GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

Capítulo 5.

Monitorización de sistemas y comunicaciones. (2ª Parte)

José Pablo Hernández

Sistemas IDS.

La cantidad de intentos de accesos no autorizados a la información que existe en Internet ha crecido durante estos últimos años.

Un Sistema de Detección de Intrusos o IDS (Intrusion Detection System) es una herramienta de seguridad encargada de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión.

Definimos intento de intrusión como cualquier intento de comprometer la confidencialidad, integridad, disponibilidad o evitar los mecanismos de seguridad de una computadora o red.

Sistemas IDS.

Las intrusiones se pueden producir de varias formas:

- Atacantes que acceden a los sistemas desde Internet.
- Usuarios autorizados del sistema que intentan ganar privilegios adicionales para los cuales no están autorizados.
- Usuarios autorizados que hacen un mal uso de los privilegios que se les han asignado.

Sistemas IDS.

La detección de intrusiones permite a las organizaciones proteger sus sistemas de las amenazas que aparecen al incrementar la conectividad en red y la dependencia que tenemos hacia los sistemas de información.

Los IDSs han ganado aceptación como una pieza fundamental en la infraestructura de seguridad de la organización.

Sistemas IDS.

Hay varias razones para adquirir y usar un IDS:

- Prevenir problemas al disuadir a individuos hostiles.
- Detectar ataques y otras violaciones de la seguridad que no son prevenidas por otras medidas de protección.
- Detectar preámbulos de ataques (normalmente pruebas de red y otras actividades).
- Documentar el riesgo de la organización.
- Proveer información útil sobre las intrusiones que se están produciendo.

Sistemas IDS.

Hay varias razones para adquirir y usar un IDS:

- Prevenir problemas al disuadir a individuos hostiles.

Al incrementar la posibilidad de descubrir y castigar a los atacantes, el comportamiento de algunos cambiará de forma que muchos ataques no llegarán a producirse.

Esto también puede jugar en nuestra contra, puesto que la presencia de un sistema de seguridad sofisticado puede hacer crecer la curiosidad del atacante.

Sistemas IDS.

Hay varias razones para adquirir y usar un IDS:

- Detectar ataques y otras violaciones de la seguridad que no son prevenidas por otras medidas de protección.

Los atacantes, usando técnicas ampliamente conocidas, pueden conseguir accesos no autorizados a muchos sistemas, especialmente a aquellos conectados a redes públicas.

Esto a menudo ocurre cuando vulnerabilidades conocidas no son corregidas.

Sistemas IDS.

Hay varias razones para adquirir y usar un IDS:

- Detectar ataques y otras violaciones de la seguridad que no son prevenidas por otras medidas de protección.

Aunque los vendedores y administradores procuran dar a conocer y corregir estas vulnerabilidades, hay situaciones en las que esto no es posible:

- En algunos sistemas heredados, los sistemas operativos no pueden ser parcheados o actualizados. Incluso en los sistemas en los que podemos aplicar parches, los administradores a veces no tienen el suficiente tiempo y recursos para seguir e instalar las últimas actualizaciones necesarias.

- Esto es un problema común, sobre todo en entornos que incluyen un gran número de hosts con sistemas operativos y hardware variado.

- Los usuarios y administradores pueden equivocarse al configurar sus sistemas.

Sistemas IDS.

Hay varias razones para adquirir y usar un IDS:

- Detectar preámbulos de ataques (normalmente pruebas de red y otras actividades).

Cuando un individuo ataca un sistema, lo hace típicamente en fases predecibles.

En la primera fase, el atacante hace pruebas y examina el sistema o red en busca de un punto de entrada óptimo.

En sistemas o redes que no disponen de un IDS, el atacante es libre de examinar el sistema con un riesgo mínimo de ser detectado. Esto le facilita la búsqueda de un punto débil en nuestra red.

Sistemas IDS.

Hay varias razones para adquirir y usar un IDS:

- Detectar preámbulos de ataques (normalmente pruebas de red y otras actividades).

La misma red con un IDS monitorizando sus operaciones le presenta una mayor dificultad.

Aunque el atacante puede examinar la red, el IDS observará estas pruebas, las identificará como sospechosas, podrá activamente bloquear el acceso del atacante al sistema objetivo y avisará al personal de seguridad de lo ocurrido para que tome las acciones pertinentes.

Sistemas IDS.

Hay varias razones para adquirir y usar un IDS:

- Documentar el riesgo de la organización.

Cuando se hace un plan para la gestión de seguridad de la red o se desea redactar la política de seguridad de la organización, es necesario conocer cual es el riesgo de la organización a posibles amenazas, la probabilidad de ser atacada o si incluso ya está siendo atacada.

Un IDS nos puede ayudar a conocer la amenaza existente fuera y dentro de la organización, ayudándonos a tomar decisiones acerca de los recursos de seguridad que deberemos emplear en nuestra red y del grado de cautela que deberemos adoptar al redactar la política de seguridad.

Sistemas IDS.

Hay varias razones para adquirir y usar un IDS:

- Proveer información útil sobre las intrusiones que se están produciendo.

Incluso cuando los IDSs no son capaces de bloquear ataques, pueden recoger información relevante sobre éstos.

Esta información puede, bajo ciertas circunstancias, ser utilizada como prueba en actuaciones legales.

También se puede usar esta información para corregir fallos en la configuración de seguridad de los equipos o en la política de seguridad de la organización.

Sistemas IDS. Tipos de IDS

Hay dos tipos básicos de sistemas de detección de intrusiones:

- Los basados en red (NIDS)
- Los basados en hosts (HIDS).

Sistemas IDS. Tipos de IDS. NIDS.

La mayor parte de los sistemas de detección de intrusos están basados en red.

Estos IDSs detectan ataques capturando y analizando paquetes de la red.

Escuchando en un segmento, un NIDS puede monitorizar el tráfico que afecta a múltiples hosts que están conectados a ese segmento de red, protegiendo así a estos hosts.

Sistemas IDS. Tipos de IDS. NIDS.

Los IDSs basados en red a menudo están formados por un conjunto de sensores localizados en varios puntos de la red.

Estos sensores monitorizan el tráfico realizando análisis local e informando de los ataques que se producen a la consola de gestión.

