ISSN: 2306-2495 | RNPS: 2343 *Serie Científica de la Universidad de las Ciencias Informáticas*
http://publicaciones.uci.cu Vol. 14, No. 11, Mes: Noviembre, 2021, Pág. 206-232

Tipo de artículo: Artículo de revisión

Sistemas SIEM aplicados a sistemas de salud: Caso de estudio TEMONET

SIEM systems applied to health systems: TEMONET case study

Jenny Arizaga Gamboa[1*], **https://orcid.org/0000-0002-2098-9077**
Eduardo Alvarado Unamuno[2], **https://orcid.org/0000-0001-6145-7926**
Jorge Chicala Arroyave[3], **https://orcid.org/0000-0001-9630-2377**

[1] Universidad de Guayaquil, Guayaquil, Ecuador. E-Mail: jenny.arizagag@ug.edu.ec
[2] Universidad de Guayaquil, Guayaquil, Ecuador. E-Mail: eduardo.alvaradou@ug.edu.ec
[3] Universidad de Guayaquil, Guayaquil, Ecuador. E-Mail: jorge.chicalaa@ug.edu.ec

*** Autor para correspondencia: jenny.arizagag@ug.edu.ec**

Resumen

La seguridad de los datos de una empresa o institución debe de ser uno de los puntos más importantes antes de la realización de esta, para ello se realiza un estudio previo para poder tener seguro los datos, dicha información solo puede tener acceso personal autorizado, si se llegara a tener un inconveniente con respecto a la seguridad de los datos las instituciones o entidades estarían en un apuro y un desprestigio por la perdida, copiado o alteraciones de los datos, para ello el área encargada de la seguridad de los datos es la encargada de blindar la información estableciendo un sin número de procesos de seguridad o se puede realizar un sistema de codificaciones o encriptaciones antes de ingresar a la base de datos de la instituciones o entidades de esta manera se asegura la información valiosa de esta misma. La fuerte demanda por parte de las organizaciones en el contexto de seguridad informática ha disparado el interés de estas por los sistemas SIEM. El presente informe nos muestra, por una parte, un enfoque teórico sobre lo que es un SIEM y sus sistemas más populares desarrollados, por otra, un enfoque práctico de la implementación de un sistema SIEM. Este sistema está compuesto por una serie de componentes basados en Open Source, en el que se describen sus funcionalidades y algunos casos de uso. El sistema implementado se basa en la integración de ElasticStack (Elasticsearch, Logstash, Kibana y beats) con otras tecnologías como Wazuh (HIDS), SearchGuard y Sentinl.

Palabras clave: Sistemas SIEM; sistemas de salud; TEMONET.

Abstract

The security of the data of a company or institution must be one of the most important points before carrying out this, for this a prior study is carried out to be able to have the data secure, said information can only be accessed by authorized personnel, if there is a problem with the security of the data, the institutions or entities would be in a hurry and a loss of prestige due to the loss, copying or alteration of the data, for this the area in charge of data security is in charge to shield the information by establishing a number of security processes or a codification or encryption system can be carried out before entering the database of the institutions or entities in this way the valuable information of this same is ensured. The strong demand from organizations in the context of computer security has triggered their interest in SIEM systems. This report shows us, on the one hand, a theoretical approach on what a SIEM is and its most popular systems developed, on the other, a practical approach to the implementation of a SIEM system. This system is made up of a series of components based on Open Source, in which its functionalities and some use cases are described. The implemented system is based on the integration of Elastic Stack (Elasticsearch, Logstash, Kibana and beats) with other technologies such as Wazuh (HIDS), Search Guard and Sentinl.

Keywords: SIEM systems; Systems of health; TEMONET

Recibido: 15/07/2021
Aceptado: 28/10/2021

Introducción

En el mundo actual donde hackers, virus de computadoras o "ciber-terrorismo" son términos cotidianos, no resulta extraño que la protección de los activos de información se haya convertido en prioridad en todo tipo de organizaciones. Sin embargo, a nivel mundial varias empresas prefieren asumir el riesgo, debido principalmente a que los costos de la inversión en tiempo y dinero de la implementación de un sistema de seguridad, es significativamente alta y que en aquellas que los poseen, mientras no se produzca un "ciber-ataque", el sistema implementado no tendrá mucha oportunidad de demostrar su importancia y valor en la defensa de los activos de información. Estas consideraciones básicas, determinan que las organizaciones desempeñan su labor al filo de la navaja digital global. El desarrollo de la TI y los sistemas digitales, automatizando la gestión en todos los procesos, ha permitido involuntaria y paralelamente el incremento de software malicioso, direccionado a secuestrar, alterar, sabotear, impedir o divulgar los activos de información de las organizaciones, a fin de obtener ilícitas ganancias materiales. La mayor parte de las organizaciones se enteran de que son víctimas de "ciber-ataques", solo en el momento en el que un evento de seguridad evidencia un impacto negativo sobre el núcleo del negocio. De ahí que, proteger los activos de información es una de las tareas más importante al interior de la organización; pues ante su omisión, son varias las historias que recogen un lamentable final en consecuencia.

La necesidad de salvaguardar los activos de información ante potenciales y latentes "ciberataques", ha motivado el desarrollo de tecnología para cumplir tal menester; constituyéndose en propiedad de los fabricantes el producto y la metodología específica creada, para su implementación en la organización del cliente final. La implementación de un sistema de "ciber-seguridad", a cuyo cargo estará el procesamiento de inmensas cantidades de datos, bajo el cumplimiento de normas y parámetros determinados, es una tarea altamente compleja que demanda recursos y personal calificado y experimentado junto a una metodología de implementación eficaz, que paso a paso guie al personal dedicado a este meticuloso trabajo, a efectos de no convertirse en una experiencia fatídica con desalentadores resultados (Perurena et al., 2013).

Considerando los artículos de investigación existentes sobre el tema a la fecha, ningún estudio ha planteado una metodología formal que derive en la implementación de un SIEM. Para la implementación en un sistema de salud es sumamente importante debido a que protegemos a los usuarios del sistema de salud, podemos brindar un mejor

servicio ya que estaría todo organizado para los que soliciten información de cada uno de los pacientes que se intervienen en este centro de salud, aunque lo primordial en este sistema es de proteger los datos de cada uno de los usuarios y dichos datos o informaciones no sean alteradas porque si no todo el sistema se vería colapsado por no tener los datos correspondientes y correctos de cada uno de los pacientes de este centro de salud.

Materiales y métodos

La tecnología SIEM (Security Information and Event Management), un Sistema de gestión de eventos y seguridad de la información, se encarga de recolectar eventos de seguridad a través de distintos dispositivos y aplicaciones mediante un software llamado agente o conector, este filtra los datos y los normaliza a un formato los analiza a través de correlaciones usando información contextual y administradores de alerta en caso de un ataque. La herramienta SIEM proporciona proactiva detección de amenazas y un análisis en tiempo real de la actividad del sistema (ROSAS et al., 2018).

SIEM, es un conjunto de tecnologías diseñadas para brindar una visión clara y precisa de la seguridad de la información de una organización (su implementación facilita el trabajo de administradores de TI y analistas de seguridad de la Información), al actuar automáticamente en respuesta a incidentes de seguridad detectados por el sistema de Gestión de Eventos de Seguridad de la Información.

