

## **Cómo seleccionar una solución SIM:**

Guía para evaluar soluciones  
para la gestión corporativa de  
la seguridad lógica

# top 10



## Importancia de las soluciones de gestión corporativa de la seguridad lógica (SIM)

- La gestión de información de seguridad (SIM) es la pieza clave de cualquier planteamiento serio en la gestión de la seguridad lógica. El creciente número de gusanos, virus, hackers e intrusos, hace que las empresas adopten las mejores infraestructuras de seguridad existentes en el mercado para protegerse. Pero al invertir grandes sumas de dinero en un amplio abanico de soluciones de seguridad como antivirus, firewalls y sistemas de detección de intrusiones, las empresas se han expuesto a un nuevo problema: una complejidad devastadora.
- Sin una gestión inteligente y centralizada y una correlación automatizada, muchas empresas han descubierto que sus infraestructuras de seguridad se han convertido en un complejo laberinto de sistemas dispares que generan un enorme flujo de datos pero que ofrecen poca visibilidad de los verdaderos ataques y amenazas. Aunque esta situación puede haber sido aceptable en el pasado, debido a las crecientes presiones reguladoras para el cumplimiento de normas y estándares y al panorama de amenazas en constante evolución, las empresas están implantando tecnologías SIM para gestionar los riesgos asociados a la información y proteger los activos IT críticos de forma centralizada.
- Sin embargo, al investigar el mercado SIM, los profesionales de la seguridad pueden encontrar que es difícil evitar los mensajes de marketing del proveedor y diferenciar de forma clara las distintas tecnologías. Esto no debería constituir una sorpresa, especialmente al no existir definiciones estándar de términos como “eventos por segundo”, “correlación de vulnerabilidad” y “criticidad de los activos”. Debido a ello algunos proveedores exageran cifras de rendimiento, haciéndolas en muchos casos imprecisas o engañosas. Como consecuencia, las empresas están descubriendo que los sistemas SIM que utilizan pueden no estar consiguiendo lo que originalmente prometían.
- ArcSight ha desarrollado la siguiente lista de buenas prácticas de evaluación para ayudar a las empresas a hacer la elección acertada de un sistema SIM considerando su entorno. Esta lista ha sido recopilada directamente a partir de las experiencias de clientes que han implementado soluciones SIM. Estas prácticas deberían usarse como una parte integral del proceso de evaluación y selección.

# 10

## En caso de duda, exija una prueba piloto

Los proveedores de SIM ofrecen con frecuencia una vertiginosa variedad de funcionalidades durante la preventa del producto que pueden sonar y parecer extraordinarias, pero la verdadera medida del rendimiento de una solución sólo se puede apreciar cuando se utiliza la herramienta con información en directo proveniente de la propia infraestructura de seguridad.

Una demostración en vivo ayuda a las empresas a evitar serios escollos que pueden surgir por confiar en demostraciones grabadas para determinar la efectividad de un producto. Como cliente, está en su derecho de pedir una prueba, normalmente algo que sólo lleva unos días, y que al final bien merece el esfuerzo extra.

# nueve

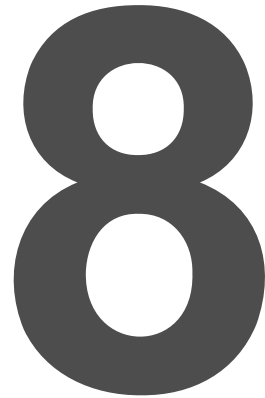
## Investigue la viabilidad del proveedor

El mercado SIM ha crecido significativamente durante los últimos tres años. Más allá de la viabilidad básica del fabricante, busque un proveedor que tenga tecnología desarrollada específicamente para el mercado SIM, experiencia demostrable y que pueda ocuparse de las cambiantes necesidades de la empresa.

Además, asegúrese de que el proveedor SIM tiene clientes en su mercado y que entiende sus necesidades específicas de negocio.

## Conozca la importancia de la independencia del proveedor

La independencia del proveedor es crucial para gestionar eficazmente y obtener beneficios de la mejor infraestructura del mercado y para evitar conflictos de intereses. Los proveedores de dispositivos de seguridad que también ofrecen productos SIM pueden no ser capaces de mantener la fluidez imprescindible en la relación con sus competidores ni de garantizar el soporte de nuevas versiones.



