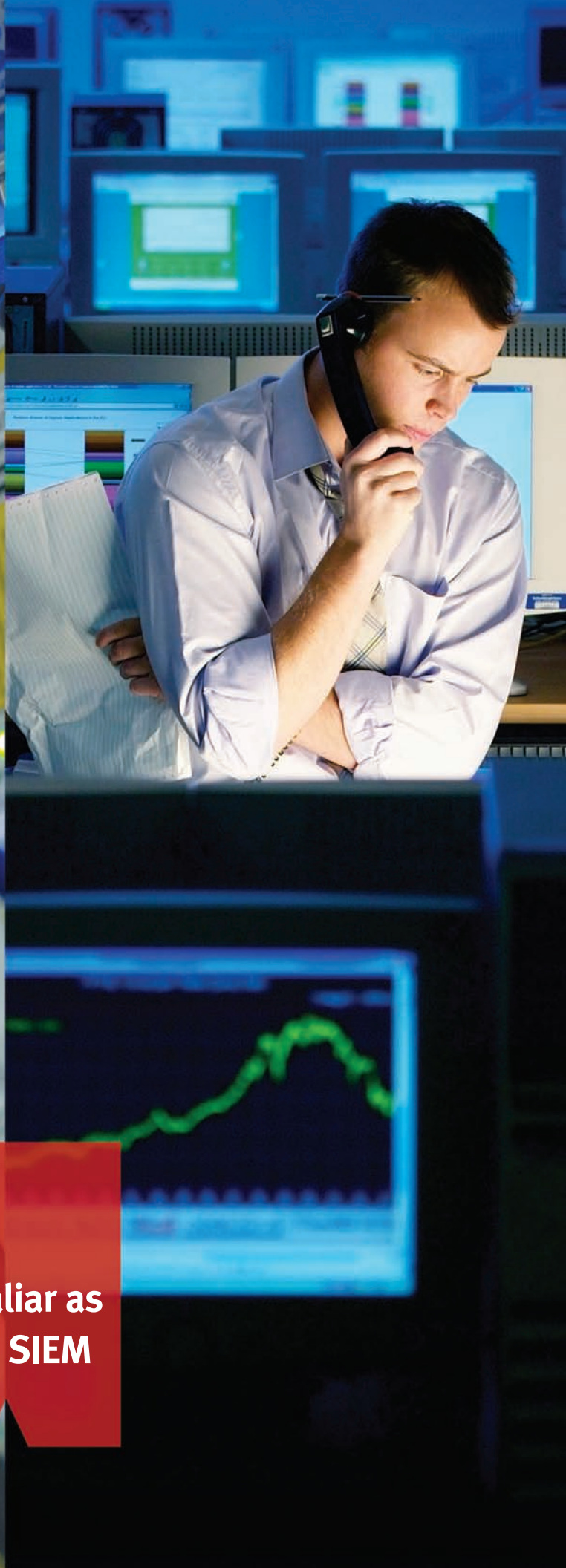




The Security Division of EMC

White paper

Verificação de segurança: 7 pontos a considerar ao avaliar as soluções do fornecedor para SIEM



A meta de uma solução de SIEM é tornar mais produtivas as pessoas envolvidas com a segurança.

As soluções de SIEM (Security Information and Event Management, gerenciamento de informações de segurança e eventos) estão se tornando um componente obrigatório da estrutura de segurança das empresas, desempenhando um importante papel na detecção de ameaças, na resposta a incidentes,

na análise forense e na conformidade relacionada à segurança. Com base na experiência com mais de 1.300 implantações bem-sucedidas de SIEM em organizações de todos os portes, a RSA oferece aos compradores potenciais sete fatores a considerar durante a avaliação de ofertas de fornecedores.

Não importa a sigla — SIEM, SEM ou SIM —, o gerenciamento de informações de segurança e eventos é uma das principais preocupações em muitas empresas (para uma breve visão geral, consulte “SIEM para segurança” na página 2). De acordo com a Forrester Research¹, mais de um terço das empresas buscavam adotar a tecnologia de SIM até meados de 2008. O motivo mais frequentemente citado para a implantação de uma solução foi a melhoria da emissão de relatórios e da conformidade (32% dos usuários na pesquisa da Forrester com 259 tomadores de decisões de empresas norte-americanas e européias), com a identificação de incidentes de segurança em segundo lugar (citada por 20% dos participantes).