Un SIEM utiliza una herramienta sofisticada inteligencia para amenazas en tiempo real, contiguo con la correlación de eventos que detectan las amenazas reales (Vazão et al., 2019).

SIEM dispone de la administración de información de seguridad, también conocida como SIM, que contiene la administración de registros, análisis e informes de cumplimiento.

También contiene la gestión de eventos de seguridad, también conocida como SEM, que establece la supervisión en tiempo real y gestión de incidentes que son generados en los eventos de seguridad de redes, dispositivos, sistemas y aplicaciones que amenazan la seguridad los datos manteniéndolos seguros.

El Sistema SIEM, es la consecuencia de dos elementos:

- **SIM “Security Information Management”**

La Gestión de la Seguridad de la Información, consiste en administrar los “logs” y generar informes técnicos correspondientes. El SIM proporciona la recolección, el reporte y el análisis de archivos de “logs” de sistemas operativos, dispositivos de red y dispositivos de seguridad.

La solución SIM administra información de riesgo, resguardando las actividades críticas de TI a través de la correlación y análisis de seguridad de los datos, en forma automatizada en un único sistema inteligente (ROSAS et al., 2018).

SEM "Security Event Management"

La Gestión o Administración de Eventos de Seguridad, analiza en tiempo real eventos y "data logs"; asegurando el contexto del seguimiento de amenazas de eventos y tomando acciones en respuesta a cualquier incidente. Los datos pueden ser recolectados desde dispositivos de seguridad, red, sistemas y aplicaciones (ROSAS et al., 2018); (Cabrera Jurado & Agüero Herrera, 2015).

Ventajas claves de SIEM

1. *Administración de "logs":* en cada dispositivo o servicio con una infraestructura basada en TI, se llega a producir alguna clase de "log" con información de eventos relacionados con el dispositivo. Estos "logs" son almacenados en una base de datos, siendo correlacionados y utilizados por el sistema de seguridad.
2. *Estándar TI:*se destacan por las regulaciones y estandarizaciones que forman parte de la gestión de administración de la seguridad de la información. La organización en todo momento debe respetar los estándares establecidos y el uso correspondiente de soluciones SIEM que son obtenidos mediante un certificado que le da credibilidad.
3. *Correlación de eventos:* es una especialidad clave de la inteligencia artificial que tienen los sistemas SIEM. Siendo un proceso que busca establecer conexiones entre eventos que suelen ocurrir en distintas partes físicas o elementos de la infraestructura.
4. *Reacción automática:* es basado en el resultado que existe en la correlación de eventos para prevenir los incidentes de seguridad en caso que se llegue a producir algún riesgo. El administrador no es capaz de reaccionar tan rápido como lo haría el sistema SIEM; sin embargo, las acciones automáticas que se producen deben ser probadas y verificadas por un administrador, de otra manera una configuración errónea significaría realizar acciones innecesarias que provocarán un impacto negativo sobre servicios y aplicaciones en la infraestructura del sistema.
5. *Seguridad de equipos finales*: es el factor más importante que se debe tener en cuenta en la infraestructura completa. La mayoría de amenazas de seguridad, son producidos por errores humanos cuando se manipulan los dispositivos que tienen contacto directo con empleados; de ahí que, es demandante la monitorización permanente de equipos finales.

6. *Administración central de seguridad:* en el mercado existen muchas compañías desarrolladoras que emplean sus propias herramientas de seguridad, usando cada una con su propia lógica, significado y consola de administración, que generalmente resultan no ser compatibles o interoperables cuando se integran; detalle imprescindible a considerar al momento de la implementación.
7. *Reportes:* en base a la infraestructura centralizada que provee valores e información concisa para la administración de los eventos e incidentes de seguridad. El uso de esta información acredita al equipo de seguridad la toma acertada de decisiones en situaciones ordinarias y críticas de la gestión de seguridad.

SIEM es una tecnología que sirve eficientemente para prevenir violaciones de datos, incluso cuando las amenazas provienen de los dispositivos IoT (Internet de las cosas) que son utilizados en la atención médica para controlar todo, desde marcapasos hasta rastreadores de ubicación portátiles para personas mayores. Este sistema de seguridad avanzada analiza cada componente de la infraestructura mediante el descubrimiento de activos. Teniendo la capacidad de ver y evaluar cada dispositivo es fundamental para proteger toda la red.

Capas de los SIEMS

Las Capas de los SIEM se pueden visualizar en la figura 1 donde se muestra las capas que tiene generalmente una herramienta SIEM.

El número de la capa indica el orden en que se configura cada una de ellas. Una vez se han parametrizado las 4 capas, la herramienta está lista para su máxima utilización, contando por supuesto con el equipo de profesionales de la seguridad que dé uso óptimo (Arias Bernal & Cogollo Bustamante, 2013).

4	Capas de reportes	Visualización y Exposición
3	Capas de correlación	Reglas e Inteligencia
2	Capas de normalización	Estandarización
1	Capa de captura de eventos	Integración

Figura 1. Capas de SIEM

El sistema de seguridad ofrece herramientas útiles para conseguir el desempeño total:

- **Automatización de seguridad y orquestación de Firewall:** Inicia la automatización de las alertas y respuestas defensivas. Elimina la necesidad de personal de TI adicional.
- **Consola de administración unificada:** todas las herramientas de seguridad se encuentran en un único lugar, para mejorar la comprensión y el análisis de los eventos y alertas de seguridad. Es ideal para expertos en seguridad y fácil de entender para ejecutivos.

- **Detección y respuesta de endpoints:** es el que ofrece las capacidades forenses para disminuir el impacto de una infracción. Rinde visibilidad completa en todos los puntos finales, incluidas redes, servidores, bases de datos, aplicaciones, procesos y comunicaciones para detectar actividades maliciosas y simplificar la respuesta a incidentes de seguridad.
- **Informes y seguimiento de cumplimiento:** Sugiere informes predefinidos que defienden las necesidades de cumplimiento. Esta solución también promete a los empleados de seguridad de TI una visión amplia y detallada de los eventos de seguridad de una organización, lo que puede prevenir violaciones de HIPAA y mantener seguros los datos de salud.
- **Monitoreo en la nube:** Se aprovecha la nube para el almacenamiento de los datos. Un SIEM proporciona herramientas automáticas y manuales para realizar, monitorear y evaluar la estructura de la nube.

Descripción de componentes de la herramienta SIEM

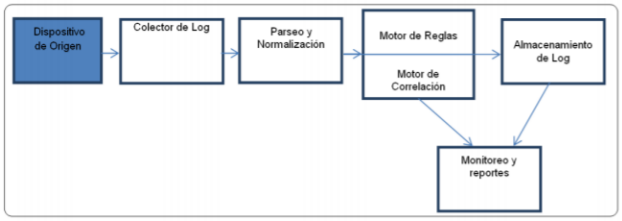

Figura 2. Diagrama de flujo de las herramientas SIEM- Dispositivos de origen

En la figura 2 se muestra los componentes que funcionan en la herramienta de SIEM y se describirán a continuación:

Dispositivo de origen. - El primer elemento de las herramientas SIEM es el dispositivo de origen que alimenta de información o registros al SIEM.

Un dispositivo origen suele ser una aplicación o cualquier equipo de red como es un router, un switch o cualquier otro servidor que genere registros logs que se requieran procesar en el SIEM.

