



The Security Division of EMC

White paper

Verificación de seguridad: Siete Factores Que Se Deben Tener en Cuenta al Evaluar Soluciones de Proveedores para SIEM



El objetivo de una solución SIEM consiste en lograr que los empleados de seguridad sean más productivos.

Las soluciones de administración de eventos e información de seguridad (SIEM, *Security Information and Event Management*) se están convirtiendo en componentes obligatorios de la infraestructura de seguridad de una organización y desempeñan una función importante en la detección de amenazas, la respuesta ante incidentes, el análisis forense

y el cumplimiento relacionado con la seguridad. Basándose en la experiencia de más de 1.300 implementaciones SIEM exitosas en organizaciones de todos los tamaños, RSA ofrece a posibles compradores siete factores que se deben tener en cuenta cuando se evalúan ofertas de proveedores.

Más allá de qué abreviatura utilice (SIEM, SEM o SIM), la administración de eventos e información de seguridad constituye la prioridad de muchas organizaciones (si desea obtener una breve visión general, consulte “SIEM para Seguridad” en la página 2). Según Forrester Research¹, más de un tercio de las empresas habían planeado adoptar tecnología SIM a mediados del año 2008. La mejora de reporting y cumplimiento de normas es el principal motivo por el que los clientes deciden implementar esta solución (según el 32% de los usuarios de la encuesta que realizó Forrester a 259 de las personas encargadas de tomar decisiones de seguridad en empresas de Norteamérica y Europa). La identificación de incidentes de seguridad ocupó el segundo lugar (mencionada por un 20% de los participantes).

Dado que una solución SIEM se extiende a toda la empresa y afecta tantos elementos de la infraestructura, la elección de la solución de un proveedor constituye un compromiso a largo plazo con un alto impacto. El costo total de propiedad, las funcionalidades, las características y las tecnologías subyacentes de las soluciones varían ampliamente, lo que dificulta aun más la elección. De hecho, muchas organizaciones se arrepintieron de la solución que eligieron porque no se adaptaba a sus necesidades.

Cuando compara soluciones, no centre su atención exclusivamente en ciertas características, en la interfaz de usuario ni en las reglas de correlación de eventos. En su lugar, como proponemos en las siete recomendaciones que se incluyen a continuación, debe ampliar la evaluación para analizar integralmente cada oferta de proveedor, lo que incluye la integridad de los datos de eventos capturados y el grado de integración de la solución en sí y con la infraestructura correspondiente. Tenga en cuenta el grado de adaptación del producto con respecto a la implementación, la escalabilidad y el costo total de propiedad de la empresa. Además, evalúe las fortalezas del proveedor, entre ellas, experiencia en seguridad general, estabilidad financiera, soporte de investigación y desarrollo e independencia de plataformas y proveedores. Si cuenta con una solución que se adapta a sus necesidades en muchos de estos aspectos, puede aumentar considerablemente las posibilidades de éxito a largo plazo.

Recomendación N.º 1: Defina el Modelo Actual de Operaciones de Seguridad y Permita que se le Comuniquen los Requerimientos Inmediatos de la Solución

Las organizaciones cuentan con modelos de operaciones de seguridad sumamente diferentes y, cuando se evalúa una solución SIEM, es importante saber dónde entra usted en el proceso para poder elegir una solución que se adapte a sus necesidades (y presupuesto) actuales y brinde la flexibilidad para escalar y ampliar sus operaciones con el paso del tiempo.

En el nivel high-end, algunas organizaciones cuentan con una instalación SOC centralizada de grandes dimensiones, que emplea gran cantidad de analistas de seguridad, cada uno con un área específica de responsabilidad (por ejemplo, eventos de servidor). En una situación más general, un grupo pequeño de analistas, que generalmente desempeñan las principales funciones de TI u operaciones de red, comparten una gama de responsabilidades de operaciones de seguridad. El tercer modelo es un “SOC virtual”, cuyos miembros están distribuidos en diferentes zonas geográficas.