Como los sensores están limitados a ejecutar el software de detección, pueden ser mas fácilmente asegurados ante ataques.

Muchos de estos sensores son diseñados para correr en modo oculto, de tal forma que sea más difícil para un atacante determinar su presencia y localización.

Sistemas IDS. Tipos de IDS. NIDS.

Ventajas:

- Un IDS bien localizado puede monitorizar una red grande, siempre y cuando tenga la capacidad suficiente para analizar todo el tráfico.

- Los NIDSs tienen un impacto pequeño en la red, siendo normalmente dispositivos pasivos que no interfieren en las operaciones habituales de ésta.

- Se pueden configurar para que sean muy seguros ante ataques haciéndolos invisibles al resto de la red.

Sistemas IDS. Tipos de IDS. NIDS.

Desventajas:

Pueden tener dificultades procesando todos los paquetes en una red grande o con mucho tráfico y pueden fallar en reconocer ataques lanzados durante periodos de tráfico alto. Algunos vendedores están intentando resolver este problema implementando IDSs completamente en hardware, lo cual los hace mucho más rápidos.

Los IDSs basados en red no analizan la información cifrada. Este problema se incrementa cuando la organización utiliza cifrado en el propio nivel de red (IPSec) entre hosts, pero se puede resolver con una política de seguridad más relajada (por ejemplo, IPSec en modo túnel).

Sistemas IDS. Tipos de IDS. HIDS.

Los HIDS fueron el primer tipo de IDSs desarrollados e implementados.

Operan sobre la información recogida desde dentro de una computadora, como pueda ser los ficheros de auditoría del sistema operativo.

Esto permite que el IDS analice las actividades que se producen con una gran precisión, determinando exactamente qué procesos y usuarios están involucrados en un ataque particular dentro del sistema operativo.

A diferencia de los NIDSs, los HIDSs pueden ver el resultado de un intento de ataque, al igual que pueden acceder directamente y monitorizar los ficheros de datos y procesos del sistema atacado.

Sistemas IDS. Tipos de IDS. HIDS.

Ventajas:

Los IDSs basados en host, al tener la capacidad de monitorizar eventos locales a un host, pueden detectar ataques que no pueden ser vistos por un IDS basado en red.

Pueden a menudo operar en un entorno en el cual el tráfico de red viaja cifrado, ya que la fuente de información es analizada antes de que los datos sean cifrados en el host origen y/o después de que los datos sea descifrados en el host destino.

Sistemas IDS. Tipos de IDS. HIDS.

Desventajas:

Los IDSs basados en hosts son más costosos de administrar, ya que deben ser gestionados y configurados en cada host monitorizado. Mientras que con los NIDS teníamos un IDS por múltiples sistemas monitorizados, con los HIDS tenemos un IDS por sistema monitorizado.

Si la estación de análisis se encuentra dentro del host monitorizado, el IDS puede ser deshabilitado si un ataque logra tener éxito sobre la máquina.

No son adecuados para detectar ataques a toda una red (por ejemplo, escaneos de puertos) puesto que el IDS solo ve aquellos paquetes de red enviados a él.

Pueden ser deshabilitados por ciertos ataques de DoS.

Usan recursos del host que están monitorizando, influyendo en el rendimiento del sistema monitorizado.

Sistemas IDS. Tipos de análisis.

Hay dos acercamientos al análisis de eventos para la detección de ataques:

Detección de abusos y detección de anomalías.

La detección de abusos es la técnica usada por la mayoría de sistemas comerciales.

La detección de anomalías, en la que el análisis busca patrones anormales de actividad, ha sido y continua siendo objeto de investigación. La detección de anomalías es usada de forma limitada por un pequeño número de IDSs.

Sistemas IDS. Tipos de análisis.

Detección de abusos o firmas.

Los detectores de abusos analizan la actividad del sistema buscando eventos que coincidan con un patrón predefinido o firma que describe un ataque conocido.

Sistemas IDS. Tipos de análisis.

Detección de abusos o firmas.

Ventajas:

Los detectores de firmas son muy efectivos en la detección de ataques sin que generen un número elevado de falsas alarmas.

Pueden rápidamente y de forma precisa diagnosticar el uso de una herramienta o técnica de ataque específico. Esto puede ayudar a los encargados de la seguridad a priorizar medidas correctivas.

Pueden permitir a los administradores de seguridad, sin importar su nivel o su experiencia en este campo, el seguir la pista de los problemas de seguridad de sus sistemas

Sistemas IDS. Tipos de análisis.

Detección de abusos o firmas.

Desventajas:

Solo detectan aquellos ataques que conocen, por lo que deben ser constantemente actualizados con firmas de nuevos ataques.

Muchos detectores de abusos son diseñados para usar firmas muy ajustadas que les privan de detectar variantes de ataques comunes.

Sistemas IDS. Tipos de análisis.

Detección de anomalías.

La detección de anomalías se centra en identificar comportamientos inusuales en un host o una red.

Funcionan asumiendo que los ataques son diferentes a la actividad normal.

Los detectores de anomalías construyen perfiles representando el comportamiento normal de los usuarios, hosts o conexiones de red.

Estos perfiles son construidos de datos históricos recogidos durante el periodo normal de operación.

Los detectores recogen los datos de los eventos y usan una variedad de medidas para determinar cuando la actividad monitorizada se desvía de la actividad normal.

Sistemas IDS. Tipos de análisis.

Detección de anomalías.

Las medidas y técnicas usadas en la detección de anomalías incluyen:

Detección de un umbral sobre ciertos atributos del comportamiento del usuario. Tales atributos de comportamiento pueden incluir el numero de ficheros accedidos por un usuario en un periodo de tiempo dado, el numero de intentos fallidos para entrar en el sistema, la cantidad de CPU utilizada por un proceso, etc. Este nivel puede ser estático o heurístico.

Medidas estadísticas, que pueden ser paramétricas, donde la distribución de los atributos perfilados se asume que encaja con un determinado patrón, o no paramétricas, donde la distribución de los atributos perfilados es aprendida de un conjunto de valores históricos, observados a lo largo del tiempo.

Otras técnicas incluyen redes neuronales, algoritmos genéticos y modelos de sistema inmune.

Sistemas IDS. Tipos de análisis.

Detección de anomalías.