## Exija una solución SIM flexible y ágil

# 7

La seguridad consiste en anticiparse, así que la solución SIM que elija debe ser muy flexible con el fin de crecer con la empresa. Una razón universal para adquirir una solución SIM es vencer el problema de la sobrecarga de datos. Pero a medida que las empresas obtienen una visión consolidada de sus logs, comienzan a surgir posibilidades de alto nivel. Éstas incluyen la capacidad de personalizar múltiples áreas del producto, tales como las políticas de captura de datos, reglas de correlación y acciones asociadas, workflow, dashboards y monitores, herramientas de investigación e informes, para así conseguir la máxima eficacia. Por ejemplo, cuando se diseña una nueva política o aparece una nueva amenaza, las empresas podrán mantener el control reajustando el SIM hacia la identificación de violaciones de políticas o eventos relacionados con la nueva amenaza. Durante el piloto, trabaje con los proveedores para comprender mejor cómo personalizar cada recurso.

# 6

## Comprenda el valor EPS

Debido a la falta de estandarización en la terminología relacionada con las soluciones SIM, el tan discutido número de eventos por segundo (EPS) aporta muy poco para evaluar el verdadero rendimiento, efectividad y extensibilidad del producto. Estos números están basados a veces en una simple recopilación de logs en bruto, especialmente cuando las soluciones SIM ofrecen poca o ninguna inteligencia ni pre-procesamiento en los agentes y en los recolectores de eventos antes de que dichos eventos lleguen a la consola SIM. Una solución SIM corporativa verdaderamente eficaz será capaz de demostrar una capacidad de recolección y procesamiento de datos eficaz con tasas de rendimiento altamente escalables al nivel requerido por una infraestructura corporativa. Este rendimiento de nivel corporativo depende directamente de varios factores, entre los que se incluyen: tasa de eventos antes y tras el filtrado y agregación, extensión y uso de las capacidades analíticas, requerimientos de gestión de información histórica y en tiempo real: y la dimensión de la base de usuarios. Basándose en estos factores, la escalabilidad que capacita a una herramienta para la implantación a nivel corporativo no se condensa en un simple número EPS, sino que se deriva de un conjunto de factores basados en los requisitos operativos, entrada de datos y uso de la tecnología SIM.

# cinco

**Comprenda la diferencia entre un dispositivo hardware de seguridad y un sistema de gestión de seguridad corporativo.**

Los dispositivos hardware SIM han sido elogiadas por su facilidad de despliegue. Las soluciones software SIM destacan por sus funcionalidades orientadas a la gestión corporativa, incluyendo workflow, personalización y amplia capacidad de identificación de amenazas. Los requerimientos de facilidad de despliegue deberían estar equilibrados con el potencial de crecimiento de las funcionalidades que ofrece la herramienta, para obtener una solución que pueda crecer continuamente con su empresa.

# Conozca el significado de la correlación

Al igual que muchos términos relacionados con tecnologías SIM, la palabra correlación carece de un significado estándar. Las tecnologías SIM que afirman realizar correlación de activos, de vulnerabilidad y de eventos lo consiguen a través de diferentes metodologías y con diferentes grados de éxito. Las cuestiones a tener en cuenta incluyen:

## ¿Cómo realiza el producto la correlación cruzada entre dispositivos?

La correlación cruzada entre dispositivos es clave para obtener auténtico valor analítico de una solución SIM. Los productos que no ofrecen un lenguaje de categorización unificado para mapear eventos de distintos dispositivos en una taxonomía común no permiten una correlación eficiente en un entorno de dispositivos multifabricante. Sin un lenguaje de categorización, los usuarios deben recordar la categorización de cada evento en cada tipo de dispositivo, lo que lleva a la falta de eficiencia y a reglas de correlación extremadamente complejas.

## ¿Cómo determina la herramienta las prioridades?

Todos los productos SIM asignan las prioridades de forma diferente. Asegúrese de que se puede priorizar según la gravedad del ataque, la criticidad del activo y el estatus de vulnerabilidad del objetivo en relación con el ataque especificado. También es importante determinar si las prioridades son reajustables. Después de implementar un SIM, las empresas necesitarán reajustar las priorizaciones basándose en factores únicos tales como los falsos positivos conocidos y los ataques de alto riesgo.

## ¿Cómo procesa el producto la información sobre vulnerabilidades?

La mayoría de proveedores SIM afirman que soportan información sobre vulnerabilidades, pero el alcance, la profundidad y la aplicabilidad de integración pueden variar.

Los aspectos clave al determinar el valor de la integración incluyen la capacidad de incorporar automáticamente los activos con vulnerabilidades detectadas, la capacidad de tener en cuenta las vulnerabilidades en las reglas de correlación para la gestión de riesgos en tiempo real y la aplicación del estatus de vulnerabilidad del sistema en la asignación de prioridades a los eventos.

## ¿Cómo incorpora la herramienta el valor de los activos?

La incorporación del valor de los activos –las características técnicas y de negocio de un sistema, tales como Sarbanes-Oxley, misión crítica, confidencial- se realiza con varios grados de extensibilidad. Hay que determinar cómo la herramienta incorpora y valora las distintas categorías técnicas y de negocio de los activos en sus capacidades de correlación y priorización.