Independientemente del modelo que utilice, el objetivo de una solución SIEM no consiste en reemplazar personas por tecnología, sino lograr que sean más productivas y eficientes en su trabajo. La elección de una solución adecuada requiere un conocimiento de los procesos de flujo de trabajo y las responsabilidades actuales. ¿Cómo se dividen las responsabilidades y las tareas entre el personal? ¿Cómo se priorizan las alertas? ¿Necesita respuesta las 24 horas, durante toda la semana? ¿Qué ancho de banda de personal puede dedicar al análisis forense?

¹ “Big Changes Are Ahead For The SIM Marketplace” (Se Avecinan Grandes Cambios en el Mercado de SIM), Paul Stamp, Forrester Research, 27 de febrero de 2008



Sepa qué no funciona y por qué

También es importante comprender que las deficiencias en el entorno actual pueden limitar la eficacia de las personas. Por ejemplo:

- Si los empleados invierten demasiado tiempo en la evaluación de falsos positivos o alertas de prioridad baja, es posible que las reglas de correlación sean demasiado amplias o no tengan en cuenta otros datos, como activos y vulnerabilidades, lo que da como resultado alertas incorrectas.
- Si las investigaciones forenses son lentas y engorrosas o poco claras, es posible que esto se deba a que los datos de eventos históricos no se pueden recuperar de manera rápida y sencilla desde una única fuente confiable. O tal vez el sistema SIEM ni siquiera los ha capturado y por esto no se pueden recuperar.
- Si los eventos no se resuelven de manera oportuna, es posible que los procesos de flujo de trabajo sean inadecuados o estén fragmentados.

Por lo general, los problemas de este tipo se originan a partir de deficiencias básicas de la solución SIEM o del alto costo que debe invertir para lograr que la funcionalidad incorporada sea operativa en el entorno real.

Recomendación N.º 2: Tenga en Cuenta estos Elementos Críticos de la Solución para las Operaciones de Seguridad

Existen tres atributos básicos para enfrentar algunas de las fallas más comunes de SIEM con respecto al soporte de operaciones de seguridad: el análisis y la captura de datos en tiempo real, la captura de todos los datos de eventos operacionales y de seguridad, y las herramientas eficaces de análisis forense.

Adquisición y Análisis Sólidos

Una solución SIEM debería realizar correctamente dos funciones principales:

- Análisis y captura de datos del log de eventos en tiempo real para soportar detección y respuesta ante amenazas en tiempo real.
- Recuperación y reporting rápidos de datos capturados con anterioridad para poder desglosarlos y realizar análisis forenses, operaciones de red, cumplimiento de normas o descubrimiento legal.

El objetivo de una solución SIEM no consiste en reemplazar personas por tecnología, sino lograr que sean más productivas y eficientes en su trabajo.

La mayoría de las soluciones se pueden optimizar para hacer una de las dos cosas bien, pero no ambas, lo que obliga al proveedor a favorecer una de las dos características. En cambio, la plataforma RSA enVision® está especialmente diseñada para equilibrar estos requerimientos, con funcionalidades de consulta, análisis y recopilación integradas de manera sólida en una tecnología de base de datos orientada al objeto que garantiza la flexibilidad y el performance óptimo.

Acceso a Todos los Datos

La mayoría de las soluciones no analizan la actividad de eventos raw de adquisiciones, ya que esto disminuiría el performance a un nivel inaceptable. Por el contrario, al normalizar y procesar previamente los datos, se reducen a un subconjunto de excepciones que se analizan con posterioridad. Algunas soluciones eliminan los datos restantes, lo que impide su uso posterior en análisis forenses, auditorías o actividades de reporting. Otras soluciones conservan los datos de evento raw en un repositorio no integrado con funciones de reporting y solicitud. Esto puede dificultar considerablemente el análisis y reporting de datos históricos.

