UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

Facultad 2

Implantación de una Tecnología SIEM (Security Information and Event Management) en la red de un Centro de Procesamiento de Datos.

Trabajo de diploma para optar por el título de Ingeniero en Ciencias Informáticas.

AUTOR

Duany Fernando Pérez Vera

TUTORES

Ing. Darvis Dorvigny Dorvigny

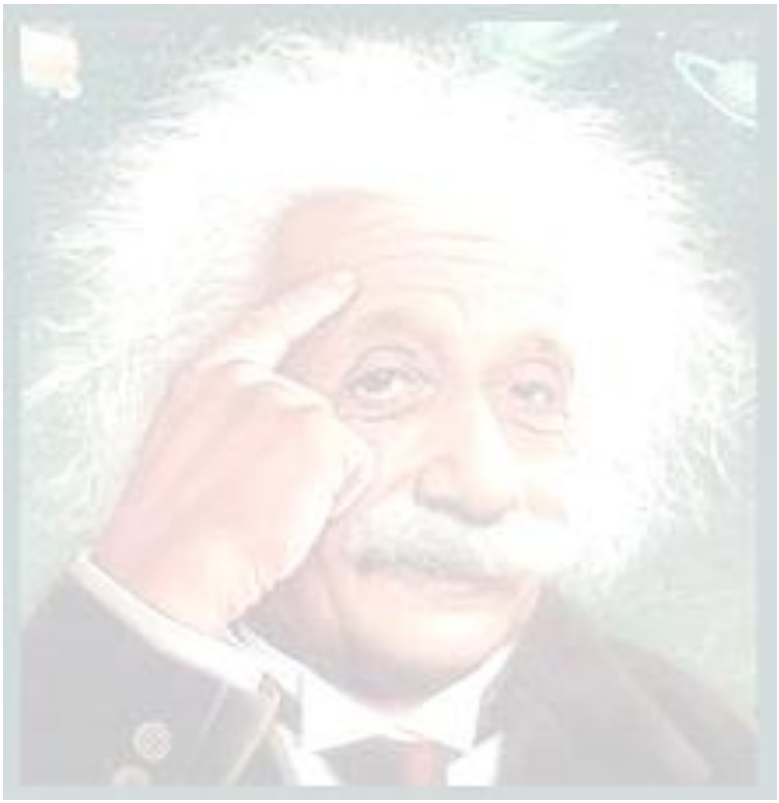
Ing. Alain Osvaldo Pérez Hernández

COTUTOR

Ing. Adrian Hernández Yeja

Ciudad de La Habana, 29 de Junio del 2012
"Año 54 de la Revolución"

PENSAMIENTO



¿Nunca consideres el estudio como una obligación, sino como una oportunidad para penetrar en el bello y maravilloso mundo del saber?

Albert Einstein (1879-1955) Científico alemán

DECLARACIÓN DE AUTORÍA

Declaro ser el único autor de este trabajo y autorizo a la Universidad de las Ciencias Informáticas hacer uso del mismo en su beneficio.

Para que así conste firmo la presente a los 29 días del mes de Junio del año 2012.

Autor:

_____

Duany Fernando Pérez Vera

Tutores:

_____ _____

Ing. Darvis Dorvigny Dorvigny. Ing. Alain Osvaldo Pérez Hernández.

DATOS DE CONTACTOS

Nombre y Apellidos del Tutor: Ing. Darvis Dorvigny Dorvigny.

Institución: Universidad de las Ciencias Informáticas.

E-mail: ddorvigny@uci.cu

Decano de la Facultad 2

Nombre y Apellidos del Tutor: Ing. Alain Osvaldo Pérez Hernández.

Institución: Universidad de las Ciencias Informáticas.

E-mail: aoperez@uci.cu

Subdirector del Centro Telemática de la Facultad 2

Nombre y Apellidos del Consultante: Ing. Raydel Montesino Perurena.
Institución: Universidad de las Ciencias Informáticas
E-mail: raydelmp@uci.cu .

Ingeniero en Telecomunicaciones y Electrónica, graduado en la CUJAE en el 2003. Desde el año 2005 ocupa el cargo de Director de Redes y Seguridad Informática de la Universidad de las Ciencias Informáticas (UCI). Debido al cargo que desempeña ha estado relacionado directamente con la gestión de la seguridad informática durante más de 5 años.

AGRADECIMIENTOS

No alcanzan las palabras para agradecer a todas aquellas personas que de una forma u otra me han apoyado y han puesto su confianza en mí durante el transcurso de todos estos años en la Universidad de Ciencias Informáticas.

Primeramente agradecer, a mi mamá, mi papá y mi hermano que son todo para mí y que sin ellos este éxito no tuviera sentido, los que siempre están apoyándome en los malos y buenos momentos, esas personas que me han enseñado a luchar, me han guiado por el camino correcto y me han dado siempre una motivación para seguir hacia delante a pesar de los problemas.

A mis abuelos, tíos, primos y toda la familia en general que siempre ha puesto esa confianza y dedicación en mí para que este sueño se hiciera realidad. A toda esa familia maravillosa, muchas gracias por su apoyo y cariño que nunca me faltó. A mi dos hermanitas del alma, Ivis y Rosalía que siempre me han dado todo su apoyo, dedicación y muchos consejos para la vida.

A todos los vecinos y amistades del barrio que siempre han estado pendiente de mí cada vez que llegaba de pase o cuando terminaba un año, siempre brindándome su apoyo y confianza, a todos ellos muchas gracias, la meta está cumplida.

A Lázaro Rodríguez, uno de los especialistas en redes de la universidad que me apoyó muchísimo con mi tesis y nunca obtuve un "No" como respuesta cada vez que lo molesté.

A los demás Doctores, Ingenieros, especialistas y profesores que me dieron muy buenos consejos y su apoyo para la elaboración de esta tesis.

Darle gracias a todas esos amigos que tengo en la universidad, que además de estar conmigo durante todos estos años siempre me han apoyado y me han brindado toda

su amistad. En especial a esos que vienen conmigo desde 1er año, que hemos compartido malos y buenos momentos. A todos esas amistades que han sido parte de este éxito y que espero que también sea el suyo.

A la Universidad de las Ciencias Informáticas y a la Revolución cubana, que ha hecho posible que un estudiante logre sus sueños de ser un Ingeniero Informático.

A todos las personas que de una forma u otra me han brindado su apoyo y han presenciado este trabajo de diploma.

¡A todos muchas gracias!

DEDICATORIA

Le dedico esta tesis a mi familia: a mis padres y mi hermano en especial que siempre ha estado apoyándome en cada momento de mi vida y son los principales ídolos que este sueño se hiciera realidad, por su dedicación y amor incondicional que siempre me han dado, por su correcta educación y todas las cosas buenas que me han enseñado y que hoy forman parte de mí.

A la memoria de mi tía Mireya y mi abuelo Jorge: que me vieron emprender este camino y no pudieron presenciar este sueño cumplido, sé que estarán orgullosos de mí.

RESUMEN

Con el desarrollo alcanzado en las nuevas Tecnologías de la Informática y las Comunicaciones (TIC), la existencia de un elevado número de aplicaciones de procesamiento de datos, así como su vertiginoso y constante crecimiento, unido a la necesidad de dotar a las organizaciones de una herramienta que controle la seguridad de la información y gestione los eventos, constituye la base sobre la que se sustenta el principio de practicar la tecnología SIEM (Security Information and Event Management) para un Centro de Procesamiento de Datos (CPD).

Sin una gestión centralizada y una correlación automatizada, muchas empresas quedan vulnerables y dejan al descubierto sus infraestructuras de seguridad, convirtiéndose en sistemas que generan un enorme flujo de datos y amenazas que no gestionan los riesgos reales asociados a la información y la protección de los activos informáticos.

Para aplacar estos problemas la tecnología SIEM integra varias herramientas de seguridad, con el fin de recoger, ordenar y correlacionar la información en tiempo real sobre el estado de la red. Lo que sirve a los administradores de red encontrar indicios de ataques que están ocurriendo o que puedan suceder en el futuro.

El presente trabajo describe un procedimiento para la implantación de una tecnología SIEM de código abierto (AlienVault OSSIM Open Source) que permite el control de la información en las redes de un CPD con el fin de minimizar los ataques y problemas de seguridad mediante la implementación de mecanismos, herramientas, roles y actividades con una arquitectura, formato y plataforma adecuada.

Palabras claves:
Procesamiento, gestión, seguridad, herramientas, información, correlación, mecanismos, tecnología, SIEM.

Índice

Índice de figuras.

Índice de tablas.

INTRODUCCIÓN

A finales del siglo XX, los sistemas informáticos se han convertido en herramientas poderosas que materializan uno de los conceptos vitales y necesarios para cualquier organización empresarial.

Los sistemas informáticos no están ajenos a las vulnerabilidades, pueden ser atacados en cualquier momento, de ahí la necesidad de lograr la seguridad en los datos que se manejan, el mínimo error o la más ligera brecha de seguridad provocaría daños severos y los resultados de un mal uso incitarían gastos millonarios así como desvíos del flujo de información.

Un sistema seguro debe cumplir con los principios de integridad (la información sólo pueden ser modificados por las personas autorizadas y de manera controlada), confidencialidad (la información sólo pueden ser accedidas por las personas autorizados), disponibilidad (la información es accedida por las personas autorizadas en el momento requerido) y no repudio (ofrece protección a un usuario frente a otro usuario negando posteriormente que en realidad se realizó cierta acción). (1)

Actualmente las empresas poseen gran cantidad de información que son almacenadas y ubicadas en un lugar específico donde se accede a la información necesaria para sus operaciones y se concentran todos los recursos para su procesamiento, que son los llamados Centro de Procesamiento de Datos (CPD), con el objetivo de garantizar la continuidad del servicio a los clientes, empleados, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicación implicados, así como servidores de bases de datos que guardan información sensible. (2)

Existe una variedad de herramientas de seguridad, tales como: herramientas de monitoreo de tráfico de red, scanner de vulnerabilidades, detectores de anomalías, Intrusion Detection System and Intrusion Prevention System (IDS/IPS), cortafuegos, antivirus, entre otros; que ayudan a minimizar los problemas de seguridad, pero la información que estos generan no da una perspectiva real de lo que ocurre en la red, cada herramienta o mecanismo tiene su propia plataforma, arquitectura y formato.

Para aplacar estos problemas la tecnología SIEM integra varias herramientas de seguridad, con el fin de recoger, ordenar y correlacionar la información sobre el estado de la red, los comportamientos de sistemas y usuarios, y la información del estado de las máquinas. En concreto, la información

viva de la red, lo que sirve a los administradores de seguridad encontrar indicios de ataques que hayan ocurrido o que puedan suceder en un futuro.

La implantación de esta tecnología involucra un conocimiento claro de la infraestructura de red que se maneje, el flujo de datos, servicios que presta, funcionamiento de la herramienta, determinación de una arquitectura de monitoreo, y la evaluación de funcionalidad y rendimiento.

La Universidad de las Ciencias Informáticas (UCI) como institución docente productiva, a través del Centro de Telemática, específicamente el Departamento de Seguridad Informática, busca promover la investigación y desarrollo de nuevas tecnologías, y en el caso de los Sistemas de Gestión de Eventos e Información de Seguridad, implantarlo en un Centro de Procesamiento de Datos de una red dinámica.

Después de analizar la situación existente surge el siguiente **problema a resolver**: ¿Cómo controlar el flujo de información de la red de un CPD?

Por tanto, el **objeto de estudio** está enfocado en la tecnología SIEM para la seguridad de la información en un CPD. Derivado de esto, el **campo de acción** son las herramientas y mecanismos que ofrece la tecnología SIEM para la seguridad y gestión de la información en la red de un CPD.

Se define como **objetivo general,** elaborar un procedimiento para la implantación de una herramienta que ofrece la tecnología SIEM para el control de la información y gestión de eventos de seguridad en la red de un CPD.

Las **tareas investigativas** que se establecieron para el cumplimiento de dichos objetivos son:

- ✓ Estudio de tecnologías SIEM que integren varias herramientas de seguridad.
- ✓ Selección del producto que ofrece la tecnología SIEM con sus herramientas y componentes pertinentes basadas en software libre.
- ✓ Diseño del despliegue de la herramienta para su implantación en un Centro de Procesamiento de Datos.
- ✓ Selección de las herramientas necesarias para su implantación.

- ✓ Elaboración de una propuesta que defina fases, roles, actividades y artefactos para la implantación de una tecnología SIEM que permita el control del flujo de información que se procesa en Centros de Procesamientos de Datos.
- ✓ Validación del procedimiento propuesto mediante el método Delphi.

Posibles resultados:

Un procedimiento que garantice la gestión de la información y administración de eventos de seguridad para la detección y monitorización de ataques que hayan ocurrido o puedan suceder en la red de un CPD mediante la correlación de varias herramientas de seguridad.

Métodos de la investigación

Durante la investigación serán utilizados varios métodos científicos, entre los que se encuentran, los métodos teóricos y los métodos empíricos.

Los **métodos teóricos** permiten estudiar las características del objeto de investigación que no son observables directamente, facilitan la construcción de modelos e hipótesis de investigación y crean las condiciones para ir más allá de las características fenomenológicas y superficiales de la realidad, contribuyendo al desarrollo de las teorías científicas y para su ejecución se apoyan en el proceso de análisis y síntesis. (3)

Los métodos teóricos utilizados en la investigación son:

- ✓ **Método histórico-lógico:** Este método permite estudiar de forma analítica la trayectoria histórica real de la tecnología SIEM, su evolución y desarrollo.
- ✓ **Método analítico-sintético:** Este método permite buscar la esencia de la tecnología SIEM, los rasgos que lo caracterizan y lo distinguen. Permitiendo la extracción de los elementos más importantes que se relacionan con la implementación de esta tecnología y las herramientas que lo integran.

Los **métodos empíricos**: Describen y explican las características del objeto, representan un nivel de la investigación cuyo contenido procede de la experiencia y es sometido a cierta elaboración racional. (3)

Los métodos empíricos utilizados en la investigación son:

- ✓ **Observación:** Mediante este método se recoge la información de algunas aplicaciones que implementan este tipo de tecnología en el mundo y más específicamente en la Universidad de Ciencias Informáticas (UCI).
- ✓ **La entrevista:** Es una conversación planificada entre el investigador y el entrevistado para obtener información. Su uso constituye un medio para el conocimiento cualitativo sobre características personales del entrevistado y se ve reflejado en el Capítulo 3 en la validación de la propuesta de solución mediante el método Delphi, en la selección y cálculo del coeficiente de los expertos.

El documento está estructurado en 3 capítulos:

En el **Capítulo 1** "Fundamento Teórico", realización de una búsqueda y revisión bibliográfica que sustenta la investigación sobre las herramientas y mecanismos que ofrece la tecnología SIEM que garanticen la seguridad en la red de un Centro de Procesamiento de Datos. Se expone una valoración del estado del arte de estas herramientas, analizan las tendencias y seleccionan las idóneas que se van a utilizar.

En el **Capítulo 2** "Características de la solución propuesta", brinda una visión de la herramienta a implantar detallando los procedimientos a seguir por pasos. Además se definen los roles, actividades y artefactos que se generan en cada una de las fases de la solución propuesta.

En el **Capítulo 3** "Validación de la propuesta", valida la propuesta del procedimiento a utilizar mediante el método Delphi, en la cual, un grupo de expertos seleccionados realizan la valoración de una encuesta, luego se calcula estadísticamente el coeficiente de coincidencia de los aspectos evaluados contra los expertos y muestran gráficas con los resultados obtenidos.

CAPÍTULO 1. FUNDAMENTO TEÓRICO

1.1 Introducción

En el presente capítulo se plantean todos los elementos teóricos que sustentan el objeto de estudio y el objetivo de la investigación científica. Se relacionan los conceptos fundamentales que desde el punto de vista teórico permiten un mejor entendimiento de la situación problémica. Con el objetivo de proporcionar mayor cantidad de información y enfatizar donde coexiste el objeto de estudio.

1.2 Antecedentes

El concepto de activo informático en las empresas ha venido replanteándose en la actualidad, ya que se ha tomado un nivel considerable de participación de la seguridad de la información, considerándose como uno de los principales aspectos para cualquier organización. A partir de esta premisa surgen todos los conceptos, actividades, procesos y planes estratégicos para administrar y proteger la información depositada en los Centros de Procesamiento de Datos.

Se deben controlar aspectos cruciales en la seguridad de la información, conceder privilegios respecto a los usuarios de los datos y también denegarlos. Con la implantación de la tecnología SIEM se busca recoger, ordenar y correlacionar los eventos de seguridad para mejorar las capacidades de detección y visibilidad en la monitorización de la información y los activos críticos que son de vital importancia, con el fin de poder minimizar los falsos positivos (es un ataque al sistema que en realidad no es verdadero) y falsos negativos (es una falla en detectar o ignora une área del sistema que está siendo realmente acatada) en la identificación de violaciones de seguridad.

1.3 Conceptos fundamentales

1.3.1 Seguridad de la Información

Se entiende por **seguridad de la información** a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad. (4)

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas; aunque estos dos conceptos están estrechamente relacionados.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo. (4)

1.3.2 Concepción de la seguridad de la información

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y se debe saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener a acceso a cierta información, ésta se clasifica como:

- **Crítica:** es indispensable para la operación de la empresa.
- **Valiosa:** es un activo de la empresa y muy valioso.
- **Sensible:** debe de ser conocida por las personas autorizadas.