A solução de SIEM chega a cada canto de sua empresa e afeta muitas peças de sua infra-estrutura, por isso a escolha da solução de um fornecedor é um compromisso de longa duração com um enorme impacto. Para dificultar sua escolha, as soluções variam muito em termos de tecnologia básica, funcionalidade, recursos, e no custo total de propriedade. Na realidade, muitas empresas viveram o “arrependimento do comprador” depois de optar por uma solução pouco adequada para suas necessidades.

Ao avaliar as soluções lado a lado, não se concentre detalhadamente em determinados recursos, na interface do usuário ou nas regras de correlação de eventos. Em vez disso, como propomos nas sete recomendações a seguir, amplie sua avaliação para contemplar a oferta de cada fornecedor em sua totalidade, inclusive a totalidade dos dados de eventos capturados e o grau de integração encontrado na solução e na infra-estrutura adjacente. Considere se um produto é favorável à empresa em termos de facilidade de implantação, dimensionamento e custo total de propriedade. E, como não poderia deixar de ser, avalie os pontos fortes do fornecedor, inclusive sua expertise geral em segurança, estabilidade financeira, apoio à P&D e independência entre fornecedor e plataforma. Com uma solução que corresponda às suas necessidades em várias dessas dimensões, a probabilidade de sucesso em longo prazo será muito maior.

Recomendação nº 1: defina seu atual modelo de operações de segurança e deixe que ele informe os requisitos imediatos da solução

As empresas têm modelos de operações de segurança muito divergentes e, na avaliação de soluções de SIEM, é importante saber onde você se encaixa no *continuum* para poder escolher uma solução que corresponda às suas necessidades (e orçamento) atuais e que, ao mesmo tempo, proporcione a flexibilidade para dimensionar e evoluir suas operações com o passar do tempo.

No extremo superior, algumas empresas mantêm uma instalação de SOC (Security Operations Center, centro de operações de segurança) ampla e centralizada, com vários analistas de segurança, cada um concentrado em uma área de responsabilidade (por exemplo, eventos de servidores). Em um cenário mais comum, um pequeno grupo de analistas, normalmente com funções primárias em TI ou operações de rede, compartilha uma gama de responsabilidades de operações de segurança. Um terceiro modelo, ainda, é um “SOC virtual”, cujos membros estão distribuídos geograficamente.

Seja qual for o modelo que você emprega atualmente, a meta de uma solução de SIEM não é substituir pessoas por tecnologia, é torná-las mais produtivas e eficazes em suas tarefas. A seleção de uma solução apropriada requer um entendimento de suas atuais responsabilidades e dos processos do fluxo de trabalho. Como estão divididas as responsabilidades e tarefas entre os membros da equipe? Como os alertas são priorizados? É necessária resposta 24 horas por dia, 7 dias por semana? Quanta largura de banda da equipe pode ser dedicada à análise forense?

¹ “Grandes mudanças a caminho no mercado de SIM”, Paul Stamp, Forrester Research, 27 de fevereiro de 2008



Entenda o que não está funcionando — e porquê

É igualmente importante entender as deficiências no ambiente atual que possam estar limitando a eficácia de seu pessoal. Por exemplo:

- Se sua equipe está gastando muito tempo caçando alertas enganosos ou de baixa prioridade, pode ser que as regras de correlação sejam muito vagas ou não levem em conta outros dados, como os ativos e as vulnerabilidades, resultando em alertas imprecisos.
- Se as investigações forenses forem lentas e inconvenientes, ou até inconclusivas, pode ser que os dados históricos do evento não possam ser fácil e rapidamente recuperados de uma fonte competente única. Ou pode ser que não tenham sequer sido capturados pelo sistema SIEM e, portanto, não possam ser recuperados de forma alguma.
- Se os eventos críticos não estiverem sendo resolvidos de forma oportuna, os processos do fluxo de trabalho talvez sejam inadequados ou fragmentados.

Freqüentemente, esses problemas surgem de falhas fundamentais na própria solução SIEM, ou porque a funcionalidade integrada é muito cara de se operacionalizar em sua configuração no mundo real.

