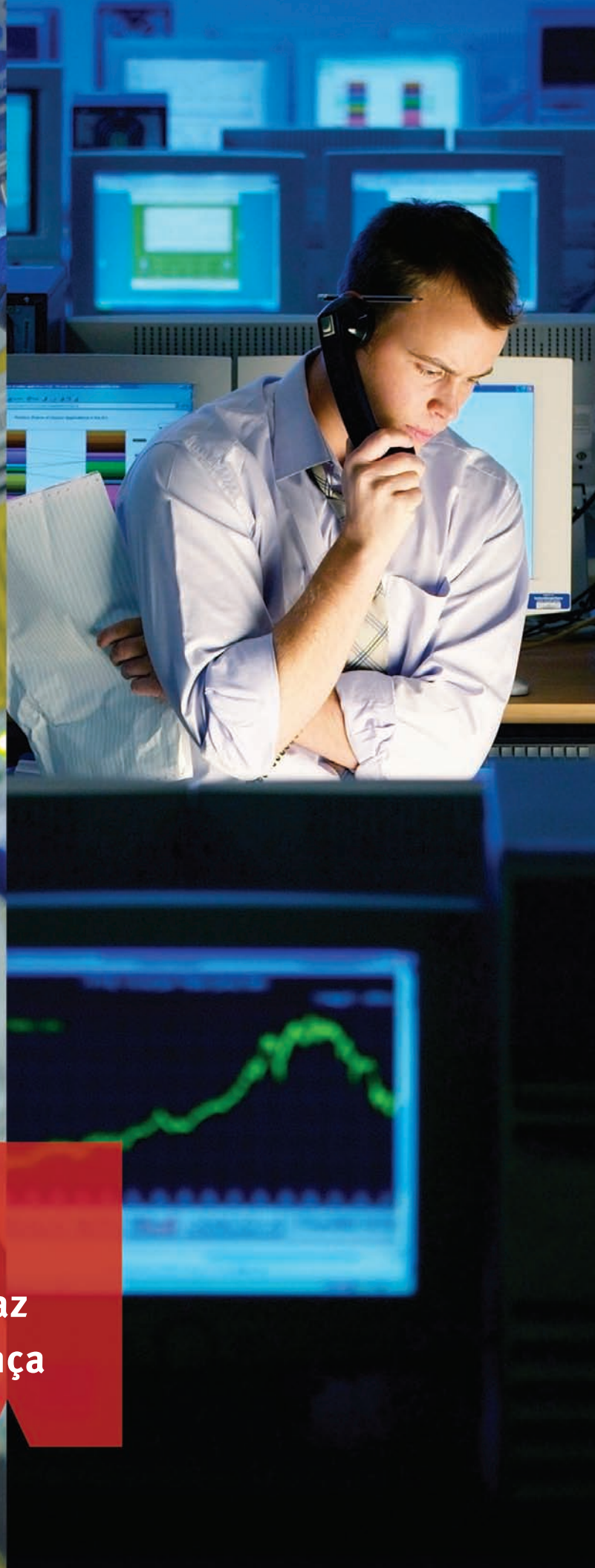




The Security Division of EMC

White paper

Criando uma função eficaz de operações de segurança



A consciência dos problemas de segurança é fundamental para uma política eficaz.

Quando pensamos em um SOC (Security Operations Center, centro de operações de segurança), freqüentemente temos a imagem de uma sala ampla, cheia de pessoas sentadas em filas perfeitas, com sua atenção dividida entre os monitores de seus computadores e uma grande tela à frente, como no Centro Espacial de Houston durante o lançamento de um ônibus espacial. É claro que tais locais existem, mas em muitas empresas, a realidade é bem diferente. Embora quase toda empresa tenha uma função de operações de segurança, ela pode assumir várias formas. Em alguns casos, é um grupo formalmente

designado, com equipe e instalações dedicadas. Em outros, as operações de segurança consistem em apenas um punhado de pessoas com várias responsabilidades que lidam com problemas de segurança de TI conforme surgem.

Onde quer que você se encontre nesse continuum, entender todas as atividades e papéis de uma função de operações de segurança é o primeiro passo para tornar essas operações mais eficazes e eficientes — permitindo que você aproveite os investimentos relacionados em tecnologia e a expertise humana para obter a melhor vantagem.

Operações de segurança definidas: “o que exatamente você faz?”