Riesgo y seguridad de la información:

- **Riesgo:** es todo tipo de vulnerabilidad, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas. Los riesgos más perjudiciales son a las tecnologías de información y comunicación.
- **Seguridad:** es una forma de protección contra los riesgos. (4)

También se debe tener en cuenta aspectos como:

- **Consistencia:** asegurar que las operaciones que se realizan sobre las operaciones se comporten de acuerdo a lo esperado. Esto implica que los programas realicen correctamente las tareas encomendadas.
- **Control:** es importante regular y vigilar el acceso a la información de la empresa. (4)

1.3.3 Objetivos de la seguridad informática

La seguridad informática está dirigida a proteger los activos. Para ello se divide en tres grupos los cuales se tratan de diferentes formas a la hora de su aseguramiento y en ella se ve incluida la seguridad de la

información. El objetivo de la seguridad informática también puede tratarse en dos áreas de forma general: el área del hardware y el área del software.

- **La información:** es el objeto de mayor valor para una organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.
- **Equipos que la soportan:** software, hardware y organización.
- **Usuarios:** individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

Dentro del área del hardware es priorizada la atención fundamentalmente a servidores, clientes y líneas de comunicaciones.

Los servidores, especialmente en instalaciones intermedias y grandes, suelen estar situados en nodos centrales, agrupados y en dependencias específicas como Centros de Procesamiento de Datos.

Los clientes son aquellos equipos remotos que interactúan entre sí o con los servidores.

Las líneas de comunicaciones son las redes que por varias vías enlazan la comunicación.

Dentro del área de software los objetos de atención son sistemas operativos, bases de datos y aplicaciones. (5)

1.3.4 Necesidad de contar con una buena seguridad de la información

La creciente demanda en el aseguramiento de la información está dado por el nivel de importancia que tiene para cada empresa asegurar que sus recursos informáticos sean utilizados de la manera que se decidió, y por la propagación cada vez más amplia de programas malignos, ataques y violaciones dentro de empresas u organizaciones, ya sea por agentes externos como internos. De esta manera, la necesidad de utilizar la seguridad de la información viene dada principalmente por las amenazas que podrían afectar el buen funcionamiento de una organización.

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento o transmisión de la información se consideran seguros, todavía deben tenerse en cuenta las circunstancias "no informáticas"

que puedan afectar los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia y la descentralización, por ejemplo, mediante estructura de redes. (5)

Estos fenómenos pueden ser causados por:

- **El usuario:** puede que no esté comprometido con el cuidado de los medios que utiliza, no se da cuenta de los errores que comete, o porque a propósito ejecuta una violación de las normas de seguridad establecidas.
- **Programas maliciosos:** es instalado en el ordenador abriendo una puerta a intrusos, o bien modificando los datos. Estos programas pueden ser: un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.
- **Un intruso:** puede ser una persona, aplicación o secuencia de comandos ejecutados de manera automática que consigue acceder a los datos o programas de los cuales no tiene acceso permitido.
- **Un siniestro (robo, incendio, inundación):** una mala manipulación o una mala intención derivan a la pérdida del material o de los archivos.
- **El personal interno de sistemas:** los incrementos de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática. (5)

1.3.5 Sistema de gestión de eventos e información de seguridad (SIEM)

Las soluciones SIEM son una combinación de los productos 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 notificarlos.

La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por el hardware de red (switches, routers, firewall) y aplicaciones (anti malware) a través de sus trazas o historial de conexiones (Log). 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 que ayuda a controlar

los privilegios de usuario y servicios, servicios de directorio y otros cambios de configuración del sistema; así como el abastecimiento de registro de auditoría y respuesta a incidentes. (6)

La tecnología SIEM se suele implantar para apoyar a tres casos de uso principales:

- Cumplimiento - la administración de registros y reportes de cumplimiento.
- Amenaza de gestión - en tiempo real el seguimiento de la actividad del usuario, acceso a datos y aplicaciones, la actividad y la gestión de incidentes.
- Un despliegue que ofrece una mezcla de cumplimiento y las capacidades de gestión de amenazas.

Las soluciones SIEM deben:

- Apoyar la obtención en tiempo real y análisis de eventos de los sistemas host, dispositivos de seguridad y dispositivos de red, combinada con la información contextual para los usuarios, activos y datos.
- Proporcionar a largo plazo los eventos y el contexto de almacenamiento de datos y análisis.
- Proporcionar funciones predefinidas que pueden ser adaptadas a la ligera y cumplir con los requisitos específicos de la empresa.
- Ser lo más fácil posible de implementar y mantener. (7)

Desarrollo actual de los sistemas SIEM

El mercado SIEM está definido por la necesidad del cliente para analizar los datos de gestión de eventos de seguridad en tiempo real de amenazas internas y externas, y para recoger, almacenar, analizar e informar sobre registro de datos para el cumplimiento normativo y forense.

SIEM proporciona productos SIM y SEM:

La Gestión de la Seguridad de la Información (SIM) proporciona un almacenamiento a largo plazo, cumplimiento de informes, análisis y reporte de datos de registro (sobre todo de los sistemas de acogida y aplicaciones, y en segundo lugar de la red y la seguridad de dispositivos) para apoyar los informes de cumplimiento normativo, en la gestión de amenazas y vigilancia de acceso a los recursos.

SIM apoya el usuario con privilegios y el control de acceso de los recursos, supervisando las actividades de la organización de seguridad de las tecnologías de información (TI), así como los informes de las necesidades de la auditoría interna y de las organizaciones de cumplimiento. (8)

La Gestión de 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 de gestión de dichos eventos relacionados con la seguridad de las redes, dispositivos y aplicaciones. SEM apoya la amenaza externa e interna con el seguimiento de las actividades de la organización de la seguridad informática, y mejora la capacidad de manejo de incidentes. (8)

1.3.6 Gestión de la seguridad de la información

La gestión de la seguridad de la información se remonta al albor de los tiempos. La ciencia de la confidencialidad de la información se remonta al inicio de nuestra civilización y ha ocupado algunas de las mentes matemáticas más brillantes de la historia, especialmente (y desafortunadamente) en tiempos de guerra.

Sin embargo, desde el advenimiento de las redes de comunicación ubicadas y en especial Internet, los problemas asociados a la seguridad de la información se han agravado considerablemente y nos afectan prácticamente a todos. (9)

La Gestión de la Seguridad debe velar por que la información sea correcta y completa, esté siempre a disposición del negocio y sea utilizada sólo por aquellos que tienen autorización para hacerlo.

1.3.7 Ventajas de la gestión de la seguridad informática

Los principales beneficios de una correcta gestión de la seguridad son:

- Se evitan interrupciones del servicio causadas por virus, ataques informáticos, entre otros.
- Se minimiza el número de incidentes.
- Se tiene acceso a la información cuando se necesita y se preserva la integridad de los datos.
- Se preserva la confidencialidad de los datos y la privacidad de clientes y usuarios.
- Se cumplen los reglamentos sobre protección de datos.

- Mejora la percepción y confianza de clientes y usuarios en lo que respecta a la calidad del servicio. (10)

1.3.8 Desventajas de la gestión de la seguridad informática

Las principales dificultades a la hora de implementar la Gestión de la Seguridad se resumen en:

- No existe el suficiente compromiso de todos los miembros de la organización con el proceso.
- Se establecen políticas de seguridad excesivamente restrictivas que afectan negativamente al negocio.
- No se dispone de las herramientas necesarias para monitorizar y garantizar la seguridad del servicio (firewalls, antivirus, entre otros).
- El personal no recibe una formación adecuada para la aplicación de los protocolos de seguridad.
- Falta de coordinación entre los diferentes procesos lo que impide una correcta evaluación de los riesgos. (10)

1.3.9 Centro de procesamiento de datos

Un Centro de Procesamiento de Datos (CPD o “Data Center” en inglés) es aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.

Un CPD viene a ser básicamente un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico (servidores, sistemas de almacenamiento de datos, equipos de comunicaciones, entre otros). Son creados y mantenidos por las organizaciones con objeto de tener acceso a la información necesaria para sus operaciones. Por ejemplo, un banco puede tener un CPD con el propósito de almacenar todos los datos de sus clientes y las operaciones que éstos realizan sobre sus cuentas. (11)

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el garantizar la continuidad y disponibilidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica.

El CPD, es la estancia donde se encuentran los servidores, sistemas de comunicaciones, almacenamiento, y toda la tecnología fundamental de la empresa. Si no hay CPD, no hay información. Si

no hay información, no hay conocimiento. Sin conocimiento, no hay existencia. Por ello, las organizaciones son cada vez más conscientes de la importancia de tener un CPD que garantice un confort y una seguridad a sus activos más valiosos: la información y recursos informáticos. (11)

Un CPD se diseña para estar operativo las 24 horas todos los días del año. A mayor disponibilidad, mejor servicio, más producción. Pero la disponibilidad no es gratis.

¿Por qué la disponibilidad es tan importante?

Porque perder la información significa perder la empresa. Además, no tener la información disponible durante un periodo de tiempo, también puede implicar graves pérdidas.

1.4. Análisis de las características arquitectónicas de un CPD

El objetivo de este análisis es tener un conocimiento sobre la estructura de la red, servicios en producción, hardware y software utilizado y determinar cuáles son los servicios más críticos. También involucra actividades como: entrevistar al administrador de seguridad, a los administradores de los servicios, analizar e interpretar el esquema de red y realizar una priorización de los servicios. La priorización se la hace en base al papel que juega un servicio dentro de las actividades operativas de la organización.

Con la información recolectada se puede conocer el estado actual de la organización y así poder definir cuáles son los servicios más críticos con los que cuenta la organización y por consiguiente, realizar una correcta implantación de la tecnología.

1.5 Productos disponibles que implementa la tecnología SIEM

La amplia adopción de la tecnología SIEM es impulsada por el cumplimiento y necesidades de seguridad. Descubrimiento dirigido a los ataques que requiere la actividad del usuario efectivo, acceso a datos y la aplicación de la actividad de vigilancia. Los vendedores están probando la demanda de soluciones más amplia de alcance.

Con la tecnología SIEM, se han desarrollado productos tanto de hardware como de software para estandarizar los eventos y así los administradores tengan la información centralizada y ordenada.

Se mostrarán las características de algunos productos que implantan este tipo de tecnología y se hará una selección del mismo para implantarlo en un CPD.

1.5.1 AlienVault

AlienVault incluye 5 capacidades esenciales en la monitorización de seguridad: descubrimiento de activos, evaluación de vulnerabilidades, detección de amenazas, seguimiento del comportamiento y SIEM.

El equipo de AlienVault comenzó a desarrollar tecnología de gestión de seguridad de código libre en el año 2001. Se construyó OSSIM para que sea más fácil ofrecer servicios MSSP (Managed Security Service Provider) y realizar un análisis remoto completo de la postura de seguridad de los clientes. AlienVault fue fundado tras la adopción masiva de OSSIM en la comunidad con el objeto de ofrecer altas capacidades y rendimiento sobre OSSIM.

Tienen sede en Silicon Valley, y oficinas en 6 países. La empresa nació y todo el equipo de desarrollo está en España. Tienen clientes en 40 países y muchos de ellos en España y Latino América. (8)

AlienVault es un participante relativamente reciente en el mercado comercial SIEM, en 2010, se reunió con los requisitos mínimos de ingresos para su inclusión en el Cuadrante Mágico de Gartner (representa el análisis de cómo ciertos proveedores se miden contra los criterios para ese mercado SIEM). La compañía se puso en marcha en 2007. Durante el año 2010, la compañía recibió una primera ronda de financiación de capital de riesgo y se trasladó a la sede de su empresa desde España a Estados Unidos. AlienVault OSSIM Open Source ofrece tecnología SIEM, evaluación de la vulnerabilidad, la red y host de detección de intrusos y control de integridad de archivos funciones a través de las opciones de software o electrodomésticos.

AlienVault SIEM está integrado por componentes propietarios y de código abierto. OSSIM es una plataforma de seguridad de código abierto de gestión que ha estado disponible desde 2003. AlienVault OSSIM incorpora en su solución SIEM, que se extiende con el desempeño mejorado, la administración consolidada, presentación de informes consolidados, y de arrendamiento múltiple de Proveedores de servicios gestionados. AlienVault OSSIM es totalmente funcional, integra una gran variedad de herramientas de código abierto que junto con el potente sistema de correlación de eventos lo convierten en una indispensable herramienta para la administración de seguridad en redes realmente completa y granular.

Durante el año 2010, el producto ha sido actualizado para ofrecer mejores paneles en tiempo real y presentación de informes. También se ha introducido soporte para NetFlow (es un protocolo de red, desarrollado para recolectar información sobre tráfico IP). La compañía de 12 meses de desarrollo del

plan, incluye la expansión de las capacidades existentes para resolver las brechas competitivas en áreas tales como la aplicación, datos y de control de usuario. El plan de dos años incluye una alternativa de control dinámico de gobernar basado en la correlación.

El propósito de OSSIM no es solo la colección que realiza y la detallada información que el IDS o los monitores pasivos proveen, también implementa procesos de abstracción en el que millones de pequeños eventos técnicos y de difícil comprensión se convierten en docenas de alarmas comprensibles. La principal parte de está abstracción es producida por el Motor de Correlación, éste permite al administrador crear Directivas de Correlación o patrones para unir diferentes eventos de bajo nivel produciendo una conclusión de nivel alto. (8)

1.5.2 HP / ArcSight

En 2010, HP (Hewlett-Packard, empresa de tecnologías de la información del mundo) adquirió ArcSight, el mayor SIEM visible por puntos de solución privado. HP continuará desarrollando y vendiendo ArcSight como una solución SIEM, pero también usará la tecnología para mantener la dirección de evento unificada, su carpeta de tecnología de seguridad. Las integraciones con HP la dirección de servicio comercial BSM (Business Service Management) también está en el proceso. La meta es integrar disponibilidad operacional y eventos de la actuación, inventarios de recursos, y mapas de dependencia de servicio con ArcSight, y para integrar los eventos de seguridad supervisando la infraestructura operacional de HP.

El software ArcSight Enterprise Security Manager (ESM), se orienta a los despliegues de gran potencia, SEM enfocados; ArcSight Express, es un aparato basado para ofrecer ESM que se diseña para el mercado medio con la pre-configuración de monitorización y reporte. Durante los 12 meses ArcSight ha pasado usuarios de ESM que supervisan las capacidades de monitorización, ha mejorado además la integración de planes perfilados con HP, con tal de que una nueva versión mayor de Identity View (Vista de Identidad). (8)

HP necesitará manejar la prioridad de integración de la tecnología HP y ArcSight, el desarrollo proyecta en cierto modo la conservación de las capacidades en los ambientes del multi-vendedor y también debe manejar la transición de ArcSight a sus propias ventas encauza y apoyo a la infraestructura en cierto modo, eso conserva la especialización de seguridad porque se ha construido ArcSight con el tiempo.

El software de ESM de ArcSight se orienta a ambientes que necesitan las capacidades para apoyar centrar los funcionamientos de seguridad, y requiere la especialización del usuario final en las áreas tal como la afinación de la base de datos.

Organizaciones que no requieren la dirección de eventos de funciones completas que pueden ser capaces para desplegar las alternativas más simples y menos caras que ArcSight ESM, y debe considerarse ArcSight Express. (8)

1.5.3 IBM (International Business Machines)

La Tivoli Seguridad de la Información y Gerente de Eventos de IBM (Tivoli Security Information and Event Manager, TSIEM) la v.2 software proporcionan funcionalidades SIM y SEM, y les permite a clientes tener un punto de partida con la gestión de log.

TSIEM proporciona capacidades para el supervisado de usuarios con privilegios, el informe de complacencia, gestión de log y elementos en tiempo real, SEM. Tivoli también proporciona a Tivoli Seguridad Funcionamientos Gerente (TSOM) a clientes que también necesitan adicionalmente capacidades de centrar operaciones de seguridad. La compañía indica una base grande instalada y creciente, pero la tecnología de SIEM de IBM no está a menudo en las listas cortas de compañías que están haciendo las evaluaciones competitivas. Un despliegue típico se enfoca en actividad del usuario que supervisa e involucra 100 o menos servidores.

Desde la escritura del último Cuadrante Mágico SIEM, las actualizaciones de producto de TSIEM de IBM han enfocado en mantener las integraciones con las versiones puestas al día de otros productos de Tivoli y comandante de las fuentes de eventos terceristas. La estrategia de SIEM global de IBM continúa siendo enfocada en la integración con su IAM (Integration and Fraud Management), seguridad y tecnologías de dirección de servicio y su influencia de Seguridad de Sistemas de Internet – gestión de servicios.

Los esfuerzos de desarrollo de IBM se enfocan en la mejora de análisis de seguridad a través de la aplicación de IBM, las tecnologías de inteligencias comerciales como Cognos (empresa adquirida por IBM que produce software de inteligencia comercial y administración del desempeño) y SPSS (Statistical Package for the Social Sciences). (8)

Aunque hay integración suelta entre TSIEM y TSOM, hay organizaciones que necesitan eventos de monitorización en tiempo real de host log de eventos y operaciones de seguridad centrados en funciones

todavía necesitan desplegar dos tecnologías, y las capacidades de SEM no son las más buenas en la clase. La tecnología no está bien preparada para despliegues moderados o grandes que requieren la supervisión de la seguridad red. IBM no es muy visible en las evaluaciones competitivas. La regeneración cliente de IBM en la función del producto y el apoyo mixto. (8)

1.5.4 SenSage

La solución de SenSage (compañía que ofrece productos SIEM) se perfecciona en el análisis de precisión y complacencia que informan eventos largos de almacenamiento de datos, y la compañía ha seguido despliegues grandes que requieren esta capacidad con éxito. SenSage continúa siguiendo grandes tratos para los casos de uso específicos dentro de ellos verticales como EE.UU, gobiernos federales europeos, y servicios financieros, mientras usa una combinación directa de ventas con sus compañeros. SenSage también ha seguido con éxito casos de uso que requieren la capa de la aplicación y/o supervisión orientada al usuario.

