VISÃO GERAL DO PRODUTO

Framework de Automação **SmartResponse**™

LogRhythm

Resposta a incidentes em segundos, não dias

Quando uma organização detecta um comprometimento em sua rede, uma resposta a incidentes ágil pode ser a diferença entre uma contenção rápida e uma brecha de dados prejudicial. As organizações que dependem exclusivamente de processos manuais têm dificuldades para reduzir os tempos de resposta e, assim, enfrentam riscos mais elevados. As empresas que trabalham para acelerar os tempos de resposta devem automatizar as ações comuns de investigação e resposta.

Infelizmente, a automação sempre esteve fora de alcance para a maioria das empresas. Desenvolver uma solução interna em geral apresenta custos muito elevados, e as opções existentes no mercado são inflexíveis ou requerem personalizações extensivas e onerosas.

Uma ferramenta de automação eficiente deve oferecer:

- Fluxos de trabalho eficientes e processos de aprovação flexíveis
- Integração direta no ambiente de TI
- Suporte para múltiplos sistemas operacionais
- Capacidade de atravessar redes díspares
- Testes integrados
- Custo e complexidade mínimos

Correção imediata que funciona

O Smart**Response**™ possibilita uma resposta a incidentes exclusiva. Ele também possibilita uma operação semiautomatizada, baseada em aprovação, para que os usuários possam avaliar a situação antes de executar contramedidas.

A LogRhythm reduz o tempo necessário para realizar as etapas de investigação e mitigação comuns, evitando que os comprometimentos de alto risco sofram um efeito bola de neve. Por exemplo, ativar uma verificação de vulnerabilidade em um ponto de extremidade suspeito, ou medidas mais drásticas, como colocar um ponto de extremidade comprometido em quarentena ou desativar uma conta de usuário suspeita.

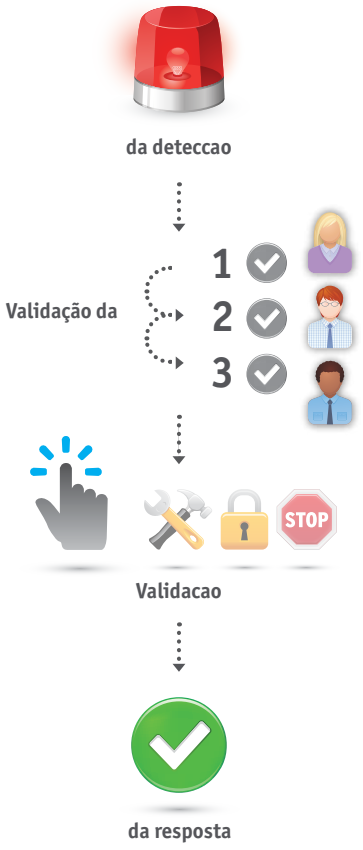
Plug-ins pré-construídos e personalizados

A LogRhythm Labs oferece uma extensa biblioteca de ações pré-construídas do Smart**Response**. A LogRhythm também ajuda os usuários a criar plug-ins personalizados usando sua tecnologia de programação/scripts preferencial, como Base, Java, .NET, Perl, PowerShell ou Python. Os usuários podem testar os plug-ins personalizados com uma ferramenta integrada que documenta as saídas e identifica erros. Essas ações pré-construídas e personalizadas do Smart**Response** colocam os clientes no controle.

Integração de alarme

O Framework de Automação Smart**Response** integra-se perfeitamente na plataforma da LogRhythm, oferecendo uma continuidade integral na detecção de ameaças end-to-end e no fluxo de trabalho de respostas.

Os usuários configuram as ações do Smart**Response** para serem ativadas por alarmes específicos. Esses alarmes podem transmitir dados para a ação do Smart**Response**, possibilitando uma execução dinâmica e precisa. Diversas ações do Smart**Response** podem ser executadas de um único alarme, possibilitando ações simultâneas de investigação e mitigação.



Processos de aprovação sofisticados

Os usuários podem optar por esperar a execução do SmartResponse até que um técnico de incidentes ou uma cadeia de aprovação formal possa verificar as ações. Com o Smart**Response**, os usuários podem implementar cenários de aprovação sofisticados como uma pré-condição para a execução. A LogRhythm também oferece suporte para cadeias de aprovação mais sofisticadas, incluindo aprovações de múltiplas partes de diferentes grupos quando forem necessárias aprovações entre diversas organizações.

Opções de execução flexíveis

O Framework de Automação Smart**Response** da LogRhythm oferece suporte para diversas opções de execução de ações:

- **Execução de cadeia completa:** Configure as ações do Smart**Response** para serem executadas de forma completamente automatizada sem aprovação. Esta capacidade acelera a contenção de comprometimentos, neutralizado ameaças de alto risco em segundos.
- **Execução de clique único:** Execute uma ação manualmente. O Framework de Automação Smart**Response** da LogRhythm permite uma execução instantânea de clique único das respostas, de dentro da interface do usuário da LogRhythm.
- **Execução remota de System Monitor:** Inicie ações em áreas remotas sobre redes díspares que não podem ser acessadas diretamente através de roteamento IP. O Smart**Response** oferece essa capacidade com respostas que podem ser transmitidas e executadas localmente nos agentes do System Monitor. Assim, a execução remota do Smart**Response** possibilita uma capacidade de resposta a incidentes distribuída e verdadeiramente global.

Auditoria completa e responsabilização

Em geral, os processos de resposta a incidentes envolvem muitas pessoas, equipes e tecnologias diferentes. Com o Smart**Response**, a LogRhythm monitora e faz o log de toda a atividade conduzida para conter e mitigar o comprometimento. Isso elimina o incômodo de capturar e consolidar manualmente as informações de resposta a incidentes, incluindo aprovações e notificações. Capturar trilhas de auditoria ajuda a organização a refinar seus processos de resposta a incidentes, comunicar-se com a gestão e desenvolver os controles de conformidade.

Tire o máximo proveito dos investimentos existentes

O Framework de Automação Smart**Response** da LogRhythm permite que os usuários se integrem facilmente com as tecnologias de segurança atuais e futuras. Ele oferece amplo suporte do fornecedor, para que os usuários possam responder em toda a rede, independentemente dos dispositivos de segurança, infraestrutura de TI, redes, sistema e aplicações implementados.

Casos de uso

As equipes de resposta a incidentes são capacitadas com plug-ins pré-preparados e personalizáveis, que podem reduzir o tempo de resposta de dias para minutos. Entre os casos de uso do Smart**Response**, estão:

- **Quarentena de ponto de extremidade:** Identifique a porta de rede onde um dispositivo suspeito está localizado e desative a porta/dispositivo.
- **Suspensão de usuários:** Se um comprometimento de conta for detectado, bloqueie o acesso do usuário — independentemente do dispositivo que ele utilizar.
- **Coleta de dados de máquina:** Em caso de malware, o SmartResponse pode coletar dados forenses do ponto de extremidade suspeito.
- **Suspensão do acesso à rede:** Se houver exfiltração de dados, a equipe de resposta a incidentes poderá encerrar a conexão atualizando a lista de controle de acesso utilizada pelos firewalls da empresa.
- **Matar processos:** Se uma equipe detectar processos desconhecidos ou constantes da lista negra em dispositivos críticos, o SmartResponse poderá matar o programa em execução específico.