O termo “operações de segurança” surgiu nos anos mais recentes para descrever uma gama de atividades cujo propósito era manter seguros os ativos de informações de uma organização. No passado, as tarefas relacionadas à segurança eram divididas, segundo as necessidades, entre o pessoal de segurança, os administradores de rede e as equipes de operações do servidor. Cada vez mais, essas responsabilidades estão sendo unidas sob a abrangência das operações de segurança.

Atividades diárias

Quer você tenha ou não um SOC formal ativo, é bem provável que os membros da equipe estejam executando determinadas obrigações rotineiras em algum aspecto ou de alguma forma. Essas atividades diárias são criadas para manter os sistemas de segurança funcionando do modo ideal, de maneira que os processos de negócios fiquem protegidos contra ataques e abusos e ainda possam operar perfeitamente e sem interrupção.

O gerenciamento de vulnerabilidades mantém hackers (e auditores) afastados.

A identificação de sistemas sem correções, senhas fracas e configurações equivocadas serve a dois propósitos: ajudar a fortalecer tanto a segurança quanto a conformidade. Ela proporciona um panorama preciso das vulnerabilidades de segurança de modo que, por exemplo, você possa encorajar a equipe de operações do servidor a corrigir seus sistemas. Por sua vez, você pode ficar um passo à frente dos hackers, que podem querer explorar essas vulnerabilidades, e dos editores, que irão considerá-lo responsável por proteger a infra-estrutura de modo conforme.

O gerenciamento de dispositivos de segurança aumenta a precisão da detecção de ameaças.

Manter as políticas do firewall atualizadas e ajustar as regras para IDS (Intrusion Detection System, sistema de detecção de intrusões) e SIEM (Security Information and Event Management, gerenciamento de informações e eventos de segurança) permite que você refine continuamente a precisão dos alertas. Quando a tecnologia que você implantou está cumprindo sua tarefa eficazmente, o tráfego de rede pode fluir para onde precisa ir, o software pode ser executado sem interrupção e o tempo da equipe não é desperdiçado com a investigação de alarmes falsos.

A monitoração propicia uma advertência precoce quando ocorrem problemas.

Examinar o ambiente de segurança em busca de sinais de problemas é uma tarefa contínua. Essa tarefa inclui verificar se os sistemas de segurança estão funcionando adequadamente, se há alertas automatizados nos vários canais de comunicação que possam exigir acompanhamento e examinar outros indicadores, como um pico inexplicável no tráfego de rede, o que pode sinalizar um ataque em andamento.

A pesquisa de ameaças informa o que procurar e como outros estão respondendo.

Muitos recursos estão disponíveis para ajudar a acompanhar as vulnerabilidades recém detectadas, como estão sendo exploradas e que correções foram desenvolvidas em resposta. Esses recursos incluem informes de segurança do fornecedor, quadros de avisos, listas de e-mail e organizações como o CERT® (Computer Emergency Response Team, equipe de resposta a emergências de informática), o SANS Internet Storm Center e os alertas de cibersegurança do Departamento de Segurança Nacional dos EUA. As informações que proporcionam podem ajudar a reconhecer rapidamente um ataque e tomar as medidas apropriadas para reduzir seu risco. Ao longo prazo, podem ajudar a priorizar investimentos de segurança para melhor proteger seu ambiente.

