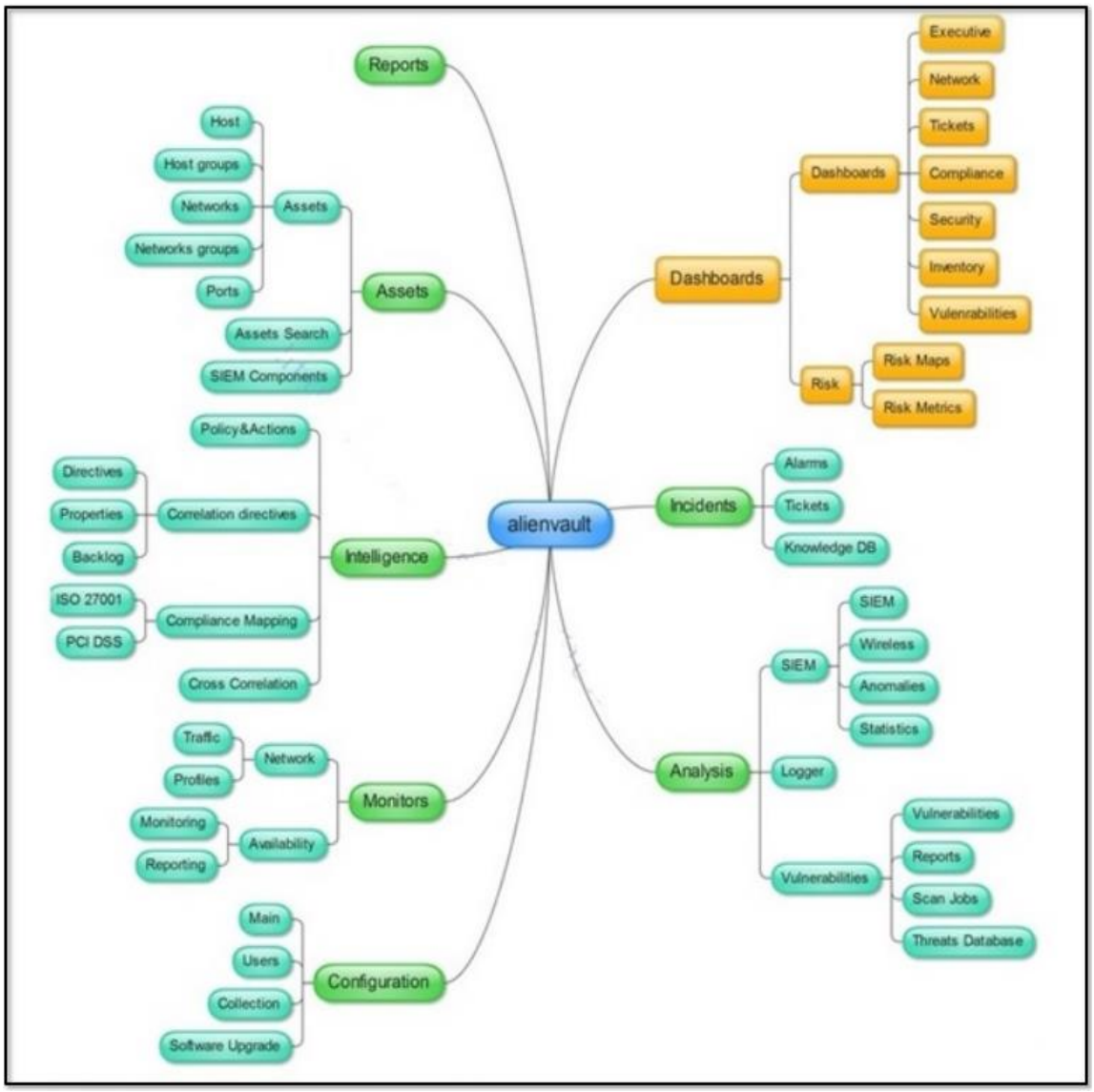
También, se recomienda seguir el tutorial de mejores prácticas de configuración de OSSIM disponible en el canal de *Youtube* de *AT&T Cybersecurity,* a través del siguiente enlace https://youtu.be/qjaO1cNj2fo.

“AlienVault OSSIM es un framework de monitorización y cumplimiento (compliance) gratuito y de código abierto, es decir, una plataforma de seguridad para pequeñas y medianas empresas. Está compuesto por una colección de herramientas todas con licencias GPL que permiten controlar los servicios ofrecidos por cada *host* de la red, incluidos switchs, routers, firewalls. También es capaz de analizar el tráfico entre los hosts de una LAN y entre una LAN y la WAN.”
López (2017).

El trabajo de *José Luis López Fernández, de la Universitat Oberta de Catalunya - UOC,* es un referente importante en la aplicación de un SIEM, en el cual se presenta con un enfoque para realizar análisis de vulnerabilidades dentro de una organización.

**Figura 6**

*Funcionalidades de OSSIM*




Nota:

http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72567/6/jlopezfernanTFG0118memoria.pdf