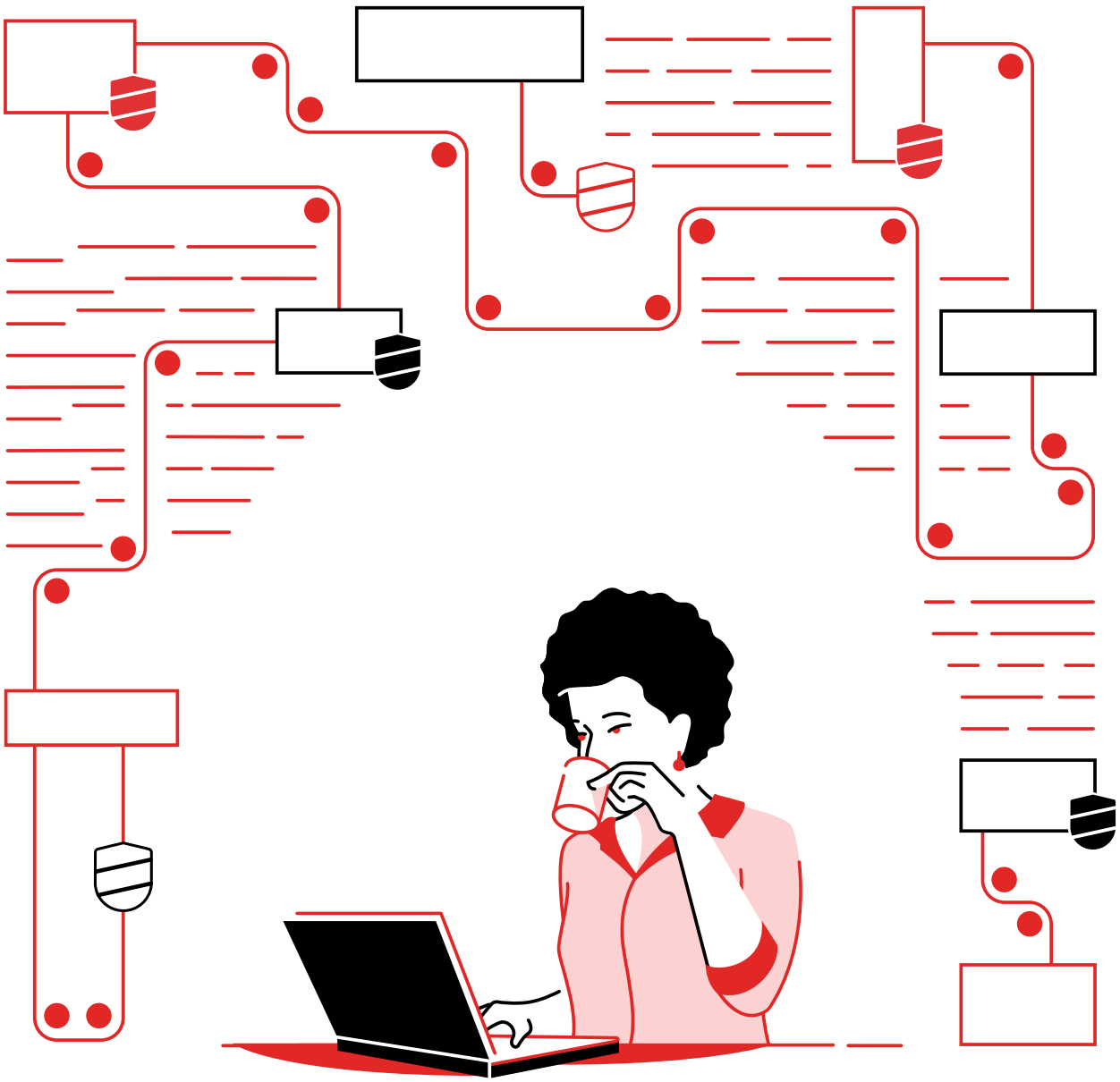
Simplifique seu centro de operações de segurança

Ganhe velocidade, tempo e segurança com uma plataforma de automação unificada



Red Hat

Conteúdo

Segurança da TI: uma grande preocupação

A segurança é uma questão de grande importância para a maioria das organizações. De fato, 33% dos CEOs estão extremamente preocupados com as ciberameaças.[1] E esta preocupação não é infundada: 32% das organizações já sofreram grandes ciberataques nos últimos dois anos.[2]

Proteger sua organização é uma tarefa crítica e desafiadora. As equipes de segurança precisam projetar, manter, gerenciar e adaptar ambientes complexos usando várias ferramentas e serviços de diferentes fornecedores que, muitas vezes, concorrem uns com os outros. Como novas opções surgindo todos os anos, as equipes precisam pesquisar, avaliar e integrar novas soluções continuamente, de acordo com as mudanças no cenário de segurança.