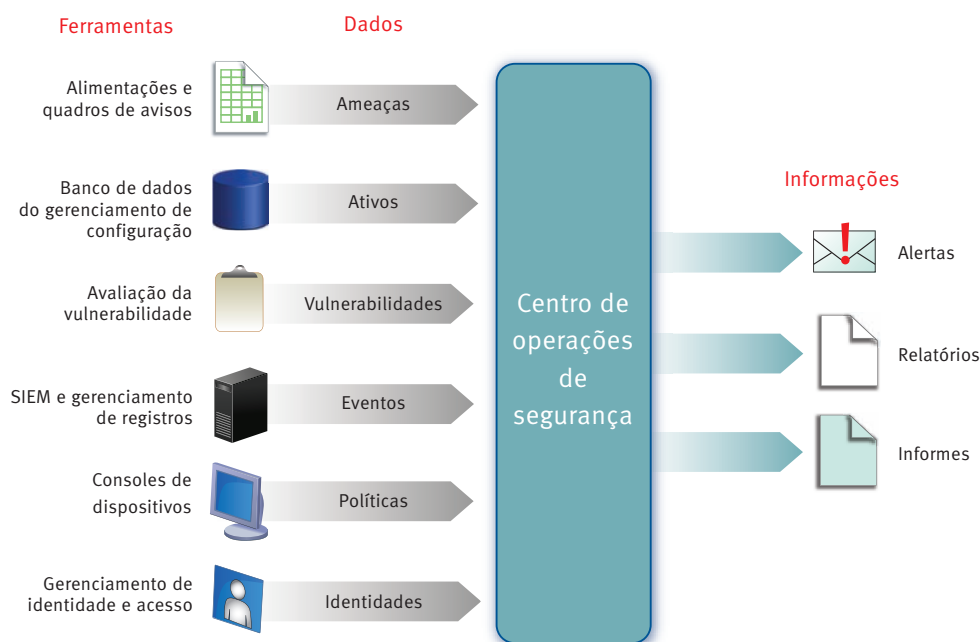


Figura 1.
Um instantâneo das operações de segurança

Aproveitando-se de várias ferramentas e recursos de informação, a função de operações de segurança monitora continuamente o ambiente de segurança de uma empresa, responde a ameaças imediatas e vulnerabilidades em longo prazo, e proporciona aconselhamento e orientação sobre questões de segurança tanto para o gerenciamento sênior quanto para as unidades de negócios.

Gerenciamento de incidentes e problemas

Além das operações diárias, outro conjunto de tarefas é realizado em resposta a incidentes de segurança. Em empresas menores, esses eventos podem acontecer apenas periodicamente; em empresas maiores, é provável que ocorram com maior frequência, exigindo a atenção de um pessoal de operações de segurança dedicado.

A rápida resposta a incidentes abranda o impacto dos ataques.

O SOC direciona a resposta a ataques e vulnerabilidades de alto risco, tomando as medidas imediatas para abrandar o impacto de um ataque em andamento e fornecer a administradores de rede e operadores de sistema orientação sobre medidas adicionais para conter ou remediar uma ameaça.

A triagem de problemas e o gerenciamento de incidentes ajudam a garantir que você esteja empregando seu tempo sensatamente.

A maioria das equipes de operações de segurança tem mais trabalho do que pode suportar. Estabelecer um processo de triagem de problemas permite que a equipe avalie rapidamente incidentes e problemas e priorize os que representam o maior risco para os negócios. Por sua vez, você pode alocar recursos experientes para os problemas mais urgentes e/ou importantes. E mais, procedimentos de fluxo de trabalho e escalonamento bem-definidos ajudam a garantir que os incidentes de alto risco sejam resolvidos o mais rapidamente possível.

A investigação forense revela a origem básica de incidentes de segurança.

Com as informações e ferramentas corretas, os analistas de segurança podem estudar as circunstâncias que envolvem um ataque ou violação e seguir o rastro da evidência até chegar à origem. Por sua vez, a equipe do SOC pode proteger contra a repetição de eventos e sua empresa pode tomar medidas contra grupos conhecidos (por exemplo, funcionários, sócios ou contratadas) que estejam envolvidos.

Aconselhamento e orientação estratégicos

Enquanto desempenha suas obrigações, as operações de segurança coletam dados valiosos sobre o ambiente de TI e o modo com o qual a empresa está abordando a segurança. Transformar esses dados operacionais em aconselhamento de negócios capazes de gerar ações também é uma tarefa essencial.

O aconselhamento estratégico sobre segurança apóia a inovação e a ampliação dos negócios.

Com uma visão do ambiente de segurança que é ampla e altamente granular ao mesmo tempo, as operações de segurança estão em uma excelente posição para aconselhar os negócios sobre como a segurança pode dar suporte a iniciativas estratégicas como aquisições e fusões, redes de parceiros e implementação de novas linhas de negócios.

Figura 2.
Quem é quem no SOC?

Mesmo em uma função relativamente pequena de operações de segurança, os papéis, as responsabilidades e o organograma normalmente lembram alguma variação desse modelo. As áreas sombreadas representam sobreposição funcional.

	Estratégico	Resposta a incidentes	Cotidiano
CSO	Aconselhamento estratégico		
	Coleta de medidas		
Gerente de segurança		Coleta de medidas	Coleta de medidas
		Supervisão de IR	
Guru de segurança		Triagem de problemas	Pesquisa de ameaças
		Investigação	
Analista de segurança			Investigação
			Monitoração e emissão de alertas
			Gerenciamento de configurações de dispositivos
			Gerenciamento de vulnerabilidades

A avaliação das operações de segurança mostra as áreas que exigem melhorias.