Recomendação nº 2: considere estes elementos essenciais da solução em relação às operações de segurança

Três atributos da solução são essenciais para solucionar algumas das falhas de SIEM mais comuns com relação ao suporte a operações de segurança: captura e análise de dados em tempo real, captura de todos os dados de eventos de segurança e operacionais e ferramentas eficazes de análise forense.

Aquisição poderosa, análise sólida

Uma solução de SIEM deve executar igualmente bem duas funções principais:

- Captura e análise em tempo real de dados que chegam ao registro de eventos para dar suporte à detecção e resposta a ameaças em tempo real.
- Rápida recuperação e emissão de relatórios sobre os dados capturados anteriormente, para que possam ser prontamente “destrinchados” em prol da análise forense, das operações de rede, da conformidade ou da detecção legal.

A meta de uma solução de SIEM não é substituir pessoas por tecnologia, é torná-las mais produtivas e eficazes em suas tarefas.

A maioria das soluções pode ser otimizada para fazer bem uma coisa ou outra, mas não ambas, forçando o fornecedor a favorecer um recurso em detrimento do outro. Já a plataforma RSA enVision® foi criada especificamente para equilibrar esses requisitos, com funcionalidade de coleta, análise e consulta amplamente integrada à tecnologia de banco de dados orientado a objetos, o que garante flexibilidade e desempenho ideal.

Acesso a todos os dados

A maioria das soluções não analisa a atividade bruta do evento na aquisição, pois isso reduziria o desempenho a um nível inaceitável. Em vez disso, com a normalização e o pré-processamento dos dados, essa atividade é reduzida a um subconjunto de exceções, submetido à análise em seguida. Algumas soluções descartam os dados remanescentes como um todo, impedindo seu uso posterior em atividades de análise forense, auditoria ou emissão de relatórios. Outras soluções ainda retêm os dados brutos do evento, mas em um repositório separado que não está bem integrado às funções de consulta e emissão de relatórios. Isso pode atrapalhar bastante os esforços para analisar dados históricos e emitir relatórios sobre eles.

Certifique-se de que a solução selecionada elimina esse problema reunindo e retendo todos os dados de eventos de entrada, conservando-os para uso posterior. À medida que você escreve novas regras de correlação para lidar com novas ameaças, emissão de relatórios ou requisitos de auditoria, essas regras podem atuar prontamente sobre todos os dados pertinentes, elevando a precisão dos alertas e permitindo a reanálise de eventos passados.

SIEM para segurança: uma rápida visão geral

Embora as soluções de SIEM difiram significativamente em suas arquiteturas, funcionalidades e recursos, todas servem a uma finalidade similar. Como a Gartner declarou, “os usuários finais precisam analisar os dados de eventos de segurança em tempo real (para o gerenciamento de ameaças, principalmente com foco em eventos de rede) e analisar e emitir relatórios sobre dados do registro (para o monitoramento da conformidade com a política de segurança, com foco principalmente nos eventos do host e dos aplicativos)”.⁷

As soluções de SIEM automatizam e simplificam o processo de reunir dados do registro de eventos — incluindo, entre outros, dados de eventos de segurança — obtidos de várias fontes em toda a rede. Usando as técnicas de agregação de dados e correlação de eventos, esses produtos analisam os dados para identificar ameaças de segurança conhecidas e reconhecer comportamento anômalo que podem indicar um problema. Ao acionar alertas, uma solução de SIEM pode dar início a processos manuais ou automatizados para investigar e conter um ataque suspeito ou conhecido.

Além disso, as soluções SIEM facilitam as investigações forenses e simplificam o processo de resposta a solicitações de auditoria. Cada vez mais, elas também incluem recursos para gerenciar o armazenamento e arquivar dados do registro, o que facilita a conformidade com requisitos normativos referentes à retenção de dados em longo prazo.

A maioria das soluções de SIEM é baseada em software ou está incluída em aplicativos otimizados para simplificar a implantação; a plataforma RSA enVision é baseada nesse último modelo. Os produtos normalmente consistem em software de servidor, um console de gerenciamento centralizado baseado na Web e, em muitos casos, software de agente que precisa ser implantado nos dispositivos que serão monitorados ou próximo deles. Muitas soluções incluem capacidade adicional de armazenamento e repositórios de dados para armazenar e gerenciar dados de eventos.