El dispositivo origen no hace parte de los componentes que se obtienen en la adquisición de un SIEM, sin embargo, se lo tiene muy en cuenta debido a que es la fuente de información de la que se mantienen los demás bloques en el procesamiento de logs.

Al establecer los dispositivos que serán la fuente de información presentes en el entorno de red, es necesario establecer lo que se quiere conseguir de los logs, con frecuencia las empresas asocian erradamente el funcionamiento de una herramienta SIEM con una y sólo una de las siguientes prestaciones:

- Cumplimiento de regulaciones o estándares mediante la generación automática de reportes.

- Copia alterna de los logs en un periodo de tiempo específico.
- Análisis de evidencia forense.

Un aspecto importante en tener en cuenta es que no todos los logs son obligatorios en todos los dispositivos, por lo que es notable tener un balance entre los dispositivos que proveen la información legítima en una detección de amenazas, y entre la información sensible o activos críticos identificados en el Sistema de Gestión de Seguridad de la Información (SGSI).

- Colector de Logs. Este componente también pertenece a la primera capa de la herramienta SIEM, la capa de captura de eventos.

La función de un colector debe llegar a ser un proceso automático que permita conseguir datos, éstos datos se generan de muchas formas y tamaños, desde agentes que corren sobre los dispositivos monitoreados hasta dispositivos centralizados de registros con pre-procesadores para fragmentar el flujo de los datos.

Los datos que llegan a la herramienta SIEM resultantes de los distintos dispositivos tiene dos tipos de mecanismos en el método de recolección, en el el primer método se refiere a configuración manual, esen el cual el dispositivo origen envía sus logs a la herramienta SIEM por medio de syslog o SNMP y se configura la dirección IP del servidor de Logs para el envío automático al SIEM. Es obligatorio configurar los parámetros básicos en el envío de logs como es la dirección IP del SIEM, nombre del DNS y puerto asociado para la transferencia de los logs.

En segundo método utilizado es en el cual el SIEM inicializa la conexión directa al dispositivo de origen, haciendo la consulta de algún archivo de texto en el que se generan los registros de una aplicación o dispositivo, ejemplo de esto son las consultas mediante el protocolo ODBC de conexión a las Bases de Datos, que por medio de una consulta y con conexión establecida desde el SIEM, permite traer los registros mediante consultas al aplicativo o base de datos que audita las transacciones de los usuarios.

Para algunas aplicaciones de desarrollo propietarias de las compañías, es decir, desarrolladas in house, es necesario utilizar agentes propietarios de SIEM, o software de terceros que permita hacer la consulta del archivo de texto que guarda el historial o registros logs, para poder convertir estos registros en formato Syslog y facilitar su fácil interpretación por la herramienta SIEM. Debido a que cada fabricante de dispositivos maneja un lenguaje por medio del cual se comunica éste con otras plataformas, el responsable de la implementación debe conocer los diversos tipos de estándar existentes en el mercado y la manera particular de parametrizarlo con la herramienta SIEM (ESPAÑOLA & REORGANIZACIÓN) (Vazão et al., 2019).

- Normalización. La normalización corresponde a la segunda capa de SIEM y se define como el proceso de cruzar varios tipos de formatos de logs y convertirlos en un formato único, de tal manera que independiente de la fuente, el ID del evento, o la descripción, un valor común puede ser derivado.

Los eventos normalizados entonces serán usados para minimizar la repetición de eventos de un mismo dispositivo, o múltiples dispositivos repitiendo el mismo evento. Los eventos también son categorizados dentro de contenedores útiles que permiten la generación de reportes en categorías de seguridad de una manera más rápida y efectiva. Por ejemplo, registros que son clasificados dentro de la categoría de cambios en configuración, auditoría de acceso a archivos o ataques de tipo Buffer Overflow, Denegación de servicio, etc.

Motor de Reglas/Motor de Correlación. El motor de reglas y el de correlación pertenecen a la capa de correlación, elemento que proveelas reglas e inteligencia a la herramienta. De hecho, la generación de alertas dentro del SIEM es un hecho destacado importantes por las que fue diseñado; dependiendo del método utilizado en la escritura de reglas, puede ser simple o llegar a ser demasiado complejo.

Las reglas son regularmente escritas utilizando una forma de lógica booleana para determinar si una condición en concreto reúne ciertos estándares dentro de determinados campos de datos (Neu et al., 2020).

La disponibilidad de contar con el módulo de Escaneo de Vulnerabilidades en el SIEM, admite incluir dentro de la correlación de alertas datos que aprueba determinar si un ataque hacia la infraestructura interna de red es satisfactorio o no.

-Almacenamiento de logs. El almacenamiento de logs de registros logs en el SIEM necesita de una base de datos robusta que permita realizar consultas de una manera eficaz de los eventos históricos que se encuentren almacenados, usualmente las plataformas utilizadas son de tipo Oracle, MySQL, Microsoft SQL y propietarias de algunos fabricantes.

En la interacción de búsqueda de logs y ejecución de reportes, también se requiere contar con Hardware robusto para la ejecución de estos procesos.

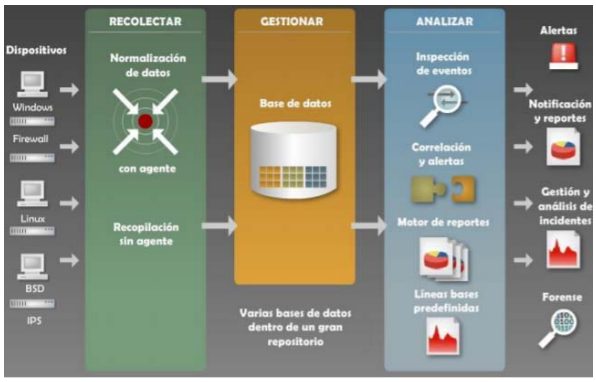

Figura 3. Flujo de eventos

La figura 4 muestra el flujo de los eventos que se prestan en un SIEM, se visualiza el proceso de captura de los logs desde dispositivos de diferente naturaleza hacia un componente que, o los convierte por medio de un agente a un formato reconocible por la herramienta SIEM o bien, los transmite sin necesidad de un agente. En cualquier caso, ambos son transportados dentro de un repositorio centralizado que los almacena para su posterior análisis y gestión.

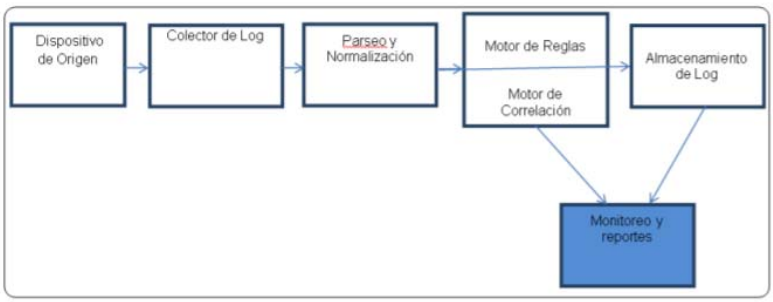

Figura 4. Diagrama de flujo de las herramientas SIEM- Monitoreo y reportes.

En la figura 4 se muestra el último módulo en la arquitectura de un SIEM es la interacción y el uso de los logs almacenados, para tener el mayor aprovechamiento en el alertamiento de monitoreo y reportes que este tipo de herramientas pueden ofrecer, caso contrario, el SIEM solo sería solo un repositorio de logs.

