Revista de
Tecnología e Innovación
en Educación Superior

SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM)

https://doi.org/10.22201dgtic.26832968e.2019.2.3

Manuel Ignacio Quintero Martínez
Sergio Anduin Tovar Balderas

https://www.ties.unam.mx/

Fecha de recepción: 2 de septiembre de 2019 • Fecha de publicación: octubre de 2019 Octubre de 2019 | número de revista 2 • ISSN 2683-2968

Acervos Digitales, Dirección General de Cómputo y de Tecnologías de Información y Comunicación, UNAM
Esta obra está bajo licencia de Creative Commons
Atribución-No Comercial 4.0 Internacional (CC BY-NC 4.0)

Manuel Ignacio Quintero Martínez
Sergio Anduin Tovar Balderas
https://doi.org/10.22201/dgtic.26832968e.2019.2.3
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM)

Resumen

Hoy en día, la evolución de las amenazas que existen hacia una red (en términos de seguridad de la información), han hecho que su detección se vuelva más compleja, por lo que se requiere de sistemas especializados en monitorización que ayuden a detectarlas, no sólo desde los dispositivos a los que afectan, sino a otros que pueden dar información complementaria. Un Sistema de Gestión de Información y Eventos de Seguridad (SIEM, por sus siglas en inglés) permite la integración de información a partir de eventos reportados por diversos dispositivos, correlacionando los mismos para emitir alertas y reportes que permitan tomar acciones que ayuden a proteger la confidencialidad, integridad y disponibilidad de la información en la organización. En este artículo se presentan las generalidades, conceptos y requerimientos a tomar en cuenta para la implementación de un SIEM.

Palabras clave:

Seguridad de la información, correlación, eventos de seguridad, SIEM.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Abstract

Currently, detection of information security threats in any network has been complexed, and requires specialized monitoring systems to detect them, not only from the devices of interest, also from devices that can give complimentary information. A Security Information an Event Management (SIEM) integrates information from reported events from different devices, correlating them to create alerts and reports, which can be used to take some actions to support organizational information' Confidentiality, Availability and Integrity. This paper presents some general information, concepts and requirements to be considered into a SIEM implementation.

Keywords:

Information security, correlation, security events, SIEM.

Esta obra está bajo licencia de Creative Commons
Atribución-No Comercial 4.0 Internacional (CC BY-NC 4.0)

TiES Revista de Tecnología e Innovación en Educación Superior

Sistemas de Gestión de Información y Eventos de Seguridad (SIEM)
Manuel Ignacio Quintero Martínez
Sergio Anduin Tovar Balderas
https://doi.org/10.22201/dgtic.26832968e.2019.2.3
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM)

Introducción

Actualmente, la infraestructura tecnológica de cualquier organización, independientemente de su tamaño, se encuentra expuesta a múltiples amenazas a su seguridad. Estas evolucionan de forma acelerada y constante, rediseñándose para no ser detectadas, por lo que muchas técnicas de evasión suelen lograr su cometido cuando se monitorea lo que sucede en cada punto de la red organizacional individualmente. Pero ¿qué sucede cuando estas amenazas dejan evidencias que son trazables en su paso por una red, incluso antes de alcanzar su objetivo, generando alertas que permitan a los administradores tomar acciones preventivas o correctivas? Este es justamente el propósito de los sistemas de gestión de información y eventos de seguridad (SIEM, *Security Information and Event Management*, por sus siglas en inglés), los cuales buscan obtener la mayor cantidad de información útil posible para ayudar al monitoreo desde diversos frentes en una infraestructura.

Un SIEM permite recopilar y correlacionar eventos e incidentes de diversas fuentes (como servidores, dispositivos de red, dispositivos de seguridad perimetral, entre otros) para poder realizar predicciones a través de la identificación de una secuencia de acciones elementales que permitan reconocer alguna estrategia de ataque [1], para así prevenir o reaccionar rápidamente ante la materialización de una amenaza de seguridad [2], ayudando a reducir las intrusiones de seguridad en la infraestructura de 76% de las organizaciones encuestadas por CyberSecurity Insiders [3].