O SIEM não impede nem mitiga ataques por conta própria e os clientes que esperam que ele funcione desse modo certamente ficarão desapontados. Contudo, quando implantado como parte de um ecossistema de segurança mais amplo que serve de base para o trabalho de analistas de segurança, o SIEM desempenha um papel essencial na detecção de ameaças, análise, correção, análise forense e emissão de relatórios de conformidade.

⁷ Ibid.

Ferramentas robustas de análise forense e fluxo de trabalho

As ferramentas de análise forense e fluxo de trabalho são elementos essenciais para aprimorar a produtividade da equipe de operações de segurança, resolvendo com êxito mais incidentes e reduzindo o tempo médio entre as investigações e a resolução. Ferramentas de análise forense robustas e fáceis de usar proporcionarão aos analistas a visibilidade, flexibilidade e completa capacidade de processamento necessárias para reproduzir eventos de interesse, filtrar dados de eventos com muitas variáveis diferentes e reconstruir completamente eventos de segurança ou operacionais.

As ferramentas de fluxo de trabalho devem ser suficientemente flexíveis para poder sustentar e simplificar os atuais processos da equipe voltados ao gerenciamento de investigações com a simultânea possibilidade de se fazer mudanças não previstas no processo que podem ser implementadas no futuro. Os recursos de fluxo de trabalho devem se estender por todo o ciclo de vida da investigação, desde a identificação e investigação inicial, passando pelo(s) membro(s) mais apropriado(s) da equipe, escalonamento automático de incidentes de alta prioridade ou difícil resolução, até a resolução, fechamento e arquivamento. A integração direta com os principais sistemas de emissão de tíquetes, como o Peregrine e o Remedy, ajuda a permitir que os incidentes e toda a pesquisa associada sejam transferidos sem dificuldades ao “sistema de registro” corporativo para a emissão de tíquetes e rastreamento de eventos.

Recomendação nº 3: incorpore requisitos estratégicos em seu processo de seleção

Cada vez mais, a eficácia dos profissionais de segurança é determinada por sua capacidade de fazer a transição entre ser protetor de ativos de informação e ser facilitador da inovação e sucesso nos negócios. Na seleção de uma solução de SIEM voltada a operações de segurança, você não precisa apenas lidar com requisitos imediatos, mas também alinhá-la às necessidades estratégicas do negócio. Por exemplo, um produto deve proporcionar funcionalidade suficiente em todos os principais resultados práticos do SIEM — segurança, conformidade e operações de rede — de modo que uma solução possa atender a todas as três finalidades, reduzindo o custo e a complexidade. As considerações estratégicas abrangem:



- **Novas iniciativas de negócios**, como uma aquisição, uma importante iniciativa de comércio eletrônico ou a expansão de um ecossistema de parceiros, colocar novas demandas operacionais e de capacidade na rede e criar novas áreas de risco de segurança. Uma solução de SIEM deve dar suporte ao planejamento em todas essas áreas, com os dados de eventos existentes proporcionando discernimento para guiar suas estratégias de segurança e operação de rede. E, é claro, quando essas iniciativas estiverem em vigor, a solução deve fazer interface facilmente com novas fontes de eventos para capturar os dados de eventos de segurança e operações de rede que geram.
- **Conformidade**. Você precisa de flexibilidade para responder a novos e imprevisíveis requisitos de conformidade. Isso exige uma capacidade de olhar para trás, para os eventos capturados anteriormente, inclusive os que atualmente não são de interesse dos controladores, mas que podem se tornar essenciais para preencher requisitos de auditoria no futuro. A coleta e retenção de todos os dados de eventos de segurança, não apenas os dados relevantes para as atuais ameaças e mandados de conformidade, é uma etapa obrigatória para a satisfação de futuros requisitos de auditoria.
- **Gerenciamento de riscos às informações**. Cada vez mais, as empresas estão desenvolvendo abordagens para a identificação e medição de onde estão os maiores riscos às informações — por exemplo, onde residem seus dados mais valiosos e onde são mais vulneráveis — e usando essas informações para priorizar investimentos em segurança. Seu fornecedor de SIEM deve ter uma visão que sustente o gerenciamento de riscos às informações e um roteiro articulado de forma clara com relação a como a solução de SIEM e outros elementos da infra-estrutura de segurança irão interagir para formar um ecossistema de segurança que reduza sistematicamente o risco às informações.