Un SIEM es controlado a través de una interfaz para el usuario, que está basado en web o por aplicación, ambas son capaces de interactuar con los registros almacenados en la generación de nuevas alertas, programación de tareas o revisión de tiquetes para el manejo de incidentes que posteriormente puedan ser asignados a cada funcionario responsable de la labor de revisión (de Oliveira, 2020).

Habitualmente para comprobar la información que proporciona el SIEM, los funcionarios se acercaran a los diferentes dispositivos que se tienen vinculados al SIEM y hacer la revisión de los logs en formato nativo. La herramienta SIEM tiene vistas de análisis y consultas por categorías que se puede acceder la información mediante la extracción de la

información de una manera más rápida, esencialmente por la normalización de los logs son más eficientes las consultas de eventos en la base de datos.

En la capa de reportes se encuentran características que perfecciona el panorama añadiendo cierto nivel de inteligencia, por ende, el oficial de seguridad no reacciona frente a un evento aislado,eventualmente se programa la herramienta para que reaccione y dispare una alarma sólo después de haber tenido en cuenta la combinación de varias condiciones (Robalino Díaz, 2018).

SIEM y administración de logs

La administración de logs contiene la recopilación de registros integral, agregación, retención del registro original,análisis de texto de logs, presentación, flujos de trabajo y contenido relacionados. Con la administración de logs, los casos de uso son amplios y cubren todos los posibles usos de los datos de registro a través de IT e incluso más allá (Robalino Díaz, 2018).

Características de un administrador de logs

- *Colección de datos de logs*:acumula todos los registros, utilizando métodos basados en agentes o sin agentes, o una combinación de los dos.
- *Retención eficiente:*tanto la recolección y el almacenamiento de datos de registro soncapaces de recoger gigabytes e incluso terabytes de datos de registro eficientemente y retenerlos mientras se provee búsquedas y acceso rápido no es trivial. Dado que muchas regulaciones muestran términos específicos para la retención de datos de registro esta función es crítica para un sistema de administración de logs.
- *Búsquedas:* La búsqueda es la forma primordial de tener acceso a la información en todos los logs, eso incluye a los logs de aplicaciones personalizadas. Buscar es vital para la investigación de registros, análisis forense de registros y la búsqueda de fallos durante el uso de logs de aplicación para la solución de problemas.
- *Indexación:* La indexación de logs es un componente esencial de un sistema de gestión de registros. La tecnología de indexación crea una estructura de datos llamada índice, que proporciona búsqueda rápida de tipo palabra clave o tipo booleano mediante todo el almacenamiento de logs.
- *Reportes:* Los reportes y reportes programados envuelven todos los datos recolectados por el producto de gestión de logs y es similar a los reportes del SIEM. Lo primordial de los reportes sea para razones de seguridad, regulaciones u operación puede hacer o deshacer la solución de gestión de logs. La exposición de reportes debe ser rápida, personalizable y fácil de usar para una amplia gama de propósitos.

Resultados y discusión

En una estrategia de defensa en profundidad, las practicas más destacadas en la industria utilizan varios dispositivos (Firewalls, IDS, AV, AAA, VPN, LDAP/NDS/NIS/X.509, logs de sistemas operativos) por ende, fácilmente arrojan cientos de miles de eventos por día, en algunos casos millones de eventos.

En el mercado de la seguridad existen diversas soluciones globales SIEM que ofrecen una gestión central para estas dos características. Algunos productos caen más en una u otra área del SIM o el SEM, y otros afirman que son capaces de ofrecer ambas bondades con "demasiada ligereza".

Algunas buenas prácticas a seguir son las siguientes:

1. Establecer el alcance y los requisitos

Se debe saber exactamente qué actividades y registros desea que supervise SIEM. Esto incluye elegir si se prefiere implementar SIEM como un software local o un servicio alojado o administrado. A continuación, se debe obtener una imagen clara de los requisitos de SIEM, incluidos los casos de uso para su industria en particular.

2. Personalizar las reglas de correlación

El valor central de SIEM proviene de la aplicación de reglas de correlación que pueden marcar eventos de seguridad que de otra manera pasarían desapercibidos. Por ejemplo, una regla de correlación que dice que, si hay varios inicios de sesión fallidos desde la misma IP en un período de tiempo determinado seguidos de un inicio de sesión exitoso, es posible que haya un ataque de fuerza bruta en curso. Si bien el software SIEM viene con su propio conjunto de reglas integradas, se puede personalizar según las necesidades requeridas eliminando falsos positivos o creando nuevas reglas.

3. Realizar previamente una prueba de funcionamiento

Una ejecución piloto en una sección de la infraestructura es una buena forma de probar la nueva implementación. Esta etapa proporciona la prueba de concepto y el potencial retorno de la inversión del sistema. Sin embargo, es importante que este subconjunto de prueba represente el contexto más amplio del sistema para permitir identificar fallas y vulnerabilidades en las políticas de seguridad.

Durante esta ejecución de prueba, se recopila la mayor cantidad de datos posible para tener una idea clara de cómo funcionaría el sistema. Por supuesto, no siempre es posible recopilar datos de todas las fuentes de la organización. En este caso, debe priorizar las secciones que se ocupan de los sistemas críticos y los datos confidenciales.

4. Instalar un plan de respuesta a incidentes

Un SIEM proporciona monitoreo y alertas casi en tiempo real para la detección de amenazas de TI, lo que permite una respuesta rápida a una gran cantidad de eventos de seguridad. Sin embargo, la organización debe aprovechar las características de SIEM mediante la implementación de un plan de respuesta a incidentes detallado y práctico.

Este protocolo integral debe cubrir cuestiones como la distribución de responsabilidades y tareas en caso de una violación de datos o un ataque, priorizar y documentar el evento y delegar quién será responsable de comunicar la violación a las partes interesadas y las autoridades pertinentes. Un plan de respuesta a incidentes bien diseñado proporciona los pasos exactos y las pautas que deben seguir los equipos de seguridad cuando ocurre un ataque, lo que ahorra tiempo y minimiza los errores resultantes.

5. Actualizar el sistema SIEM continuamente.

Dado que los atacantes mejoran constantemente sus métodos y técnicas, el SIEM debe estar un paso por delante. Se debe probar periódicamente SIEM, modelar posibles ataques y evaluar la reacción de SIEM. La simulación de ataques puede ayudar a establecer una mejor configuración de SIEM ajustando reglas, políticas y procedimientos de correlación para mantenerse por delante de los atacantes malintencionados (Li et al., 2017).

Importancia de un SIEM para la seguridad informática

Para mejorar la capacidad de identificar una actividad inapropiada o inusual, las organizaciones pueden integrar el análisis de la información con análisis de vulnerabilidades, los datos de rendimiento, monitoreo de red y el registro de auditoría del sistema (log), esta información se logra a través del uso de herramientas SIEM.

Las herramientas SIEM son un tipo de software de registro centralizado que puede facilitar la agregación y consolidación de los registros de múltiples componentes del sistema de información. Las herramientas SIEM también pueden facilitar la auditoría de correlación de registros y análisis. La correlación de la información de registro de auditoría con la información de análisis de vulnerabilidades es importante para determinar la veracidad de los análisis de vulnerabilidad y correlacionar eventos de detección de ataques con resultados de la exploración.