La extensibilidad es también importante a la hora de adecuar la capacidad analítica del producto a su organización. Pida al proveedor que cree una categoría personalizada de activos y que asocie acciones relevantes como respuesta a ataques contra ese activo.

## ¿Cómo rastrea y escala el producto los niveles de amenaza?

Con millones de eventos por día, la capacidad de un SIM de rastrear la actividad y escalar basada en los ataques sucesivos es clave para identificar las amenazas más peligrosas.

## ¿Puede el producto realizar la correlación en tiempo real y con datos históricos a la vez?

Mientras que muchas SIMs ofrecen la capacidad de correlar la información en tiempo real, también es importante correlar información histórica. Esto permite identificar fácilmente amenazas recientemente descubiertas que pueden haber ocurrido inadvertidamente en el pasado. Adicionalmente, las utilidades de correlación deberían permitirle comprobar la calidad de las reglas de correlación recientemente creadas con información histórica.

## ¿Puede el producto descubrir amenazas desconocidas?

Mientras que las reglas de correlación pueden encontrar amenazas conocidas, los clientes de herramientas SIM deberían solicitar técnicas analíticas adicionales que puedan analizar los datos entrantes y construir nuevas reglas para el descubrimiento automático de amenazas desconocidas.

## ¿Cómo gestiona el tiempo el producto en el proceso de correlación?

El tiempo es un aspecto importante para una correlación eficaz. Asegúrese de que el proveedor correla la información basándose en el momento en el que se generó el evento y que también ofrece la capacidad de correlar basada en la secuenciación temporal de los eventos. Esto asegurará que no se omita ningún ataque debido al tiempo de latencia y asimismo, permitirá que el SIM realice una identificación exacta de amenazas para los ataques lentos y en fases.

## ¿Cómo es de fácil alterar, reajustar y crear nuevas reglas?

Los equipos de seguridad corporativos valorarán extraordinariamente que la interfaz de una herramienta SIM permita el tuning personalizado e intuitivo y la creación de reglas de correlación. A la inversa, la falta de un sistema robusto de creación de reglas supone un obstáculo fundamental.

# tres

## **Observe cuidadosamente la relación de dispositivos soportados.**

Los usuarios de SIM se enfrentan normalmente a serias limitaciones como por ejemplo la necesidad de integrar datos de dispositivos no soportados por el proveedor SIM. Tenga cuidado con los proveedores que sólo soportan un número limitado de productos o aquellos cuya lista de productos esté “en desarrollo”. Éste es un signo inequívoco de que el proveedor no tiene una política ágil de soporte de nuevos agentes. Pida a los proveedores información acerca de sus procesos de desarrollo de agentes, el alcance de sus asociaciones con proveedores de productos soportados y la cantidad de productos y dispositivos soportados. Asimismo, evalúe las capacidades de desarrollo de agentes personalizados. Pregunte sobre los agentes personalizados que están siendo utilizados por clientes activos y el número de clientes que están desarrollando en la actualidad sus propios agentes con el kit de herramientas proporcionado. Además, confirme que las funcionalidades standard de agente están disponibles para los agentes desarrollados personalizados. Algunos proveedores sólo ofrecen simples parsers bajo la apariencia de entornos de desarrollo de agentes. Se ha demostrado que esta simplificación degrada gravemente la funcionalidad y el rendimiento de los agentes desarrollados de forma personalizada.

# dos

## Capture y normalice todos los datos de los eventos.

En pocas palabras, la normalización es el proceso de reorganización de las relaciones entre los datos para que sean más fáciles de almacenar y recuperar. Esto le permite utilizar sus datos para realizar una correlación de alto rendimiento en tiempo real y consultar dichos datos eficazmente a la hora de crear informes. La mayoría de productos SIM no capturan y normalizan toda la información relevante. De hecho, sólo le ofrecen los datos que más se han usado, tales como la IP de origen, la IP de destino y la descripción de tiempos y eventos. Los datos de los restantes eventos están truncados o dentro de una cadena de caracteres que no puede usarse eficazmente en una correlación. Éste es un serio problema dado que los datos no están disponibles para ser verificados ni para la gestión de amenazas en tiempo real, lo que limita enormemente el valor del SIM.