Origen y uso de la información en una infraestructura tecnológica

regularmente los Administradores de una Red conocen el diseño y funcionamiento de esta; la información sobre el desempeño y qué sucede dentro de la misma, podría permitirles reaccionar ante una posible falla o intrusión de seguridad por lo que, deberían de conocerse en el menor tiempo posible algunos aspectos como:

- Cuántos dispositivos importantes existen en la red y cuáles deberían ser monitorizados.
- Cuánto se sabe acerca de lo que sucede en cada uno de esos dispositivos.
- De las alertas que puede generar un dispositivo, cuántas son realmente monitoreadas por el personal a cargo.
- Cuánta información generada puede ayudar a mejorar la seguridad.

Responder a estos aspectos resultaría un serio inconveniente para cualquier administrador de red con tantos servicios, conexiones, usuarios, clientes, etc. Podría parecer imposible conocer lo que sucede en ellos, incluso, ¿qué sucede si esa información ya es recopilada

Esta obra está bajo licencia de Creative Commons
Atribución-No Comercial 4.0 Internacional (CC BY-NC 4.0)

Manuel Ignacio Quintero Martínez
Sergio Anduin Tovar Balderas
https://doi.org/10.22201/dgtic.26832968e.2019.2.3
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

Figura 1.
G. Altmann, "Protección a la información en línea," 2016. [Fotografía]. Disponible en: https://pixabay.com/es/illustrations/binaria-castillo-protecci%C3%B3n-1538721/ [Consultado en septiembre 18, 2019].

de forma central en un repositorio y se generan alarmas sólo cuando se cumple con un parámetro establecido? Es por ello que se vuelve poco viable pensar que esta implementación podrá informar sobre cualquier incidente de seguridad, ya que las amenazas actuales son capaces de evadir las formas de detección más comunes y conocidas.

Esto enfrenta a los administradores a las siguientes complicaciones:

- La información obtenida podría ser insuficiente por sí misma para detectar la mayor cantidad de incidentes de seguridad.
- La información aislada puede no ser óptima e incompleta para un dispositivo en específico o incluso, manipulada por un adversario.

Estos dilemas se vuelven cada vez más complejos y conforme se han desarrollado diversas formas de afrontarlos, la manera más efectiva de hacerlo es a través de la automatización (*operación, monitorización y revisión*) del seguimiento de eventos de seguridad en la infraestructura tecnológica, siendo los SIEM, los que han mostrado mejores resultados [2].

Funciones de un SIEM

l os siem integr An l As c ApAcid Ades de dos sistem As preced entes:

Algunas de las aplicaciones de la IA son: [2], [4], [5].

- Sistema de Gestión de Información de Seguridad (SIM, *Security Information Management*, por sus siglas en inglés), encargado de la recolección de eventos de seguridad para realizar trazas y reportes sobre estos.
- Sistema de Gestión de Eventos de Seguridad (SEM, *Security Event Management*, por sus siglas en inglés), encargado de la monitorización de los eventos en tiempo real, así como la gestión de incidentes derivados de estos aunque permitiendo la respuesta sólo de aquellos eventos con patrones preestablecidos[4].

Los SIEM integran las capacidades de los SIM y SEM, siguiendo el principio básico en donde la información que puede considerarse relevante para una infraestructura no procede de una sino de múltiples fuentes y esta

Esta obra está bajo licencia de Creative Commons
Atribución-No Comercial 4.0 Internacional (CC BY-NC 4.0)

Manuel Ignacio Quintero Martínez
Sergio Anduin Tovar Balderas
https://doi.org/10.22201/dgtic.26832968e.2019.2.3
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

información puede concentrarse y correlacionarse para encontrar patrones más robustos que permitan detectar posibles problemas de seguridad en tiempo real, o al menos en periodos muy cortos [2], pudiendo variar en su mayoría entre minutos y segundos [3]. Estos sistemas son utilizados actualmente en todos tipos y tamaños de organizaciones y existen en general, tres opciones que permiten implementar un SIEM para monitorizar una red. En términos generales son:

- Versiones propietarias en sitio o administradas por un tercero en la nube.
- Versiones gratuitas con restricciones sobre el uso.
- Productos de distribución libre.

Por otro lado, algunos de los SIEM que existen actualmente en el mercado son los siguientes (se menciona su sitio web y tipo de licenciamiento):

- Solarwinds https://www.solarwinds.com/, Licencia comercial.
- Splunk Enterprise Security https://www.splunk.com, Licencia comercial y versión gratuita con restricciones.
- LogRhythm NextGen SIEM https://logrhythm.com, Licencia comercial y versión gratuita con restricciones.
- IBM Qradar https://www.ibm.com/security/security-intelligence/qradar, Licencia comercial.
- Alienvault Unified Security Management https://www.alienvault.com/products, Licencia comercial.
- Alienvault OSSIM https://www.alienvault.com/products/ossim, Licencia libre, con restricciones de uso.