Los productos SIEM generalmente incluyen soporte para muchos tipos de orígenes de registros de auditoría, tales como sistemas operativos, servidores de aplicaciones (por ejemplo, servidores web, servidores de correo electrónico), y software de seguridad, e incluso pueden incluir soporte para dispositivos de control de seguridad física, tales como lectores de tarjetas.

Un servidor SIEM analiza los datos de los diferentes orígenes de registros de auditoría, correlaciona eventos entre las entradas de registro de auditoría ,identifica y prioriza los eventos importantes, y se puede configurar para iniciar las respuestas a los acontecimientos. Para cada tipo de origen de registros de auditoría, los productos SIEM normalmente

se pueden configurar para proporcionar la funcionalidad de categorizar los campos de registro de auditoría más importantes que puede mejorar significativamente la normalización, análisis y correlación de datos de registro de auditoría.

El software SIEM también puede realizar la reducción de eventos al prescindir de los campos de datos que no son importantes para la seguridad del sistema de información, que podría reducir el ancho de banda de la red y los datos de uso del almacenamiento del software SIEM.

El papel fundamental que juega un SIEM en la seguridad informática de una compañía es vital, posteriormente, se explica la importación de un SIEM como una medida preventiva y de contención al momento de un ataque informático.

Taxonomía de un ataque: Se expondrá un ejemplo para una mejor comprensión del papel de un SIEM en la infraestructura de seguridad de una industria donde se explicará un ataque informático con y sin un SIEM.

a) Ataque sin un SIEM

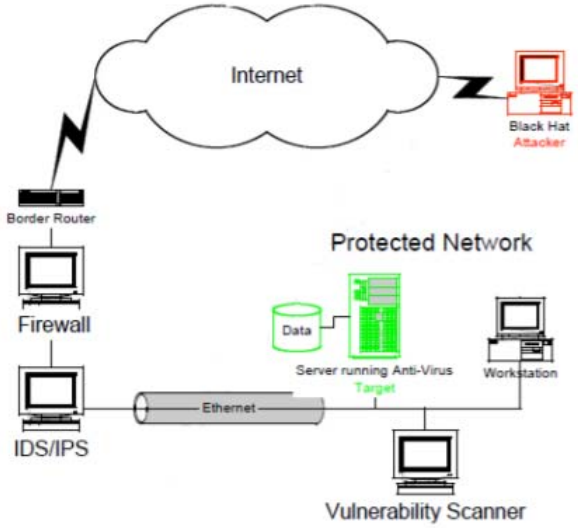

Figura 5. Ataque sin un SIEM

En la figura 6 se observa el diagrama de un ataque sin un SIEM, y se detallara a continuación las fases que conlleva el ataque.

Fase de descubrimiento

a) El atacante escanea el firewall utilizando herramientas como NMAP, HPING, Firewalker (herramienta para escaneo intrusivo de firewalls), para determinar qué dirección IP responde. Y a su vez sabes cuantos puertos

estarán abiertos y así de una forma sigilosa ingresar a la red, y evitando ser detectado por sistemas de detección/prevención de intrusos.

b) Utilizando técnicas de fingerprinting contra blancos encontrados, para determinar que sistemas operativos se encuentran en los hosts descubiertos, descubriendo cuales aplicaciones estarán ejecutándose en los hosts.

Envió de ataques con evasión de IDS

En esta fase se envían ataques de vulnerabilidades conocidas, tales como buffer overflow, paquetes fragmentados (fragroute, nemesis) con patrones de evasión de firmas (admutate, metasploit).

Comprometimiento del sistema

En la última fase ya han sido alcanzados los sistemas de información ocasionando lo siguiente:

- Caídas del sistema
- Denegaciones de servicio
- Robo de datos
- Instalación de sniffers
- Instalación de backdoors o rootkits

Ataque con un SIEM

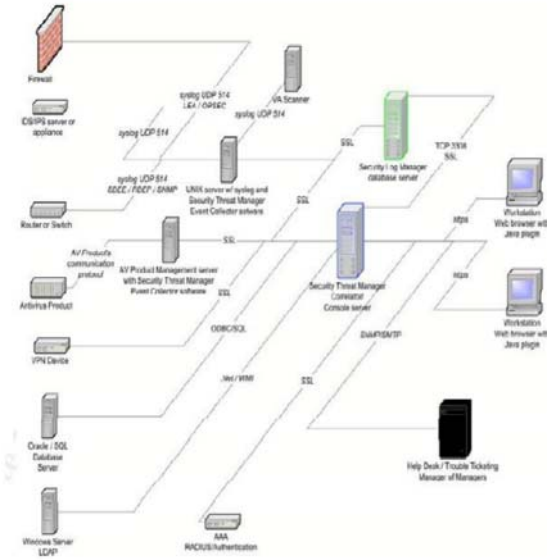

Figura 6. Ataque con un SIEM

En la figura 6 se observa el diagrama de un ataque con un SIEM, y a continuación se describirán las fases que conlleva el ataque generado.

Fase de descubrimiento

El enrutador o cortafuegos envían eventos al SIEM, mostrando que se está ejecutando un escaneo de puertos y generando una alerta menor o de advertencia.

FingerPrinting

EL IDS/IPS reporta escaneo de sistemas y otras coincidencias de firmas, la alerta es elevada a un nivel alto, el equipo de seguridad es notificado (correo electrónico, sms, etc)

Envió de ataques con evasión

El Firewall reporta paquetes que han sido fragmentados, el IDS puede reportar ciertas firmas y el nivel de alerta se eleva, si el IDS conoce el evento y alescanearlas vulnerabilidades sabe que el evento puede complicar el sistema, la alerta es escalada a nivel crítico. El equipo de seguridad es notificado de una alta probabilidad de amenaza y se generan las respuestas automáticas tales como (reglas de control de acceso en el cortafuego, apagado de sistemas, etc)

Comprometimiento del sistema

Bajo el peor escenario posible, la descarga del exploit será detectada por el IDS/IPS y el software de antivirus. El equipo de seguridad es notificado de un evento crítico y las respuestas automáticas son tomadas (reglas de control de acceso, apagado del sistema, etc).

Incluso si los eventos individuales son conseguidos con éxito en pasar por el cortafuego, evadir el IDS y software de antivirus, el número total de paquetes en cuestión debería de generar una mayor amenaza.

En vez de haber pasado exitosamente, cada dispositivo está reportando en los eventos no satisfactorios y alcanzados el nivel de amenaza de una alerta con una posición defensiva y respuestas de un equipo de seguridad alertado.

A. Soluciones

Cuando se aplican las soluciones SIEM estás ofrecen inteligencia de amenazas, perfiles de comportamiento y análisis para ayudar a detectar ataques y defenderse contra malware y ransomware.

Las entidades que se involucran con este sistema buscan soluciones SIEM que incluyan soporte para el monitoreo de actividades, monitoreo de actividad de aplicaciones, funciones de respuesta a incidentes y escalabilidad.

Las soluciones generales de SIEM deberían contener lo descrito a continuación:

- Soporte para la recopilación y el análisis en tiempo real de eventos de sistemas host, dispositivos de seguridad y dispositivos de red, combinado con información contextual para amenazas, usuarios, activos y datos.
- Proporcionar almacenamiento y análisis de datos de contexto y eventos a largo plazo.
- Proporcionar funciones predefinidas que se pueden personalizar ligeramente para satisfacer los requisitos específicos de la empresa.