Os dados operacionais recolhidos de registros de eventos de segurança e relatórios de incidentes expõem lacunas entre suas expectativas quanto a como o SOC deve operar e as realidades cotidianas com as quais sua equipe deve lutar. Examinando as tendências nos dados operacionais, você pode identificar áreas que exigem melhorias nos membros da equipe, em treinamento, política ou tecnologia.

Por exemplo, uma falha persistente na correção de vulnerabilidades pode indicar que há necessidade de uma comunicação mais forte ou treinamento de conscientização voltado ao pessoal de operações do servidor. O aumento das lentidões de rede causadas por ataques iniciados externamente pode indicar a necessidade de monitoração mais sensível a ameaças ou um processo de escalonamento mais disciplinado. Nesses e em outros cenários, uma vez tomadas as medidas corretivas, os dados de tendência também podem medir se essas ações estão tendo o efeito desejado.

Os informes específicos da empresa elevam a consciência e levam à mudança.

Uma responsabilidade importante da equipe de SOC é traduzir os próprios incidentes de segurança da empresa e também as informações de ameaças sendo geradas pelo CERT, SANS e outras fontes competentes em recomendações que podem gerar ações específicas da organização. Quando sistematicamente aplicadas de modo oportuno, essas recomendações podem melhorar constantemente a postura de segurança geral. Por exemplo, os informes podem oferecer orientação aos arquitetos corporativos e outros sobre os tipos de controles que precisam estar em vigor para proteger o negócio.

Além disso, os informes que são mais estratégicos por natureza podem elevar a consciência dos executivos sobre problemas de segurança e influenciar os tomadores de decisões a dar à segurança um nível mais elevado de atenção e investimento.

Funções e responsabilidades: quem é quem nas operações de segurança

O ingrediente mais importante em um centro de operações de segurança bem-sucedido é uma equipe que funciona bem. Em pequenas empresas, isso pode incluir apenas uma ou duas pessoas que lidem com todas as tarefas do SOC, ainda que com um foco necessariamente limitado nas atividades mais urgentes ou essenciais. As empresas maiores podem ter uma equipe considerável de pessoal dedicado a operações de segurança, cada um com áreas especializadas de expertise. A Figura 2 mostra as principais atividades que cada função desempenha e como podem se relacionar entre si.

Analistas de segurança

Os analistas de segurança estão nas “linhas de frente” das operações de segurança. Eles têm a responsabilidade de garantir que as ferramentas de segurança sejam implantadas adequadamente e estejam em execução da forma ideal. Eles monitoram constantemente o ambiente em busca de sinais de problemas e freqüentemente são o primeiro ponto de contato quando um alerta de alto risco é emitido ou um ataque suspeito começa a afetar as operações de negócios. Normalmente, os analistas também conduzem os estágios iniciais da investigação pericial.

Especialistas em pesquisa

Nos bastidores dos SOCs mais bem-sucedidos há um ou mais "gurus" de segurança, cujo título formal pode ser Especialista em Pesquisa ou Analista Sênior. Normalmente, esses indivíduos têm vasta expertise técnica e ampla experiência. Eles "vivem, respiram e comem segurança"

e são chamados para auxiliar em incidentes de segurança que são particularmente complexos e/ou de alta pressão. Em função de sua compreensão dos desafios e tecnologias de segurança, eles também podem atuar como consultores para o Gerente do SOC e para o CISO (Chief Information Security Officer, diretor de segurança das informações), aconselhando-os sobre estratégia de segurança.

Gerente de SOC

O gerente de SOC supervisiona as operações de segurança cotidianas, adequando pessoal, ferramentas, processos e métodos de medição necessários para alcançar os objetivos do SOC no tocante ao apoio aos negócios. O gerente de SOC também serve de interface entre o SOC e o CISO. Nessa função, ele traduz as metas e requisitos do CISO em um conjunto de ações para a equipe do SOC executar e, reciprocamente, comunica o CISO de problemas que exigem atenção e/ou investimento executivo.

