

Serviço de gerenciamento de operações de segurança

Excelência em operações de segurança e resposta a incidentes

Resumo geral

- Implementar processos e procedimentos de segurança e gerenciamento de serviços para operações de segurança e gerenciamento de incidentes, todos eficazes
- Identificar processos existentes de automação
- Definir e implementar procedimentos operacionais abrangentes e livro de execução
- Identificar os principais relatórios e exibições do painel de controle para automação
- Melhorando a eficiência e a automação de suas operações de segurança em toda a empresa

Com o aumento nas ameaças de segurança externas e internas e com uma onda crescente de incidentes de segurança, as organizações estão aprimorando suas operações de segurança e seus métodos e procedimentos de respostas a incidentes para aplicar inteligência a fim de desviar proativamente ameaças à segurança e melhorar a capacidade de resposta a eventos de segurança, melhorar a eficiência e acelerar a automação de operações de segurança. Para se beneficiar do potencial dessas tecnologias, você precisa de procedimentos abrangentes que englobem operações de segurança e resposta a incidentes que se alinham aos objetivos de negócios, ajustados a seus riscos específicos e personalizados para seu setor e para os processos abrangentes de gerenciamento de negócios e serviços.

Um bom conjunto de procedimentos e um livro de execução operacional eficaz, unindo seus processos de operações de segurança e resposta a incidentes com sua abordagem de gerenciamento de negócios e serviços, pode transformar com eficiência possíveis eventos e visões de segurança em medidas proativas para eliminar ameaças de segurança ou melhorar a resposta a riscos potenciais. Processos de gerenciamento eficazes promoverão o tratamento de incidentes viável e aumentarão a eficácia geral de seu gerenciamento de segurança.

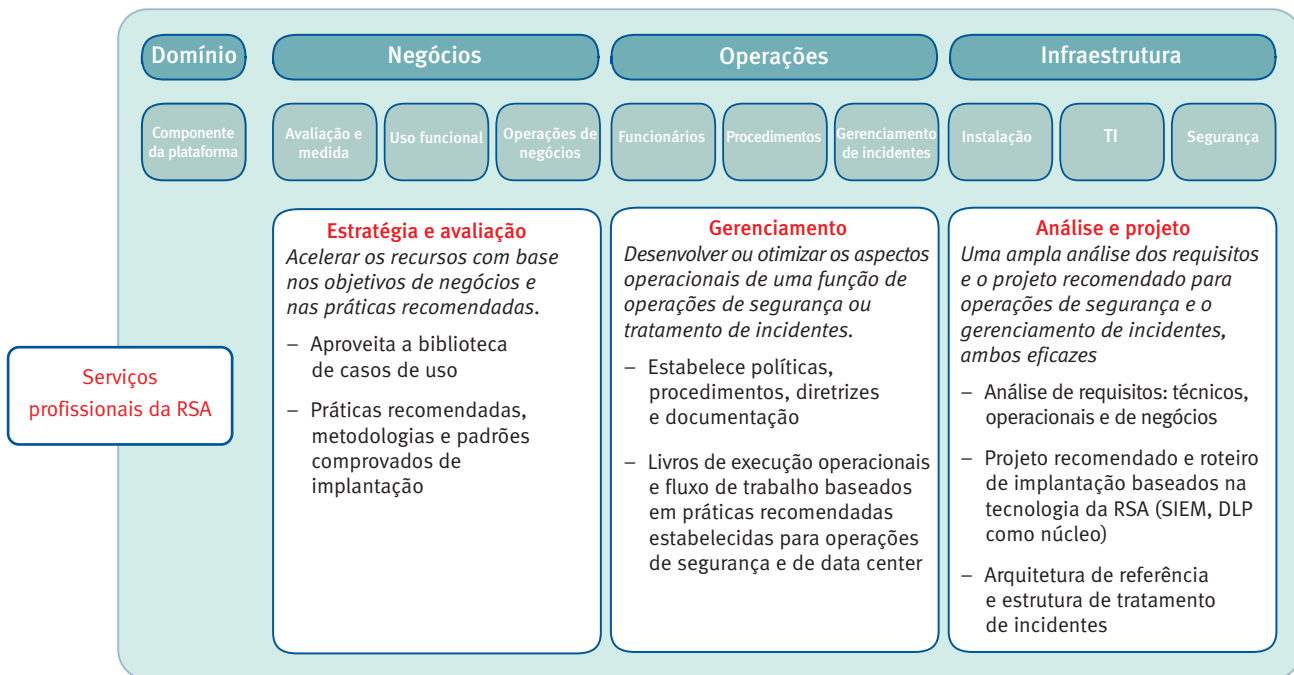
Serviço de gerenciamento de operações de segurança

O serviço de gerenciamento de operações de segurança foi projetado para ajudar as organizações no alinhamento estratégico e automação de segurança, operações, processos e relatórios de conformidade e para permitir que elas administrem diariamente um programa de tratamento de incidentes. Com o desenvolvimento de processos e procedimentos, esse serviço alinha estratégias e metodologias operacionais às necessidades dos negócios.