Con la adquisición de ArcSight por HP, SenSage perdió HP como una de las ventas mayores encauzadas al mercado SIEM general. SenSage responde bastante bien a la funcionalidad pero en las áreas de implementaciones de la simplicidad son un desafío. El problema más grande por lo que se refiere a la visión es que la compañía no ha podido alcanzar el centro del "mercado de SIEM eficazmente. (8)

Organizaciones que requieren sólo funciones de las trazas básicas que deben considerar más simples y ofrecer menos caras que enfoquen en la colección y elementos esenciales para informar. La tecnología SenSage no se despliega ampliamente para casos de usos que se enfocan en SEM, aunque ha mejorado las capacidades de supervisión en tiempo real. La mayoría de los clientes continúan llevando a cabo una combinación de monitoreo en tiempo real y supervisión de ciclo corto. (8)

1.5.5 Selección de la herramienta a utilizar

Una vez mostradas las particularidades de algunos de los productos que implantan tecnologías SIEM, se llega a la conclusión que el producto que posee las características de interés para implantar la herramienta es AlienVault, los creadores de OSSIM Open Source. La tabla 1 muestra los detalles.

Producto / Características	AlienVault	HP / ArcSight	IBM	SenSage
Software Libre	**Si**	No	No	No
Integración de varias herramientas de seguridad de código abierto	**Si**	No	No	No
Detección y monitorización de eventos de seguridad en tiempo real	**Si**	Si	Si	Si

Tabla 1. Comparación entre los productos disponibles.

Lo principal que ofrece OSSIM es su potente motor de correlación que permite a los administradores de seguridad crear directivas de correlación o patrones para unir diferentes eventos de bajo nivel y producir una conclusión de alto nivel. También garantiza una detección y monitoreo continuo, detallando la información que los IDS o los monitores pasivos proveen para llegar a un proceso de abstracción mayor de varios eventos técnicos y difíciles de comprender. En sí, AlienVault Open Source SIEM (en lo adelante OSSIM) es un sistema de seguridad integral de código abierto que cubre desde la detección hasta la generación de métricas e informes a un nivel ejecutivo; que permite integrar en una única consola todos los dispositivos y herramientas de seguridad que disponga la red. Además el sistema brinda la posibilidad de cuando se generan los eventos por las diferentes herramientas, realizar una valoración del riesgo para cada evento, detectar los ataques reales o problemas en la red y notificarlos. Por lo que se hace factible utilizar este tipo de herramienta como solución SIEM integral en un CPD.

1.6 Análisis de la herramienta OSSIM

El objetivo de este análisis es tener conocimiento de los componentes, su arquitectura, las herramientas que lo integran y cómo interactúan.

Esta herramienta se encarga de recolectar los datos entregados por las diferentes aplicaciones de monitoreo y mostrarlos a través de una interfaz Web con su integración, logrando abstraer al administrador de lo que sucede de fondo. En lugar de tener que mirar por separado miles de trazas, la interfaz Web junta todos los datos en un solo lugar y permite tener una vista detallada de cada aspecto de las redes, host y servidores.

OSSIM es un sistema de seguridad integral para las empresas, que quiere suplir las necesidades que un grupo profesionales encuentran en el mundo de la seguridad día a día. Sorprende que con el fuerte desarrollo tecnológico producido en los últimos años que ha provisto de herramientas con capacidades como las de los IDS, sea tan complejo desde el punto de vista de seguridad de obtener una visión de una red con un grado de abstracción que permita una revisión práctica y asumible. La intención inicial en el desarrollo de este proyecto es mejorar esta situación a través de una función que se resume con el nombre de correlación. (12)

Incluye varias herramientas de monitorización de seguridad que tiene como objetivo fundamental ofrecer un marco para centralizar, organizar y mejorar las capacidades de detección y visibilidad de los eventos de seguridad de la organización. Posee una arquitectura formada por cuatro componentes: servidor (Consola de Gestión), framework o marco de trabajo (Interacción entre Módulos), base de datos (Eventos) y agentes (Sensores Colectores).

Con esto se consigue que una empresa pueda, no sólo tener un gran número de dispositivos tecnológicos, sino que además sepa en cada momento el nivel de seguridad que tiene y el que desea tener. Gracias al motor de correlación de OSSIM se alcanza detectar entre otras cosas, virus antes incluso que los propios fabricantes de antivirus, ya que al trabajar de manera centralizada con muchas herramientas, es capaz de detectar anomalías en el funcionamiento de las máquinas, detectando nuevos virus que aún no han sido identificados por nadie.

Esta plataforma es una solución de seguridad, que puede ser personalizada a las necesidades de cada entidad. Permite la visibilidad de todos los eventos de los sistemas en un punto central y en un mismo formato. Mediante la correlación relaciona y procesa la información minimizando así los “falsos positivos” y “falsos negativos” (13)

Solución Integral

Es una solución integral pues es capaz de ofrecer las herramientas y funcionalidad para monitorización de todos los niveles desde el más bajo (firmas detalladas de un IDS, dirigido al técnico de seguridad), hasta el más alto (El Cuadro de Mandos dirigido a la Dirección Estratégica), pasando por: niveles de correlación, inventariado de activos y amenazas, y monitores de riesgos.

Solución vs Producto

OSSIM no quiere ser un producto, sino una solución, un sistema personalizado para las necesidades de cada organización formado por la conexión e integración de varios módulos especialistas. En nuestra solución tan importante como el código son los conceptos o definiciones de:

- La arquitectura
- Los Modelos y Algoritmos de Correlación
- La definición del Entorno y el Framework
- El Modelo de Gestión de la Seguridad Perimetral
- El Mapa y los Procedimientos de Auditoría de la Capacidad de Detección. (14)

Arquitectura Abierta

OSSIM es una arquitectura de monitorización abierta pues integra diversos productos del mundo libre, intentando seguir siempre los estándares y las tendencias del mundo open source (los cuales creemos que en soluciones de monitorización serán los estándares en todos los entornos). (14)

Software de Código Libre

OSSIM se propone como un proyecto de integración, la intención no es desarrollar nuevas capacidades sino aprovechar las ventajas, beneficios y facilidades del software libre, programas desarrollados por la inspiración de prestigiosos especialistas del mundo (como pueden ser Snort, Nagios, Nmap, OpenVas, o Ntop) integrándolas en una arquitectura abierta que heredará todo su valor y capacidades. Estas herramientas de código libre son, por la naturaleza de este, probadas y mejoradas por decenas o centenas de miles de instalaciones en el mundo convirtiéndose en elementos robustos y altamente probados o tanto fiables. (14)

1.6.1 Diagrama del funcionamiento de OSSIM

Figura 1. Diagrama del funcionamiento de OSSIM.

Se realiza una monitorización de todos los niveles desde el más bajo (firmas detalladas de un IDS por la detección de patrones y anomalías) hasta el más alto (Cuadro de mandos), pasando por: consola forense, niveles de correlación, normalización, priorización, inventarios de activos y monitores de riesgo. (15)

1.6.2 Componentes de OSSIM

Esta herramienta está formada por cuatro componentes:

- ✓ **Servidor.** Es el componente principal de OSSIM. Se encarga de recibir los eventos enviados por los distintos agentes, también realiza las funciones de priorización y correlación.
- ✓ **Agente.** Son hosts (huésped, computadoras conectadas a una red, que proveen y utilizan servicios) distribuidos en diferentes segmentos de red, para monitorear los distintos eventos. Esta distribución es en base a los servicios que se va a monitorear. Cada agente o sensor tendrá configurado un conjunto de detectores o monitores, que generan eventos para que el agente los recolecte y reporte al servidor central.
- ✓ **Framework.** Es el intermediario entre el servidor central y el usuario. Es un marco de trabajo bajo el cual se desarrolla la herramienta de administración, utilizada para configurar y organizar los diferentes módulos tanto externos como propios que integra OSSIM. Mediante este se puede

definir una topología, inventariar activos, definir políticas de seguridad, definir reglas de correlación y unir las diferentes herramientas integradas.

- ✓ **Base de datos.** Es el lugar donde se almacenan los diferentes eventos recolectados por los agentes, y las configuraciones de las distintas herramientas y OSSIM. (15)

En su instalación se divide en tres subsistemas fundamentales: ossim-server, ossim-framework y ossim-agent. Además utiliza una base de datos para almacenar los eventos y la información necesaria para los plugins (analizador sintáctico).

Ossim-server: este programa es un demonio (tipo especial de proceso informático no interactivo) que se ejecuta en el fondo y se conecta con la base de datos para obtener/ingresar datos desde los agentes y el framework. El propósito principal de este programa es:

- Recolectar datos de los agentes y otros servidores.
- Priorizar los eventos recibidos.
- Correlacionar los eventos recibidos de diferentes fuentes.
- Realizar la evaluación de riesgos y disparar alarmas.
- Almacenar eventos en la base de datos.
- Reenviar eventos o alarmas a otros servidores.

Ossim-framework: es otro demonio que ejecuta tareas misceláneas, no realizables por los agentes, servers o el front-end (interfaz web, visualización del usuario navegando). Este accede tanto a la base de datos de conocimiento del OSSIM, como a la BD de eventos. El propósito principal de este programa es:

- Leer/escribir en los archivos del sistema, evitando que el servidor web lo haga directamente.
- Ejecutar comandos externos.
- Ejecutar en el fondo tareas que requieran uso intensivo de CPU, para acelerar la visualización y el análisis.

Ossim-agent: se instala un agente en cada máquina que se desea utilizar como monitor (llamadas sensores). Los agentes se encargan de recolectar todos los datos enviados por los diferentes dispositivos conectados a la red, estandarizar estos datos para que OSSIM pueda entenderlos, y luego enviarlos al servidor. (16)

Dados los tres programas anteriores, la arquitectura de OSSIM se divide en cuatros elementos:

1. Sensores.
2. Servidor de Administración.
3. Base de Datos.
4. Front-end.

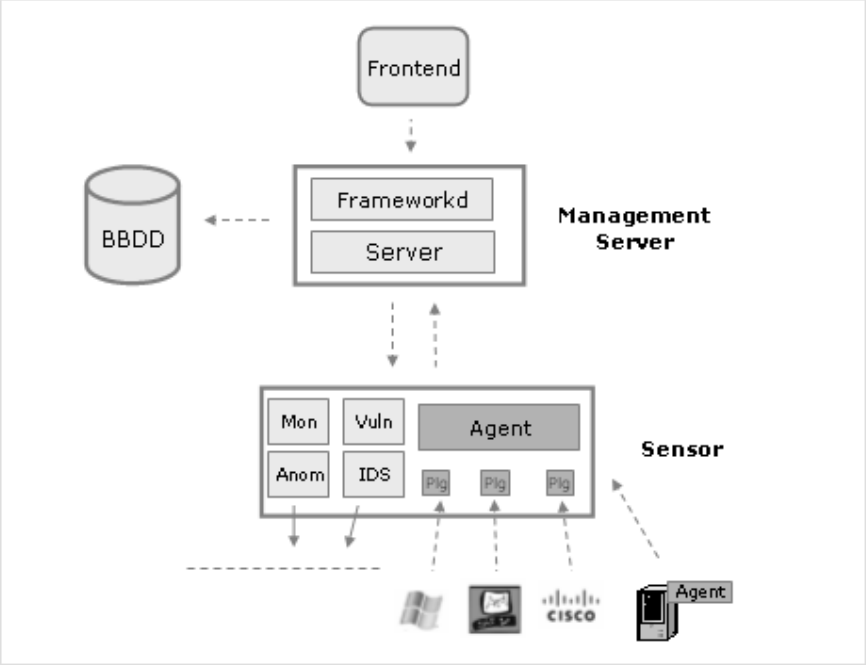


Figura 2. Arquitectura simple de OSSIM.

En la configuración predeterminada, los sensores se encargan de realizar las tareas de IDS, escáner de vulnerabilidad, detección de anormalidades, monitoreo de red, recolección de datos de routers (es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes

entre redes o determinar la ruta que debe tomar el paquete de datos), e incluso pueden funcionar como firewall (es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra). Los sensores se encargan de enviar toda la información al servidor de administración, luego de haberla estandarizado.

Por su parte, el servidor de administración contiene el framework y el servidor OSSIM. Este servidor se encarga de recolectar la información de todos los sensores y normalizar, priorizar, coleccionar eventos, así como realizar análisis de riesgo. Además se encarga de realizar copias de seguridad, inventarios en línea, y ejecución de escaneos. (16)

La base de datos almacena eventos e información útil para la administración del sistema.

El front-end, como se mencionó, es una aplicación web donde se puede visualizar todo lo que sucede.

1.6.3 Correlación de eventos de OSSIM

Una parte principal de la abstracción está sobre todo producida por el Motor de Correlación, que permite al administrador crear Directivas de Correlación o patrones para relacionar diferentes eventos, generando conclusiones de más alto nivel.

La correlación puede reducir el número de eventos de un día de millones a menos de una docena, comprobando cada uno de ellos antes de alertarlos o notificarlos Esto ofrece información a la consola con la que puede generar alarmas e informar de ellas en un formato abstracto mucho más comprensible y fácil de leer.

La aproximación del motor de correlación lógica es comprobar todos los eventos, ya que se pueden tener millones de alertas en un día y no se puede confiar en ellas a menos que se comprueben. El motor de correlación buscará evidencias o síntomas para analizar si el ataque es real o es un falso positivo.

La correlación se realiza de 3 formas diferentes:

1. Correlación de diferentes eventos (Correlación Lógica).
2. Correlación de eventos y vulnerabilidades (Correlación Cruzada).
3. Correlación de eventos y sistemas operativos - servicios (Correlación de Inventario). (17)

1. Correlación Lógica

El principal propósito de la correlación lógica consiste en relacionar eventos provenientes de distintas fuentes y que cumplen con ciertas condiciones de tiempo, origen y destino para generar alertas. Este es un tema importante en los sistemas de seguridad actuales. Se pueden tener millones de eventos por día, pero la mayoría de ellos serán falsos positivos. Es necesario tener procesos automáticos para comprobar si un ataque se está llevando a cabo en realidad.

El motor de correlación lógica de OSSIM tiene como características:

- Origen híbrido: acepta información de entrada tanto de los patrones de los detectores como de los indicadores de los monitores.
- Arquitectura recursiva: la salida serán eventos que pueden ser correlacionados de nuevo por otras directivas de correlación.
- Arquitectura jerárquica distribuida: se pueden definir varios niveles de correlación en una topología distribuida.
- Definiciones flexibles orientadas a objetos y a rangos de tiempo para el escenario de cada directiva.

La correlación lógica se realiza mediante directivas de correlación que están implementadas como un árbol de nodos de condiciones lógicas. Este tipo de estructura es también conocido como árbol AND/OR, utilizado generalmente en sistemas de inteligencia artificial y del que OSSIM utiliza un tipo específico.

Cuando la condición de un nodo es satisfecha, el motor de correlación saltará al primer nodo hijo. Si no, saltará al siguiente hermano (nodo a la derecha al mismo nivel con el mismo padre). Esto implementa la operación “AND” en el eje Y y la operación “OR” en el eje X.

La variable de fiabilidad crece según el motor de correlación avanza a través de los nodos comprobando las coincidencias de las condiciones: cuantas más coincidencias en los nodos se tenga (evidencias), más posibilidades habrá de que el ataque sea cierto.

Cada directiva define un nuevo tipo de evento (heredando su nombre de la directiva) y tiene una prioridad específica, ya que la mayor parte de las veces indica patrones más amplios que los eventos que lo han generado.

Este nuevo evento se tratará como uno más de los que analiza OSSIM (probablemente con una alta fiabilidad) y será reinsertado en la cola de ejecución tal y como si procediese de un agente externo. Se crea así un camino recursivo donde se pueden implementar diferentes niveles de correlación. (17)

2. Correlación Cruzada

La correlación cruzada permite priorizar o suprimir las prioridades de eventos de los cuales se sabe que son o no lo son vulnerables, a partir de la correlación de la información del IDS y el escáner de vulnerabilidades.

La correlación cruzada de OSSIM depende de bases de datos de vulnerabilidades y de tablas de correlación cruzada para cada detector. OSSIM utiliza la base de datos de vulnerabilidades de OSVDB (Open Source Vulnerability Data Base, es una base de datos independiente y de fuente abierta creada por y para la comunidad) y actualmente incluye tablas de correlación cruzada para el IDS Snort y para OpenVas. (17)

3. Correlación de Inventario

Los ataques que se lanzan son siempre contra objetivos con un S.O. y/o servicio específico.

La correlación de inventario comprueba si la máquina atacada utiliza ese S.O. y/o servicio específico para el cual se está lanzando el ataque. Si lo utiliza estaremos seguros de que existe un riesgo, pero si no, podemos confirmar que el evento de ataque es un falso positivo.

Este tipo de correlación depende de la precisión del inventario. OSSIM tiene capacidades de realizar inventarios manuales y automáticos para ajustar estos detalles. (17)

1.6.4 Motor de correlación de OSSIM

El motor de correlación de OSSIM funciona por medio de directivas que se definen utilizando XML (Extensible Markup Language o Lenguaje de Marcas Extensibles). Al iniciar el motor de correlación carga todas las directivas definidas en un árbol de estructuras lógicas de tipo “IF” y “OR”, que se relacionan entre sí para identificar ataques o comportamientos sospechosos en la red.