Além disso, a quantidade, a gravidade e o prejuízo causado pelas violações de segurança continuam a crescer. Atualmente, a probabilidade de ocorrer uma violação de segurança nos próximos dois anos é de 29,6%, ante 22,6% em 2014.[3] De 2018 a 2019, o número médio de registros envolvidos em cada violação de dados aumentou em 3,9%.[3] E o prejuízo médio relacionado a uma violação de segurança subiu para US$ 3,92 milhões em 2019.[3]

A maioria das organizações cuida de suas operações de segurança de forma manual. As tarefas relacionadas à segurança podem ser lentas, tediosas e suscetíveis a erros quando a intervenção humana é necessária. E isso deixa as equipes de segurança sobrecarregadas. Elas precisam lidar com um número cada vez maior de alertas de ameaças gerados por várias ferramentas. Na realidade, 60% das equipes de segurança recebem mais de cinco mil alertas por dia, enquanto 16% recebem mais de 100 mil.[4]

E, com o aumento de tamanho e complexidade das infraestruturas, torna-se ainda mais difícil identificar e verificar todas as vulnerabilidades e violações reportadas. As ferramentas de segurança, em sua maioria, não podem ser integradas umas às outras, o que gera mais trabalho manual para a equipe de segurança. Por isso, a investigação de incidentes e os tempos de resposta estão aumentando. Em 2019, o tempo médio para identificar e conter uma violação de dados era de 279 dias, um aumento de 4,9% em relação a 2018.[3] Além disso, é difícil encontrar novos talentos para expandir as equipes e acompanhar o ritmo das mudanças. Ainda em 2019, 39% das organizações relataram escassez de mão de obra especializada em cibersegurança.[2] Por fim, o orçamento para atividades de cibersegurança é limitado. Apenas 33% das organizações afirmam ter recursos financeiros suficientes para alcançar um nível alto de ciber-resiliência.[5]

Como consequência, apenas 48% dos alertas recebidos são verificados e respondidos pelas equipes de segurança comuns, e só metade das ameaças é corrigida.[4] Por isso, muitas organizações ficam vulneráveis a ataques.

77% das organizações planejam aumentar a automação para simplificar e acelerar o tempo de resposta em seus ecossistemas de segurança.[4]

Impactos da segurança ineficaz

A quantidade, a gravidade e o prejuízo causado pelas violações de segurança continuam a crescer.

US$ 3,92 milhões
é o custo médio de uma violação de dados em 2019[3]

279 dias
é o tempo médio para identificar e conter uma violação de dados em 2019[3]

US$ 1,22 milhão
são economizados quando uma violação é identificada e contida em
200 dias
ou menos[3]

29,6%
é a probabilidade de sofrer uma violação em dois anos[3]

50%
das ameaças reais são corrigidas[4]

1 *PWC, "23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty", 2020.* pwc.com/ceosurvey.
2 *Harvey Nash e KPMG, "CIO Survey 2019: A Changing Perspective", 2019.* home.kpmg/xx/en/home/insights/2019/06/harvey-nash-kpmg-cio-survey-2019.html.
3 *IBM Security, "2019 Cost of a Data Breach Report", 2019.* ibm.com/security/data-breach.
4 *Cisco, "Cisco Benchmark Study: Securing What's Now and What's Next", fevereiro de 2020.* cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html.
5 *Ponemon Institute, patrocinado pelo IBM Security, "The Cyber Resilient Organization", abril de 2019.* ibm.com/account/reg/us-en/signup?formid=urx-37792.

O que é automação da segurança?