Asegúrese de que la solución que elija resuelva este problema mediante la recopilación y conservación de todos los datos de eventos entrantes para uso posterior. A medida que crea nuevas reglas de correlación para enfrentar nuevos requerimientos de auditoría, reporting o amenazas, esas reglas pueden actuar rápidamente en todos los datos pertinentes, lo que mejora la precisión de las alertas y permite volver a analizar eventos anteriores.

SIEM de Seguridad: Una Breve Visión General

A pesar de que las soluciones SIEM difieren considerablemente en cuanto a sus arquitecturas, funcionalidades y características, todas tienen el objetivo similar. Como menciona Gartner, “Los usuarios finales deben considerar los datos de eventos de seguridad en tiempo real (para administración de amenazas, principalmente orientada a eventos de red) y analizar y realizar reporting de los datos de logs (para el monitoreo del cumplimiento de políticas de seguridad, principalmente orientado a eventos de aplicaciones y hosts)”.²

Las soluciones SIEM automatizan y optimizan el proceso de recopilación de datos de log/eventos (lo que incluye datos de seguridad, entre otras opciones) de diversas fuentes en toda la red. Mediante el uso de técnicas de correlación de eventos e incorporación de datos, estos productos analizan los datos para identificar amenazas de seguridad conocidas y reconocer comportamientos irregulares que indican la existencia de un problema. Mediante la activación de alertas, las soluciones SIEM pueden poner en funcionamiento procesos manuales o automatizados para la investigación y contención de ataques reales o posibles.

Además, las soluciones SIEM simplifican las investigaciones forenses y el proceso de respuesta de solicitudes de auditoría. También incluyen capacidades de administración de almacenamiento de información y archiving de datos de logs, lo que simplifica el cumplimiento de requerimientos normativos con respecto a la retención de datos a largo plazo.

La mayoría de las soluciones SIEM se basan en software o paquetes en dispositivos optimizados para simplificar la implementación; la plataforma RSA enVision se basa en este último modelo. Por lo general, los productos consisten en software de servidor, una consola de administración centralizada basada en la Web y, en muchos casos, software de agente necesario para implementar en los dispositivos que desea monitorear, o más próximos a estos. Muchas soluciones incluyen capacidad incorporada de almacenamiento de información y repositorios de datos para almacenar y administrar datos de eventos.

Por sus propios medios, SIEM no impide ni disminuye la cantidad de ataques. Por lo tanto, es probable que los clientes que esperan que SIEM funcione de esa manera no estén conformes con los resultados. Sin embargo, cuando se implementa como parte de un ecosistema de seguridad de gran envergadura para soportar el trabajo de los analistas de seguridad, SIEM desempeña una función fundamental en la detección, el análisis y la solución de ataques, así como también en cuanto al reporting de cumplimiento normativo y análisis forense.

² Ibíd.

Herramientas Sólidas de Flujo de Trabajo y Análisis Forense

Las herramientas de flujo de trabajo y análisis forense constituyen elementos críticos para mejorar la productividad de los empleados de operaciones de seguridad, ya que logran resolver más incidentes y reducir el tiempo de resolución promedio para investigaciones. Las herramientas de análisis forense brindarán al analista la visibilidad, flexibilidad y capacidad de procesamiento necesaria para “reproducir” eventos de interés, filtrar datos de eventos con muchas variables diferentes y reconstruir eventos de seguridad u operacionales end-to-end.

Las herramientas de flujo de trabajo deberían ser lo suficientemente flexibles para soportar y optimizar los procesos actuales de su equipo para administrar investigaciones al mismo tiempo que se permiten cambios imprevistos de procesos que se pueden implementar en el futuro. Las funcionalidades de flujo de trabajo deben contemplar el ciclo de vida de la investigación, es decir, desde la identificación e investigación inicial, el direccionamiento a los miembros del equipo adecuado, el escalamiento automático de incidentes de alta prioridad o difíciles de resolver, hasta la resolución, el cierre y el archiving. La integración directa con los principales sistemas de tickets, como Peregrine y Remedy, ayuda a que los incidentes y todas las investigaciones asociadas se transmitan de manera transparente al “sistema de registros” corporativo para realizar tickets y seguimiento de eventos.

