**¿Qué es OSSEC?**

Ellos mismos se definen como “*un sistema de detección de intrusiones (HIDS) escalable, multiplataforma y de código abierto basado en host*”.

Ossec es una herramienta que integra el análisis de registros, monitoreo de integridad de archivos, detección de rootkits, alertas en tiempo real y aplicación centralizada de políticas. Esta herramienta puede operar en diversos sistemas operativos como Linux, MacOS o Windows.

Este software es gratuito y de licencia GNU (versión 3) publicada por el FSF – Free Software Foundation, por lo que se puede redistribuir y modificar siempre bajo este tipo de licencia.

Ossec es una herramienta utilizada por grandes empresas y agencias gubernamentales como su principal sistema de detección de intrusos de servidores. Además, se usa como herramienta de análisis de registros, monitoreando y analizando firewalls, IDS, servidores web y registros de autenticación.

Las características principales de Ossec, de las que hablaremos más adelante, son la detección de intrusos basada en registros (LID), detección de malware y rootkits, respuesta activa, auditoría de cumplimiento, monitoreo de integridad de archivos (FIM) y recopilación de información del sistema.

**BENEFICIOS CLAVE:**

Requisitos de cumplimiento:

Permite detectar y alertar a los clientes sobre modificaciones no autorizadas del sistema de archivos y comportamientos maliciosos incrustados en los archivos de registro. También cubre las secciones de monitoreo de integridad de archivos, inspección y monitoreo de registros y aplicación/verificación de políticas.

Alertas configurables y en tiempo real:

Permite configurar incidentes sobre los que desean recibir alertas, y les permite centrarse en aumentar la prioridad de los incidentes críticos sobre el ruido normal de cualquier sistema. La integración con smtp, sms y syslog permite a los clientes estar al tanto de las alertas enviándolas a dispositivos habilitados para correo electrónico. Las opciones de respuesta activa para bloquear un ataque de inmediato también están disponibles.

Gestión centralizada:

OSSEC proporciona un servidor de administración centralizado simplificado para administrar políticas en múltiples sistemas operativos. Además, también permite a los clientes definir anulaciones específicas del servidor para políticas más específicas.

Supervisión de agente y sin agente:

OSSEC ofrece la flexibilidad de la supervisión basada en agentes y sin agentes de sistemas y componentes de red como enrutadores y firewalls. El monitoreo sin agente permite a los clientes que tienen restricciones en la instalación de software en sistemas (como sistemas o dispositivos aprobados por la FDA) cumplir con las necesidades de seguridad y cumplimiento.

**ARQUITECTURA:**

OSSEC está compuesto de múltiples piezas:

Gerente

Almacena las bases de datos de comprobación de integridad de archivos, los registros, los eventos y las entradas de auditoría del sistema. Todas las reglas, decodificadores y las principales opciones de configuración se almacenan centralmente en el administrador  
Los agentes se conectan al servidor en el puerto 1514 / udp. Se debe permitir la comunicación a este puerto para que los agentes se comuniquen con el servidor.

Agentes

El agente es un pequeño programa, o colección de programas, instalado en los sistemas a monitorear. El agente recopilará información y la enviará al gerente para su análisis y correlación.

Nota: OSSEC solo se puede instalar como agente en plataformas Microsoft Windows. Estos sistemas requerirán un servidor OSSEC, que se ejecute en Linux u otro sistema similar a Unix.

Sin agentes

Para los sistemas en los que no se puede instalar un agente, el soporte sin agente puede permitir que se realicen verificaciones de integridad. Los escaneos sin agente se pueden usar para monitorear firewalls, enrutadores e incluso sistemas Unix.

Virtualizacion/VMWare

OSSEC le permite instalar el agente en los sistemas operativos invitados. También se puede instalar dentro de algunas versiones de VMWare ESX.

Firewalls, switches y routers

OSSEC puede recibir y analizar eventos de syslog de una gran variedad de firewalls, conmutadores y enrutadores.

**Sistemas operativos**

Los siguientes sistemas operativos son compatibles con el agente OSSEC:

* GNU / Linux (todas las distribuciones, incluidas RHEL, Ubuntu, Slackware, Debian, etc.)
* Windows XP, 2003, Vista, 2008, 2012
* VMWare ESX 3.0,3.5 (incluidas las comprobaciones de CIS)
* FreeBSD (todas las versiones actuales)
* OpenBSD (todas las versiones actuales)
* NetBSD (todas las versiones actuales)
* Solaris 2.7, 2.8, 2.9, 10 y 11.4
* AIX 5.2 y 5.3
* Mac OS X 10.x
* HP-UX 11

**Instalación:**

<https://www.ossec.net/docs/docs/manual/installation/index.html>

**Agentes**

Hay dos tipos de agentes dentro de OSSEC: agentes instalables y agentes sin agente. Los agentes instalables se instalan en los hosts e informan a un servidor central OSSEC a través del protocolo de mensajes cifrados OSSEC. Los agentes sin agente no requieren instalación en hosts remotos. Son procesos iniciados desde el administrador OSSEC, que recopilan información de sistemas remotos y utilizan cualquier método RPC (por ejemplo, ssh, snmp rdp, wmi).

