

Serviço de análise e projeto de operações de segurança

Melhorando seu recurso de operações de segurança

Resumo geral

- Estabelece um plano para a implementação ou o aprimoramento dos recursos e procedimentos de operações de segurança, abrangendo domínios técnicos, operacionais e de negócios
- Fornece um projeto geral, centrado em SIEM e DLP, bem como uma estrutura de tratamento de incidentes.
- Baseado em práticas recomendadas e metodologias e padrões comprovados de implantação, como ISO, SANS e NIST.
- Aproveita a experiência real do cliente da RSA e também da equipe global de resposta a incidentes críticos da EMC.

Hoje as empresas enfrentam desafios opostos quando protegem suas operações e informações contra riscos. De um lado, as ameaças estão cada vez maiores, da mesma forma que a sofisticação dos ataques. Por outro lado, estão as realidades econômicas atuais; os orçamentos estão sendo reduzidos, os recursos são restritos e os custos de gerenciamento de um incidente de segurança são maiores do que nunca.

Uma função de operações avançadas de segurança é centralizada em processos que, diariamente, permitem que uma organização proteja os recursos essenciais com mais eficiência e garanta a conformidade por meio de detecção, resposta e atividades-chave de correção de incidentes. Especificamente:

- Identificação e desenvolvimento cuidadosos de um programa abrangente de operações de segurança
- Projeto eficaz de um sistema de operações de segurança que seja centrado no uso integrado de tecnologias e sistemas de SIEM, DLP e inteligência contra ameaças.
- Integração com tecnologias de gerenciamento de serviços e operações de rede, como suporte técnico, gerenciamento de alterações e configurações e estruturas operacionais como ITIL.

- Criação de uma estrutura sustentável para obter segurança e gerenciamento de riscos às informações duradouros

Com uma função de operações avançadas de segurança estabelecida, as organizações terão os processos e os recursos em vigor para iniciar, de maneira eficaz, um programa abrangente de gerenciamento de riscos às informações.

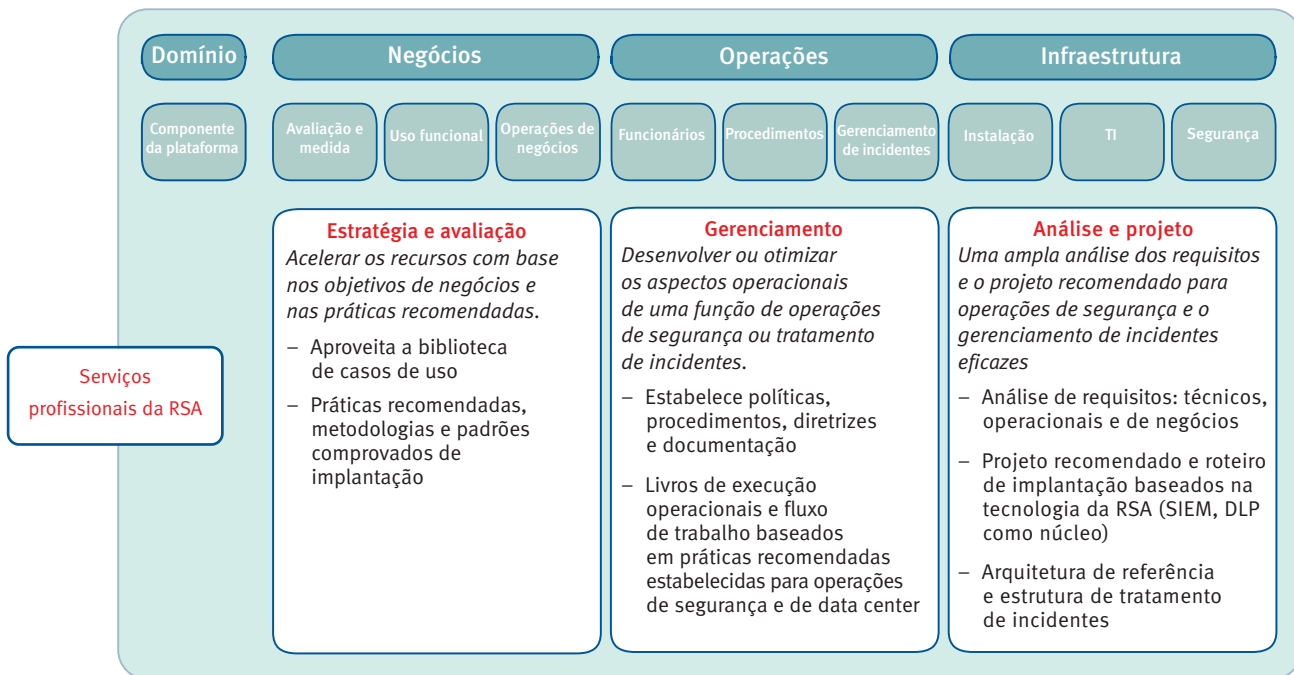
Análise e projeto de operações de segurança