Ventajas:

Los IDSs basados en detección de anomalías detectan comportamientos inusuales.
De esta forma tienen la capacidad de detectar ataques para los cuales no tienen un conocimiento específico.

Los detectores de anomalías pueden producir información que puede ser utilizada para definir firmas en la detección de abusos.

Sistemas IDS. Tipos de análisis.

Detección de anomalías.

Desventajas:

La detección de anomalías produce un gran número de falsas alarmas debido a los comportamientos no predecibles de usuarios y redes.

Requieren conjuntos de entrenamiento muy grandes para caracterizar los patrones de comportamiento normal.

Sistemas IDS. Tipos de análisis.

Respuesta.

Desventajas:

Una vez se ha producido un análisis de los eventos y hemos detectado un ataque, el IDS reacciona.

Las repuestas las podemos agrupar en dos tipos:

Las pasivas envían informes a personas, que se encargarán de tomar acciones al respecto, si procede.

Las activas lanzan automáticamente respuestas a dichos ataques.

Sistemas IDS. Tipos de análisis.

Respuestas pasivas.

En este tipo de respuestas se notifica al responsable de seguridad de la organización, al usuario del sistema atacado o a algún CERT (**Computer Emergency Response Team**)de lo sucedido.

También es posible avisar al administrador del sitio desde el cual se produjo el ataque avisándole de lo ocurrido, pero es posible que el atacante monitorice el correo electrónico de esa organización o que haya usado una IP falsa para su ataque.

Sistemas IDS. Tipos de análisis.

Respuestas activas

Las respuestas activas son acciones automáticas que se toman cuando ciertos tipos de intrusiones son detectados.

Podemos estableces dos categorías distintas:

Recogida de información adicional: consiste en incrementar el nivel de sensibilidad de los sensores para obtener más pistas del posible ataque (por ejemplo, capturando todos los paquetes que vienen de la fuente que originó el ataque durante un cierto tiempo o para un máximo número de paquetes).

Cambio del entorno: otra respuesta activa puede ser la de parar el ataque; por ejemplo, en el caso de una conexión TCP se puede cerrar la sesión establecida inyectando segmentos TCP RST al atacante y a la víctima o filtrar en el router de acceso o en el firewall la dirección IP del intruso o el puerto atacado para evitar futuros ataques.

Sistemas IDS. Tipos de análisis.

Respuestas activas

Las respuestas activas son acciones automáticas que se toman cuando ciertos tipos de intrusiones son detectados.

Podemos estableces dos categorías distintas:

- Recogida de información adicional: consiste en incrementar el nivel de sensibilidad de los sensores para obtener más pistas del posible ataque (por ejemplo, capturando todos los paquetes que vienen de la fuente que originó el ataque durante un cierto tiempo o para un máximo número de paquetes).

- Cambio del entorno: otra respuesta activa puede ser la de parar el ataque; por ejemplo, en el caso de una conexión TCP se puede cerrar la sesión establecida inyectando segmentos TCP RST al atacante y a la víctima o filtrar en el router de acceso o en el firewall la dirección IP del intruso o el puerto atacado para evitar futuros ataques.

Sistemas IDS. Tipos de análisis.

Honeypots.

Son sistemas complementarios que están diseñados para ser atacados y que capturan de forma silenciosa todos los movimientos del atacantes.

Se usan principalmente para lo siguiente:

Evitan que el atacante pase su tiempo intentado acceder a sistemas críticos.

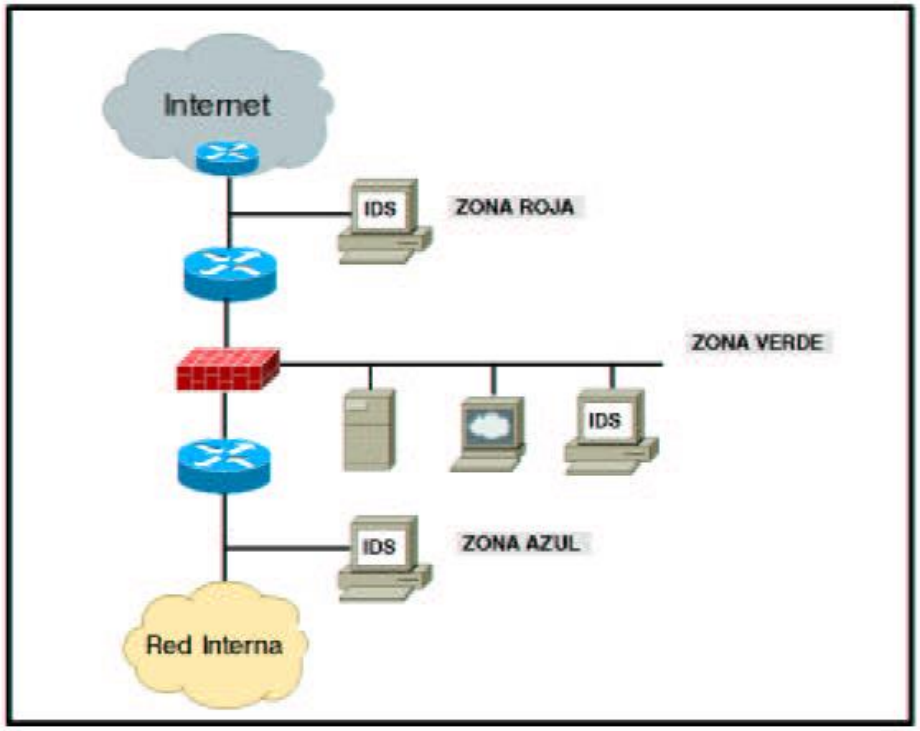
Recogen información sobre la actividad del atacante.

Permiten al administrador recabar pruebas de quién es el atacante y responda ante su CERT o el administrador del sistema origen de la agresión.