La etiqueta de inicio de toda directiva contiene dos atributos: un identificador (ID) que consiste en un número decimal único y una descripción general de la directiva:

<directive id="1" name="Successful Dcom exploit" priority=“5“>

Toda directiva contiene también una etiqueta de regla (<rule>) inicial, que marca el inicio de la correlación:

<rule type="detector" name="Snort dcom signature" reliability="1" time_out="60" occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="135,445" plugin_id="1001" plugin_sid="2192"> (18)

En la actualidad Snort se encuentra en la versión Snort-2.9.0.5-1, lo que demuestra un avance sustancial en el desarrollo de dicha herramienta por parte de la comunidad desarrolladores que apuestan por ella y alcanza así una madurez mucho mayor.

1.6.5 Filtrado de falsos positivos

Un objetivo importante de correlacionar los eventos de seguridad es luchar contra el enorme volumen de falsos positivos creados por los IDS y por los dispositivos de seguridad en general. Las organizaciones reciben millones de ellos por día, haciendo imposible para un administrador comprobarlos todos.

Las Directivas de Correlación de OSSIM revisan estos eventos buscando evidencias para asegurarse de si son o no ataques reales. Por defecto se estima un valor bajo al parámetro “Fiabilidad” de la mayoría de eventos; solamente aumentará si las comprobaciones proporcionadas por el Motor de Correlación resultan positivas. (19)

Falsos Positivos

Un falso positivo es un error por el cual el software reporta que un archivo o área del sistema está siendo atacado, cuando en realidad no ha ocurrido ningún ataque o no se considera como un ataque verdadero.

Falsos Negativos

Un falso negativo es un error mediante el cual el software de alerta falla en detectar, o ignora, un archivo o área del sistema que está siendo realmente acatado.

1.6.6 Gestión del riesgo

OSSIM actúa, informa y lanza respuestas utilizando parámetros de riesgo. El riesgo se calcula y almacena para cada uno de los eventos recolectados. En el Proceso de Gestión de Seguridad se utiliza esta valoración; se desencadenan respuestas automáticas, se generan informes de alarmas y se toman medidas de la situación de riesgo de las redes. (17)

La veracidad del ataque se calcula con un valor del riesgo del evento y se decide si el ataque es real; donde finalmente es lanzada una alarma. Se generan las alarmas cuando el valor de riesgo del evento es igual o mayor que uno, además del criterio del especialista. El riesgo se calcula usando la siguiente fórmula:

Riesgo del Evento = (Valor del Recurso * Prioridad * Fiabilidad) / 25.

Dónde: El Recurso y la Prioridad tendrán un valor entre (0-5) y la Fiabilidad un valor entre (0-10).

La evaluación del riesgo estará dada por un valor entre 0 y 10. (20)

1.6.7 Plugins en OSSIM

Un aspecto fundamental en OSSIM son los plugins, que gestionan todas estas aplicaciones y centralizan sus resultados, es muy probable que aunque no se necesite crear sus propios plugins, si se necesite modificar algunos.

Los plugins son controlados por los agentes de OSSIM, por lo tanto es el módulo de agente el que se encarga de arrancar y gestionar los programas asociados a los plugins. Para ver los plugins que se tienen activos en un agente, localizamos el fichero /etc/ossim/agent/config.cfg y dentro de él la directiva [plugins]. Dentro de esa directiva se encuentra el fichero de configuración de cada plugin, que por defecto es /etc/ossim/agent/plugins/.

Dentro de la configuración de cada plugin, se puede observar que no es muy complicado de entender, estos plugins se encargan de registrar los logs obtenidos por los programas asociados a los plugins, parsearlos con expresiones regulares y asociar a cada log unos pesos que determinan su importancia. (21)

Los plugins son cada uno de los elementos definidos en el agente a analizar y estandarizar la información de un dispositivo. En general, cada uno del plugins puede leer y puede enviar los datos de un dispositivo específico, identificado por su plugin_id, así como todos y cada uno de la pertenencia de tipos de evento a ese plugin, identificó como su plugin_sid, como:

Plugin_id	PLugin_sid	Descripción
1504	1	FW-1 Accept
1525	7	nagios: service alert - hard critical

Tabla 2. Plugins.

En OSSIM hay dos tipos de plugins que son usados en la correlación para generar las alarmas:

Tipos de Plugins	Name of plugin	Example of message description
Detectors	IIS	"HTTP 404 - File not found"
Monitors	tcptrack	How long has this session been executing?

Tabla 3. Tipos de Plugins.

Por lo tanto, para cualquier dispositivo de cuál desea coleccionar los datos un plugin tiene que haber sido creado de antemano para que OSSIM sea capaz de procesarlo. Esto se logra gracias a la creación de un plugin como se había mencionado, que básicamente consiste en una serie de expresiones regulares y una lista que permiten ver el tipo de evento para ser identificado inequívocamente, incluso las evaluaciones de Fiabilidad. (22)

1.6.8 Herramientas integradas en OSSIM

Para la implantación de OSSIM es importante conocer las herramientas que serán utilizadas para la monitorización de los eventos de seguridad en un CPD y su funcionamiento.

La forma utilizada para estandarizar los datos recolectados de los diferentes programas, se realiza a través de plugins. Cada herramienta que se utiliza, debe tener su correspondiente plugin en OSSIM.

Existen dos tipos de plugins fundamentales:

Detectores: encargados de leer los logs creados por las diferentes herramientas y estandarizarlos para que el Agente pueda enviarlos al servidor. Ejemplos típicos de plugins detectores son: Snort, OSSEC, Nmap, Arpwatch, Spade y OCS-Inventory NG.

Monitores: reciben pedidos del servidor OSSIM y los envían a la herramienta correspondiente, obtienen la respuesta y le avisan al servidor si la herramienta acepta lo que se le pide. Ejemplos de algunos monitores son: Nagios, OpenVas y Ntop.

A continuación se detallan algunas de las herramientas integradas en OSSIM en cuanto a tipos de plugins mencionados anteriormente, que son necesarias para la detección y monitorización del flujo de información en las redes de un CPD.

Dentro de los **Detectores:**

Snort

Snort en particular es un Sistema de Detección de Intrusos basado en Red (Network Intrusion Detection System) **NIDS**, opera sobre los flujos de información intercambiados en una red que se encarga de analizar el tráfico de red, inspeccionando el contenido de los paquetes para disparar alertas, o incluso, realizar algún tipo de acción cuando detecta trafico sospechoso. Los IDSs utilizan distintas técnicas de análisis para alertar al administrador en caso de ver acciones sospechosas.

Snort sniffea (registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador) la red y a través de un conjunto de reglas que deciden si el tráfico es sospechoso. Las reglas contienen la información que debería contener un paquete para considerarlo sospechoso, como puede ser la dirección de red: IP origen, el puerto origen, la IP destino, el puerto destino y el contenido del paquete. En las reglas se pueden utilizar expresiones regulares y se debe incluir un mensaje que describa qué es lo que detecta.

Además del motor de detección, Snort provee preprocesadores. Los preprocesadores permiten a los usuarios y programadores extender la funcionalidad. El código de los preprocesadores se ejecuta antes del motor de detección, pero después de que el paquete fue decodificado. (16)

OSSEC (Open Source Security)

OSSEC es un Sistema de Detección de Intrusos basado en Servidor (Host Intrusion Detection System) HIDS. Un sistema de detección de intrusos basado en el host se encarga de analizar los datos del host y detectar a través de ellos si el host está siendo víctima de algún ataque. OSSEC realiza esta tarea analizando logs, chequeando integridad, monitoreando el registro de Windows, detectando rootkits, y generando y respondiendo en tiempo real.

Los IDSs basados en análisis de logs son llamados LIDS (L de Log), porque detectan errores (o ataques) usando logs como su fuente de información primaria.

OSSEC (desarrollado por Trend Micro) está formado por un administrador (manager) central de monitoreo, que recibe información desde agentes, syslog (herramienta de mensajes o trazas del sistema), bases de datos y dispositivos sin agentes (agentless).

El administrador almacena las bases de datos del chequeo de integridad de archivos, las trazas, los eventos, y las entradas de auditoría del sistema. Todas las reglas, decodificadores y configuraciones importantes se almacenan en el manager.

Los agentes son pequeños programas que se instalan en los sistemas que deseamos monitorear, estos coleccionan información en tiempo real y se la envían al administrador para ser analizada.

En los sistemas donde no se puede instalar agentes (Agentless), OSSEC puede realizar monitoreo de integridad de archivos.

OSSEC corre en la mayoría de los sistemas (Windows, Linux, OpenBSD/FreeBSD, y MacOS), y el análisis lo realiza a través de reglas escritas en lenguaje XML. Al igual que Snort, estas reglas son relativamente simples de escribir y se basan en la búsqueda de patrones (se pueden usar expresiones regulares) en los archivos analizados. También se pueden crear reglas compiladas, escritas en lenguaje C. (16)

OCS – Inventory NG

Acrónimo de Open Computer and Software Inventory Next Generation, es una aplicación que se utiliza para realizar inventario de los equipos de la red mediante un agente que se instala en el cliente. También permite el despliegue de paquetes en computadores Windows y Linux. OCS Inventory NG es una herramienta que facilita el seguimiento de la configuración y el software instalado en los ordenadores de una red local, así como la instalación remota de aplicaciones desde un servidor Web. OCS Inventory es software GPL, libre de usar y copiar. OCS Inventory también es código abierto, usted debe prever sus actualizaciones bajo los términos de la licencia GPL.

El Servidor de Gestión contiene 4 componentes principales:

- Servidor de base de datos (almacena la información del inventario).
- Comunicación con servidor (que se encarga de las comunicaciones HTTP entre el servidor de base de datos y los agentes).

- Despliegue de servidor (que almacena todos los paquetes de configuración desplegados).
- Consola de Administración (que permite a los administradores consultar el servidor de base de datos a través de su navegador web favorito.

El diálogo entre los equipos cliente y servidor se basa en el Protocolo de Transferencia de Hipertexto (HTTP) y el formato de los datos es XML. El servidor de administración utiliza Apache, MySQL y Perl. OCS es multi-plataforma: se ejecuta en sistemas operativos Unix, así como en Microsoft Windows (2000 o posterior).

Tiene una interfaz web privativa escrita en PHP que ofrece servicios complementarios:

- Consulta del inventario.
- Gestión de los derechos de los usuarios.
- Una interfaz de servicio de (o escritorio de ayuda) para los técnicos. (23)

Nmap

Nmap — Herramienta de exploración de redes y de sondeo de seguridad / puertos.

Nmap ("mapeado de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos. (24)

La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiendo de las opciones utilizadas. La información primordial es la "tabla de puertos interesantes". Dicha tabla lista el número de puerto y protocolo, nombre más común del servicio, y su estado. El estado puede ser open (abierto), filtered (filtrado), closed (cerrado), o unfiltered (no filtrado). Abierto significa que

la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Filtrado indica que un cortafuego, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto o cerrado. Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como no filtrados son aquellos que responden a los sondeos de Nmap, pero para los que Nmap no puede determinar si se encuentran abiertos o cerrados. Nmap informa de las combinaciones del estado open|filtered y closed|filtered cuando no puede determinar en cuál de los dos estados está un puerto. La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones.

Además de la tabla de puertos interesantes, Nmap puede dar información adicional sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP, un listado de sistemas operativos posibles, los tipos de dispositivo, y direcciones MAC. (24)

Dentro de los **Monitores**:

OpenVAS

OSSIM incluye OpenVAS (Open Source Vulnerability Assessment Scanner), la herramienta libre basada en Nessus, creado a partir del motor de Nessus 2 (que era libre). Se entiende a partir de esto que OpenVAS funciona igual a Nessus y persigue el mismo propósito, escanear en busca de vulnerabilidades.

Esta herramienta tiene todavía algunas limitaciones (relativamente nuevas) y no llega a ser Nessus, pero el trabajo detrás es interesante, porque además se pueden utilizar los plugins libres de Nessus. (25)

OpenVAS sigue un modelo cliente-servidor. El componente servidor es responsable de la planificación y ejecución de los análisis de red, y el componente cliente se utiliza para configurarlo y acceder a los resultados. El servidor normalmente se instala en un servidor Unix o Linux, y el cliente se ejecuta usualmente desde la estación de trabajo del administrador. En la actualidad, el cliente debe estar conectado al servidor durante todo el tiempo que dure el análisis; sin embargo, algunos de los desarrollares se encuentran actualmente trabajando en un componente nuevo que soportará muchas más interfaces.

La autoridad de asignación de números de Internet asignó oficialmente a OpenVAS el puerto TCP 9390. OpenVAS es un proyecto concienciado con la seguridad, y la conexión a este puerto desde los clientes se

realiza siempre por medio de un túnel SSL (Secure Sockets Layer) con cifrado fuerte para asegurarse de que sólo el usuario previsto pueda acceder a los datos generados por OpenVAS. (26)

Nagios

Nagios es de las herramientas más complejas, pero permite a un administrador de seguridad tener una visión central del estado de los hosts de la red. A través del monitoreo de hosts, Nagios puede enviar alertas en caso de fallas. La descripción de la funcionalidad es simple, monitorear hosts y alertar en caso de fallas. Además posee un front-end web desde donde se puede observar el estado de la red.

Nagios es un sistema de monitorización de redes de código abierto ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

Nagios se basa en un demonio central que recibe datos de plugins y los almacena en una base de datos. La configuración de todo el sistema se realiza a través de archivos de texto. Nagios no incluye mecanismos de chequeo de estado de hosts y servicios, deja este trabajo a los plugins. Simplemente se limita a ejecutar los plugins, recibir los resultados, procesar los resultados y ejecutar las acciones necesarias.

Lo bueno del sistema de plugins es que abstraen a Nagios del chequeo en sí, logrando que sea extremadamente flexible y extensible, abarcando varias plataformas. Los plugins pueden ser scripts o ejecutables que se pueden ejecutar desde la línea de comandos.

Si bien todo el monitoreo se puede realizar desde una sola máquina, algunos plugins requieren que se instale un agente monitor en la máquina que deseamos monitorear. Ejemplo de este caso es cuando deseamos monitorear el uso del procesador, memoria, disco duro, de alguna máquina en particular. El agente monitor se comunica con el servidor Nagios para enviar la información necesaria.

Actualmente existen plugins para monitorear varios dispositivos y servicios incluyendo:

- HTTP (Hypertext Transfer Protocol), POP3 (Post Office Protocol 3), SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol), FTP (File Transfer Protocol), SSH (Secure SHell), DHCP (Dynamic Host Configuration Protocol).
- Carga del procesador, uso de disco duro, uso de memoria, usuarios actuales.

- Unix/Linux, Windows, y servidores Netware.
- Routers o enrutador (dispositivo de hardware que se utiliza para interconectar computadoras que operan en nivel de red) y Switches o conmutador (dispositivo que permite la interconexión de redes).

Alertar sobre fallas es la principal función de Nagios, pero éste también es capaz de ejecutar event handlers (comando opcional que podemos ejecutar cuando un host o servicio cambia de estado). Los event handlers, al igual que los plugins, son comandos del sistema (ejecutables o scripts), y tratan de arreglar el problema antes de notificarlo. Entre los usos se incluye:

- Reiniciar un servicio que falló.
- Ingresar un ticket de problemas en un sistema de ayuda de escritorio.
- Registrar información del evento en una base de datos.
- Reinicio del sistema (hay que tener mucho cuidado con este).

La configuración de Nagios no es simple, pero está muy bien documentada. Lleva un tiempo hasta que logramos que nos alerte lo que deseamos, o tomar las acciones necesarias. Al principio puede resultar bastante molesto la cantidad de alertas arrojadas, pero gracias a la configuración de umbrales, y a la inteligencia para detectar flip-flos (cuando un servicio/host cae y se levanta muchas veces en un intervalo corto de tiempo) es posible lograr el funcionamiento deseado. (16)

Ntop

Otra gran herramienta que permite ver el uso de la red. Ntop lleva su nombre por la analogía con el comando top de Unix que muestra el uso de la memoria, CPU, etc., de los procesos.

Ntop, al igual que nfdump[1], lee los datos de la red, la almacena en archivos y a partir de ellos genera gráficas visualizables a través de una interfaz Web (puerto 3000 por defecto). Ntop es mucho más completo que nfdump, porque no solo distingue entre tráfico UDP (User Datagram Protocol), TCP, ICMP

[1] NFDUMP es un conjunto de herramientas encargadas de recolectar y procesar flujos de datos en la red que funcionan por línea de comandos.

(Internet Control Message Protocol), sino que también distingue protocolos de la capa aplicación, como ser HTTP, SNMP (Simple Network Management Protocol), SSH, DNS (Domain Name System), etc.

La variedad de gráficas que Ntop es capaz de generar hacen que el administrador tenga una excelente visión de lo que sucede en la red. Se pueden generar gráficas por host, e incluso distingue que servidores ejecuta un host dado.

No hay mejor resumen de lo que se puede hacer con Ntop que el que nos da su autor en la página:

- Ordenar el tráfico de red de acuerdo a varios protocolos.
- Mostrar el tráfico de red ordenado de acuerdo a varios criterios.
- Mostrar estadísticas del tráfico.
- Almacenar en disco estadísticas del tráfico en formato RRD (Round Robin Database).
- Identificar la identidad (direcciones de e-mail) de computadoras de usuarios.
- Identificar pasivamente (sin enviar paquetes de prueba) el Sistema Operativo de los hosts.
- Mostrar la distribución del tráfico IP entre varios protocolos.
- Analizar el tráfico IP y ordenarlo de acuerdo a la fuente/destino.
- Mostrar la matriz del tráfico IP de la subred (quién está hablando con quién).
- Reportar el uso del protocolo IP ordenado por tipo de protocolo.
- Actuar como recolector de flujo de red para los flujos generados por routers o switches. (16)

Syslog

Es un estándar para la transferencia de mensajes de eventos y alertas. Los mensajes son enviados por el Sistema Operativo, al inicio o fin de una aplicación, o reporte actual de un proceso.