Agentes instalables:

La comunicación entre los agentes y el servidor OSSEC generalmente ocurre en el puerto 1514/udp en modo seguro. Si usa el modo syslog para ossec-remote , entonces el puerto 514 es el predeterminado (se admiten tanto UDP como TCP). Estos puertos son configurables en la sección [remota](https://www.ossec.net/docs/docs/syntax/head_ossec_config.remote.html) de ossec.conf

Ejemplo de configuración:

**<agent\_config**  os = "Linux" **>**

**<localfile>**

**<location>** /var/log/my.log2 **</location>**

**<log\_format>** syslog **</log\_format>**

**</localfile>**

**</agent\_config>**

Sin agentes:

**La supervisión** sin agente le permite ejecutar la verificación de integridad en sistemas sin un agente instalado (incluidos enrutadores, firewalls, conmutadores e incluso sistemas Linux / BSD). Se puede ejecutar al igual que nuestra comprobación de integridad de archivos normal (alerta de cambios en la suma de comprobación) o haciendo diferencias y mostrando exactamente lo que ha cambiado.

Ejemplo de configuración:

**<agentless>**

**<type>** ssh\_integrity\_check\_linux **</type>**

**<frequency>** 36000 **</frequency>**

**<host>** root@example.net **</host>**

**<state>** periodic **</state>**

**<arguments>** /bin/etc//sbin **</argumentos>**

**</agentless>**

**Análisis/monitorización de registros**

Se realiza dentro de OSSEC por el recolector de registros y los procesos analizados. El primero recopila los eventos y el segundo los analiza (decodifica, filtra y clasifica). OSSEC puede leer eventos desde archivos de registro internos, desde el registro de eventos de Windows y también recibirlos directamente a través de syslog remoto.

Opciones de configuración

Estas opciones deben especificarse localmente en el archivo ossec.conf de cada agente o en el recurso compartido agent.conf. Dentro del elemento, puede tener las siguientes opciones.

* <location>: Especifica la ubicación del registro que se leerá. Los formatos de strftime pueden usarse para nombres de archivos de registro

Default:/var/log/messages  
Valor permitido: Cualquier fichero log

* <log\_format>: El formato del registro que se lee.  
  Default: syslog  
  Valores permitidos:
  + *syslog*: Este formato es para archivos de texto sin formato en un formato tipo syslog. También se puede usar cuando no hay soporte para el formato de registro, y los registros son mensajes de una sola línea
  + *snort-full*: Se usa para el formato de salida completo de Snort.
  + *snort-fast*: Se usa para el formato de salida rápida de Snort.
  + *eventlog*: Se usa para el formato de registro de eventos de Microsoft Windows
  + *eventchannel*: Se usa para los registros de eventos de Microsoft Windows
  + *mysql\_log*: Se usa para los registros de MySQL. No admite registros de varias líneas.
  + *postgresql\_log*: Se usa para los registros de PostgreSQL. No admite registros de varias líneas.
  + *nmapg*: Se usa para monitorear archivos que se ajustan a la salida grepable de nmap.
  + *apache*: Se usa para el formato de registro predeterminado de apache
  + *command*: Este formato será el resultado del comando (como lo ejecuta la raíz) definido por él. Cada línea de salida se tratará como un registro separado. No se puede usar en agent.conf
  + *full\_command*: Este formato será el resultado del comando (como lo ejecuta la raíz) definido por él. Toda la salida se tratará como un único registro. No se puede usar en agent.conf
  + *multi-line*: Esta opción permitirá monitorear las aplicaciones que registran varias líneas por evento. Este formato requiere que el número de líneas sea consistente. Será seguido por el número de líneas en cada entrada de registro. Cada línea se combinará con las líneas anteriores hasta que todas las líneas estén reunidas en una sola
  + *multi-line\_indented*: Este formato de registro acepta registros que abarcan varias líneas con líneas posteriores que comienzan con un espacio o una pestaña.
* <command>:  
  El comando a ejecutar. Todos los resultados de este comando se leerán como uno o más mensajes de registro dependiendo de si se usa el comando o full\_command.  
  Valores permitidos: Cualquier línea de comando y argumentos.
* <alias>:  
  Un alias para identificar el comando. Este reemplazará el comando en el mensaje que muestre el registro.
* <frequency>:  
  El tiempo mínimo en segundos entre ejecuciones de comandos. Esto se usa con command y full\_command.  
  Valores permitidos: Tiempo en segundos.
* <check\_diff>:  
  La salida de un evento se almacenará en una base de datos interna. Cada vez que se recibe el mismo evento, la salida se compara con la salida anterior. Si la salida ha cambiado, se generará una alerta.
* <only-future-events>:  
  Solo se usa con el eventchannel de registro. OSSEC solo recibirá eventos que ocurrieron después del inicio de logcollector.  
  Valor permitidos: Yes/No
* <query>:  
  Solo se usa con el eventchannel de registro. Es posible especificar una consulta XPATH siguiendo el esquema de eventos para filtrar los eventos que procesará OSSEC.