Recomendación N.º 3: Incorpore Requerimientos Estratégicos en el Proceso de Selección

De manera progresiva, la capacidad de los profesionales de seguridad de pasar de ser protectores de activos de la información a impulsores de innovación y éxito comercial determina su eficacia. Al elegir una solución SIEM para operaciones de seguridad, debe enfrentar los requerimientos inmediatos y alinearse con las necesidades estratégicas del negocio. Por ejemplo, un producto debe brindar la funcionalidad suficiente a todos los principales productos de SIEM (operaciones de red, seguridad y cumplimiento de normas) para que una solución sirva para los tres objetivos, y la reducción de costos y complejidad. Las consideraciones estratégicas incluyen:



- **Las nuevas iniciativas de negocios**, como la adquisición, una iniciativa importante de e-commerce o la ampliación de un ecosistema de asociados de negocios, generan nuevas exigencias operacionales y capacidad en red, y crean nuevas áreas de riesgos de seguridad. Una solución SIEM debe soportar la planificación en todas estas áreas. Los datos de eventos existentes proporcionan información para guiar las estrategias de operaciones de red y seguridad. Y, por supuesto, una vez que las iniciativas se implementan, la solución se debe interconectar de manera sencilla con las nuevas fuentes de eventos para capturar los datos de eventos de operaciones de red y seguridad que generan.
- **Cumplimiento de normas**. Necesita la flexibilidad para responder ante requerimientos de cumplimiento de normas nuevos e imprevistos. Esto requiere el análisis de eventos capturados con anterioridad, incluso aquellos que actualmente no tienen importancia para los reguladores, pero pueden resultar críticos para cumplir requerimientos de auditoría en el futuro. La recopilación y retención de todos los datos de eventos de seguridad, no solo los datos pertinentes para los mandatos de cumplimiento de normas y amenazas actuales, constituye un paso obligatorio para cumplir los requerimientos de auditoría en el futuro.
- **Administración de riesgos de la información**. De manera progresiva, las organizaciones están desarrollando enfoques para identificar y medir cuáles son los riesgos de información más importantes, por ejemplo, dónde residen los datos más valiosos y dónde es más vulnerable, y usar dicha información para priorizar las inversiones en seguridad. El proveedor de SIEM debe tener una visión de soporte de administración de riesgos de la información y un plan de acción claramente determinado sobre cómo la solución SIEM interoperará con otros elementos de la infraestructura de seguridad para generar un ecosistema de seguridad que reduzca de manera sistemática los riesgos de seguridad.

Al tener en cuenta estos requerimientos más generales, obtiene un entorno estratégico para evaluar soluciones que compiten entre sí. Esto ayuda a garantizar que la funcionalidad de las operaciones de seguridad y las prioridades corporativas sean consideradas adecuadamente en el proceso de selección.

Las herramientas de flujo de trabajo y análisis forense constituyen elementos críticos para mejorar la productividad de los empleados de operaciones de seguridad.


Recomendación N.º 4: El Sistema SIEM se Debe Integrar Fácilmente con Todos los Demás Elementos

Como notaron gran cantidad de observadores industriales, existe una clara tendencia a dejar de usar varias soluciones “segmentadas” de seguridad de la información y cumplimiento de normas, las cuales son costosas y difíciles de administrar, y brindan baja visibilidad en entornos complejos. Los clientes están eligiendo soluciones SIEM que formen parte de ofertas más amplias de los principales proveedores de tecnología. Gartner observó que “La consolidación tuvo un importante efecto en el mercado de SIEM y los grandes proveedores adquirieron los mejores productos para ampliar las carteras de seguridad. Esta evolución del mercado afecta las tendencias de compra, y los usuarios finales adquieren SIEMs como complemento de productos de seguridad más amplios”.³ Gartner considera que la facilidad de implementación y una buena integración con las infraestructuras existentes de los clientes constituyen factores cada vez más importantes en la selección de productos.