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.

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 o rsyslog permiten usar TCP en vez de UDP, y también ofrecen tunel 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. (27)

Análisis de Selección de las herramientas

En este grupo de herramientas de seguridad de código abierto que ofrece OSSIM se muestran las características que garantizan la gestión de eventos e información de seguridad que se buscan para un CPD, para ello se muestran en la tabla 4 las seleccionadas y las idóneas para la implantación.

Características	**Herramientas**
Sistema de Detección de Intrusos	Snort
Escáner de Red	Nmap
Escáner de Vulnerabilidad	OpenVas
Monitor de Disponibilidad	Nagios
Inventario de Hardware y Software	OCS-Inventory
Trazas de Eventos (Logs)	Syslog

Tabla 4. Herramientas seleccionas para la implantación.

Con estas herramientas se mantiene un monitoreo y detección continuo de los problemas que surjan en la redes o subredes, además de las notificaciones en tiempo real de los eventos de seguridad.

Hay que tener en cuenta para la implantación de la herramienta, las características arquitectónicas e infraestructura que el CPD posee, el flujo de información que se desea monitorear y los servicios a priorizar.

1.6.9 Ventajas de OSSIM

- ✓ Involucra un conocimiento claro del sistema de la red, flujo de datos que se manejan y servicios que se prestan.
- ✓ Determina una arquitectura de monitoreo en tiempo real.
- ✓ Integra diferentes aplicaciones para la seguridad de la información.
- ✓ Disminuye los falsos positivos y falsos negativos con la ayuda de la correlación.
- ✓ Genera en la Web métricas e informas a un nivel ejecutivo.
- ✓ Tiene soporte de una comunidad abierta mundial que se encuentra en crecimiento constante. (5)

1.6.10 Desventajas de OSSIM

- ✓ Solo se encarga de almacenar los eventos y reportarlos, pero no realiza ninguna acción para detener los ataques, excepto que puede definírsele que en casos previamente especificados levante una aplicación adicional o externa. Dicha aplicación será desde ese momento la encargada de realizar acciones para contrarrestar un ataque o dificultad. Claro está, el control, efectividad y funcionamiento de la aplicación llamada quedará fuera del dominio de OSSIM. (5)

1.7 Conclusiones parciales

En el presente capítulo se abordaron conceptos fundamentales de la seguridad de la información, los beneficios y la importancia que tiene proteger los datos de un Centro de Procesamiento de Datos, así como el análisis de la tecnología OSSIM que es una solución SIEM verdaderamente integral. Se detallaron todas las diferentes herramientas que implementa este tipo de tecnología de código libre para seleccionar cuál de ellas se necesitan implantar de acuerdo a las características arquitectónicas que el CPD posee. Todo ello con vistas a concretar una propuesta de un procedimiento donde se definan fases, roles, artefactos y actividades para monitorizar el flujo de información de una red y mantener controlados los sucesos de seguridad mediante la correlación de eventos.

CAPÍTULO 2. CARACTERÍSTICAS DE LA SOLUCIÓN PROPUESTA

2.1 Introducción

En el actual capítulo se mostrará cómo se deben implantar algunas de las herramientas que forman parte de la tecnología OSSIM y la ubicación del servidor central, así como los procedimientos, roles, estrategias y actividades que se deben realizar en cada una de sus fases para garantizar la seguridad de la información en Centros de Procesamiento de Datos. Se describirá en concreto una propuesta de solución para este tipo de tecnología, dirigida a mantener una estrecha correlación de eventos centralizados que se irán generando por dichas herramientas con el tiempo.

Hardware y Software

Se hace un análisis de los servicios, se determina los servidores con los que cuenta y se realiza un inventario de hardware y software que posee la organización, con la finalidad de determinar las plataformas y aplicaciones con las que se trabaja. Con esto se determina cuáles serías las herramientas con las que va a trabajar el sistema, debido a que existen herramientas para servicios específicos, que funcionan relacionadas con lo que se quiere monitorizar.

Priorización de los Servicios

El objetivo principal de la priorización es identificar los servicios críticos que se deben proteger y mantener un correcto funcionamiento, así como también a los servicios cuya inhabilitación causan detenciones prolongadas a otros servicios. Cabe destacar que la integración de la herramienta al CPD no afecta en nada a la prestación de los servicios que se están actualmente ofreciendo.

Se debe considerar algunos aspectos para determinar los servicios a monitorear, de acuerdo al nivel de importancia dentro del centro de CPD.

2.2 Implantando OSSIM

Para la implantación de la plataforma OSSIM en un CPD se deben conocer los requerimientos mínimos tanto de software como de hardware para que no existan problemas, como: lentitud del servicio de monitoreo, bloqueo del sistema, limitación de espacio en disco, entre otros.

Es importante realizar un análisis de las características arquitectónicas para ubicar el servidor y los agentes de manera estratégica en la red, y definir las herramientas que se instalarán con los agentes, de acuerdo a los servicios a monitorear.

2.2.1 Requerimientos de hardware

Los requerimientos mínimos de hardware a tomar en cuenta son: procesador, memoria y disco duro, ya que el servidor se almacenan y se procesan los logs que envían los agentes, y estos tendrán además diferentes procesos corriendo, de acuerdo a las herramientas instaladas.

Para ello, se realiza un análisis del tráfico que genera la red, se determina la cantidad de equipos y redes que se van a monitorear, y de acuerdo a estos aspectos se obtienen los requerimientos mínimos de hardware, tanto para el servidor como para los agentes que serán incorporados en la red.

Se recomienda como mínimo para un aprovechamiento adecuado del sistema, una correcta captura de paquetes y una mayor rapidez en el funcionamiento de los procesos que estarán corriendo en el servidor, instalar OSSIM en una máquina con 2GB de RAM o superior, 500 GB disco duro o más, procesador Dual Core o cualquiera que tenga varios hilos de procesamiento de 64 bits y con dos tarjetas de red de 1Gbps (una para la conexión a la interfaz gráfica de OSSIM o administrativa y otra para que actué en modo promiscuo o puerto espejo capturando todos los paquetes de red tanto de entrada como de salida) donde se desplieguen los sensores. Preferentemente se debe utilizar un servidor con bastante espacio en disco duro para poder almacenar la inmensa cantidad de eventos registrados, las trazas y con suficiente memoria RAM para no sobrecargar el equipo; todo ello depende de cuán grande sea el CPD.

Si hubiera que desplegar agentes en otras máquinas que no fuera el servidor central, debería contar como mínimo, 512 MB de RAM y una tarjeta de red de 1Gbps. Los requerimientos de disco duro no se especifican, pues por lo general los agentes requieren de poco espacio en disco, ya que los eventos son enviados al servidor central o porque puede ser en la misma computadora donde se instale el servidor central de OSSIM.

2.2.2 Requerimientos de software

No hay muchas especificidades con el software, ya que el equipo de desarrollo de AlienVault distribuye un instalador en el que incluye el sistema operativo y los componentes que tienen todos los programas necesarios, acompañados de un potente sistema de configuración y actualización para que se ejecute

correctamente la versión de OSSIM a utilizar. El instalador de AlienVault está basado en el sistema operativo de Debian GNU/Linux y está disponible en 32 y 64 bits.

2.3 Alcance y Objetivos

El procedimiento a emplear garantiza, de manera centralizada, la seguridad de la información y la gestión de eventos para la prevención y detección de ataques que hayan ocurrido o que puedan suceder en el Centro de Procesamiento de Datos. Mantiene un monitoreo continuo en la infraestructura de red en tiempo real y protegiendo los activos informáticos tanto de hardware como de software. Se detallan los recursos disponibles y se valora la criticidad de los sucesos, definiendo fases, roles, actividades y artefactos; lo que permite dar una respuesta aceptada y una continua evolución del sistema.

Los **objetivos** que se pretenden alcanzar con el procedimiento son:

- Establecer un proceso de mejora en la prevención de ataques mediante las fases, actividades, capital humano, artefactos y roles establecidos en un CPD.
- Lograr una estrecha relación entre el proceso de análisis de vulnerabilidades y la detección de ataques que generan las herramientas de seguridad.
- Minimizar los falsos positivos y falsos negativos mediante la correlación de eventos con una distribución precisa de los diferentes mecanismos de seguridad.
- Brindar una mayor visibilidad de los eventos detectados mediante métricas e informes.
- Contribuir a la implantación de una solución flexible y eficiente para los CPD.

A continuación se muestra la topología de red para un CPD genérico:

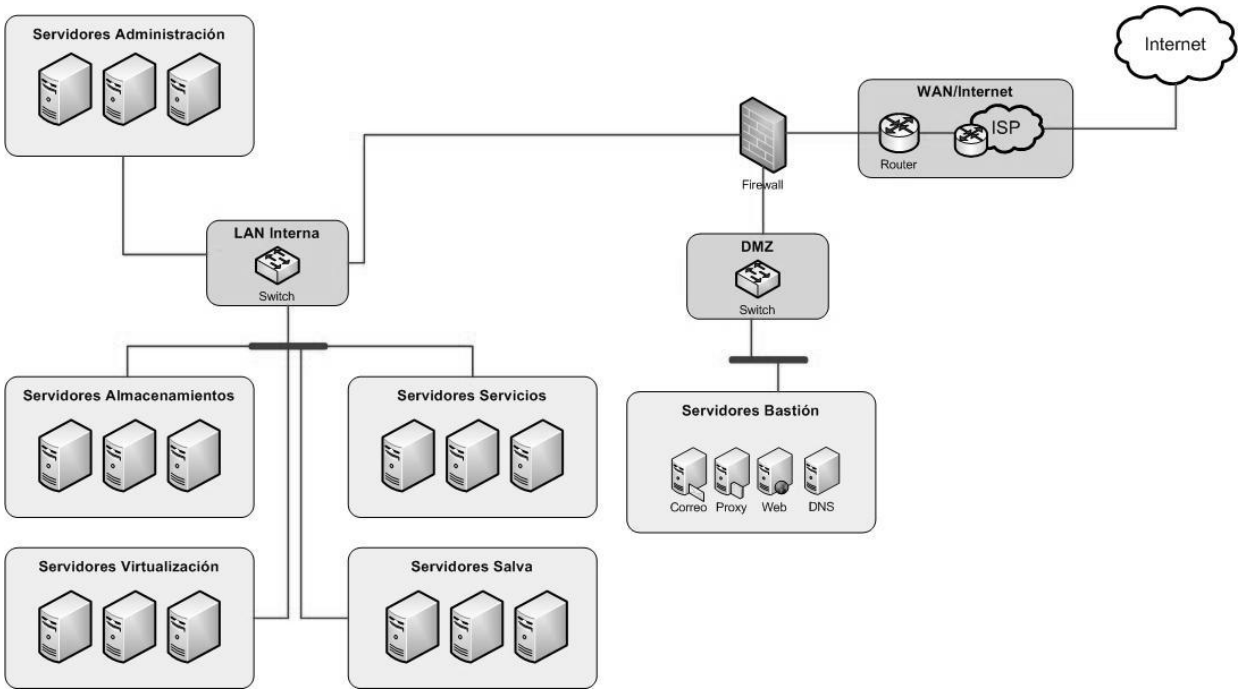


Figura 3. Topología de Red para un CPD genérico.

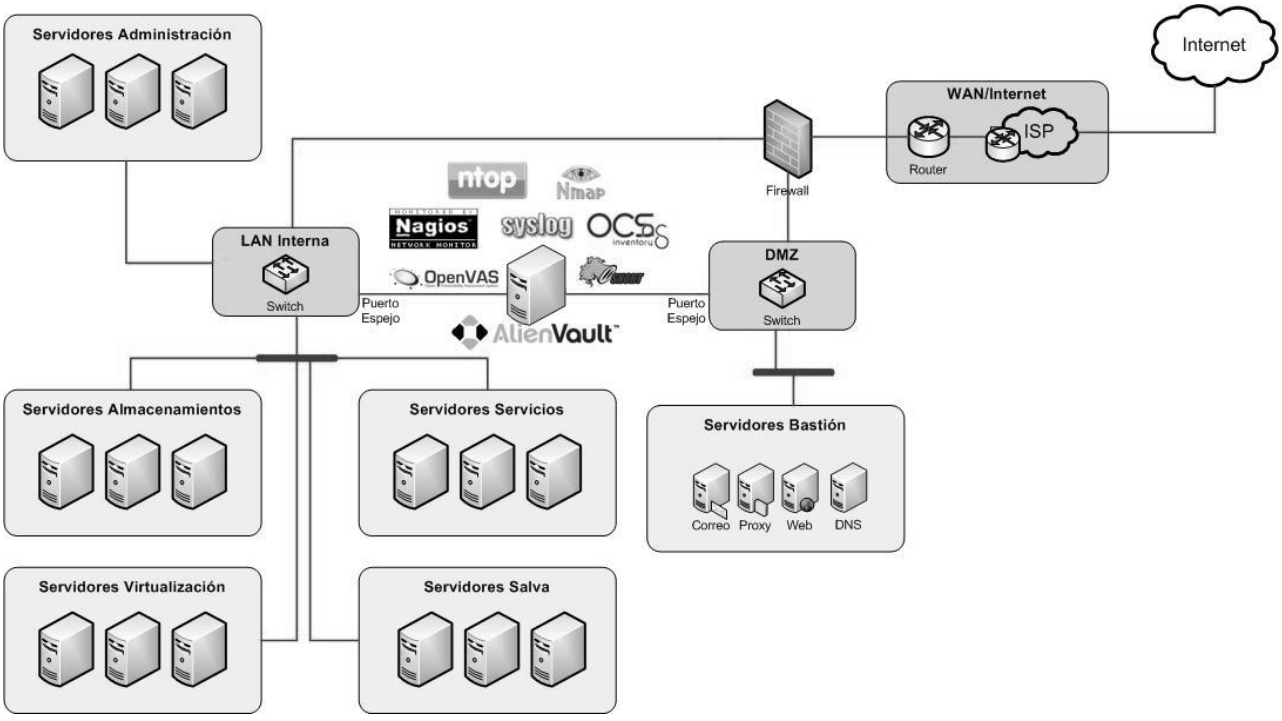


Figura 4. Despliegue de la herramienta para la solución de la Topología de un CPD.

2.4 Roles

En la seguridad de la información y gestión de eventos de una red dinámica se requiere la especificación de roles para las diferentes actividades que se desarrollarán en cada una de las fases que cubrirán las expectativas deseadas por el CPD, así como el personal capacitado que tenga un buen dominio de las herramientas y mecanismos a utilizar. Se definen tres roles generales para un CPD: Administrador, Especialista y Técnico, de los cuales se establecieron tres roles específicos dentro de los Especialistas.

A continuación se describen los roles establecidos:

1. **Especialista en Instalación y Agentes:** este es el rol fundamental, ya que es el encargado de llevar a cabo un análisis de las características arquitectónicas e infraestructura del CPD para lograr una correcta ubicación e instalación de la herramienta OSSIM con todos los agentes definidos y sus respectivos plugins para su buen funcionamiento**.** Además, realiza periódicamente las actualizaciones de los agentes y tiene una estrecha relación con el **Especialista en Seguridad**. Es el responsable de establecer una adecuada configuración de cada agente para lograr una estrecha correlación de eventos, así como un buen funcionamiento de los mismos. Vela por la veracidad de los ataques detectados por los agentes analizándolos y tiene el privilegio de modificar o agregar nuevos plugins. Es el encargado de ejecutar una herramienta si es necesario para garantizar que el ataque es real.

2. **Especialista en Análisis de Impacto:** es el encargado de tomar medidas para recuperarse ante un ataque o mitigarlo, de obtener toda la evidencia digital para evitar la corrupción de los datos y garantizar la confidencialidad de la información. Avisar en caso crítico o necesario al **Especialista en Instalación y Agentes** si el ataque es considerado brutal al sistema o áreas del CPD.

3. **Especialista en Seguridad:** es el encargado de establecer junto con el Administrador de Seguridad del CPD las nuevas políticas de seguridad para esta nueva herramienta implantada. Tiene la autoridad de cambiar las políticas de seguridad, si es necesario, y en total sincronización con el **Especialista en Análisis de Impacto y Administrador de Seguridad del CPD** en cuanto a las afectaciones que hayan ocurrido.

2.5 Presentación del Procedimiento

Se presenta un procedimiento que cuenta con cinco fases en general: Fase de Análisis e Implantación, Fase de Monitorización, Fase de Detección del Ataque, Fase de Análisis de Impacto y Preservación y Fase de Retroalimentación. Durante las cuales se llevarán a cabo una serie de actividades por los roles definidos anteriormente.