Levar em conta esses requisitos mais amplos proporciona uma estrutura estratégica para a avaliação de soluções concorrentes. Isso ajuda a garantir que tanto a funcionalidade das operações de segurança quanto as prioridades corporativas receberão a atenção adequada em seu processo de seleção.

As ferramentas de análise forense e de fluxo de trabalho são elementos essenciais para aprimorar a produtividade da equipe de operações de segurança.


Recomendação nº 4: o SIEM deve se integrar facilmente a tudo que está a seu redor

Como muitos observadores do setor notaram, há uma clara tendência de afastamento das soluções de vários “escapes” com relação à segurança e conformidade das informações, cujo gerenciamento é caro e inconveniente, além de proporcionar uma visibilidade insatisfatória em meio a ambientes complexos. Os clientes estão optando por soluções de SIEM que fazem parte de uma oferta mais ampla distribuída por grandes fornecedores de tecnologia. A Gartner observa que “o mercado de SIEM foi significativamente afetado pela consolidação, com os maiores fornecedores adquirindo os melhores jogadores para expandir seus portfólios de produtos em segurança. Essa evolução do mercado vem influenciando as tendências de aquisição, com os usuários finais comprando o SIEM cada vez mais como uma adição a produtos de segurança mais amplos”.³ A Gartner vê a facilidade de implantação e a boa integração com as infra-estruturas existentes dos clientes como fatores cada vez mais importantes por trás da seleção do produto.

Garanta ampla visibilidade nas fontes de dados de eventos

Como um componente do portfólio RSA de segurança, a solução RSA enVision se alinha perfeitamente a essas tendências e se destaca em uma área especialmente vital: proporcionar visibilidade nas fontes de eventos. Muitas soluções de SIEM proporcionam visibilidade apenas em um subconjunto do ambiente. Algumas são centradas na rede; outras, em sistemas operacionais ou servidores. Em qualquer caso, você é forçado a conviver com “pontos cegos” ou assumir integrações caras para ampliar suficientemente sua visão dos eventos de segurança e de operações da rede.

³ Gartner, Dataquest Insight: Forecast Analysis for Security Information and Event Management, Worldwide, 2007-2012 (Análise de previsão relacionada a informações de segurança e gerenciamento de eventos, mundial, 2007-2012) por Ruggero Contu e Mark Nicolett, 5 de março de 2008



A plataforma RSA enVision é compatível com a mais ampla série de fontes de eventos prontas para uso, entre elas:

- Segurança perimetral (por exemplo, firewalls e sistemas de detecção de intrusões)
- Outras ferramentas de segurança (por exemplo, gerenciamento de identidades e acessos)
- Elementos de rede (por exemplo, roteadores e switches)
- Ferramentas de operações de rede (por exemplo, gerenciamento de configurações)
- Mainframes e servidores
- Armazenamento
- Aplicativos de negócios (por exemplo, SAP)
- Bancos de dados e sistemas operacionais

Além disso, por meio do suporte universal a fontes de eventos, a tecnologia enVision permite adicionar novas fontes de eventos, inclusive aplicativos e dispositivos exclusivos, sem exigir programação. Com a mais ampla visão possível de seu ambiente, uma solução de SIEM está melhor posicionada para detectar toda a gama de eventos que exigem investigação ou ação corretiva.

Recomendação nº 5: complemento a correlação de eventos com outras fontes de inteligência

A correlação de eventos é um aspecto importante de qualquer solução SIEM, lidando com a sobrecarga de informações causada por uma torrente ininterrupta de dados do registro de eventos. Por meio da aplicação de regras de correlação, um mecanismo de correlação filtra informações irrelevantes, reconhece padrões que sugerem anomalias ou atividade suspeita e consolida os dados relacionados em eventos acionáveis, que podem ser manipulados por analistas de segurança ou administradores de rede. Se otimizadas para o ambiente exclusivo do cliente, a combinação das regras de correlação de eventos e um mecanismo de correlação reduz amplamente o número total de eventos e alarmes, suprime falso-positivos e eleva, de forma confiável, os eventos de prioridade mais alta para ação.