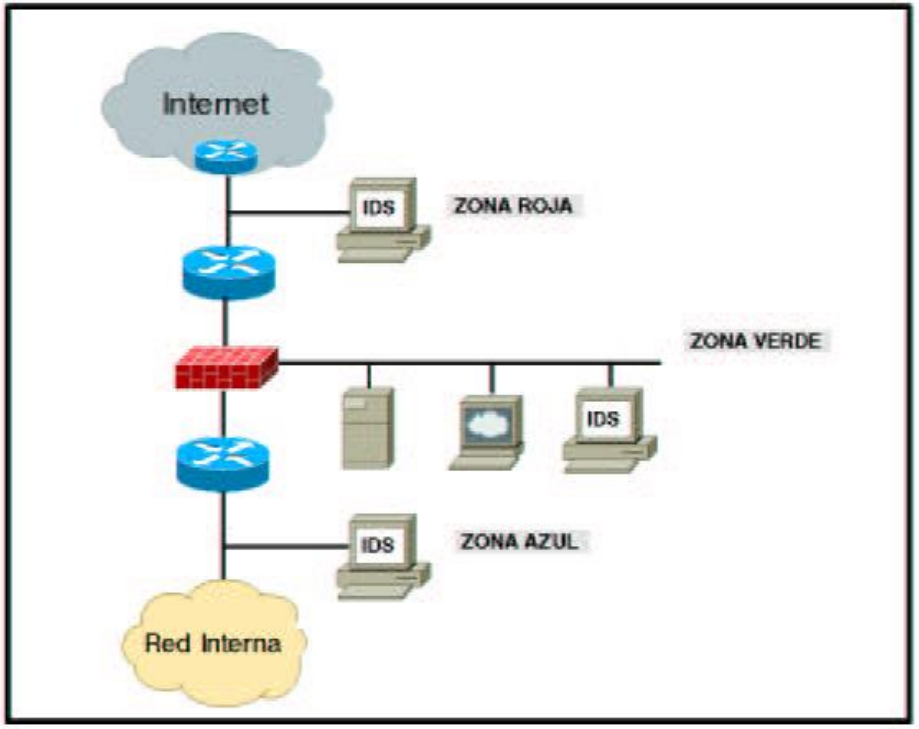
Sistemas IDS. ¿Dónde colocar un IDS?

La decisión de donde localizar el IDS es la primera que hay que tomar una vez que estamos dispuestos a instalar un IDS.

De esta decisión dependerá tanto el equipo que usemos, como el software IDS o la base de datos.



Sistemas IDS. ¿Dónde colocar un IDS?

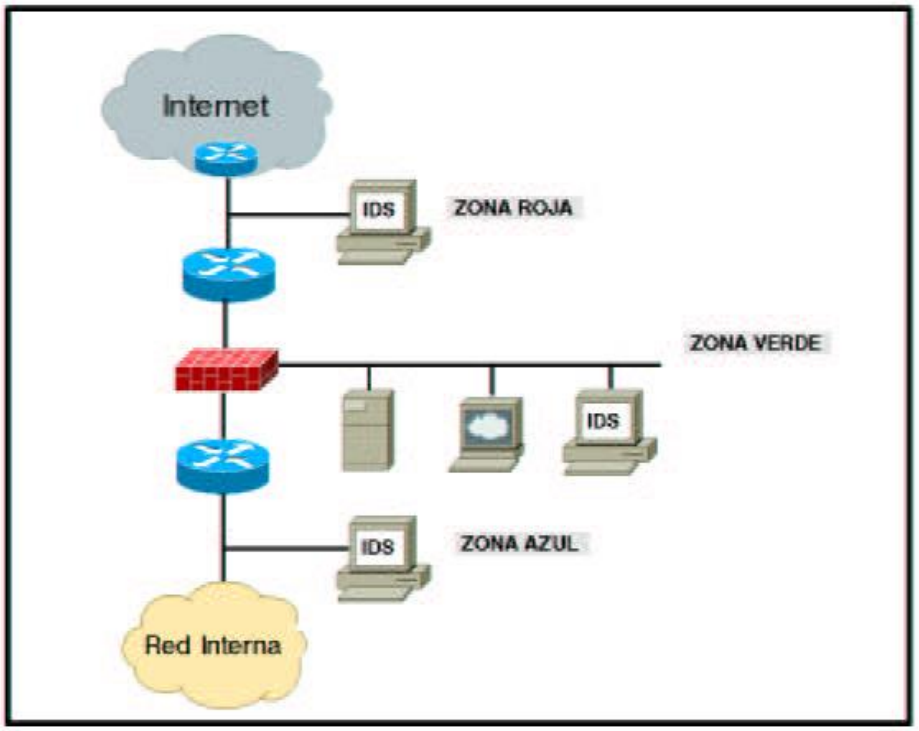


Zona roja:

Esta es una zona de alto riesgo.

En esta zona el IDS debe ser configurado para ser poco sensible, puesto que verá todo el tráfico que entre o salga de nuestra red y habrá más posibilidad de falsas alarmas.

Sistemas IDS. ¿Dónde colocar un IDS?

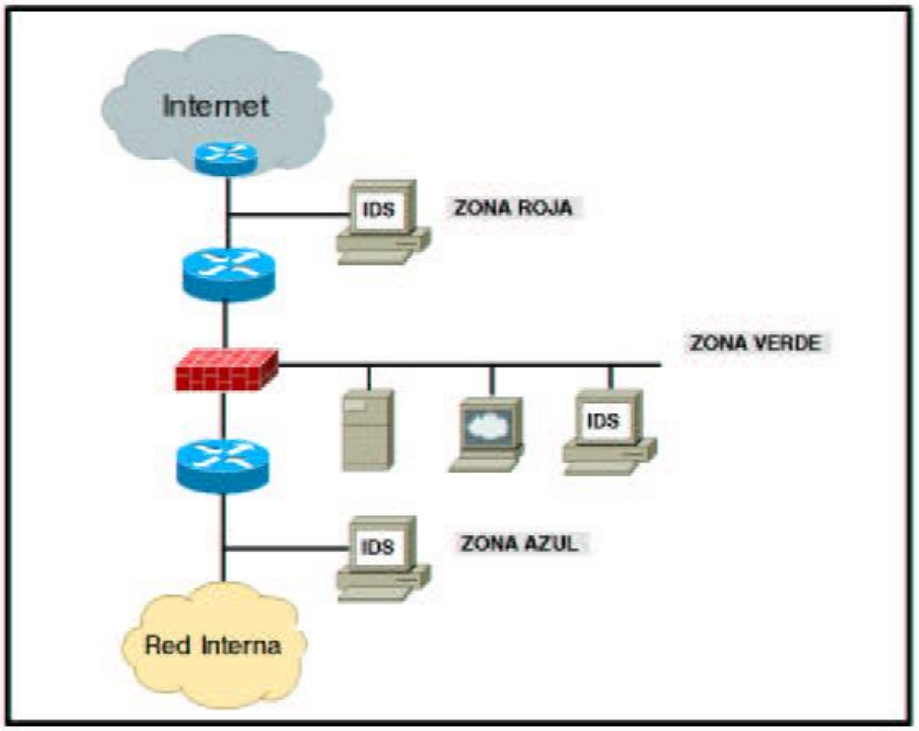


Zona verde:

El IDS debería ser configurado para tener una sensibilidad un poco mayor que en la zona roja, puesto que ahora, el firewall deberá ser capaz de filtrar algunos accesos definidos mediante la política de nuestra organización.