# Defina los requisitos operativos.

El valor de cualquier producto SIM está directamente relacionado con los datos que se introducen en el sistema, con la información que el sistema puede obtener de los datos y con las acciones que el sistema tiene programado realizar. Las checklists de control pueden ser útiles, pero deben estar adaptadas para reflejar los requisitos operativos de la empresa. Para depurar eficazmente las listas de control, primero deben determinarse los principales entornos de utilización del producto. Los entornos de utilización más comunes son, entre otros:

## Soporte 24X7 para el centro de operaciones de seguridad

Para asegurarse la priorización efectiva y la respuesta a incidentes, las operaciones de seguridad deben tener vigilancia 24X7, con flujo de trabajo definido. Los sistemas SIM para las necesidades de los SOC (Centro de operaciones de seguridad) deben ofrecer las mejores características de flexibilidad y personalización para asegurar que la organización puede cambiar el foco cuando sea necesario ocuparse de amenazas emergentes. Además, dado que los gastos de personal suponen una parte significativa del coste de mantenimiento de un SOC, el sistema que ofrezca la mayor precisión en la identificación de amenazas generará el mayor retorno de la inversión. Además, la capacidad de los sistemas de monitorizar continuamente y el rendimiento en la resolución de problemas son claves para mantener fluido el soporte 24 horas del SOC.

## Uso de la SIM como un "SOC virtual".

Esta opción es para empresas cuyos presupuestos no permiten la implementación de un centro de operaciones de seguridad 24X7 o para empresas que tienen un perfil de riesgo más tolerante. Estas empresas eligen usar los SIMs como un SOC virtual para ofrecer una identificación de amenazas precisa y alertar al personal de cualquier problema urgente. Los SOC virtuales tienen por lo general poco personal, lo que significa que sus soluciones SIM necesitan estar altamente personalizadas para evitar llamadas nocturnas debidas a falsas alarmas.

Como los SOC virtuales no son centros 24X7, las empresas necesitan un producto que ofrezca análisis en tiempo real para la identificación instantánea de amenazas en tiempo real además de capacidades de análisis histórico para la revisión de registros históricos en horario de oficina.

## Capacidades de auditoría y conformidad con estándares y normas.

La auditoría y conformidad requieren la integración de un gran conjunto diferente de orígenes de datos, tales como sistemas operativos, mainframes, bases de datos y aplicaciones de gestión de identidades. Asegúrese de que su proveedor ofrece la capacidad de crear agentes personalizados para que los dispositivos capturen eventos desde fuentes no tradicionales tales como aplicaciones propietarias que no están directamente soportadas. Mientras que algunos productos SIM ofrecen plantillas para realizar los informes de normalización o adaptación a estándares, es aún más importante que el producto clasifique los activos relevantes que deban ser auditados, y ofrezca una significativa capacidad de personalización y correlación para obtener la información relevante de acuerdo con la norma o estándar al que ha de adaptarse.

## Amenazas internas

Este entorno de utilización requiere que dispositivos internos monitoricen la actividad del usuario e identifiquen el uso sospechoso o no autorizado de información confidencial. Más que auditoría y conformidad con estándares, este escenario requiere un análisis amplio y profundo y la integración de fuentes de datos no tradicionales. Los requisitos clave de los SIM son la capacidad probada para integrar con aplicaciones, bases de datos, sistemas operativos, sistemas de gestión de identidad y sistemas físicos de seguridad que ayuden a perfilar la actividad de los usuarios de confianza, y la flexibilidad para establecer valores de referencia y analizar basándose en el comportamiento.



# Empiece

## Empiece hoy mismo

ArcSight ofrece soluciones corporativas de gestión de información de seguridad capaces de cubrir una amplia gama de necesidades, con una excelente relación coste-beneficio. Le invitamos a comparar directamente nuestro producto con cualquier otro del mercado. Nuestros ejecutivos de cuenta pueden ofrecerle información dirigida a sus criterios específicos, hacerle una demostración del producto y ofrecerle la posibilidad de realizar un piloto para probar a fondo nuestra solución. No es casualidad que las publicaciones líderes del mercado reconozcan en ArcSight ESM su superior flexibilidad, funcionalidad, escalabilidad superiores y su facilidad de uso. Si necesita ayuda para resolver las necesidades de gestión de seguridad de su empresa, contacte con nuestro agente en España en [info@breyer.es](mailto:info@breyer.es), [www.breyer.es](http://www.breyer.es) llame al 91 391 04 12 o visítenos online en [www.arcsight.com](http://www.arcsight.com)

# ahora

## Acerca de ArcSight

ArcSight, el líder reconocido en Gestión de seguridad empresarial (SIM), ofrece gestión de amenazas en tiempo real y conformidad con estándares mediante el análisis y correlación masiva de información de dispositivos de seguridad. Mediante la captura, análisis y gestión detallada de los datos de seguridad, ArcSight ESM™ permite a las empresas, entidades del gobierno y proveedores de servicios de seguridad gestionados explotar centralizadamente la información de riesgos de forma más eficaz. La lista de clientes de ArcSight cuenta con empresas internacionales líderes de todo el mundo y más de 20 del top 30 de Agencias Federales de EEUU.