Na seleção de uma solução, é essencial que todos os registros sejam reunidos e que o mecanismo de correlação possa lidar com o processamento de todos os dados de eventos que entram, em todas as localidades, em tempo real. Os acúmulos de trabalho e os atrasos minarão sua capacidade de reconhecer e responder imediatamente a ameaças. Ainda pior, se apenas um subconjunto de dados for correlato, você pode perder completamente um alerta de segurança crítico. A plataforma RSA enVision tem um poderoso mecanismo de correlação que, combinado com a capacidade de reunir um vasto volume de dados de eventos em todas as locais, permite o processamento em tempo real para alertar os clientes de eventos de alta prioridade assim que ocorrerem.

Esteja preparado para adaptar regras de correlação a seu ambiente

É importante ter um entendimento realista do esforço necessário para otimizar a correlação de eventos. As regras de correlação, que predefinem padrões, cenários e relacionamentos entre eventos que possam indicar que uma atenção adicional é justificada, são um mecanismo essencial na correlação de eventos. Os modelos integrados e as regras de correlação padrão simplificam o processo de escrita das regras para seus analistas de segurança, mas não vão além disso. Como a Network World³ escreveu, “você tem que querer se aprofundar naquilo com o que você realmente se importa e escrever ou ativar regras que farão o produto funcionar... Os usuários têm de querer ajustar minuciosamente um produto antes de implementá-lo e fazer isso continuamente para mantê-lo funcionando eficazmente na redução do ruído de não-eventos e identificar eventos essenciais para proteger o ambiente”.

Na seleção de uma solução de SIEM, você não precisa apenas lidar com requisitos imediatos, mas também alinhá-la às necessidades estratégicas do negócio.

³Guia do comprador de TI da NetworkWorld em <http://www.networkworld.com/buyersguides/guide.php?cat=865479>



Ao escrever regras, o contexto é essencial

Geralmente, a tentativa de antecipar e escrever regras de correlação para lidar com cenários teóricos de ataques futuros resultou em falha, por exemplo, aumento do volume de alarmes, muitos alertas enganosos e de baixa prioridade; é como tentar prever onde, no futuro, você deve procurar uma agulha em um palheiro. As regras de correlação são mais eficazes e precisas quando sustentadas por dados reais sobre seu ambiente, combinadas com informações contextuais distribuídas por outras ferramentas, como informações de ameaças emergentes, dados de vulnerabilidade, dados de ativos, informações em nível de aplicativo e informações do gerenciamento de identidades.

Por exemplo, um evento de segurança, como uma autenticação com defeito em um servidor Windows, pode ser considerado de alta prioridade. Contudo, esse evento de segurança, combinado com dados de ativos, proporciona um contexto adicional. Se os dados de ativos revelarem que o ativo tem um valor baixo, a autenticação com defeito resultará em um evento de prioridade mais baixa.

Recomendação nº 6: gerencie o ciclo de vida das informações dos dados do registro

O armazenamento de dados do registro é um elemento essencial de uma solução de SIEM. No decorrer do tempo, os dados do registro se acumulam cada vez mais rápido, em função de dois fatores principais:

- Aumento do número de dispositivos e aplicativos em sua rede
- Requisitos normativos referentes à retenção de dados de eventos de segurança.

Um possível acréscimo ao seu ônus de armazenamento é a exigência de algumas soluções de extenso pré-processamento, indexação e metadados para dar suporte à análise de eventos. Isso pode aumentar em até dez vezes os requisitos para armazenamento, aumentando drasticamente os custos de gerenciamento do armazenamento durante a vida útil de sua solução.

Certifique-se de que a solução selecionada tenha opções de ciclo de vida de dados projetadas adequadamente. Pelo menos um importante fornecedor de utilitários oferece somente armazenamento on-board para dados de eventos. Uma solução bem projetada deve ser compatível com SANs (Storage Area Networks, redes da área de armazenamento) ou NAS (Network-Attached Storage, armazenamento conectado à rede). Isso proporcionará uma solução mais flexível e econômica e também mais resiliente sob uma perspectiva de disponibilidade e recuperação de desastres.