En esta zona aparece un menor número de falsas alarmas que en la zona roja, puesto que en este punto solo deberían estar permitidos accesos hacia nuestros servidores.

Sistemas IDS. ¿Dónde colocar un IDS?



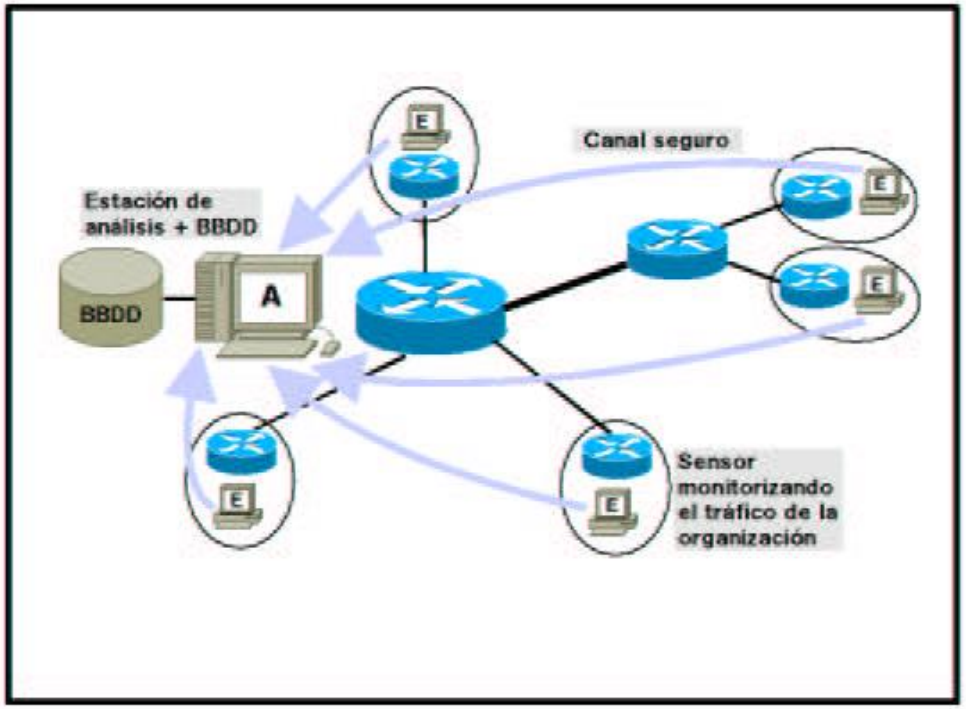
Zona azul:

Esta es la zona de confianza.

Cualquier tráfico anómalo que llegue hasta aquí debe ser considerado como hostil.

En este punto de la red se producirán el menor número de falsas alarmas, por lo que cualquier alarma del IDS debe de ser inmediatamente estudiada.

Sistemas IDS. ¿Dónde colocar un IDS?



Es posible que el tráfico a la entrada de una gran empresa sea demasiado grande como para ser técnicamente imposible instalar un único IDS que lo analice todo.

Para estos casos es necesario un sistema de detección de intrusos que pueda separar los sensores de la estación de análisis.

Una posible solución podría ser la de instalar un sensor en cada uno de los nodos que conectan físicamente con las delegaciones, y que estos sensores envíen las alertas generadas a la estación de análisis.

Sistemas IDS. Limitaciones de un IDS.

Los ataques de denegación de servicio también pueden dar al traste con una política de seguridad basada en un IDS.

Es entonces cuando hay que decidir si el IDS será ’fail-open’ o ’fail-closed’.

En el primer caso tenemos que cuando el IDS caiga, la red quedará totalmente abierta a merced de cualquier ataque, mientras que en el segundo caso, el trafico hacia el exterior y viceversa quedará bloqueado.

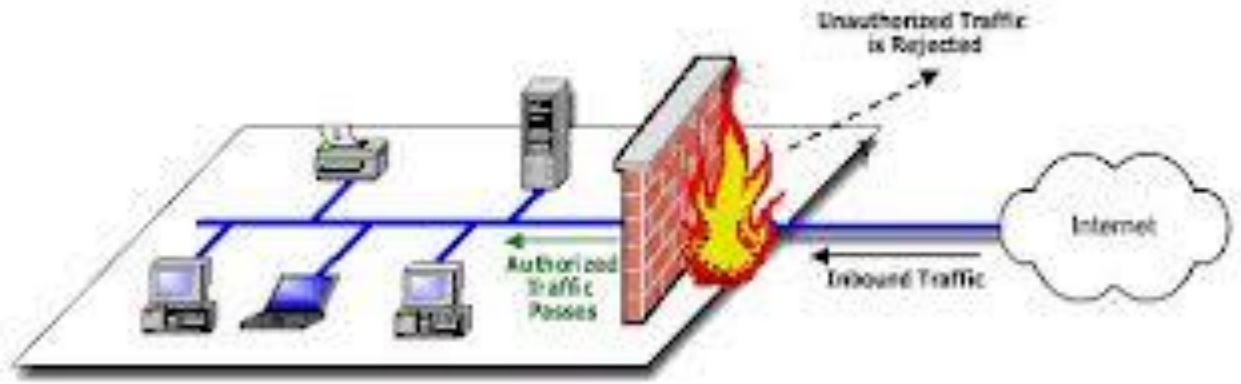
Los NIDSs son inherentemente ’fail-open’.

Cortafuegos (firewall).