Aplicando soluciones SIEM, recopilan cantidades masivas de datos de seguridad y registro, lo que representa que solicitan mucha demanda espacio de almacenamiento, así como la capacidad de volver fácilmente y buscar datos. Los sistemas deben ser escalables para satisfacer las necesidades de las organizaciones de diferentes tamaños y los eventos que sostienen.

La implementación de una solución SIEM requiere que un miembro del personal de TI dedicado exclusivamente a la supervise y administre exclusivamente. Dependiendo del tamaño de una organización, puede ser necesario más de un miembro del personal. Sin embargo, las organizaciones tienen la opción de subcontratar su mantenimiento de SIEM a contratistas externos para minimizar los costos.

También cuando se aplican las soluciones SIEM proporcionan a los empleados de seguridad de TI una mirada consolidada y general a los eventos de seguridad de una organización, lo que puede evitar infracciones de HIPAA y mantener seguros los datos de salud. Si bien este tipo de monitoreo es invaluable para los datos de atención médica,

las organizaciones deben considerar lo que pueden gastar y cómo implementar mejor a su personal para aprovechar al máximo una solución SIEM(González-Granadillo et al., 2021)

Beneficios de un SIEM

Los beneficios que contiene el tener el sistema SIEM implementado se detallan a continuación:

* *Mayor valor de la inversión en seguridad de la tecnología:* SIEM gestiona un uso más eficaz del registro de seguridad e información de eventos, lo que otorga al equipo de seguridad darse cuenta de todo el potencial de los sistemas de seguridad.

* *Reportes eficientes:* Desarrollo y entrega de informes completos y eficientes a la gerencia de TI.

Mediante el soporte a una amplia gama de sistemas y facilitar la mayor parte del proceso de recopilación y notificación de registro a través de herramientas automatizadas y plantillas de informes, una solución SIEM, puede reducir una tarea que antes llevaba días a una cuestión de horas, liberando al administrador de seguridad para centrarse mejor en prioridades y responsabilidades.

* *Reducción de capital y costos operacionales:* Herramientas convergentes tales como SEM, SIM, sistemas de análisis y administración de logs y sistemas de monitoreo de actividad en bases de datos, todo englobado en una misma solución, otorgando a la compañía ahorrar en tiempo y dinero. Los costos de compra y mantenimiento asociados con muchos sistemas de monitoreo y análisis pueden ser reducidos teniendo una única solución SIEM.

* *Reducción del riesgo de incumplimiento de los sistemas:* SIEM proporcionara a la empresa informes detallados. Durante una auditoría o investigación, la empresa tendrá la información necesaria para demostrar el cumplimiento o la debida diligencia.

* *Amplio apoyo de la organización para obtener información*: Un sistema de seguridad SIEM eficaz implica una amplia base de actores que deben trabajar juntos, con frecuencia en equipos multi-funcionales, para evaluar los eventos, crear informes y tomar acciones para abordar los incidentes señalados por el sistema SIEM.

* *Detección temprana de incidentes de seguridad:* una adecuada solución SIEM proporciona a los analistas de seguridad con un conjunto de herramientas que pueden mejorar en gran medida su eficacia. Un equipo de seguridad más eficaz tiene una mayor probabilidad de interceptar y abordar los eventos de seguridad en sus primeras etapas antes de que puedan afectar significativamente a la empresa.

Sistemas SIEM más populares

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

Para tener conocimientos acerca de los sistemas SIEM más populares nos basaremos en el Cuadrante Mágico de Gatner para los sistemas SIEM, publicado en junio de 2021.

En el cuadrante se puede observar que los sistemas SIEM líderes son Exabeam, QRadar (IBM), SecurOnix, Splunk, Rapid7, LogRhythm.

A continuación, se muestra una breve explicación de los sistemas SIEM líderes en el mercado.

Figura 7. Cuadrante Mágico de Gartner de Sistemas SIEM.

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

Ventajas

El SIEM con el añadido (UBA) presenta un magnífico motor de búsqueda. Podría ser el mejor junto con LogRhythm.

Es un producto apreciado por los clientes.

Gran parque de empresas asociadas que facilita la implementación en las organizaciones.

Puede convivir con otros sistemas, utilizando otros casos de uso, facilitando el camino para los equipos de seguridad que buscan agregar una solución SIEM a su entorno donde la infraestructura central y las fuentes de registro deeventos ya están en funcionamiento.

Desventajas

Elevado precio de licenciamiento.

Splunk no ofrece una versión Appliance, se debe instalar sobre hardware soportado.

QRadar

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

Ventajas

Se adapta a medianas y grandes organizaciones.

Arquitectura flexible que soporta varios entornos. Solución disponible como física o virtual, centralizada o distribuida, también puede ser "oncloud" o cogestionada con partners de IBM QRadar.

Posibilidad de conectar al SIEM seguridad de terceros.

Buen sistema de monitorización en tiempo real e históricos.

Desventajas

No integra monitorización de clientes finales (SO) (endpoints), necesita plugins de terceros.

Buen motor de búsqueda, aunque competidores como Splunk y LogRhythm lo mejoran.

La herramienta de respuesta a incidentes (IBM Resilient) no es nativa y debe conectarse a través de la herramienta de conexión de terceros.

El licenciamiento es confuso y complejo.

Exabeam

Exabeam es un sistema SIEM que ayuda a las operaciones de seguridad y los equipos de amenazas internas a trabajar de manera más inteligente, lo que les permite detectar, investigar y responder a los ciberataques en un 51 por ciento menos de tiempo. Con la plataforma modular de administración de seguridad Exabeam, los analistas pueden usar análisis de comportamiento para detectar ataques, automatizar la investigación y la respuesta a incidentes, y reducir los costos de almacenamiento.

Ventajas

Consta de una arquitectura escalable basada en Elasticsearch yHadoop (HDFS), además usan Kafka y Spark.

A nivel de licencia existe un modelo de fácil entendimiento basado en usuarios y entidades.

Funciones de orquestación y respuesta incluyéndose playbooks automáticos para la respuesta ante los incidentes.

Proporciona acceso a los datos y al flujo detrabajo de forma granular (predefinidos y personalizables)relacionados con laprivacidad.

Capacidades de Advanced Analytics, posee una UEBA muy madurodado que esta fue el origen de su producto antes de entrar en el mercado de los SIEM.

Sus clientes destacan de este producto sus altas capacidades encuanto al servicio de implementación y soporte.

Desventajas

Es un sistema relativamente caro y solo cuenta con pruebas gratis.

Algunos clientes han indicado que la funcionalidad de respuesta ante incidentes no está tanavanzada en comparación con otros productos del sector.

Se ha reportado algún problema referente a respuestas lentas del administrador técnico de lacuenta junto a otros problemas de soporte que han dificultado el crecimiento de la solución SIEM.