Monitoreo de procesos

OSSEC agrega la capacidad de monitorear la salida de comandos y tratar la salida de esos comandos como si fueran registros. A partir de OSSEC v2.3 se puede monitorear comandos directamente en OSSEC siguiendo la configuración (/var/ossec/etc/ossec.conf)

Monitoreo de archivos

OSSEC tiene un proceso llamado ossec-logcollector que monitorea los archivos de registro configurados para nuevos eventos. Cuando llegan nuevos mensajes de registro, los reenvía a otros procesos para su análisis o transporte a un servidor OSSEC.

**Syscheck**

Syscheck es el nombre del proceso de verificación de integridad dentro de OSSEC. Se ejecuta periódicamente para verificar si algún archivo configurado (o entrada de registro en Windows) ha cambiado.

La comprobación de integridad es una parte esencial de la detección de intrusos, que detecta cambios en la integridad del sistema. OSSEC lo hace buscando cambios en las sumas de verificación MD5 / SHA1 de los archivos clave en el sistema y en el registro de Windows. La forma en que funciona es que el agente escanea el sistema cada pocas horas (definido por el usuario) y envía todas las sumas de verificación al servidor. El servidor almacena las sumas de comprobación y busca modificaciones en ellas. Se envía una alerta si algo cambia.

Ejemplo de configuración:

**<syscheck>**

**<directories** check\_all="yes"**>**/etc,/usr/bin,/usr/sbin**</directories>**

**</syscheck>**

**Rootcheck**

OSSEC HIDS realizará la detección de rootkits en todos los sistemas donde esté instalado el agente. El rootcheck (motor de detección de rootkit) se ejecutará cada X minutos (especificado por el usuario, por defecto cada 2 horas) para detectar cualquier posible rootkit instalado. Utilizado con el análisis de registro y el motor de verificación de integridad, se convertirá en una solución de monitoreo muy poderosa.

**Testing Ossec rules**

El primer problema que tiene la mayoría de las personas al solucionar problemas de OSSEC o al intentar escribir nuevas reglas y decodificadores es cómo probarlos. En el pasado, esto requeriría reiniciar manualmente OSSEC o crear una instalación de prueba. A partir de la versión 1.6, existe una herramienta para simplificar esta tarea (ossec-logtest). La herramienta ossec-logtest está instalada en /var/ossec/bin. Leerá las reglas actuales y el decodificador (desde /var/ossec) y aceptará la entrada de registro desde stdin.

Búsquedas de la lista de CDB desde dentro de las reglas

OSSEC permite búsquedas de CDB desde dentro de las reglas (ossec-analysisd) de todos los campos posibles.

Los archivos CDB deben compilarse antes de que puedan usarse. [ossec-makelists](https://www.ossec.net/docs/docs/programs/ossec-makelists.html" \l "ossec-makelists) se usa para compilar listas.

El comando [ossec-makelists](https://www.ossec.net/docs/docs/programs/ossec-makelists.html" \l "ossec-makelists) procesará y compilará todas las listas si se han cambiado las reglas del texto maestro. Básicamente, la lógica es la siguiente:

* Lee ossec.conf para todas las listas
* Verifica el tiempo m de cada lista y lo compara con el tiempo m del archivo compilado .cdb
* Si mtime es más nuevo, crea un nuevo archivo de base de datos que termina en .tmp
* Usa el cambio de nombre atómico para cambiar el .tmp a .cdb. Esto invalidará todas las páginas mmap actualmente en uso por ossec-analysisd y hará que se vuelvan a cargar con los nuevos datos según sea necesario.

Cada lista necesitará ser definida y se le pedirá que esté disponible usando el archivo ossec.conf. Usando la siguiente sintaxis:

**<ossec\_config>**

**<rules>**

**<list>** reglas / registros **</list>**

Crear reglas personalizadas

Una de las principales características de OSSEC es el sistema de monitoreo y los registros de aplicaciones. Muchos servicios populares tienen registros y decodificadores, pero hay cientos que no están cubiertos. Las aplicaciones y servicios personalizados tampoco estarán cubiertos. Agregar decodificadores y reglas para servicios es generalmente muy fácil.

Agregar un archivo de registro a la configuración para el monitoreo es simple. En el sistema ossec.conf agregue una entrada como esta:

**<localfile>**

**<log\_format>** syslog **</log\_format>**

**<location>** / path / to / log / file **</location>**

**</localfile>**

Carga de ruta de directorio de reglas y decodificadores

Ossec-anaylistd permite cargar directorios completos de archivos como decodificadores, listas o reglas. Simplifica enormemente el trabajo con decodificadores, ya que puede haber tantos archivos como sea necesario. También hará que el empaquetado de reglas y decodificadores sea una operación simple de descompresión / descompresión y reinicio. Esto también reducirá en gran medida la cantidad de código necesario para administrar los scripts de actualización de ossec. Toda la carga del directorio se realiza en forma alfabética.