Un firewall es la combinación de diferentes componentes:

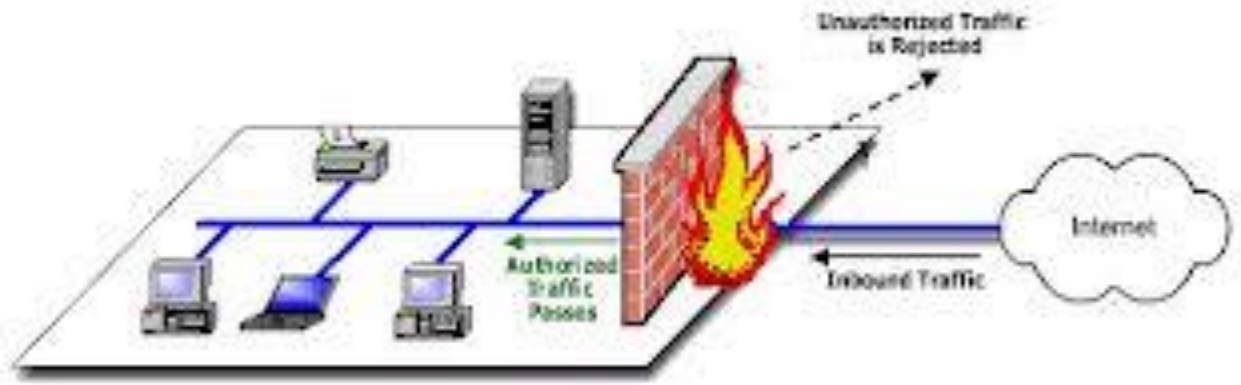
dispositivos físicos (hardware), programas (software) y actividades de administración, que, en conjunto, permitirán aplicar una política de seguridad de una red, haciendo efectiva una estrategia particular, para restringir el acceso entre ésta red y la red pública a la cual esté conectada.

El objetivo es protegerla de cualquier acción hostil proveniente de un host externo a la red.



Cortafuegos (firewall).

La función de un firewall es tal que todo el tráfico de entrada y salida de la red privada debe pasar a través de él; el tráfico permitido por el firewall es autorizado mediante su evaluación en base a la política de seguridad.

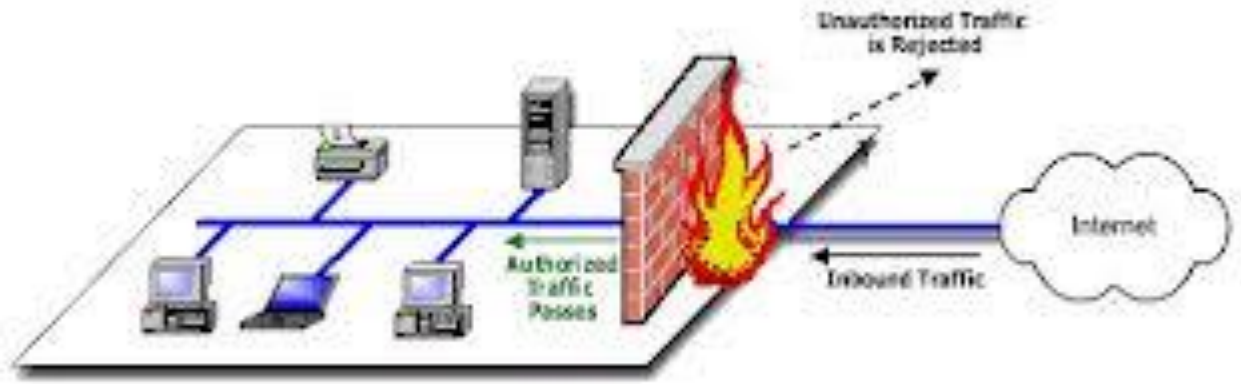


Cortafuegos (firewall).

La tarea de un firewall consiste en inspeccionar y controlar todo el tráfico entre la red local e Internet.

De esta forma se intenta detectar y rechazar todo el tráfico potencialmente peligroso antes de que alcance otras partes de la red interna, en algunos casos también se efectúan registros de tales actividades.

La determinación de qué es peligroso para la red local, es especificada en la política de seguridad adoptada por el sitio.



Sistemas IPS.

Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos.

Dado que los IPS fueron extensiones literales de los sistemas IDS, continúan en relación.

Sistemas IPS.

Un Sistema de Prevención de Intrusos, al igual que un Sistema de Detección de Intrusos, funciona por medio de módulos, pero la diferencia es que este último alerta al administrador ante la detección de un posible intruso (usuario que activó algún Sensor), mientras que un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo proactivamente y un IDS lo protege reactivamente.

Sistemas IPS.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

- Detección Basada en Firmas, como lo hace un antivirus.
- Detección Basada en Políticas, el IPS Requiere que se declaren muy específicamente las políticas de seguridad.
- Detección Basada en Anomalías, Función con el patrón de comportamiento normal de tráfico.
- Detección Honey Pot (Jarra de Miel), Funciona usando un equipo que se configura para que llame la atención de los hackers.

Sistemas IPS.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

- Detección Basada en Firmas

Una firma tiene la capacidad de reconocer una determinada cadena de bytes en cierto contexto, y entonces lanza una alerta.

Por ejemplo, los ataques contra los servidores Web generalmente toman la forma de URLs.

Por lo tanto se puede buscar utilizando un cierto patrón de cadenas que pueda identificar ataques al servidor Web. Sin embargo, como este tipo de detección funciona parecido a un Antivirus, el Administrador debe verificar que las firmas estén constantemente actualizadas.

Sistemas IPS.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

- Detección Basada en Políticas

En este tipo de detección, el IPS requiere que se declaren muy específicamente las políticas de seguridad. Por ejemplo, determinar que hosts pueden tener comunicación con determinadas redes. El IPS reconoce el tráfico fuera del perfil permitido y lo descarta.

Sistemas IPS.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

- Detección Basada en Anomalías

Este tipo de detección tiende a generar muchos falsos positivos, ya que es sumamente difícil determinar y medir una condición ‘normal’. En este tipo de detección tenemos dos opciones:

Detección Estadística de Anormalidades: El IPS analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.