Es importante tomar en cuenta que un SIEM (como muchas otras herramientas de monitoreo), requieren una etapa de aprendizaje; es decir, en un principio comenzarán a recopilar datos de sus diferentes fuentes para poder reconocer lo que deberán tratar como un comportamiento normal de los equipos que monitorea y posteriormente comenzar a emitir alertas de patrones que podría considerar anómalos.

Desarrollo
Implementación de un SIEM

un dispositiv o gener A bit ácor As en su propio fo r-mAt o y est As no son igu Ales entre fAbri c Antes , de tal manera que el trabajo más importante antes que el SIEM comience a correlacionar eventos, es poner estos en un formato común para finalmente operarlos como unidades básicas, tras las cuales todas tengan la misma estructura básica. Este proceso se llama *normalización* [5].

Los eventos pueden proceder de múltiples fuentes: Montesino, Perurena, Baluja y Porvén [6] mencionan que pueden recopilarse por cuatro medios principales:

- Recepción de una cadena de datos en formato *syslog*[1] proveniente de la fuente de datos.
- Aplicaciones agentes instaladas directamente en los dispositivos a monitorear.
- Invocación de la interfaz de línea de comandos de los sistemas monitoreados.
- Interfaces de programación de aplicaciones (API) provistas por los desarrolladores de los sistemas monitoreados.

El proceso de normalización puede ser realizado por el mismo SIEM pues muchas implementaciones ya cuentan con los protocolos adecuados para procesar los eventos de los sistemas operativos o dispositivos de red, más comúnmente usados desde un conector desarrollado por el mismo proveedor. Inclusive, estos conectores pueden ser creados por el usuario para ser adaptados a sistemas específicos que los administradores requieran para la monitorización de eventos o sistemas específicos.

Con las bitácoras normalizadas, el siguiente paso se centra en el almacenamiento de la información procedente de cada dispositivo, lo que se realiza generalmente en el mismo sistema o también fuera de este, pero no es una práctica común y ocurre regularmente por requerimientos específicos de la organización que lo implementa o de regulaciones a las que se encuentra sujeta.

Aunque comúnmente los SIEM ya cuentan con un registro de posibles comportamientos anómalos en una red o de amenazas bien conocidas, es importante que este sistema se adapte de forma específica a la infraestructura que monitorizará; además deberá tener un periodo de aprendizaje al que suele llamarse “modo monitor.” En este punto es importante entender que para todo proceso de aprendizaje se requiere de un refinamiento, regularmente tiene que ser realizado por personal que conoce el entorno en el que se encuentra el equipo y pueda determinar que alertas corresponden a falsos positivos.

1 Servicio de recopilación de eventos sin ser estandarizados o normalizados en un servidor local.

Esta obra está bajo licencia de Creative Commons
Atribución-No Comercial 4.0 Internacional (CC BY-NC 4.0)

Manuel Ignacio Quintero Martínez
Sergio Anduin Tovar Balderas
https://doi.org/10.22201/dgtic.26832968e.2019.2.3
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

Figura 2.
"Carpeta de Datos," [Fotografía]. Disponible en: https://www.piqsels.com/en/public-domain-photo-zbgvd [Consultado en septiembre 20, 2019].

Por ejemplo, si un equipo genera tráfico de escaneo para la búsqueda de puertos abiertos hacia una red externa, regularmente generará una alerta. Sin embargo, si dentro de la organización se realizan pruebas de penetración regulares como parte de los procesos de aseguramiento de la red, este comportamiento debería ser aceptable desde ciertos equipos o direcciones hacia otro grupo o segmento de red, así como en horarios preestablecidos para evitar falsos positivos.

Tras algún tiempo en este modo con los datos recopilados y afinados, el SIEM será capaz de reconocer el comportamiento regular de la red en la que se ha implementado[7], por lo que posteriormente (y no desde el inicio) podrá comenzar a generar alertas de actividades anómalas.

En este punto, el SIEM puede comenzar a correlacionar la información a partir de patrones conocidos y aún más importante, de otros aprendidos o en algunos casos, también heurísticos y emitir alertas por medio de correo electrónico o mensajes de texto, entre algunas opciones.