É o processo de automação de tarefas manuais associadas à manutenção das medidas de segurança da sua empresa. A automação da segurança inclui várias práticas, divididas em quatro categorias gerais:

Resposta e correção
Atividades orientadas a eventos que envolvem instruções de analistas de segurança, a participação deles ou ambos

Operações de segurança
Atividades diárias orientadas a processos e políticas que as equipes de tecnologia realizam na infraestrutura de segurança

Conformidade
Atividades para manter a infraestrutura em conformidade com as regulamentações e as políticas de segurança

Fortalecimento
Atividades para aplicar políticas de segurança personalizadas à infraestrutura com as metas e os objetivos desejados

Saiba mais sobre conformidade e fortalecimento da segurança

Descubra como a automação pode ajudar na conformidade e no fortalecimento da segurança:

- Aumente a segurança na nuvem híbrida (Ebook)
- Por que automatizar a conformidade e a segurança? (Visão geral)
- Red Hat Services – Automatize os fluxos de trabalho de segurança e confiabilidade (Datasheet)

Este ebook tem como foco a automação das operações de segurança e das atividades de resposta e correção.

Benefícios da automação para as atividades de correção, resposta e operações de segurança

Ganhe mais velocidade e eficiência

Com a automação, você otimiza tarefas e elimina a necessidade de intervenção manual. Isso acelera as operações de segurança e direciona o foco das equipes para iniciativas de alto valor. Além disso, a automação reduz a complexidade da infraestrutura de TI: 40% das organizações com alto índice de automação afirmam ter a quantidade certa de tecnologias e soluções de segurança.[6]

Aumente a segurança em escala

Ao usar a automação na sua infraestrutura de segurança, você melhora a consistência e adota uma abordagem de proteção mais completa. Cada membro da equipe pode gerenciar mais ferramentas, dispositivos e sistemas, possibilitando a execução em escala. A automação também reduz os riscos de erros humanos e aumenta a precisão dos processos.

Reduza riscos e prejuízos

As organizações que têm um nível alto de automação estão melhor preparadas para evitar interrupções e incidentes de segurança.[6] Implantar a automação da segurança totalmente reduz em 95% o prejuízo médio de uma violação.[7] Por isso, 52% das organizações já implantaram algum tipo de automação, enquanto 36% planejam fazer isso nos próximos 24 meses.[7]

6 *Ponemon Institute, patrocinado pela IBM Security, "The Cyber Resilient Organization", abril de 2019.* ibm.com/account/reg/us-en/signup?formid=urx-37792.

7 *IBM Security, "2019 Cost of a Data Breach Report", 2019.* ibm.com/security/data-breach.

Automação integra processos, sistemas e ferramentas de segurança

Use uma plataforma consistente e flexível para unificar equipes, processos e ferramentas

Uma plataforma de automação pode servir como uma camada de integração entre suas equipes de segurança, suas ferramentas e processos. Com uma plataforma flexível e interoperável, é possível:

- Conectar equipes, ferramentas e sistemas de segurança.
- Coletar e direcionar informações de sistemas a locais e ambientes predefinidos com rapidez e sem intervenção manual.
- Alterar e propagar configurações rapidamente em interfaces centralizadas.
- Criar, manter e acessar conteúdos de automação personalizado relacionados às suas ferramentas e processos de segurança.
- Executar ações automatizadas em várias ferramentas de segurança quando uma ameça for detectada.

Com o uso de uma plataforma de automação e linguagem consistentes na organização, você aprimora a comunicação e a colaboração. Quando todas as soluções em um portfólio de segurança são automatizadas por meio de uma mesma linguagem, analistas e operadores podem executar várias ações em diferentes soluções com mais rapidez, aumentando a eficiência geral da equipe de segurança. E, com uma linguagem e framework comuns, as equipes de TI e de segurança compartilham designs, processos e ideias internamente ou com a organização com mais facilidade.