Basado en big data, SecuronixNext-Generation SIEM combina la administración de registros, el análisis de comportamiento de usuarios y entidades (UEBA) y la respuesta a incidentes de seguridad en una plataforma de operaciones de seguridad completa y de extremo a extremo. Recopila grandes volúmenes de datos en tiempo real, utiliza algoritmos de aprendizaje automático patentados para detectar amenazas avanzadas y proporciona capacidades de respuesta a incidentes de seguridad basadas en inteligencia artificial para una rápida reparación

Rapid7

Rapid7 es líder en la detección de amenazas. Sus soluciones analíticas recogen, contextualizan y analizan los datos de seguridad que necesita para luchar contra un adversario cada vez más engañoso y potente. A diferencia de la evaluación de la vulnerabilidad tradicional o la gestión de incidentes, Rapid7 ofrece información sobre el estado de seguridad de los activos y de los usuarios a través de redes virtuales en la nube, móviles, privadas y públicas. Rapid7 ayuda a mejorar la gestión de riesgos, simplificar el cumplimiento y detener las amenazas más rápidamente cuando se produce un compromiso

LogRhythm

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

Ventajas

Es una plataforma sólida y escalable desde un solodispositivo hasta arquitecturas de n niveles.

Poderosa interfaz de usuario que proporciona una sólida experiencia de monitorización en tiempo real.

Integra actividades de respuesta automática y manual frente a incidentes de seguridad.

Muy adecuado para entornos ICS/SCADA

Buen modelo de implementación y soporte a través

del servicio de implementación central.

Desventajas

Difícil integración con soluciones de terceros. APIsmenos abiertas a terceros que sus competidores.

Dificultad de escalado para soportar volúmenes de eventos muy altos.

Diferencias entre SIEM y otras tecnologías de seguridad.

Mientras que otras herramientas de seguridad brindan solo un servicio de seguridad, las capacidades de SIEM consolidan diferentes tecnologías de seguridad juntas. Las principales funciones de SIEM abarcan la detección de amenazas, la investigación y el tiempo de respuesta. Existen varias características adicionales, que incluyen:

- Monitoreo de seguridad básico
- Recolección de registros
- Normalización
- Almacenamiento y seguimiento de datos de registro
- Detección de incidentes de seguridad
- Detección avanzada de amenazas
- Análisis Forense y respuesta a incidencias
- Notificación y alertas
- Flujo de trabajo de respuesta a amenazas
- Paneles y visualizaciones de patrones de datos

I. Diferencia entre SIEM y una herramienta de gestión de registros

Las capacidades de una herramienta de gestión de registros son:

- Recopilación de datos de todos los sistemas operativos y aplicaciones dentro de una red
- Retención eficiente de grandes volúmenes de datos durante períodos de tiempo prolongados
- Filtrado y clasificación de registros de eventos, así como una función de búsqueda para localizar fácilmente la información requerida
- Informar sobre el estado operativo, de cumplimiento o de seguridad de la infraestructura de TI de una organización.

Un software de administración de registros (LMS) simplemente recopila registros y eventos para su almacenamiento, que es solo un aspecto de la funcionalidad SIEM. Si bien las herramientas LMS se diseñaron para ayudar a los analistas de sistemas a revisar los archivos de registro por razones que no son específicas de la seguridad, las herramientas SIEM se adaptan a las aplicaciones de ciberseguridad. Además, está completamente automatizado, mientras que un sistema de gestión de registros no lo está.

II. Diferencia entre un SIEM y un producto de administración de información de seguridad (SIM)

SIM y SIEM son dos conceptos que a menudo se utilizan indistintamente en el área de gestión de la seguridad por quienes no están familiarizados con estos productos. Aunque poseen similitudes, existen diferencias significativas entre sus capacidades. El software SIM se especializa en lo siguiente:

- Recopilación y almacenamiento de archivos de registro en un repositorio central
- Normalizar y limpiar registros para reducir la congestión del ancho de banda de la red
- Análisis e informes de los datos.
- Informes para el cumplimiento de estándares regulatorios de seguridad como HIPPA, PCI, VISA CISP, etc.

SIM se puede definir como una herramienta de gestión de registros creada para la seguridad. Esta herramienta es solo una parte de la tecnología SIEM. Otra diferencia importante es que la correlación de datos y eventos de SIM se basa en análisis anteriores, mientras que los procesos SIEM se llevan a cabo en tiempo real. Por lo tanto, prevenir una amenaza inminente solo sería posible con SIEM.

III. Diferencia entre SIEM y una herramienta de seguridad basada en host

Las herramientas de seguridad basadas en host se utilizan para detectar amenazas de seguridad contra una aplicación o sistema. Por lo general, se centran en el tráfico del servidor o de la tarjeta de interfaz de red (NIC). Sus capacidades básicas son:

- Recopilación y análisis de datos de tráfico
- Monitoreo basado en firmas para detectar firmas conocidas de ataques cibernéticos
- Monitoreo basado en anomalías para detectar comportamientos inusuales de la red y del usuario

Un sistema de detección de intrusiones basado en host (HIDS) es una de las tecnologías de seguridad más destacadas para detectar actividades maliciosas. Su arquitectura les permite solo detectar y reportar vulnerabilidades. Por otro lado, un SIEM irá más allá para tomar acciones preventivas contra el ciberataque. Mientras que un SIEM es una herramienta de seguridad activa, un HIDS es pasivo. SIEM también es más una aplicación basada en la red, ya que se enfoca en el tráfico entrante y saliente a través de dispositivos de red, firewalls, enrutadores, etc.

IV. Diferencia entre un SIEM y una herramienta de gestión de activos

Una herramienta de gestión de activos permite a las empresas rastrear todos los activos de TI como servidores, enrutadores, firewalls, impresoras, computadoras y otros dispositivos conectados en tiempo real. Una herramientade gestión de activos realiza lo siguiente:

- Almacena detalles y documentos para cada activo.
- Permite a los analistas detectar fácilmente todos los sistemas conectados a la red.
- Ayuda a priorizar los problemas del sistema.
- Proporciona una perspectiva a largo plazo de los costos de los activos.

Para las grandes organizaciones, monitorear miles de activos en una hoja de cálculo sería una molestia para los empleados. Con el software de gestión de activos, el trabajo se hace cien veces más fácil.

V. Diferencia entre un SIEM y el software de monitoreo y control de aplicaciones (AMC)

Este software, monitorea y controla la actividad de las aplicaciones en una red. El control de aplicaciones impide que las aplicaciones no autorizadas se ejecuten de formas que pongan en riesgo los datos. Por lo tanto, garantiza la privacidad y seguridad de los datos transmitidos entre sistemas.

Las capacidades del software AMC incluyen:

- Garantizar el procesamiento completo de registros de principio a fin
- Asegurarse de que solo se ingresen y procesen datos válidos
- Proporcionar un mecanismo de autenticación para sistemas de aplicaciones.
- Permitir el acceso autorizado solo a los usuarios comerciales aprobados
- Garantizar la integridad de los datos que ingresan al sistema de la aplicación.

A juzgar por el alcance de la cobertura, los productos AMC son útiles para reducir los riesgos de malware e intrusión de terceros no autorizados, ya que eliminan aplicaciones desconocidas y no deseadas en la red. Sin embargo, SIEM ofrece una solución de seguridad más completa. Reúne datos de distintas herramientas de seguridad e incluye datos de dispositivos de seguridad de red y aplicaciones de seguridad. También posee la inteligencia para contrarrestar ataques automáticamente. SIEM a menudo utiliza datos de productos AMC.

VI. Diferencia entre un SIEM y una herramienta de gestión de auditorías

Este tipo de software ayuda a las empresas a optimizar sus procesos de auditoría y cumplir con las políticas internas y los estándares regulatorios.