Mas allá de las alertas

Al contar con información generada de los activos importantes, un SIEM también puede ayudar a reconocer la vida general de los dispositivos que se encuentran dentro de una misma red. Para ello, es común que estos sistemas incluyan una interfaz gráfica que permita monitorear en tiempo real o de forma histórica el desempeño de algunas métricas establecidas de interés para los administradores por medio de la generación de reportes e incluso para la dirección de la organización, pudiendo en algunos casos, personalizar el tipo de panel o paneles al que cierto usuario puede acceder.

También es importante pensar que algunos estándares, como PCI DSS[2] o HIPAA[3], requieren ciertas métricas de monitoreo para los sistemas e infraestructura dentro

2 PCI DSS (*Payment Card Industry Data Security Standard*), es un estándar internacional de protección a datos tarjetas de pago. Más información en https://www.pcisecuritystandards.org
3 HIPAA (*Health Insurance Portability and Accountability Act*) es una legislación estadounidense que regula el resguardo de la información médica de pacientes, así como su privacidad y seguridad. Más información en https://www.hhs.gov/hipaa/index.html

Esta obra está bajo licencia de Creative Commons
Atribución-No Comercial 4.0 Internacional (CC BY-NC 4.0)

Manuel Ignacio Quintero Martínez
Sergio Anduin Tovar Balderas
https://doi.org/10.22201/dgtic.26832968e.2019.2.3
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

del alcance de cada uno. La mayor parte de los fabricantes de SIEM incluyen de forma predeterminada herramientas o complementos que permiten la implementación de estos controles dentro de sus sistemas.

Factibilidad de la implementación de un SIEM

sin dudA, es difícil estAblecer si estA fActibilidAd existe, yA que depende de cAdA orgAnizAción de forma individual, pero podríamos decir en general que contar con un SIEM brinda la posibilidad de poder contar con información en la mayor parte de los casos, de forma casi instantánea sobre lo que sucede en la red. Sin embargo, es importante establecer cuál será la intención de generar esta información; si no se cuenta o se planea tener una forma de responder a las alertas, a los eventos o la forma de generar y usar los reportes que los SIEM ofrecen, este sistema no ayudará a la mejora de la seguridad en la organización.

De hecho, la respuesta a las alertas deben darse tan rápida y eficientemente como sea posible. Como lo señala 451 Research [8], uno de los puntos clave para el éxito en la implementación de un sistema de correlación de eventos es la integración con flujos de trabajo automatizado, ayudando así a la mejora de la seguridad de la información.

Figura 3.
Pixabay, "Unidad de Control Computadora," 2018. [Fotografía]. Disponible en: https://www.pexels.com/photo/airport-business-cabinets-center-236093/ [Consultado en septiembre 18, 2019].

Eficiencia de un SIEM

como cuAlquier herrAmientA o técnicA, un siemno previene o evitAlAtotAlidAd de los problemAs de seguridad existentes, por lo que su efectividad se puede medir en términos de un porcentaje, el cual depende no sólo de la herramienta técnica utilizada, sino también de cómo se haya configurado la misma. La experiencia en la atención de incidentes del equipo que la ha puesto a punto y asumir que siempre existirán nuevas amenazas que no sean conocidas o detectables en la red. Por ejemplo, Morteza Zeinali [2] menciona que algunos sistemas eficientes pueden reportar eventos en algo muy cercano al tiempo real, con una eficiencia del 90% dentro de los 60 segundos desde que se generó el incidente de seguridad.

Sin embargo, un estudio de *Cybersecurity insiders*, mostró que 86% de las organizaciones que tienen un SIEM como parte de su estrategia de seguridad se encuentran satisfechos con su efectividad, mencionando que esta satisfacción se centra en tres elementos [3]:

- Detección y respuesta de incidentes más rápida.
- Mayor eficiencia en las operaciones de seguridad.
- Mejora de la visibilidad de amenazas.

A su vez, esta misma encuesta mostró los tipos de ataques que fueron eficientemente detectados:

- Acceso no autorizado (46%).
- Amenazas avanzadas persistentes / ataques dirigidos (42%).
- Ataques internos (maliciosos o por descuido 37%)

Por otro lado, en cuanto a la penetración de esta tecnología en instituciones superiores en México, la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) en su encuesta ANUIES-TIC 2018 [9] reporta que los SIEM sólo forman parte de mecanismos de protección de la infraestructura en 24% de ellas, y aunque aún es un porcentaje bajo en comparación con otros sectores, mostró un crecimiento del 17% del año anterior, lo que muestra que este tipo de tecnología ha comenzado a ser parte de la estrategia de seguridad.