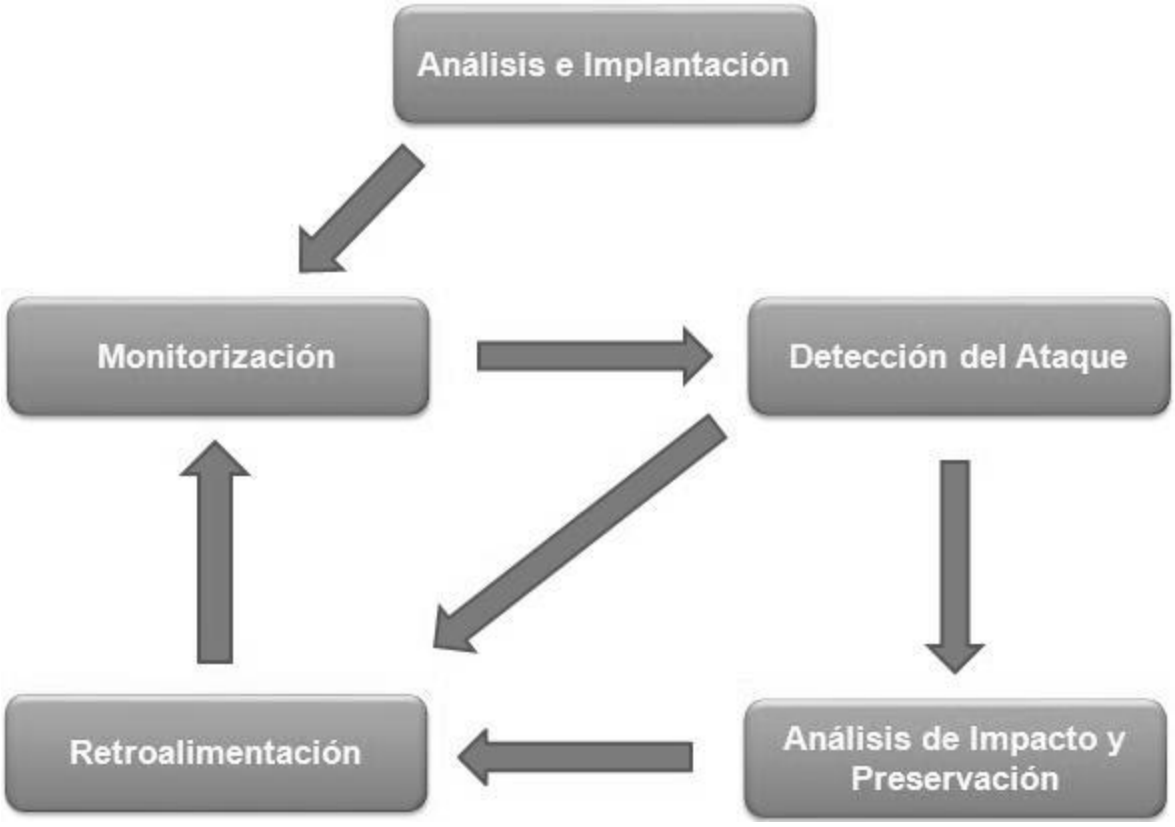


Figura 5. Fases del Proceso en General.

2.5.1 Funcionamiento del Procedimiento

En la elaboración del procedimiento se definieron 3 roles en total, con responsabilidades y actividades específicas a lo largo de las fases propuestas en la solución. En algunas fases se generan artefactos y se realizan tareas concretas asignadas a los diferentes roles definidos.

A continuación se detallan cada una de las fases y sus respectivas actividades junto con sus roles y los artefactos que se generan.

- **Fase de Análisis e Implantación**

La fase de Análisis e Implantación es la más importante, la que garantiza la efectividad del sistema y que las otras fases alcancen su objetivo, es donde se realiza un minucioso análisis de los activos del CPD y las características arquitectónicas que éste presenta para determinar y definir los agentes a utilizar. Luego realizar una correcta instalación y configuración de la herramienta con todos los agentes y plugins necesarios para lograr el buen funcionamiento de acuerdo a las necesidades de la empresa.

Detalles a tener en cuenta:

Se debe seleccionar la instalación avanzada o personalizada para decidir que agentes (detectores y monitores) con sus respectivos plugins se necesitan instalar, ya que la instalación automatizada los instala todos.

Es importante seleccionar la interfaz de red que actuará en modo promiscuo, es decir, la encarga de capturar el flujo de paquetes, garantizando que los paquetes pasen primeramente por el servidor central de OSSIM, y así pueda detectar y monitorear los ataques.

Se deben definir las redes que se desean monitorear y especificarlas.

Los agentes deben ser ubicados en determinadas posiciones para lograr una mejor captura de paquetes.

Herramienta: Paquete OSSIM.

Artefactos: Informe de Equipamiento Informático (ver Anexo 1).

Informe de Infraestructura (ver Anexo 2).

Roles que intervienen: Especialista en Instalación y Agentes, y Especialista en Seguridad.

Actividades

Valorar los activos informáticos que presenta el CPD y caracterizar el mismo para una correcta instalación y ubicación del servidor central de OSSIM en estrecha relación con el jefe del CPD.

Instalar la herramienta OSSIM con todos los agentes, sensores y plugins necesarios.

Actualizar los Agentes periódicamente.

- **Fase de Monitoreo**

La fase de monitoreo es donde se lleva a cabo el proceso de detección y prevención de ataques, es la fase donde el especialista vela y verifica por la correcta configuración de los agentes para llegar a obtener una correlación de eventos efectiva y una centralización de logs de uno o varias alertas que darán el indicio de un ataque que haya ocurrido o que pueda suceder en el futuro. En esta fase las herramientas son las encargadas de lograr una efectiva monitorización de eventos de seguridad, por lo que hay que enfatizar en la precisa configuración de cada una.

Herramientas: Snort, OSSEC, OCS – Inventory, Nagios, Ntop, OpenVas, Syslog.

Artefactos: -

Roles que intervienen: Especialista en Instalación y Agentes.

Actividades

Configuración de los diferentes agentes con sus respectivos plugins.

Chequeo de los dispositivos de interconexión.

Supervisión del monitoreo de red y detección de intrusos.

Control en la monitorización de la disponibilidad de los Host y los servicios.

- **Fase de Detección del Ataque**

La fase de detección del ataque tiene lugar cuando el CPD está siendo atacado externo o interno en la red o las subredes, es una fase crítica porque es donde se toman decisiones de cuan cierto es el ataque y que problemas nos puede ocasionar. Se identifica si el ataque es un falso positivo para que nos ayude en la retroalimentación o si es un ataque verdadero; esto es detectado principalmente por el sensor Snort como un Sistema de Detección de Intrusos basado en Red.

Gracias a las posibilidades que ofrece la mayoría de las herramientas de OSSIM, la veracidad del ataque se calcula con un valor del riesgo del evento y se decide si el ataque es real; donde finalmente es lanzada una alarma. En esta fase también se ejecutan agentes que trabajan de forma pasiva y se necesitan que se haga un nuevo análisis para profundizar más en el objetivo que busca el atacante.

Se generan las alarmas cuando el valor de riesgo del evento es igual o mayor que uno, en dependencia de la criticidad del evento y el criterio del especialista. También dependiendo del evento ocurrido, puede dispararse el valor del riesgo de una alerta a 10 y convertirse en una alarma.

El riesgo se calcula usando la siguiente fórmula:

Riesgo del Evento = (Valor del Recurso * Prioridad * Fiabilidad) / 25.

El valor del Recurso y la Prioridad tendrán un valor entre (0-5) y la Fiabilidad un valor entre (0-10).

La evaluación del riesgo que es el resultado final de la alerta estará dada por un valor entre 0 y 10.

Herramientas: Snort, OSSEC, OpenVas, Nagios, Ntop.

Artefactos: -

Roles que intervienen: Especialista en Instalación y Agentes.

Actividades

Velar por las alertas emitidas por los diferentes agentes, donde se generan tickets de alertas, alarmas y eventos de seguridad en tiempo real.

Ejecutar agentes en tiempo real para lograr una mayor certeza del ataque.

Reconfigurar los agentes y sus plugins si es necesario para una buena retroalimentación y correcto funcionamiento de cada agente involucrado en el ataque después de ocurrido un falso positivo o de emitida una alarma.

Generar informes detallados del evento o alarma emitida.

Identificar el o los objetivo(s) del atacante.

- **Fase de Análisis de Impacto y Preservación**

La fase de análisis de impacto y preservación es importante porque es donde se toman medidas para contrarrestar o neutralizar una alarma, es donde se evidencia la vulnerabilidad del sistema y qué impacto ha logrado. Es una fase que tributa completamente a la fase de retroalimentación y se ven las amenazas

que son desconocidas. También se deja una evidencia digital para evitar la corrupción de los datos y garantizar la confidencialidad de la información.

Herramientas: Syslog, OCS – Inventory, Nagios, Ntop.

Artefactos: Bitácora de incidencias (ver Anexo 3).

Roles que intervienen: Especialista en Análisis de Impacto.

Actividades

Tomar medidas para mitigar o contrarrestar el ataque que nos haya afectado el CPD o sistema involucrado.

Supervisión del proceso de recuperación.

Reportar y notificar las amenazas.

Actualizar la bitácora de incidencias.

- **Fase de Retroalimentación**

Esta fase es fundamental ya que recopila toda la información necesaria para la retroalimentación del sistema mediante el análisis de las trazas generadas por las herramientas, la cual se convierte en un proceso continuo capaz de perfeccionarse en el futuro, gracias a los resultados emitidos por la **Fase de Detección del Ataque** y la **Fase de Análisis de Impacto y Preservación**. Es donde se actualizan los mecanismos y políticas de seguridad para reducir las vulnerabilidades del CPD y se fortalece el sistema con los nuevos ataques que ocurran.

Herramientas: Syslog

Artefactos: -

Roles que intervienen: Especialista en Seguridad.

Actividades

Identificación de nuevas vulnerabilidades y ataques.

Fortalecer la seguridad informática.

Análisis en profundidad de las trazas del sistema de acuerdo a las alertas o alarmas detectadas.

2.6 Conclusiones parciales

Se puede concluir que con el desarrollo de este procedimiento se garantiza un perfeccionamiento continuo y una forma efectiva de logar la Seguridad de la Información y Gestión de Eventos con la herramienta implantada en un CPD. Se describieron los roles y los objetivos a cumplir, así como todas las actividades en cada una de las fases por la que transita el procedimiento general, además de las tareas a desempeñar en cada uno de los procesos y subprocesos con sus respectivos artefactos generados para lograr calidad y eficiencia del sistema.

CAPÍTULO 3. VALIDACIÓN DE LA PROPUESTA

3.1 Introducción

En el presente capítulo se evaluará el procedimiento de la implantación de la herramienta OSSIM en un CPD a través del método Delphi. Se seleccionarán un grupo de expertos a los cuales se les realizará una encuesta para comprobar la efectividad y eficiencia del procedimiento. Para la validación del procedimiento se empleó la entrevista para obtener la información referente al tema, el criterio de los expertos para la validación y aceptación del procedimiento mediante el uso de técnicas propuestas por el método Delphi.

3.2 Método Delphi

El método Delphi pretende extraer y maximizar las ventajas que presentan los métodos basados en grupos de expertos y minimizar sus inconvenientes. Para ello se aprovecha la sinergia del debate en el grupo y se eliminan las interacciones sociales indeseables que existen dentro de todo grupo. De esta forma se espera obtener un consenso lo más fiable posible del grupo de expertos. La operativa del método consiste en el envío de encuestas sucesivas a un grupo de expertos previamente elegidos. El consenso se obtiene por un procedimiento matemático de agregación de juicios individuales. (28)

Este método presenta tres características fundamentales:

- Anonimato: Durante un Delphi, ningún experto conoce la identidad de los otros que componen el grupo de debate. Esto tiene una serie de aspectos positivos, como son:
    - Impide la posibilidad de que un miembro del grupo sea influenciado por la reputación de otro de los miembros o por el peso que supone oponerse a la mayoría. La única influencia posible es la de la congruencia de los argumentos.
    - Permite que un miembro pueda cambiar sus opiniones sin que eso suponga una pérdida de imagen.
    - El experto puede defender sus argumentos con la tranquilidad que da saber que en caso de que sean erróneos, su equivocación no va a ser conocida por los otros expertos.

- Iteración y realimentación controlada: La iteración se consigue al presentar varias veces el mismo cuestionario. Como, además, se van presentando los resultados obtenidos con los cuestionarios anteriores, se consigue que los expertos vayan conociendo los distintos puntos de vista y puedan ir modificando su opinión si los argumentos presentados les parecen más apropiados que los suyos.
- Respuesta del grupo en forma estadística: La información que se presenta a los expertos no es sólo el punto de vista de la mayoría, sino que se presentan todas las opiniones indicando el grado de acuerdo que se ha obtenido. (29)

Para aplicar este método se siguieron tres etapas:

- Selección de los expertos y conseguir su compromiso de colaboración.
- Elaboración del cuestionario para la validación de la propuesta.
- Explotación de los resultados y desarrollo práctico.

3.3 Selección del grupo de expertos

Para la evaluación de la propuesta, se seleccionaron 5 expertos, se señala que es necesaria una cantidad mínima de 5 expertos para un por ciento de error del 10%, debido a que el error disminuye notablemente por cada experto añadido, no es aconsejable recurrir a más de 30 expertos, ya que la mejora en la previsión es muy pequeña y normalmente el incremento en coste y trabajo de investigación no compensa la mejora. (30)

Para la selección del grupo de expertos se analizaron los siguientes criterios:

- Experiencia en la administración de redes (mínimo 3 años y graduados de nivel superior).
- Experiencia en proyectos que hayan implantado OSSIM.
- Conocimientos y habilidades en actividades con la herramienta OSSIM y sus agentes.

También existen una serie de características propias que poseen cada uno de los expertos seleccionados y que se tuvieron en cuenta para conformar el panel:

- Responsabilidad.

- Competencia.
- Creatividad.
- Honestidad.
- Seriedad.
- Disposición en participar en la encuesta.
- Capacidad de análisis.

Se estableció un coeficiente de competencia para seleccionar a los posibles expertos a partir de la fórmula siguiente:

$$K = ½ (kc + ka)$$

K: Coeficiente de competencia para cada experto.

Kc: Coeficiente de conocimiento o información que tiene cada experto acerca del tema, calculando la valoración de cada experto en una escala de 0 a 10 y multiplicándola por 0,1. Quiere decir que, la evaluación “0” significa que éste no tiene ningún conocimiento en el tema, mientras que la evaluación “10” indica que el experto tiene pleno conocimiento del tema tratado. Entre estas dos evaluaciones extremas existen nueve intermedias. (31)

El experto debe marcar la casilla que estime pertinente como se muestra en la **tabla 6**.

Ka: Coeficiente de argumentación o fundamentación de los criterios del experto, obtenido como resultado de la suma de los puntos alcanzados a partir de una tabla de patrones como se muestra en la **tabla 7**.

El coeficiente de competencia calculado para cada experto se muestra en el **tabla 8**.

El objetivo de este proceso es darles validez a la solución propuesta mediante, la aplicación de cuestionarios a los expertos seleccionados. Las respuestas de este grupo de expertos pueden contribuir al perfeccionamiento del procedimiento propuesto.

3.4 Datos del Experto

Se muestra una breve introducción de la herramienta que se quiere implantar para recoger los datos de los expertos a seleccionar y así calcular el coeficiente de competencia para cada uno.

Datos del Experto para su Selección

Compañero (a):

En la tesis para optar por el título de Ingeniero en Ciencias Informáticas se desea someter a la valoración de un grupo de expertos sobre una propuesta de un procedimiento para la implantación de la herramienta OSSIM en un Centro de Procesamiento de Datos para garantizar la gestión de la información, con el fin de recoger, ordenar y correlacionar los eventos de seguridad sobre el estado de la red, el comportamiento de sistemas y usuarios, y la información del estado de las máquinas. En concreto, la información viva en la red, lo que sirve a los administradores de seguridad encontrar indicios de ataques que hayan ocurrido o que puedan suceder en un futuro.

Para ello se necesita saber el grado del dominio que usted posee sobre el tema y que responda algunas preguntas que se le piden a continuación.

Nombre y Apellidos:	
Labor que realiza:	
Especialidad:	**Años de experiencia:**
Categoría Docente:	
Categoría Científica:	

Tabla 5. Datos del experto.

1. Marque con una cruz (X) el grado de conocimiento que usted posee sobre la temática:

0	1	2	3	4	5	6	7	8	9	10

Tabla 6. Grado de conocimiento del experto.

2. Elementos a tener en cuenta para seleccionar el coeficiente de cada experto. Debe marcar con una cruz (X) las fuentes que le han servido para argumentar el conocimiento que tiene sobre la temática. Se muestra los valores que tomarían cada una de las fuentes marcadas por el experto.

No.	Fuentes de Argumentación	Grado de influencia de cada una de las fuentes en sus criterios		
		Alto	Medio	Bajo
1	Análisis teóricos realizados por usted.	0.3	0.2	0.1
2	Experiencia obtenida.	0.5	0.4	0.2
3	Trabajos de autores nacionales.	0.05	0.04	0.03
4	Trabajos de autores internacionales.	0.05	0.04	0.03
5	Su propio conocimiento en el tema.	0.05	0.04	0.03
6	Su intuición.	0.05	0.04	0.03

Tabla 7. Coeficiente de argumentación del experto.

Cálculo del Coeficiente de Competencia para cada Experto

Una vez recopilado todos los datos del experto, se calcula el coeficiente de competencia para cada uno y se llena la siguiente tabla, donde se explicará los resultados de la selección de los expertos.

Expertos	Coeficiente de competencia	Coeficiente Alto Si 0,8 < K < 1,0	Coeficiente Medio Si 0,5 < K < 0,8	Coeficiente Bajo Si K < 0,5
1	**0.915**	**X**		
2	**0.835**	**X**		
3	**0.935**	**X**		
4	**0.965**	**X**		
5	**0.89**	**X**		

Tabla 8. Coeficiente de competencia calculado para cada experto.