Este serviço de consultoria e assessoria oferece uma ampla análise dos requisitos de operações de segurança e dos recursos no estado atual e recomenda um projeto de solução para atender aos objetivos específicos de operações de segurança e gerenciamento de incidentes. Ele também inclui uma estrutura de tratamento de incidentes e as próximas etapas para o desenvolvimento de políticas e procedimentos operacionais e de gerenciamento apropriados. O serviço de análise e projeto de operações de segurança pode estabelecer sua linha de base para operações avançadas de segurança e também pode ser o primeiro passo em direção a um programa mais avançado de operações de segurança ou a um conjunto de recursos do SOC (Security Operations Center, centro de operações de segurança).

Com base em uma análise da empresa e dos requisitos operacionais e técnicos para um recurso de tratamento geral de incidentes e prevenção contra perda de dados, este contrato abrange quatro componentes principais:

- Uma análise de alto nível das necessidades dos negócios para dar suporte a uma função de operações de segurança.
- Uma análise detalhada dos requisitos técnicos e operacionais para dar suporte a uma função de operações de segurança, particularmente aos requisitos do SIEM (Security Information and Event Management, gerenciamento de eventos e informações de segurança) e do DLP (Data Loss Prevention, prevenção contra perda de dados), como as principais tecnologias de segurança dentro do SOC.
- Arquiteturas de referência para a plataforma RSA enVision® e as soluções RSA® Data Loss Prevention para atender aos requisitos previstos.
- Estrutura de tratamento de incidentes e próximas etapas para projeto de soluções e planejamento de operações mais abrangentes.





Estrutura de operações de segurança Os serviços profissionais da RSA oferecem um pacote de serviços de consultoria e assessoria que atende aos requisitos de qualquer empresa que procura melhorar sua função de operações de segurança.

Escopo e abordagem

O aumento na sofisticação dos ataques de hackers e o risco interno está levando as organizações a lidarem com a exposição aos riscos às informações de maneira mais agressiva. Isso está testando a visão tradicional das operações de segurança – limitadas principalmente à coleta e análise de eventos de segurança – e ampliando o escopo das operações de segurança. Um recurso avançado atualmente precisa englobar a monitoração e a proteção de informações confidenciais, bem como a infraestrutura em que ele possa residir ou passar, e ser capaz de monitorar e emitir relatórios de riscos à segurança de informações de várias origens em toda empresa.

Em resposta a essa necessidade, os serviços profissionais da RSA desenvolveram o serviço de análise e projeto de operações de segurança, que adota uma visão ampla para englobar todos os aspectos da melhoria da função de operações de segurança de um cliente – desde a coleta e análise de requisitos até o projeto de uma solução apropriada, do roteiro e do conjunto da estrutura de respostas a incidentes.

O escopo e a abordagem para oferecer esse serviço envolvem as quatro fases seguintes:

Fase 1: estratégia da solução

- Lançamento antes da instalação, descrevendo a estratégia, os objetivos e o planejamento do contrato
- Análise com base em workshops no local dos requisitos das operações de segurança, conforme definido pelas necessidades operacionais, técnicas e de negócios
- Identificação de origens e dados de eventos para monitoração
- Procedimentos detalhados do processo de tratamento de incidentes

Fase 2: projeto da solução

- Desenvolvimento do projeto da solução técnica com base nos requisitos
- Identificação de origens de eventos de segurança, requisitos de proteção de dados, configuração, volumes de eventos e desempenho e requisitos de armazenamento
- Desenvolvimento de configurações apropriadas das soluções de SIEM e DLP

Fase 3: revisão da análise da solução preliminar e do relatório do projeto

Fase 4: relatório final e apresentação



The Security Division of EMC

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

©2009 RSA Security Inc. Todos os direitos reservados.
RSA, RSA Security e o logo da RSA 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. SOCOD DS 1009