No papel de divisão de segurança da EMC, a líder mundial em desenvolvimento e fornecimento de tecnologia e soluções de infra-estrutura de informações, a RSA agrega às soluções de SIEM expertise e inovação em armazenamento incomparáveis. Por exemplo, uma abordagem de armazenamento hierárquico permitirá mover dados de eventos eficientemente para níveis mais baratos de armazenamento no decorrer do tempo, à medida que diminuir as necessidades de acesso, embora ainda garanta total visibilidade e fácil recuperação para atender a necessidades legais, normativas, de detecção e de análise forense. Com a viabilização de compactação de dados de eventos em até 70%, sem comprometer o desempenho, uma solução EMC/RSA pode reduzir ainda mais os custos de ciclo de vida do armazenamento.

É importante ter um entendimento realista do esforço necessário para otimizar a correlação de eventos. Os modelos integrados e as regras de correlação padrão simplificam o processo de escrita das regras para seus analistas de segurança, mas não vão além disso.



Recomendação nº 7: entenda os verdadeiros custos da solução

Antes de se comprometer com uma determinada solução, é preciso entender quais serão os custos iniciais e os contínuos. Uma solução deve atender suas necessidades iniciais com o mínimo custo, para garantir que você não esteja incorrendo em custos antecipados desproporcionais aos benefícios, e ao mesmo tempo permitir que você dimensione, com investimento razoável, até uma implementação em toda a empresa. Além de considerar o custo do gerenciamento do armazenamento, como discutido anteriormente, esteja certo de que entende outros elementos do custo:

- **Hardware do servidor.** Para soluções baseadas apenas em software, isso quase sempre é um custo adicional.
- **Taxas de licenciamento de software.** Quais os custos iniciais e contínuos para a plataforma da solução central, software de agente e produtos de terceiros como software de banco de dados?
- **Suporte à fonte de eventos.** Quais fontes são compatíveis e qual o custo para adicionar outros tipos e números de fontes?
- **Módulos opcionais.** Que módulos de emissão de relatórios, emissão de alertas e auditoria estão inclusos no preço sendo orçado e qual o custo dos módulos opcionais necessários para atender a suas metas estabelecidas para a funcionalidade da solução?
- **Custos com pessoal.** Especialmente ao falar com referências oferecidas pelo fornecedor, explore francamente quais recursos especializados foram necessários para implantar e dar suporte à solução. Esses recursos podem incluir analistas de segurança, consultores envolvidos com os esforços de integração, recursos de suporte ao banco de dados e à plataforma



The Security Division of EMC

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

RSA, enVision e RSA Security são marcas registradas ou marcas comerciais da RSA Security Inc. nos Estados Unidos e/ou em outros países. EMC é marca registrada da EMC Corporation. Todos os outros produtos e serviços mencionados são marcas comerciais de seus respectivos proprietários. ©2008 RSA Security Inc. Todos os direitos reservados.

7SIEM WP 0708

White paper da RSA

Algumas soluções exigem extenso pré-processamento, indexação e metadados para dar suporte à análise de eventos. Isso pode aumentar em até dez vezes as exigências de armazenamento.

e suporte contínuo para milhares de agentes de software. Os custos com pessoal representam uma parcela significativa de um projeto e as operações complexas e necessidades de integração podem levar a custos não previstos (nem no orçamento).

- **Aprimoramentos de capacidade e software.** Quais são os custos associados com a expansão de sua capacidade de lidar com um volume maior de dados de eventos ou de fazer upgrade de uma solução baseada apenas em software?

Para mitigar os riscos do projeto, peça a seu fornecedor um orçamento firme e abrangente que trate desses elementos de custo, junto com uma sólida garantia de que a configuração inicial proposta será confiavelmente compatível com o volume de eventos previsto.

Sobre a RSA

RSA, a divisão de segurança da EMC, é a melhor fornecedora de soluções de segurança para a aceleração de negócios, ajudando as mais importantes empresas do mundo a alcançar a solução de seus desafios de segurança mais complexos e delicados. A abordagem de segurança centrada em informações da RSA protege a integridade e a confidencialidade das informações em todo o ciclo de vida — independentemente do local para onde são transferidas, quem as acessa e como são utilizadas.

A RSA oferece soluções líderes do setor quanto à segurança de identidade e controle de acesso, prevenção contra perda de dados, gerenciamento de chaves e criptografia, gerenciamento de informações de segurança e conformidade e proteção contra fraude. Essas soluções levam confiança às identidades de milhões de usuários, às transações executadas por eles e aos dados gerados. Para obter mais informações, visite <http://brazil.RSA.com> e <http://brazil.EMC.com>.