Atualmente, em muitas organizações, uma tecnologia como o SIEM (Security Information and Event Management, gerenciamento de informações de segurança e eventos) é implantada taticamente para tratar de um problema específico ou simplesmente para uso como um integrador de registros. Essa implantação limitada que agrega registros de segurança, sem dar suporte a processos e procedimentos, falha ao explorar todo o potencial da plataforma SIEM para reduzir o risco e automatizar as operações de segurança. Quando o SIEM é implantado estrategicamente para atender aos desafios críticos da empresa, é mais fácil gerenciar a segurança consistentemente em toda a empresa e reduzir os custos associados à conformidade e à sobrecarga de TI. Um recurso operacional abrangente permite que você automatize tantos processos quantos forem possíveis a fim de atender aos objetivos de segurança e conformidade, enquanto mantém a equipe em níveis existentes ou reduzidos.

Este serviço da RSA aumenta o retorno sobre o investimento em operações de segurança, definindo processos e procedimentos eficazes, centralizando atividades e identificando desempenho de automação que, coletivamente, assegura o alinhamento a geradores de negócios e a seus objetivos gerais. O serviço inclui o desenvolvimento de processos e procedimentos para gerenciamento de segurança, resposta a incidentes, emissão de relatórios de conformidade e operações de TI. Por exemplo, uma análise de segurança pode resultar no desenvolvimento de planos para automatizar aspectos do SOC (Security Operations Center, centro de operações de segurança), como a emissão corporativa de tíquetes.





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 serviço de gerenciamento de operações de segurança engloba estratégias para gerenciamento de segurança, resposta a incidentes, emissão de relatórios de conformidade e operações de TI:

- **O gerenciamento de segurança** fornece uma avaliação e um roteiro para melhorar o gerenciamento da segurança das informações e as operações e os procedimentos de tratamento de incidentes. O contrato determina as ameaças e as prioridades para tratamento de incidentes em sua organização. Isso permite a implantação de soluções de tecnologia associadas, como o SIEM, para fornecer a criação de uma visão centralizada de segurança das informações e tratamento de incidentes para melhorar as operações e aumentar a eficiência.
- **Funcionários.** Identificação e desenvolvimento do modelo de equipe e recursos; requisitos de seleção e treinamento da equipe, funções e responsabilidades.
- **Resposta a incidentes.** Desenvolvimento do fluxo de trabalho de gerenciamento de operações de segurança e processo para desenvolvimento, escalonamento e correção de incidentes e alertas
- **A emissão de relatórios de conformidade** considera necessidades dos negócios, requisitos contratuais, legislativos e normativos. Mostra onde alinhar os requisitos de conformidade normativa aos controles

da ISO 27002. As recomendações abrangem procedimentos para automatizar seus requisitos de emissão de relatórios de conformidade.

- **Procedimentos.** Desenvolvimento das políticas, padrões e diretrizes necessárias para a equipe junto com documentação abrangente e livro de execução operacional para administração diária.
- **As operações de TI** fornecem avaliação de operações de TI e recomendações de automação para melhorar as operações e aumentar a eficiência. Entre os exemplos estão planejamento de capacidade, solução de problemas, detecção de falhas/eventos, suporte técnico e gerenciamento de incidentes e desempenho. O contrato também ajuda a determinar a relevância de componentes de infraestrutura e os requisitos de acesso a ativos de informações.

Baseado em práticas recomendadas, metodologias e padrões comprovados de implantação, como ISO, SANS e os padrões NIST para gerenciamento de registros, gerenciamento de eventos e procedimentos de tratamento de incidentes. Os consultores de segurança da RSA e de TI detectarão os recursos atuais, registrarão o status atual e alinharão esses elementos a suas metas e objetivos de negócios. O relatório final documenta áreas para simplificar e onde melhorar a eficiência por meio da automação de processos.



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