Detección No Estadística de Anormalidades: En este tipo de detección, es el administrador quien define el patrón ‘normal’ de tráfico. Sin embargo, debido a que con este enfoque no se realiza un análisis dinámico y real del uso de la red, es susceptible a generar muchos falsos positivos.

Sistemas IPS.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

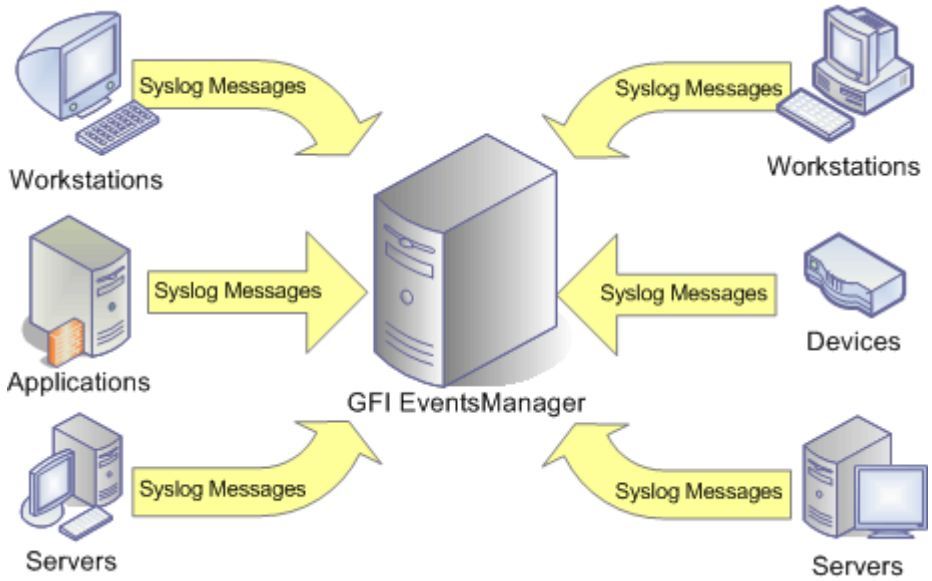
- Detección Honey Pot (Jarra de Miel)

Aquí se utiliza un ‘distractor’.

Se asigna como Honey Pot un dispositivo que pueda lucir como atractivo para los atacantes.

Los atacantes utilizan sus recursos para tratar de ganar acceso en el sistema y dejan intactos los verdaderos sistemas. Mediante esto, se puede monitorizar los métodos utilizados por el atacante e incluso identificarlo, y de esa forma implementar políticas de seguridad acordes en nuestros sistemas de uso real..

Sistemas de registro. Syslog.



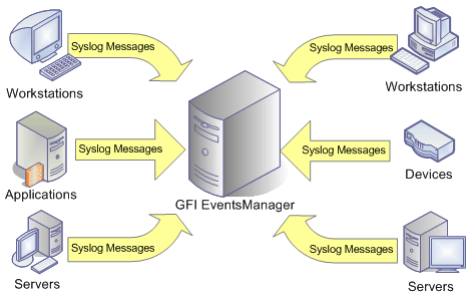
Syslog es un estándar de facto para el envío de mensajes de registro en una red informática IP.

Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

Un mensaje de registro suele tener información sobre la seguridad del sistema, aunque puede contener cualquier información.

Junto con cada mensaje se incluye la fecha y hora del envío.

Sistemas de registro. Syslog.

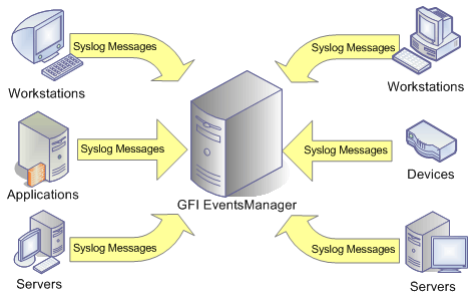


Es útil registrar, por ejemplo:

-Un intento de acceso con contraseña equivocada.
-Un acceso correcto al sistema.
-Anomalías: variaciones en el funcionamiento normal del sistema.
-Alertas cuando ocurre alguna condición especial.
-Información sobre las actividades del sistema operativo.
-Errores del hardware o el software.

También es posible registrar el funcionamiento normal de los programas; por ejemplo, guardar cada acceso que se hace a un servidor web, aunque esto suele estar separado del resto de alertas.

Sistemas de registro. Syslog.



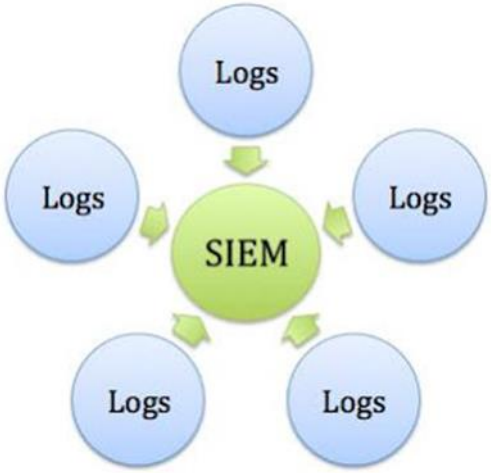
El protocolo syslog es muy sencillo: existe un ordenador servidor ejecutando el servidor de syslog, conocido como syslogd (demonio de syslog). El cliente envía un pequeño mensaje de texto (de menos de 1024 bytes).

Los mensajes de syslog se suelen enviar vía UDP, por el puerto 514, en formato de texto plano.

Algunas implementaciones del servidor, como syslog-ng, permiten usar TCP en vez de UDP, y también ofrecen Stunnel para que los datos viajen cifrados mediante SSL/TLS.

Aunque syslog tiene algunos problemas de seguridad, su sencillez ha hecho que muchos dispositivos lo implementen, tanto para enviar como para recibir. Eso hace posible integrar mensajes de varios tipos de sistemas en un solo repositorio central.

Sistemas de gestión de información y eventos de seguridad.