Garantice una Amplia Visibilidad de las Fuentes de Datos de Eventos

Como componente de la cartera de productos de seguridad de RSA, la solución RSA enVision se alinea perfectamente con estas tendencias y sobresale en un área que es particularmente fundamental: brinda visibilidad de las fuentes de eventos. Muchas soluciones SIEM solo brindan visibilidad de un subconjunto del entorno. Algunas se centran en redes y otras en servidores o sistemas operativos. En cualquier caso, se verá forzado a vivir con “puntos ciegos” o a realizar integraciones costosas para ampliar lo suficientemente su visión de eventos de operaciones de red y seguridad.

³ Gartner, Dataquest Insight: Forecast Analysis for Security Information and Event Management, en todo el mundo, 2007-2012, por Ruggero Contu y Mark Nicolett, 5 de marzo de 2008.



La plataforma RSA enVision soporta una de las más amplias gamas de fuentes de eventos listas para usar, entre ellas:

- Perímetro de seguridad (por ejemplo, firewalls y sistemas de detección de intrusiones)
- Otras herramientas de seguridad (por ejemplo, administración de acceso e identidades)
- Elementos de red (por ejemplo, routers y switches)
- Herramientas de operaciones de red (por ejemplo, administración de configuraciones)
- Mainframes y servidores
- Almacenamiento de información
- Aplicaciones de negocios (por ejemplo, SAP)
- Sistemas operativos y bases de datos

Además, gracias al soporte universal de fuente de eventos, la tecnología enVision permite agregar nuevas fuentes de eventos, lo que incluye dispositivos y aplicaciones propietarias, sin necesidad de realizar programaciones. Una solución SIEM tiene mayor capacidad para detectar toda la gama de eventos que requieren investigación o medidas correctivas, ya que brinda la vista más amplia del entorno.

Recomendación N.º 5: Complemente la Correlación de Eventos con Otras Fuentes de Inteligencia

La correlación de eventos constituye un aspecto importante de toda solución SIEM, ya que enfrenta la sobrecarga de información causada por un flujo continuo de datos del log de eventos. Mediante la aplicación de reglas de correlación, un motor de correlación filtra la información irrelevante, detecta patrones que indican actividades sospechosas o irregulares y consolida los datos relacionados en eventos útiles para que los administradores de red o los analistas realicen tareas administrativas. Cuando se optimiza para el entorno único del cliente, la combinación de reglas de correlación de eventos y un motor de correlación reduce considerablemente la cantidad total de eventos y alarmas, impide los falsos positivos y eleva de manera confiable los eventos de alta prioridad para que se tomen medidas.

Al elegir una solución, resulta crítico recopilar todos los logs y que el motor de correlación pueda administrar el procesamiento de todos los datos de eventos entrantes en todas las ubicaciones y en tiempo real. La acumulación de trabajos (backlog) y los retrasos disminuirán la capacidad de reconocer amenazas y responder a ellas de manera inmediata. La situación podría ser peor si solo correlaciona un subconjunto de datos, ya que es posible que no detecte una alerta de seguridad crítica. La plataforma RSA enVision cuenta con un poderoso motor de correlación que, combinado con la capacidad de recopilar grandes cantidades de datos de eventos en todas las ubicaciones, permite el procesamiento en tiempo real para emitir alertas a los clientes sobre eventos de alta prioridad a medida que se producen.