De los expertos seleccionados todos obtuvieron un coeficiente de competencia mayor que 0.8, y con una tendencia alta al rango máximo para su selección. Además del conocimiento de los expertos se tuvieron en cuenta todos los criterios, recomendaciones y críticas para mejorar el procedimiento y su efectividad en la implantación en los CPD. Finalmente de los expertos que tuvieron real participación y consagración con el proceso valorativo; 4 de ellos son ingenieros informáticos con más de 3 años de experiencia vinculados

a la seguridad informática, redes, servicios telemáticos y telecomunicaciones en la Universidad de las Ciencias Informáticas (UCI). El otro experto es doctor en telecomunicaciones con más de 15 años de experiencia en el tema y actualmente vinculado a la seguridad informáticas en la Instituto Superior Politécnico José Antonio Echeverría (ISPJAE). En el Anexo # 6 se muestran los datos de los expertos seleccionados que participaron en la encuesta para la valoración del procedimiento.

3.5 Elaboración del cuestionario

Una vez seleccionados los expertos, se prosigue a la elaboración de la encuesta de validación del procedimiento, por lo que se hace preciso conformar preguntas acordes a la temática planteada. Se tomaron en cuenta 4 criterios importantes: mérito científico, implantación, flexibilidad e impacto del procedimiento de la implantación de la herramienta en un CPD. También para la elaboración de la encuesta se tuvieron en cuenta recomendaciones de los expertos consultados y la maestría (30).

La encuesta elaborada para validar el procedimiento de la implantación de la herramienta OSSIM en un CPD se muestra en el Anexo # 4, la cual fue aplicada a todos los expertos seleccionados. Además se le envió a cada experto una descripción del procedimiento propuesto para que tuvieran conocimiento de la propuesta y pudieran responder las preguntas correspondientes. Se tuvo en cuenta que, cada consejo o buena práctica dado por los expertos está validad por su seriedad, honestidad, sinceridad y experiencia en el tema.

3.6 Concordancia de los expertos mediante el coeficiente de Kendall

Un buen acuerdo entre los expertos ofrece una mayor validez a la propuesta, por lo que se necesita calcular el Coeficiente de Concordancia de Kendall (W) que ayuda a comprobar el grado de coincidencia de las valoraciones realizadas. Esto constituye una estadística útil en estudios de confiabilidad entre los expertos en la temática, al determinar la asociación entre distintas variables.

Para la aplicación de este coeficiente se construye una tabla de aspectos a evaluar contra los expertos donde se sitúan los rasgos de valoración de cada aspecto evaluado por cada uno de los expertos; estos son tomados de los resultados de las preguntas de la encuesta, consultar Anexo # 5.

Después de la elaboración de la tabla se realizan los siguientes pasos:

- Determinar la suma de los valores numéricos asignados a cada aspecto a evaluar, según el criterio dado por cada experto (Rj).

- Determinar de la media de Rj, dado por la sumatoria de los Rj entre N, siendo N el total de aspectos a evaluar (los aspectos serán las preguntas del cuestionario, en este caso N = 10).
- Determinación de la desviación media, dada por la diferencia entre cada Rj y el valor de la media.
- Determinación de la suma de los cuadrados de las desviaciones medias, S.
- Determinación del cuadrado del número total de expertos, K. En este caso K = 5.

Una vez que se tienen todos estos datos es posible calcular el Coeficiente de Kendall (W) a través de la fórmula siguiente:

$$W = \frac{12s}{k^2(N^3 - N)}$$

El coeficiente de Kendall ofrece el valor que posibilita decidir el nivel de concordancia entre los expertos. El valor W siempre es positivo y oscila entre 0 y 1. Con el mismo se puede calcular el Chi-Cuadrado real con el objetivo de ver si existe o no concordancia entre los expertos, el mismo se obtiene a través de la fórmula siguiente:

$$X^2 = K\,(N - 1)W$$

El Chi-Cuadrado se compara con el de la tabla inversa de la función de distribución de la variable Chi-Cuadrado (32). Si X^2 real < X^2 (α, N-1), entonces existe concordancia en el trabajo de los expertos.

Luego de la realización de los cálculos pertinentes se obtuvieron los siguientes resultados: X^2 real = 2.623 y el X^2 (0.10, 9) = 4.168, lo cual corrobora el cumplimiento de la comparación y por lo tanto existe concordancia entre los expertos.

3.7 Desarrollo práctico y explotación de los resultados

Para llegar a conclusiones objetivas acerca de la propuesta, los resultados de los cuestionarios se procesan según plantea (33). Con el objetivo de recoger y visualizar los resultados aportados se fueron confeccionando tablas, con la ayuda de cálculos mediante Microsoft Excel 2010.

El cuestionario elaborado consta de 10 preguntas, las cuales fueron agrupadas por criterios (mérito científico, implantación, flexibilidad e impacto) donde cada pregunta de la encuesta tiene un valor entre 0-10 puntos asociado una categorización: muy adecuado-MA (C1) entre 9-10 puntos, bastante adecuado-BA (C2) entre 7-8 puntos, adecuado-A (C3) entre 5-6 puntos, poco adecuado-PA (C4) entre 3-4 puntos y no adecuado-NA (C5) entre 0-2 puntos.

Inicialmente se calculó las frecuencias absolutas como se muestra en la tabla 9.

No.	Aspectos	C1	C2	C3	C4	C5	Total
1	Valor de la propuesta	0	5	0	0	0	5
2	Calidad de la investigación	2	3	0	0	0	5
3	Contribución científica	1	1	2	1	0	5
4	Responsabilidad científica y profesionalidad del investigador	4	1	0	0	0	5
5	Necesidad de empleo de la propuesta	4	1	0	0	0	5
6	Posibilidades de aplicación	4	1	0	0	0	5
7	Adaptabilidad de la herramienta a otros CPD	4	1	0	0	0	5
8	Capacidad del proceso evaluativo de la herramienta	2	3	0	0	0	5
9	Impacto en los CPD	4	1	0	0	0	5
10	Organización en el proceso de desarrollo	2	3	0	0	0	5

Tabla 9. Frecuencias absolutas.

A partir de la frecuencia absoluta se obtienen las frecuencias acumuladas donde los datos de cada fila se suman con el anterior como se muestra en la tabla 10.

No.	Aspectos	C1	C2	C3	C4	C5
1	Valor de la propuesta	0	5	5	5	5
2	Calidad de la investigación	2	5	5	5	5
3	Contribución científica	1	2	4	5	5
4	Responsabilidad científica y profesionalidad del investigador	4	5	5	5	5
5	Necesidad de empleo de la propuesta	4	5	5	5	5
6	Posibilidades de aplicación	4	5	5	5	5
7	Adaptabilidad de la herramienta a otros CPD	4	5	5	5	5
8	Capacidad del proceso evaluativo de la herramienta	2	5	5	5	5
9	Impacto en los CPD	4	5	5	5	5
10	Organización en el proceso de desarrollo	2	5	5	5	5

Tabla 10. Frecuencias absolutas acumuladas.

La frecuencia absoluta acumulada se divide entre la cantidad de expertos y se obtiene la frecuencia relativa acumulada (en esta tabla desaparece la columna C5) tal y como se muestra en la tabla 11.

No.	Aspectos	C1	C2	C3	C4
1	Valor de la propuesta	0	0,9999	0,9999	0,9999
2	Calidad de la investigación	0,4	0,9999	0,9999	0,9999
3	Contribución científica	0,2	0,4	0,8	0,9999
4	Responsabilidad científica y profesionalidad del investigador	0,8	0,9999	0,9999	0,9999
5	Necesidad de empleo de la propuesta	0,8	0,9999	0,9999	0,9999
6	Posibilidades de aplicación	0,8	0,9999	0,9999	0,9999
7	Adaptabilidad de la herramienta a otros CPD	0,8	0,9999	0,9999	0,9999
8	Capacidad del proceso evaluativo de la herramienta	0,4	0,9999	0,9999	0,9999
9	Impacto en los CPD	0,8	0,9999	0,9999	0,9999
10	Organización en el proceso de desarrollo	0,4	0,9999	0,9999	0,9999

Tabla 11. Frecuencias relativas acumuladas.

Por último se buscan las imágenes de las frecuencias relativas acumuladas por medio de la función (Distribución Normal. Estándar Invertida) y se adicionan las siguientes salidas:

- **Suma**: Sumatoria de cada fila y de cada columna según sea el caso.
- **P**: Promedio de la suma de cada fila.
- **N**: División de la sumatoria de las sumas de las filas entre el resultado de multiplicar el número de categorías por el número de pasos.
- **N-P**: Es entonces el valor promedio que le otorgan los expertos consultados a cada paso de la metodología.
- **Punto de corte**: Promedio de la suma de cada columna.

La tabla 12 muestra los resultados de los puntos de corte.

						N = 0,80		
No.	**C1**	**C2**	**C3**	**C4**	**Suma**	**P**	**N - P**	
1	0	3,72	3,72	3,72	11,16	2,79	-1,990	Muy Adecuado
2	-0,25	3,72	3,72	3,72	10,91	2,728	-1,928	Muy Adecuado
3	-0,84	-0,25	0,84	3,72	3,47	0,868	-0,068	Muy Adecuado
4	0,84	3,72	3,72	3,72	12	3	-2,200	Muy Adecuado
5	0,84	3,72	3,72	3,72	12	3	-2,200	Muy Adecuado
6	0,84	3,72	3,72	3,72	12	3	-2,200	Muy Adecuado
7	0,84	3,72	3,72	3,72	12	3	-2,200	Muy Adecuado
8	-0,25	3,72	3,72	3,72	10,91	2,728	-1,928	Muy Adecuado
9	0,84	3,72	3,72	3,72	12	3	-2,200	Muy Adecuado
10	-0,25	3,72	3,72	3,72	10,91	2,728	-1,928	Muy Adecuado
Suma	2,61	33,23	34,32	37,2	**107,36**			
Puntos de Corte	0,261	3,323	3,432	3,72				

Tabla 12. Puntos de corte.

Los puntos de corte sirven para determinar la categoría o el grado de adecuación de cada pregunta según la opinión de los expertos. Para determinar el grado de adecuación de cada aspecto a validar se realiza como se muestra en la tabla 13.

Muy Adecuado	**Bastante Adecuado**	**Adecuado**	**Poco Adecuado**	**No Adecuado**
N-P =< 0,26	> N-P =< 3,32	> N-p =< 3,43	> N-P =< 3,72	

Tabla 13. Grado de adecuación de los aspectos a validar.

A partir de este análisis todos los aspectos a validar en las preguntas de la encuesta fueron considerados por los expertos como “Muy Adecuados” demostrando la utilidad y aplicabilidad del procedimiento planteado para la implantación de la herramienta.

3.8 Resultados de la validación de los indicadores propuestos en la encuesta

De acuerdo a los criterios de cada una de las preguntas realizadas a los expertos, se realizó un análisis mediante gráficas del valor del procedimiento de la solución mostrada.

Los indicadores a evaluar en la encuesta realizada a los expertos fueron agrupados por criterios de mérito científico, criterios de implantación, criterios de flexibilidad y criterios de impacto.

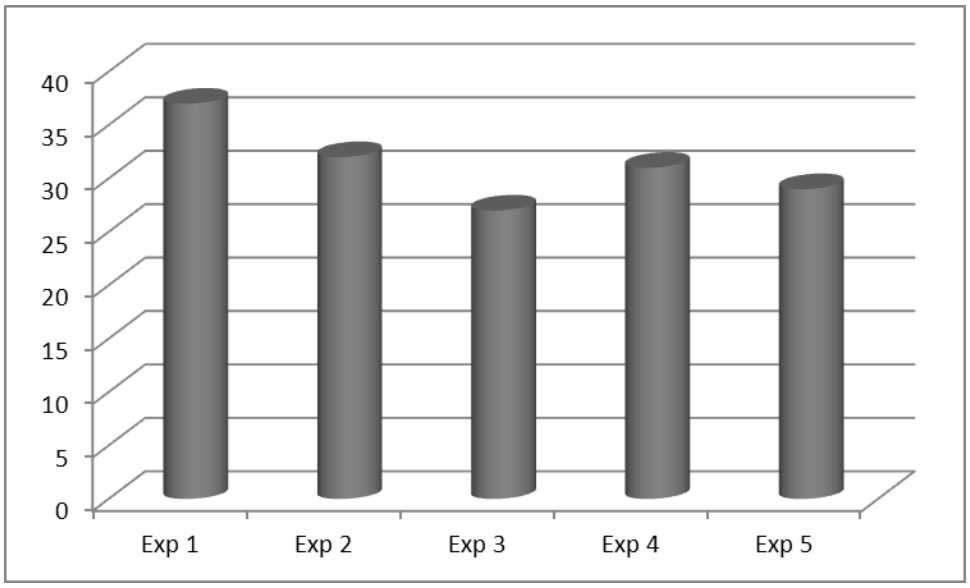


Figura 6. Criterios de Mérito Científico.

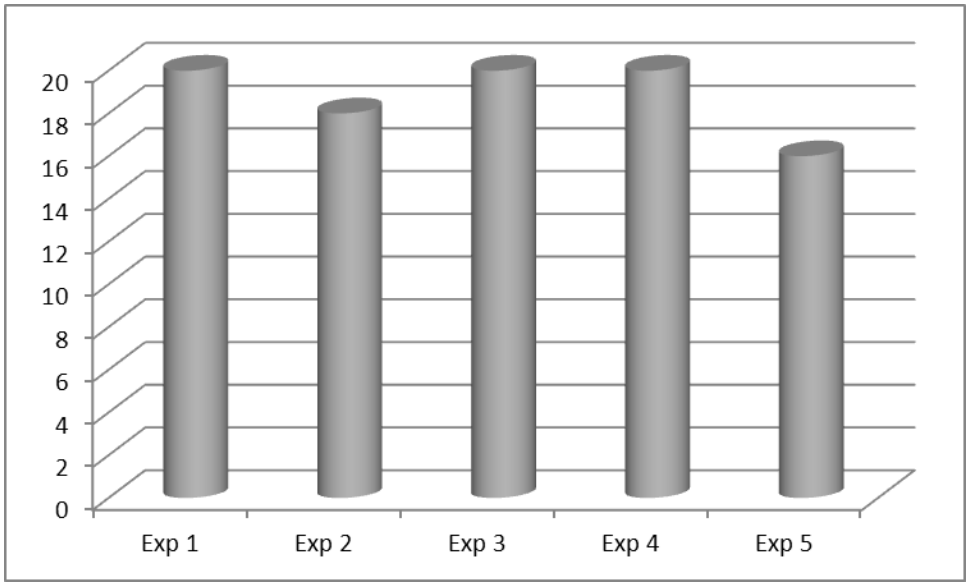


Figura 7. Criterios de Implantación.

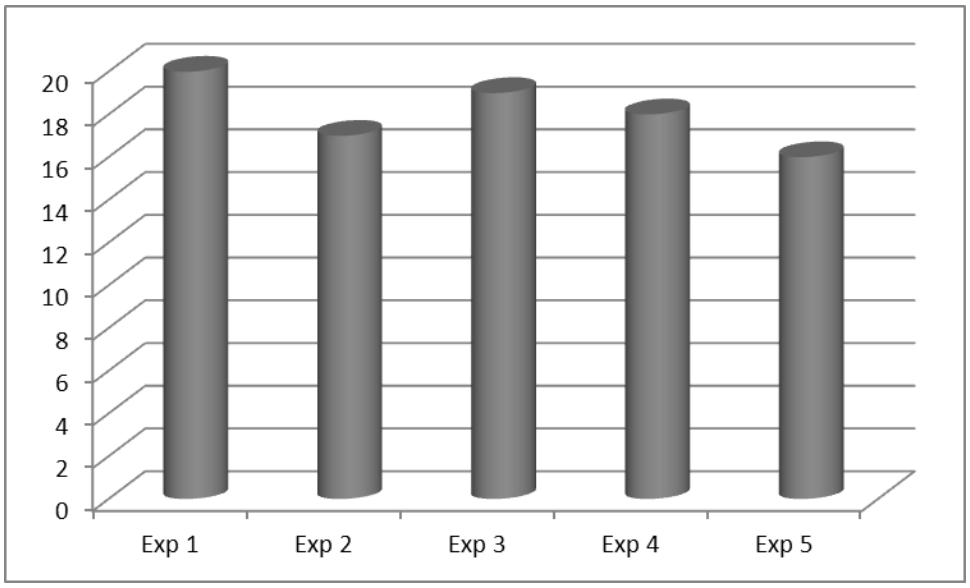


Figura 8. Criterios de Flexibilidad.

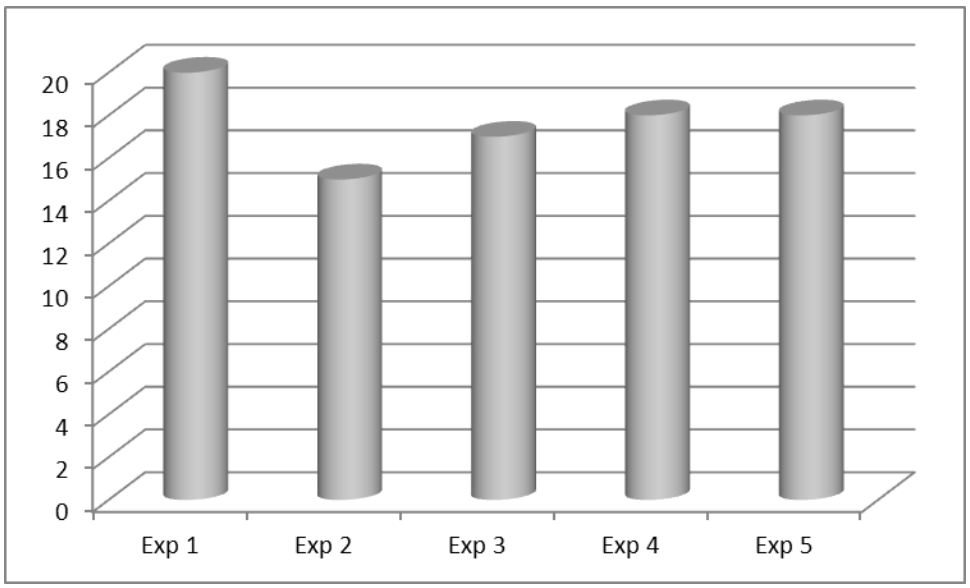


Figura 9. Criterios de Impacto.