- Automatiza las tareas relacionadas con la auditoría para una documentación precisa y completa de los datos.
- Programa auditorías en diferentes departamentos simultáneamente.
- Implementa, analiza e informa los resultados de las auditorías.

- Permite modificaciones en tiempo real, incluso mientras se ejecuta un programa.
- Facilita el almacenamiento de los resultados de la auditoría para facilitar el acceso y la comparación.

El software también se puede utilizar para recopilar, almacenar y proporcionar datos sobre eventos de seguridad, en cuyo caso podría servir como un recurso para los procesos SIEM.

B. Futuro de SIEM

El Sistema SIEM continuará evolucionando a medida que el personal de TI de seguridad precise controlar servicios en la nube, dispositivos móviles, Internet de las cosas (IOT) y otras tecnologías que el departamento de TI no controla.IoT será un gran factor por el que deba evolucionar, ya que impulsa la cantidad de puntos finales vulnerables a los atacantes.

Cada vez es más difícil para los atacantes infiltrarse en las computadoras, pero sigue siendo bastante fácil piratear cámaras, refrigeradores, microondas, herramientas Bluetooth y otros dispositivos conectados y usarlos como vector de ataque.Los servicios en la nube y los dispositivos de IoT generarán rápidamente cantidades cada vez mayores de datos, y los sistemas SIEM tendrán que adaptarse aprendiendo a recopilar y organizar el flujo de información. El futuro de SIEM probablemente será una evolución, y no una revolución.

Conclusiones

Un SIEM es una herramienta muy eficiente y eficaz para lo que es la administración de la seguridad de la información de los datos de una institución o compañías de gran envergadura, ya que brinda un repositorio centralizado de logs y eventos que se consideran pueden ayudar a realizar monitoreo del estado de la seguridad de la información y de la trazabilidad de eventos de esta manera tendríamos todo registrado y sabremos el ingreso de los usuarios y así tener un control sobre la información que tenemos en nuestra base de datos, esto se lo realiza para proteger a la institución o empresa de esta manera información valiosa e importante no la posea cualquiera y así no ocasione ni daños ni perjuicios a la institución o empresa . Sin duda alguna este sistema nos brinda un sin número de beneficios, pero podemos resaltar los siguientes: Los beneficios que entrega un SIEM es la centralización de la gestión de la seguridad de la información y el único punto de monitoreo por parte de los analistas de seguridad, además brinda al oficial de seguridad un panorama completo del estado de la seguridad de la información en la compañía. De esta manera tendremos a la institución o empresa asegurada a los distintos ataques cibernéticos que las empresas y grandes instituciones están sometidas, por gente maliciosa que solo busca dañar el prestigio e interrumpir en la privacidad de los usuarios de la institución, que se encuentren registrados en nuestro sistema de base de datos.

Conflictos de intereses

Los autores no poseen conflicto de intereses.

Contribución de los autores

1. Conceptualización: Jenny Arizaga Gamboa, Eduardo Alvarado Unamuno, Jorge Chicala Arroyave.
2. Curación de datos: Eduardo Alvarado Unamuno.
3. Adquisición de fondos: Jenny Arizaga Gamboa, Eduardo Alvarado Unamuno.
4. Investigación: Jenny Arizaga Gamboa, Eduardo Alvarado Unamuno.
5. Metodología: Eduardo Alvarado Unamuno, Jorge Chicala Arroyave.
6. Software: Eduardo Alvarado Unamuno, Jorge Chicala Arroyave.
7. Supervisión: Jenny Arizaga Gamboa, Eduardo Alvarado Unamuno
8. Validación: Eduardo Alvarado Unamuno, Jorge Chicala Arroyave.
9. Visualización: Jenny Arizaga Gamboa, Eduardo Alvarado Unamuno
10. Redacción – borrador original: Jenny Arizaga Gamboa, Eduardo Alvarado Unamuno, Jorge Chicala Arroyave.
11. Redacción – revisión y edición: Jenny Arizaga Gamboa, Eduardo Alvarado Unamuno, Jorge Chicala Arroyave.

Financiamiento

La investigación ha sido financiada por los autores.

Referencias

Arias Bernal, L. E., & Cogollo Bustamante, J. (2013). *Procedimiento para la implementación de una herramienta SIEM en empresas que cuenten con un sistema de gestión de seguridad de la información* Universidad Piloto de Colombia]. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2586/Trabajo%20de%20grado.pdf?sequence=1

Cabrera Jurado, R. C., & Agüero Herrera, L. C. (2015). Planificación de un SIEM para la red de la UACJ y desarrollo virtual de un IDS. *Licenciatura en Ingeniería en Sistemas Computacionales*.

de Oliveira, E. D. F. (2020). Aprofundamento do estudo e desenvolvimento do módulo de vigilância de interações medicamentosas do Sistema de Informações Estratégicas Municipais SisVIM-SIEM. *Anais dos Seminários de Iniciação Científica*(24). http://periodicos.uefs.br/index.php/semic/article/download/7045/5676

ESPAÑOLA, V., & REORGANIZACIÓN, L. Una innovación importante es la creación de las Comisiones Delegadas del Gobier-no, que no existían anteriormente. La medida está justificada por la acumulación siem-pre reciente de los problemas que la Administración Central del Estado debe resolver. https://revistasonline.inap.es/index.php/DA/article/download/992/1047

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (siem): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759. https://www.mdpi.com/1424-8220/21/14/4759/pdf

Li, R., Smolyakova, A., Maayan, G., & Rimer, J. D. (2017). Designed peptoids as tunable modifiers of zeolite crystallization. *Chemistry of Materials*, *29*(21), 9536-9546. https://gmaayanlab.net.technion.ac.il/files/2012/06/Alisa-CM-1.pdf

Neu, C. V., Trebien, E., Bertoglio, D. D., Lunardi, R. C., & Zorzo, A. F. (2020). Gerenciamento de incidentes em SIEM seguindo ITIL. *Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação*, *3*(1). https://revistas.setrem.com.br/index.php/reabtic/article/download/372/168

Perurena, R. M., García, W. B., & Rubier, J. P. (2013). Gestión automatizada e integrada de controles de seguridad informática. *Revista Ingeniería Electrónica, Automática y Comunicaciones ISSN: 1815-5928*, *34*(1), 40-58. https://rielac.cujae.edu.cu/index.php/rieac/article/download/152/pdf

Robalino Díaz, J. W. (2018). *Propuesta Metodológica y Simulación de la Implementación de un SIEM basado en la Norma ISO 27001 y/o 27002* Quito, 2018.]. http://bibdigital.epn.edu.ec/bitstream/15000/19672/1/CD-9078.pdf

ROSAS, L. F., CABRERA, A. G. L., & GALICIA, L. G. T. (2018). ANÁLISIS DE LA POLÍTICA DEL SERVICIO DE COBRO EN UNA PYME USANDO SIMULACIÓN CON SIMIO®. *MERCADOTECNIA EN LAS PYMES CASOS Y APLICACIONES*, 226. https://www.academia.edu/download/61399220/Mercadotecnia-11-120191202-60547-1tpl4dh.pdf#page=230

Vazão, A., Santos, L., Piedade, M. B., & Rabadão, C. (2019). SIEM Open Source Solutions: A Comparative Study. 2019 14th Iberian Conference on Information Systems and Technologies (CISTI),