Esté Preparado para Diseñar Reglas de Correlación que se Ajusten a su Entorno

Es importante contar con una comprensión realista de los esfuerzos necesarios para optimizar la correlación de eventos. Las reglas de correlación, que predefinen patrones, situaciones y relaciones entre eventos que pueden indicar que es necesario prestar un mayor nivel de atención, constituyen un mecanismo clave en la correlación de eventos. Las reglas de correlación predeterminadas y las plantillas incorporadas se limitan a optimizar el proceso de escritura de reglas para los analistas de seguridad. Según Network World³, “Debe estar preparado para analizar detalladamente qué es lo que realmente le importa y escribir o activar las reglas que harán que el producto funcione. Los usuarios deben estar preparados para adaptar el producto antes de implementarlo y ajustarlo continuamente para que siga funcionando de manera eficaz en la reducción de ruidos que no provengan de eventos y la identificación de eventos críticos para la protección del entorno”.

Al elegir una solución SIEM, debe enfrentar los requerimientos inmediatos y alinearse con las necesidades estratégicas del negocio.

³NetworkWorld IT Buyer's Guide
<http://www.networkworld.com/buyersguides/guide.php?cat=865479>



Cuando se Escriben Reglas, el Contexto Resulta Clave

El hecho de anticipar y escribir reglas de correlación para enfrentar situaciones de ataques futuras y teóricas no suele ser exitoso, por ejemplo, mayor volumen de alarmas, falsos positivos altos o alertas de baja prioridad. Es algo imposible de predecir. Las reglas de correlación son más eficaces y precisas cuando están respaldadas por datos reales del entorno y se combinan con información contextual brindada por otras herramientas, como información sobre amenazas emergentes, datos de vulnerabilidad, datos de activos e información sobre administración de identidades y nivel de aplicaciones.

Por ejemplo, un evento de seguridad, como un error de autenticación de un servidor Windows, se puede considerar de alta prioridad. Sin embargo, el evento de seguridad combinado con datos de activos brinda contexto adicional. Si los datos de activos muestran que este activo tiene un valor bajo, el error de autenticación dará como resultado un evento de menor prioridad.

Recomendación N.º 6: Administración del Ciclo de Vida de la Información de los Datos de Log

El almacenamiento de datos de log constituye un elemento crítico de una solución SIEM. Con el paso del tiempo, los datos de log se acumularán a una tasa cada vez mayor e impulsada por dos factores clave:

- Aumento de la cantidad de dispositivos y aplicaciones de la red.
- Requerimientos normativos para la retención de datos de eventos de seguridad.

Algunas soluciones requieren un procesamiento previo extenso, indexación y metadatos para soportar el análisis de eventos, lo que incrementa potencialmente la carga de almacenamiento de información. Esto permite aumentar hasta diez veces los requerimientos de almacenamiento de información, lo que incrementa drásticamente los costos de administración de almacenamiento de información durante la vida de la solución.

Asegúrese de que la solución seleccionada cuente con opciones de ciclo de vida de los datos diseñadas correctamente. Como mínimo, un importante proveedor de dispositivos ofrece únicamente almacenamiento de información incorporado para datos de eventos. Una solución diseñada adecuadamente debe soportar entornos de almacenamiento de información en red (SANs, *Storage Area Networks*) o almacenamiento de información conectado en red (NAS, *Network-Attached Storage*). Esto le proporcionará una solución más flexible y rentable con una mayor resiliencia desde el punto de vista de la disponibilidad y la recuperación ante desastres.

Como la División de Seguridad de EMC, el desarrollador y proveedor de soluciones y tecnología de infraestructura de la información líder en el mundo, RSA ofrece innovación y experiencia inigualable en almacenamiento de información para soluciones SIEM. Por ejemplo, un enfoque de almacenamiento de información en niveles permitirá mover eficazmente datos de eventos a niveles de almacenamiento menos costosos, a medida que disminuyen las necesidades de acceso, y aún así garantizar la visibilidad completa y la fácil recuperación de necesidades legales, normativas, de descubrimiento y de análisis forense. Al permitir una compresión de los datos de eventos de hasta un 70% sin que esto afecte el performance, una solución de EMC/RSA puede reducir aún más los costos de almacenamiento de información del ciclo de vida.