CISO

Como a principal interface entre o departamento de segurança e o negócio, o CISO é responsável por garantir que os recursos e atividades do SOC estejam alinhados para apoiar a estratégia geral de negócios e estejam ajudando a criar valor de negócios. O SOC traduz as necessidades dos negócios em objetivos de operações de segurança, prioriza onde o orçamento é gasto e freqüentemente serve como um divulgador, ensinando os executivos de negócios sobre como a segurança pode permitir a inovação dos negócios e ser usada para gerenciar o risco às informações.

Os mais avançados centros de operações de segurança estão se voltando para ferramentas como o SIEM, bem como para o gerenciamento de registros, a fim de automatizar a coleta de informações, emissão de alertas e de relatórios.

As mais avançadas equipes de SOC enriquecem ainda mais sua percepção do ambiente de segurança com informações contextuais oferecidas por outras ferramentas e fontes de informação.

Ferramentas do SOC: da básica à avançada

A tecnologia é um elemento-chave de operações de segurança, proporcionando os meios para centralizar processos, automatizar tarefas repetitivas e tornar seu pessoal mais produtivo de modo geral. A maioria das equipes de operações de segurança utiliza as seguintes ferramentas básicas:

- Cada dispositivo e software de segurança perimetral (por exemplo, firewalls, IDS e produtos antivírus) tem seus próprios mecanismos de emissão de relatórios e alertas, além de consoles para fazer alterações nas políticas. Em SOCs rudimentares, essas ferramentas freqüentemente são o primeiro ponto de entrada para que os analistas investiguem ou remediem um problema de segurança.
- As ferramentas de avaliação de vulnerabilidades podem ser produtos comerciais ou ferramentas de código aberto, como o Nessus. De qualquer modo, elas proporcionam uma valiosa percepção de quais sistemas estão corrigidos e configurados corretamente e quais representam um risco de segurança para o ambiente.
- As ferramentas freeware de diagnóstico podem ser facilmente encontradas para download e são extremamente úteis, mesmo para o mais avançado analista de operações de segurança. As ferramentas de varredura de rede, como o nmap, as ferramentas de varredura sem fio (Kismet) ou ferramentas de teste de penetração como o Metasploit podem ser inestimáveis no teste e diagnóstico de problemas de segurança.

Além do básico

Os mais avançados centros de operações de segurança estão se voltando para ferramentas como o SIEM, além de ferramentas de gerenciamento de registros para automatizar a coleta de informações, a emissão de alertas e os recursos de emissão de relatórios. Por exemplo, a solução de SIEM da RSA — a plataforma RSA enVision® — simplifica as operações de segurança ao:

- **Proporcionar informações de segurança em tempo real que podem gerar ações.** Os alertas em tempo real destacam problemas de alto risco, permitindo que os profissionais de segurança priorizem suas atividades. Os recursos de correlação dimensionáveis melhoram a produtividade do analista ao reduzir os falsos positivos.
- **Permitir investigações periciais.** A plataforma RSA enVision serve de apoio para o trabalho investigativo sobre incidentes de segurança passados ao proporcionar a capacidade de pesquisar eventos de vários modos, por exemplo, por período, ID de usuário, número de porta e servidor host, para chegar rapidamente à origem do incidente. O fluxo de trabalho acelera o ciclo de vida da resolução de problemas desde a investigação inicial, o direcionamento aos membros apropriados da equipe, o escalonamento automático de incidentes de alta prioridade ou de difícil resolução, até a resolução, o fechamento e o arquivamento.
- **Aumentar a visibilidade na eficácia das medidas de segurança.** A tecnologia RSA enVision ajuda as empresas a avaliar a eficácia do programa de segurança especificando informações sobre o quão bem os controles de acesso estão sendo aplicados, e também sobre quaisquer aplicativos e serviços de rede não-autorizados.

O contexto é a chave

As mais avançadas equipes de operações de segurança enriquecem ainda mais sua percepção do ambiente de segurança com informações contextuais oferecidas por outras ferramentas e fontes de informação. Por exemplo, o banco de dados de gerenciamento de configurações, que captura os dados de configuração de vários ativos, facilita a avaliação tanto dos requisitos para a implementação de alterações de segurança em toda a empresa quanto do possível impacto operacional e de negócios de tais alterações. Os sistemas de IAM (Identity and Access Management, gerenciamento de identidades e acessos) propiciam visibilidade do comportamento do usuário, não somente quanto a incidentes de segurança específicos, mas também para reconhecer tendências mais amplas de IAM. Isso ajuda a aumentar a responsabilidade do usuário, permitindo simultaneamente que a equipe do SOC detecte mais facilmente o uso indevido de privilégios por pessoas de dentro.