Conclusión

unAfrAse común en segurid Ad de lA info rmAción, dice que no se trAtA de si hAbrá un problemA de seguridad (es casi un hecho de que éste ocurrirá en algún momento en cualquier organización), sino cómo se

Esta obra está bajo licencia de Creative Commons
Atribución-No Comercial 4.0 Internacional (CC BY-NC 4.0)

Manuel Ignacio Quintero Martínez
Sergio Anduin Tovar Balderas
https://doi.org/10.22201/dgtic.26832968e.2019.2.3
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

responderá cuando ocurra. Es aquí donde un SIEM puede cobrar relevancia para cualquier organización. Si se tiene una implementación exitosa, permitirá contar con información ágil y certera para la detección y resolución de incidentes.

El SIEM sin duda, requerirá de un proceso de planeación para su implementación, así como del aprendizaje y refinamiento que le permita identificar de forma puntual que comportamiento es normal para poder emitir alertas sobre conductas que salgan de este, lo cual puede requerir una inversión no sólo de recursos financieros, sino de tiempo y conocimientos previos de los administradores de la infraestructura tecnológica. Sin duda redituará en la detección, respuesta e inclusive la posible prevención de incidentes de seguridad.

Sin embargo, es importante pensar que este SIEM no puede ser pensado como un medio para eliminar problemas de seguridad, sino como el disparador para iniciar métodos que los solucionen, ya sea por algún otro proceso automatizado, la intervención de un administrador de los recursos, o incluso la intervención de un equipo de respuestas a incidentes, así como de otros relacionados a la mejora continua y optimización de los recursos tecnológicos.

Esta obra está bajo licencia de Creative Commons
Atribución-No Comercial 4.0 Internacional (CC BY-NC 4.0)

https://doi.org/10.22201/dgtic.26832968e.2019.2.3
Octubre 2019 • Número 2 • ISSN 2683-2968
https://www.ties.unam.mx/

BIBLIOGRAFÍA

[1] E. Anumol, "Use of machine learning algorithms with SIEM for attack prediction," *Intelligent Computing, Communication and Devices Springer*, 2015.

[2] S. M. Zeinali, "Analysis of security information and event management (SIEM) evasion and detection methods," Tesis de Maestría, Universidad Tecnológica de Tallinn, Estonia, 2014.

[3] Cybersecurity Insiders, "2019 SIEM Report," Cybersecurity Insiders, 2019.

[4] A. Sapegin, D. Jaeger, F. Cheng, et al., "Towards a system for complex analysis of security events in large-scale networks," *Computers and Security*, no. 67, pp. 16–34, 2017.

[5] S. Bhatt, P. Manadhata, y L. Zomlot, "The operational role of security information and event management systems," *IEEE Security and Privacy Magazine*, vol. no. 5, pp. 35–41, 2014.

[6] R. M. Perurena, W. B. García y J. P. Rubier, "Gestión automatizada e integrada de controles de seguridad informática," *Ingeniería Electrónica, Automática y Comunicaciones*, vol. 34, no.1, pp. 40-58, 2013.

[7] T. Liy, L. Yan, "SIEM Based on Big Data Analysis," *Cloud Computing and Security*, 167-175, ICCCS 2017

[8] 451 Research, "Security Analytics. Transforming Enterprise Security Strategy," 451 Research Advisory, Abril 2018.

[9] Asociación Nacional de Universidades e Instituciones de Educación Superior, "Estado actual de las tecnologías de la información y las comunicaciones en las instituciones de educación superior en México, Estudio 2018," ANUIES, 2018.

Cómo se cita:

M.I. Quintero Martínez y S.A. Tovar Balderas, "Sistemas de Gestión de Información y Eventos de Seguridad SIEM," *TIES, Revista de Tecnología e Innovación en Educación Superior*, n.o. 2, octubre, 2019. [En línea]. Disponible en: https://www.ties.unam.mx/ [Consultado en octubre, 2019].

Esta obra está bajo licencia de Creative Commons
Atribución-No Comercial 4.0 Internacional (CC BY-NC 4.0)