Es importante contar con una comprensión realista de los esfuerzos necesarios para optimizar la correlación de eventos. Las reglas de correlación predeterminadas y las plantillas incorporadas se limitan a optimizar el proceso de escritura de reglas para los analistas de seguridad.



Recomendación N.º 7: Comprenda los Costos Reales de la Solución

Antes de elegir definitivamente una solución en particular, debe comprender cuáles son los costos iniciales y continuos. Una solución debe cumplir sus necesidades iniciales a un costo mínimo, para garantizar que no se estén realizando gastos iniciales desproporcionados con respecto a los beneficios, y, al mismo tiempo, permitir el escalamiento a una implementación que comprenda a toda la empresa con una inversión razonable. Además de considerar los costos de administración del almacenamiento de la información, como se mencionó anteriormente, asegúrese de comprender otros elementos relacionados con los costos:

- **Hardware de servidor:** en el caso de soluciones exclusivas de software, esto casi siempre constituye un costo adicional.
- **Pago de licencias de software:** ¿cuáles son los costos iniciales y continuos de la plataforma central de la solución, el software agente y los productos de otros fabricantes, como el software de base de datos?
- **Soporte de origen de eventos:** ¿cuáles son los orígenes soportados? ¿Cuál es el costo que implica incorporar orígenes y tipos adicionales?
- **Módulos opcionales:** ¿qué módulos de reporting, alertas y auditoría se incluyen en el precio cotizado? ¿Cuál es el costo de los módulos opcionales requeridos que le permitirán cumplir sus objetivos de la funcionalidad de la solución?
- **Costos del personal:** especialmente cuando se trata con referencias proporcionadas por el proveedor, investigue cuáles fueron los recursos especializados requeridos para la implementación y el soporte de la solución. Esto puede incluir analistas de seguridad, consultores

Algunas soluciones requieren un procesamiento previo extenso, indexación y metadatos para soportar el análisis de eventos. Esto permite aumentar hasta diez veces los requerimientos de almacenamiento de información.

involucrados en esfuerzos de integración, recursos de soporte de plataformas y bases de datos, y soporte continuo para miles de agentes de software. Los costos de personal representan una parte importante de un proyecto; además, las necesidades de integración y las operaciones complejas pueden generar costos imprevistos (no contemplados en el presupuesto).

- **Software y mejoras de capacidad:** ¿cuáles son los costos asociados con la expansión de la capacidad para el manejo de un mayor volumen de datos de eventos o la actualización de una solución exclusiva de software?

A fin de reducir los riesgos del proyecto, solicite a su proveedor que proporcione una cotización firme e integral que tenga en cuenta estos elementos de costos, y una sólida garantía de que la configuración inicial que se está proponiendo soportará el volumen de eventos anticipados de manera confiable.

Acerca de RSA

RSA, la División de Seguridad de EMC, es el principal proveedor de soluciones de seguridad para aceleración del negocio y ayuda a las más importantes organizaciones del mundo a alcanzar el éxito resolviendo los más complejos y delicados desafíos de seguridad. El enfoque hacia la seguridad centrado en la información que ofrece RSA protege la integridad y la confidencialidad de la información durante todo su ciclo de vida, sin importar dónde se la mueva, quién acceda a ella o cómo se la use.

RSA ofrece soluciones líderes en verificación de la identidad y control de acceso, prevención de pérdida de datos, encriptación y administración de claves, administración de información de seguridad y cumplimiento de normas, y protección contra fraudes. Estas soluciones brindan confianza a millones de identidades de usuarios, las transacciones que realizan y los datos que se generan. Para obtener más información, visite argentina.rsa.com y argentina.emc.com.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA, enVision y RSA Security son marcas registradas o marcas comerciales de RSA Security Inc. en los Estados Unidos y en otros países. EMC es una marca registrada de EMC Corporation. Todos los otros productos o servicios mencionados son marcas comerciales de sus respectivos dueños. ©2008 RSA Security Inc. Todos los derechos reservados.

7SIEM WP 0708