De los expertos seleccionados cuatro de ellos evaluaron el procedimiento de bueno y aplicable a los Centros de Procesamiento de Datos y uno lo evaluó de regular; en la figura 11 se muestran los resultados.

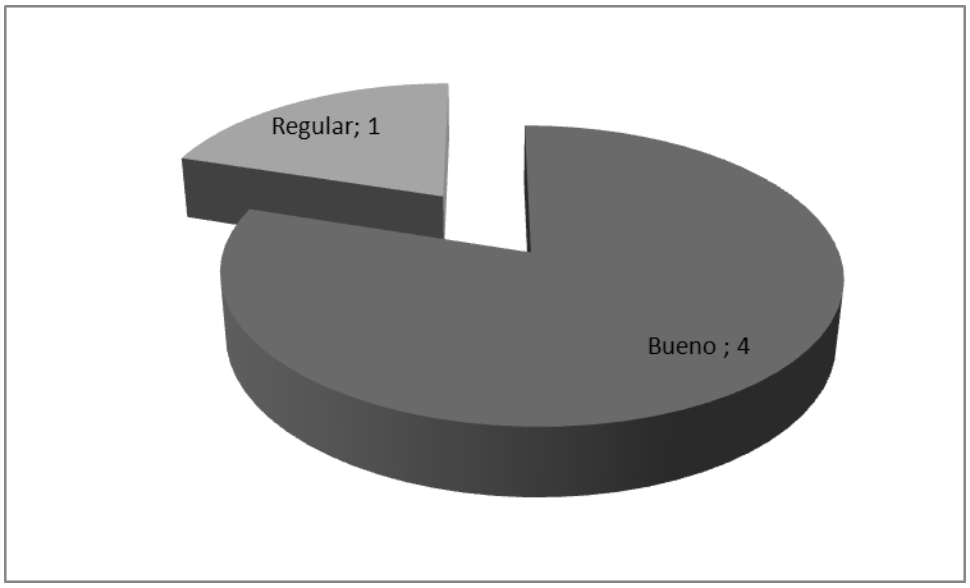


Figura 10. Evaluación de los expertos.

3.9 Conclusiones parciales

La validación del procedimiento propuesto para la implantación de la herramienta OSSIM en un Centro de Procesamiento de Datos se realizó mediante el método Delphi, en el cual se obtuvieron resultados satisfactorios, ya que todos los expertos encuestados valoraron la propuesta como útil, correcta, aplicable y efectiva para gestionar los eventos de seguridad de la información y problemas en las redes o subredes. Se tuvieron en cuenta todas las recomendaciones, sugerencias y críticas dadas por los expertos para mejorar el procedimiento y perfeccionar el despliegue de la herramienta.

CONCLUSIONES GENERALES

- Con la realización de esta investigación se desarrolló un estudio de los productos que implantan tecnologías SIEM y dentro de ellas AlienVault OSSIM de código abierto.
- Se estudió en detalles varias de las herramientas de seguridad para establecer una detección y monitoreo continuo y ser habilitadas en la versión de OSSIM a utilizar, siempre en correspondencia con las características arquitectónicas que posea el Centro de Procesamiento de Datos.
- Se detalló un procedimiento que pone en marcha la implantación de la herramienta OSSIM y sus sensores, con el establecimiento de 5 fases.
- Se realizó la validación de la herramienta propuesta por el método Delphi donde un grupo de expertos dieron sus criterios, sugerencias y recomendaciones a la hora de desplegar este tipo de herramienta en un Centro de Procesamiento de Datos, la cual arrojó resultados positivos en la grado de concordancia entre los expertos y las valoraciones de la encuesta realizada.

RECOMENDACIONES

- Se recomienda llevar a cabo en profundidad la configuración de cada uno de los sensores y plugins que brinda la herramienta AlientVault OSSIM con vista a los tipos de correlación que ofrece (lógica, cruzada y de inventario) para mejorar la detección de ataques informáticos y problemas en la red de un CPD.

- Utilizar esta investigación como referencia, estudio y muestra de implantación de la herramienta OSSIM para la detección y monitorización continua de la gestión de la información y eventos de seguridad en otras áreas informáticas.

REFERENCIAS BIBLIOGRÁFICAS

1. CLAUDIO MARCIAL, J. Z. *Seguridad Informática.* publicado el: 29/03 de 2011, última actualización: 29/03. 45 p.

2. MARTÍN, C. *Auditoría de bases de datos: el camino hacia la solución* [Consultado el: 20 de Abril de 2012]. Disponible en: http://www.datati.es/auditoria-de-bases-de-datos-el-camino-hacia-la-solucion/.

3. MELÉNDREZ, E. H. *METODOLOGÍA DE LA INVESTIGACIÓN.* 2006. 51 p.

4. ENRIQUE, H. O. *Seguridad y Privacidad en los Sistemas Informáticos.* 2003, 9 p.

5. LÁZARO ESTEBAN ARCE RODRÍGUEZ, S. G. G. *Análisis y Configuración de la Herramienta de Seguridad Informática OSSIM en la Universidad de las Ciencias Informáticas.* Universidad de las Ciencias Informáticas, 2008.

6. INFORMACIÓN, A. S. D. L. *Servicios Seguridad TIC Gestión de Eventos de Seguridad, Gestión de Eventos de Seguridad* [Consultado el: 17 de Marzo de 2012]. Disponible en: http://www.audea.com/servicios/tecnologias-seguridad/ctsim/.

7. CASAL, J. *Alien Vault OSSIM Open Source* [Consultado el: 19 de Marzo de 2012]. Disponible en: http://www.alienvault.com/alienvault-en-espanol/.

8. MARK NICOLETT, K. M. K. *Magic Quadrant for Security Information and Event Management.* publicado el: 20/Marzo/2012 de 2011, última actualización: 20/Marzo/2012. 20 p.

9. TI, O. I.-G. D. S. *Gestión de la Seguridad, Visión General* [Consultado el: 20 de Octubre Disponible en: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_seguridad/vision_general_gestion_de_la_seguridad/vision_general_gestion_de_la_seguridad.php.

10. SERVICIOS-TL, I.-G. D. *Gestión de la Seguridad, Introducción y Objetivos* [Consultado el: 20 de Octubre Disponible en: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_seguridad/introduccion_objetivos_gestion_de_la_seguridad/introduccion_objetivos_gestion_de_la_seguridad.php.

11. QUINTANA, J. D. F. *CENTRO DE PROCESO DE DATOS: EL CEREBRO DE NUESTRA SOCIEDAD.* publicado el: 21 de Septiembre de 2009, última actualización: 21 de Septiembre. 46 p.

12. MILNE, K. *OSSIM - Open Source Security Information Manager - User Manual.* publicado el: 2 de Septiembre de 2004, última actualización: 2 de Septiembre.

13. MARTÍNEZ, A. N. *Propuesta de una Plataforma de Gestión de Información de Seguridad en la Intranet de la UCLV "Marta Abreu".* publicado el: 11 de Diciembre de 2008, última actualización: 11 de Diciembre.

14. GIL, D. *OSSIM - Descripción General del Sistema.* publicado el: 21 de Octubre de 2003, última actualización: 21 de Octubre. 34 p.

15. MARIA P. ESPINOZA, J. A. P. Y. M. X. S. *Implementación de una Herramienta SIM (Security Information Management) en la Red de la Universidad Técnica Particular de Loja.* publicado el: 20 de Junio de 2007, última actualización: 20 de Junio. 10 p.

16. SIM, A. O. S. *Monitoreo de red: OSSIM Review Parte I (OSSIM, Snort y OSSEC)* [Consultado el: 15 de junio Disponible en: http://itfreekzone.blogspot.com/2010/06/monitoreo-de-red-ossim-review-parte-i.html.

17. COVARRUBIAS, F. D. *Descripción General de OSSIM - Alien Vault.* 2009, 18 p.

18. GARDUÑO, G. B. A. Y. N. G. *ARQUITECTURA DE MONITOREO EN TIEMPO REAL DE UNA RED.* INSTITUTO POLITÉCNICO NACIONAL. ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA UNIDAD CULHUACAN, 2010.

19. PALACIOS, J. D. *La solución integral SIEM - OSSIM.* España: 2009,

20. OLMOS, A. P. *Análisis de la plataforma Ossim - Sistema de Gestión de la Información Open Source.* Universidad Politécnica de Valencia, 2008.

21. PLUGIN, A. *Data Source Plugins* Disponible en: http://communities.alienvault.com/community/plugins.

22. ALIENVAULT. *Plugins OSSIM* Disponible en: http://www.alienvault.com/wiki/doku.php?id=documentation:agent#creating_a_new_plugin.

23. TEAM, O. I. *Welcome to OCS Inventory NG* Disponible en: http://www.ocsinventory-ng.org/en/.

24. NMAP.ORG. *Guía de referencia de Nmap (Página de manual)* Disponible en: http://nmap.org/man/es/index.html#man-description.

25. TOM, D. P. *OpenVas - Open Vulnerability Assessment System - Manual Práctico.* 2011,

26. GALITZ GEOFF, B. T. Y. M. T. *Exploramos el analizador de vulnerabilidades OpenVAS.* 2010,

27. LONVICK, C. M. Security Issues in Network Event Logging (syslog). 2011, nº Disponible en: http://datatracker.ietf.org/wg/syslog/charter/.

28. MARÍN, D. V. *Aplicación del método Delphi en la selección de contenidos formativos para el profesorado en TIC.* Córdoba: 2011, 14 p.

29. DEUSTO, U. D. *EL MÉTODO DELPHI.* 2004, 14 p.

30. VALDIVIA, I. M. M. *PROCESO PARA PLANEAR LA CARTERA DE SERVICIOS EN LA ADOPCIÓN DE UNA INICIATIVA SOA.* Ciudad de la Habana: 2010, 109 p.

31. PADRÓN, A. L. *VALIDACIÓN MEDIANTE MÉTODO DELPHI DE UN CUESTIONARIO PARA CONOCER LAS EXPERIENCIAS E INTERÉS HACIA LAS ACTIVIDADES ACUÁTICAS CON ESPECIAL ATENCIÓN AL WINDSURF.* Universidad Agraria de la Habana (Cuba): 2010, 22 p.

32. BOUZA C.N., S. V. *Estadística. Teoría básica y ejercicios.* La Habana, Cuba: Editorial Félix Varela: 2004,

33. FERNÁNDEZ, A. Y. R., R. *Modelo Informático para la autogestión del aprendizaje para la universalización de la enseñanza.* Granada, España: 2005,

BIBLIOGRAFÍA CONSULTADA

- ADRIÁN, P. O. Análisis de la plataforma Ossim - Sistema de gestión de la información Open Source. Universidad Politécnica de Valencia, 2008.
- ALFARO, M. R. Redes de Computadora - Manul de OSSIM (Opem Source Security Information Management). 2009, 112 p.
- ALIENVAULT. AlienVault Site [Consultado el: 20 de Mayo de 2012]. Disponible en: http://www.alienvault.com/.
- ALIENVAULT. Plugins OSSIM Disponible en: http://www.alienvault.com/wiki/doku.php?id=documentation:agent#creating_a_new_plugin.
- ALVARO, G. V. TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS. 2009,
- ANGEL, A. P. OSSIM, una plataforma clave para la seguridad en profundidad. Publicado el: 6 de Noviembre de 2007, última actualización: 6 de Noviembre.
- ARGENTINA, A.-C. D. E. E. R. T. D. L. A. P. Manual de Seguridad en Redes. 2011,
- ASENSIO, G. A. Gestión de la Seguridad con OSSIM. Publicado el: 10 de Mayo de 2006, última actualización: 10 de Mayo. 44 p.
- BRIAN, E. L. OSSIM - Open Source Security Information Management. Publicado el: 29 de Mayo de 2008, última actualización: 29 de Mayo.
- CASAL, J. AlienVault OSSIM Open Source [Consultado el: 19 de Marzo de 2012]. Disponible en: http://www.alienvault.com/alienvault-en-espanol/.
- CLAUDIO MARCIAL, J. Z. Seguridad Informática. Publicado el: 29/03 de 2011, última actualización: 29/03. 45 p.
- COVARRUBIAS, F. D. Descripción General de OSSIM - AlienVault. 2009, 18 p.
- GALITZ GEOFF, B. T. Y. M. T. Exploramos el analizador de vulnerabilidades OpenVAS. 2010,
- GARDUÑO, G. B. A. Y. N. G. ARQUITECTURA DE MONITOREO EN TIEMPO REAL DE UNA RED. INSTITUTO POLITÉCNICO NACIONAL. ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA UNIDAD CULHUACAN, 2010.
- GIL, D. OSSIM - Descripción General del Sistema. Publicado el: 21 de Octubre de 2003, última actualización: 21 de Octubre. 34 p.

- HERNEY CIFUENTES JESUS, A. N. B. C. MANUAL DE DETECCIÓN DE VULNERABILIDADES DE SISTEMAS OPERATIVOS LINUX Y UNIX EN REDES TCP/IP. UNIVERSIDAD DEL VALLE, 2004.
- HUGO, G. P. Estudio de un IDS Open Source frente a herramientas de análisis y explotación de vulnerabilidades. UNIVERSIDAD CARLOS III DE MADRID, 2010.
- IGNACIO, B. Port-mirroring en switches 3COM [Consultado el: 22 de Mayo de 2012]. Disponible en: http://tecnoquia.blogspot.com/2009/12/port-mirroring-en-switches-3com.html.
- ISABEL, G. G. M. Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral. Universidad de Almería, 2008.
- JOAQUIN, J. H. J. A. G. A. Seguridad en redes de computadoras. Universidad Oberta de Cataluña, 2008.
- JOAQUÍN, M. M. J. ARQUITECTURA DIRIGIDA POR EVENTOS PARA UN SISTEMA DE DETECCIÓN DE INTRUSIONES BASADO EN PATRONES. UNIVERSIDAD DE MURCIA, 2008.
- JOSÉ, I. A. OSSIM/SOC: el binomio de la seguridad corporativa. 2006.
- JUAN MANUEL MADRID MOLINA, L. E. M. S., CARLOS ANDREY MONTOYA GONZÁLEZ, JUAN DAVID OSORIO BETANCUR, y LUIS ERNESTO CÁRDENAS, R. B., CRISTIAN LATORRE. IMPLEMENTACIÓN Y MEJORA DE LA CONSOLA DE SEGURIDAD INFORMÁTICA OSSIM: UNA EXPERIENCIA DE COLABORACIÓN UNIVERSIDAD-EMPRESA. Universidad ICESI, Santiago de Cali (Colombia): publicado el: 10/12 de 2008, última actualización: 10/12. 29 p.
- LÁZARO ESTEBAN ARCE RODRÍGUEZ, S. G. G. Análisis y Configuración de la Herramienta de Seguridad Informática OSSIM en la Universidad de las Ciencias Informáticas. Universidad de las Ciencias Informáticas, 2008.
- MARIA P. ESPINOZA, J. A. P. Y. M. X. S. Implementación de una Herramienta SIM (Security Information Management) en la Red de la Universidad Técnica Particular de Loja. Publicado el: 20 de Junio de 2007, última actualización: 20 de Junio. 10 p.
- MARIANA, M. T. M. MANUAL DE OSSIM (Open Source Security Information Management). Universidad Nacional de Ingeniería FEC, 2009.
- MARK NICOLETT, K. M. K. Magic Quadrant for Security Information and Event Management. Publicado el: 20/Marzo/2012 de 2011, última actualización: 20/Marzo/2012. 20 p.

- MARTÍNEZ, A. N. Propuesta de una Plataforma de Gestión de Información de Seguridad en la Intranet de la UCLV "Marta Abreu". Publicado el: 11 de Diciembre de 2008, última actualización: 11 de Diciembre.
- MELÉNDREZ, E. H. METODOLOGÍA DE LA INVESTIGACIÓN. 2006. 51 p.
- MILNE, K. OSSIM - Open Source Security Information Manager - User Manual. Publicado el: 2 de Septiembre de 2004, última actualización: 2 de Septiembre.
- NMAP.ORG. Guía de referencia de Nmap (Página de manual) Disponible en: http://nmap.org/man/es/index.html#man-description.
- OLIVER WAGNER JAN, W. M., BROWN TIM, KOCH MAUTHE CARSTEN. OpenVAS Compendium. 2009.
- OSSIM, A. V. AlienVault Technical Documentation [Consultado el: 15 de Mayo de 2012]. Disponible en: http://communities.alienvault.com/community/technical-documentation.
- OSSIM, A. V. C. O. AlienVault Unified SIEM. 2011, 47 p.
- PALACIOS, J. D. La solución integral SIEM - OSSIM. España: 2009,
- QUINTANA, J. D. F. CENTRO DE PROCESO DE DATOS: EL CEREBRO DE NUESTRA SOCIEDAD. Publicado el: 21 de Septiembre de 2009, última actualización: 21 de Septiembre. 46 p.
- RUIZ ROBLES ANTONIONI LEANDRO, D. L. O. C. J. M. Diseño de un esquema de seguridad en redes de datos. Universidad de los Andes, 2010.
- TOM, D. P. OpenVas - Open Vulnerability Assessment System - Manual Práctico. 2011.