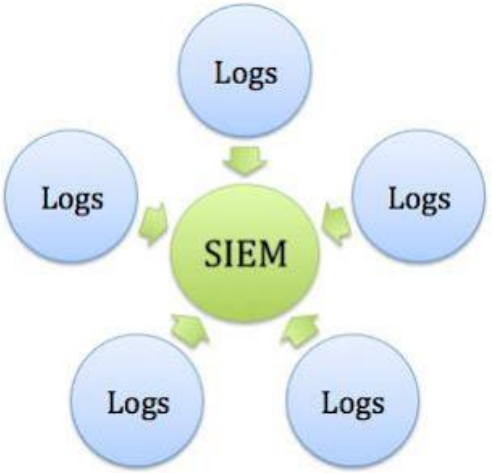


Hoy en día los ataques a organizaciones son cada vez más sofisticados e inmunes a la detección por parte de dispositivos IDS/IPS convencionales.

Los indicios de posibles actividades maliciosas pueden ser difíciles de observar y pueden llegar a pasar desapercibidas.

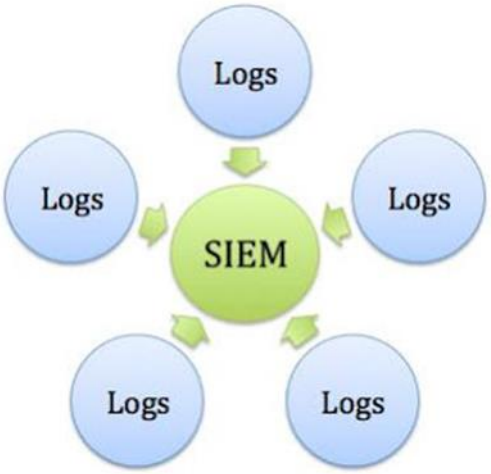
Se hace necesario por tanto revisar y correlacionar los eventos de varios dispositivos de nuestra red para encadenar y entender una serie de sucesos que nos lleven a la posibilidad real de detectar una posible intrusión en nuestros sistemas.

Sistemas de gestión de información y eventos de seguridad.



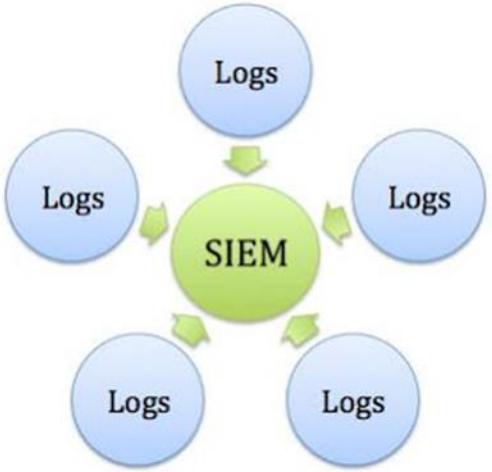
La Gestión Eventos de Seguridad (SEM) es el segmento de gestión de la seguridad que se ocupa de la monitorización en tiempo real, correlación de eventos de seguridad, notificaciones y la consola gestión de dichos eventos.

Sistemas de gestión de información y eventos de seguridad.



La Gestión de Seguridad de la Información (SIM) proporciona un almacenamiento a largo plazo, análisis y reporte de datos de registro.

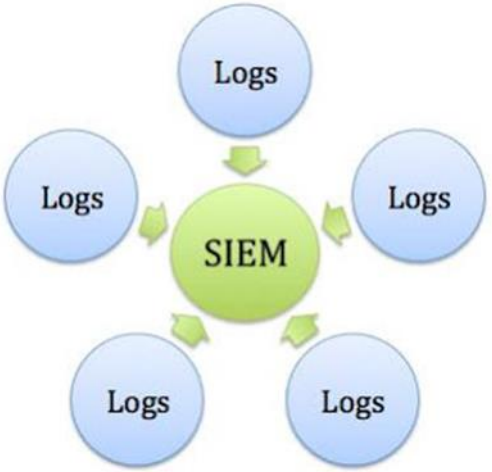
Sistemas de gestión de información y eventos de seguridad.



El término Gestión de Seguridad de la Información y de Eventos (SIEM) describe las capacidades de recolección, análisis y presentación de información de dispositivos de red y de seguridad, aplicaciones de control de identidades y accesos, gestión de vulnerabilidades y herramientas de política de cumplimiento, sistema operativo, base de datos y registros de aplicación, y datos externos potencialmente amenazadores.

Un aspecto clave es controlar y ayudar a controlar los privilegios de usuario y de servicios, servicios de directorio y otros cambios de configuración del sistema; así como el abastecimiento de registro de auditoría y respuesta a incidentes.

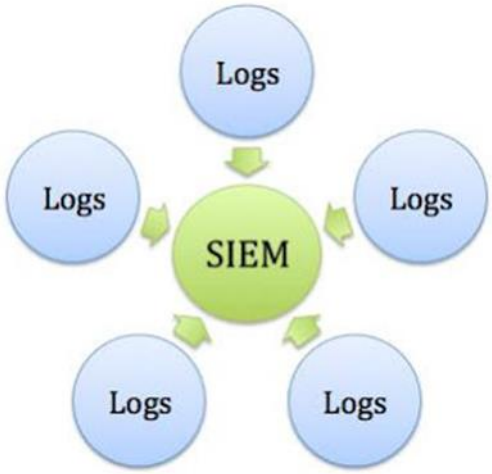
Sistemas de gestión de información y eventos de seguridad.



Los sistemas de seguridad de la información de las organizaciones suelen funcionar como entidades independientes frente a la evolución de los ataques actuales cada vez más sofisticados. Un escaneo de puertos no levantará ninguna sospecha por parte de los dispositivos de seguridad, estos generaran un Log por cada puerto pero no una alerta de seguridad. Solo posteriormente podremos ver los efectos del ataque que se estaba preparando gracias a ese escaneo de puertos previo.

La evolución de los ataques de seguridad cada vez es más compleja y distribuida, sin embargo, nuestros sistemas de seguridad de la información (anti malware, firewall, etc.) al actuar independientemente no son capaces de detectar esos ataques a partir de pequeños indicios.

Sistemas de gestión de información y eventos de seguridad.



Las soluciones de seguridad de la información y gestión de eventos de seguridad (SEIM) son una combinación de los productos anteriormente dispares de gestión de seguridad de la información SIM (Security Information Management) y gestión de eventos de seguridad SEM (Security Event Management) cuyo resultado es un sistema capaz de detectar ataques complejos de seguridad, de gestionarlos y neutralizarlos.