Como começar: como você mantém as operações de segurança ativas e funcionais?

Depois de identificar as atuais funções das operações de segurança de sua empresa, você desejará identificar as lacunas e ineficiências e começar a solucioná-las. Algumas das principais práticas recomendadas empregadas pelas melhores organizações de TI estão resumidas a seguir.

Comece facilitando a vida do analista

O cargo de analista de segurança pode ser frustrante. Frequentemente esse cargo é altamente reativo e, se não houver estrutura definida em vigor para priorizar e escalonar os problemas, pode facilmente se tornar uma tarefa de combate a incêndio, em que a equipe fica constantemente suprimindo os sintomas mais óbvios das ameaças de segurança sem solucionar os problemas básicos. Além do mais, se seus analistas de segurança não puderem acessar informações oportunas e precisas sobre o que está acontecendo em seu ambiente, é impossível que saibam se você está instaurando os controles corretos.

Durante um mês inteiro, avalie as atividades nas quais seus analistas estão empregando o tempo e priorize os pontos onde você acredita que uma equipe ou tecnologia adicional possa ter o maior impacto na melhoria da eficácia dos analistas.

Dê às pessoas as informações corretas para realizarem suas tarefas

Em todas as áreas do SOC, fazer a tarefa eficazmente depende de estar armado com as informações certas no momento certo. Considere o uso inteligente da tecnologia para colocar essas informações nas mãos das pessoas.

- **Analistas** — alertas oportunos, priorizados com base na urgência. Dados de registros e ativos para fornecer informações contextuais sobre incidentes de segurança.
- **Especialistas em pesquisa** — informações aprofundadas sobre incidentes de segurança à medida que ocorrem para acelerar a resolução. Dados sobre ameaças emergentes para que possam recomendar medidas de proteção.
- **Gerentes de segurança** — status atualizado sobre problemas de segurança pendentes. Dados sobre como os recursos da equipe estão sendo utilizados.
- **CISOs** — informações resumidas sobre os mais urgentes problemas e incidentes de segurança. Postura geral do negócio quanto ao risco e à segurança.

Foco nas melhorias de processos em vez de na automação do SOC

É improvável que a tecnologia venha realmente a substituir o pessoal de operações de segurança, mas ferramentas como o gerenciamento de registros e SIEM podem simplificar alguns dos processos mais tediosos e repetitivos com os quais eles lidam e, assim, torná-los mais produtivo.

Um exemplo seria pegar os alertas do IDS, fazer uma referência cruzada entre eles e uma lista de máquinas vulneráveis ao ataque específico detectado e reiniciar os serviços nos dispositivos afetados. Nos casos em que os dispositivos pertençam a outro grupo, pode ser necessário negociar a permissão para automatizar a ação corretiva.

Faça a tecnologia trabalhar para o seu pessoal, e não o contrário

Uma função bem-sucedida de operações de segurança depende, principalmente, de se ter uma equipe coesa, com suporte de processos bem-definidos e informações oportunas que os capacite a tomar decisões bem-informadas. A tecnologia é útil até onde ela torna seu pessoal mais eficaz, portanto, use soluções como o SIEM criteriosamente para simplificar seus processos e tornar as informações disponíveis de um modo facilmente digerível.

Ao decidir sobre a tecnologia SIEM correta para sua função de operações de segurança, procure por:

- Uma solução facilmente empregável que acelere e simplifique seus processos.
- Uma solução que torne prontamente disponíveis todos os dados de que seu pessoal precisa para realizar suas tarefas.
- Uma solução que ofereça as ferramentas para transformar dados operacionais em informações que podem ser convertidas em ações, as quais irão melhorar sua postura de segurança e apoiar as iniciativas estratégicas do negócio.

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 centralizada nas informações, como é feito pela RSA, protege a integridade e a confidencialidade das informações em todo o ciclo de vida delas — não importando para onde são transferidas, quem as acessa nem 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 que eles executam e aos dados gerados. Para obter mais informações, visite www.RSA.com e www.EMC2.com.br.



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

The Security Division of EMC

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. O CERT é uma marca registrada da Carnegie Mellon University. Todos os outros produtos e serviços mencionados são marcas comerciais de seus respectivos proprietários. ©2008 RSA Security Inc. Todos os direitos reservados.

SOC WP 0808

White paper da RSA