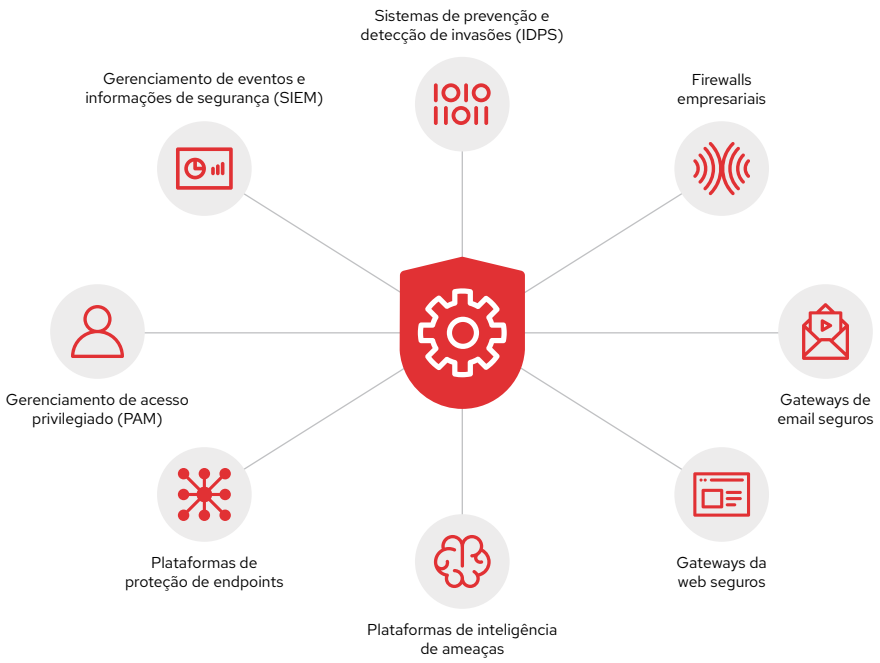


Figura 1. Uma plataforma de automação conecta equipes, ferramentas e sistemas de segurança.

Equipes + processos + plataforma = sucesso da automação

Aproveitar todas as vantagens da automação requer muito mais do que apenas uma ferramenta: é necessário pensar nas equipes, nos processos e na plataforma.

- **Equipes:** a parte fundamental de qualquer iniciativa empresarial. Ao incentivar a participação interna e entre as equipes, os funcionários compartilham ideias e colaboram de maneira mais eficaz.
- **Processos:** são o que movem os projetos do início ao fim dentro da organização. É essencial ter processos bem definidos e documentados para realizar uma automação eficaz.
- Plataforma de **automação:** Oferece os recursos para criar, executar e gerenciar todos os ativos da automação. Em comparação com ferramentas de automação simples, uma plataforma de automação proporciona à organização uma base unificada para a criação, implantação e compartilhamento consistente de conteúdo e conhecimento relacionado em escala.

Leia o ebook

Jornada da automação da segurança

Automatizar qualquer aspecto da sua organização não é um processo instantâneo nem uma proposta radical do tipo "ou tudo ou nada". A automação da segurança é uma jornada. De acordo com as necessidades, cada organização possui um ponto de partida e de chegada diferentes. Essas necessidades também determinam o caminho que as organizações seguirão. Mesmo assim, seja qual for o seu estágio nesta jornada, até mesmo pequenos esforços de automação da segurança podem gerar benefícios.

Avalie o nível de maturidade da sua automação da segurança

A maioria das organizações se enquadra em um dos três estágios principais de maturidade da automação da segurança. Ao determinar o estágio atual da sua organização, você adota os processos e as ferramentas certas no momento correto, alcançando mais sucesso nessa jornada.

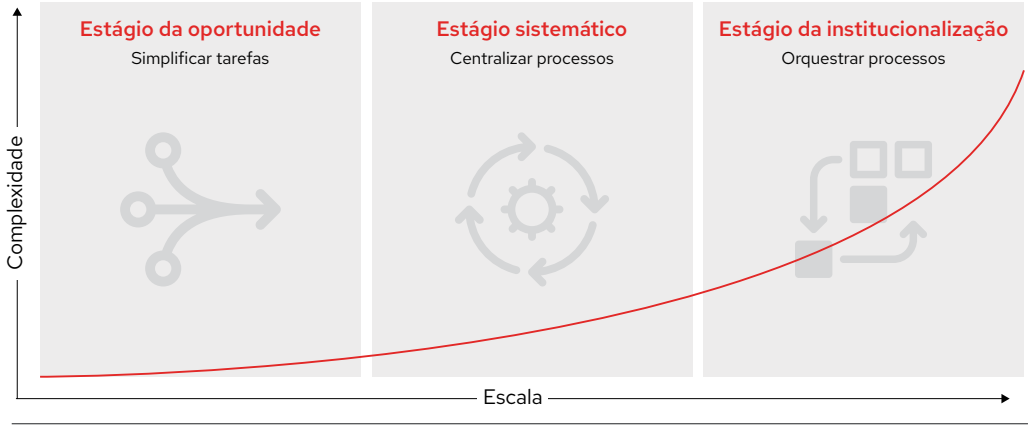


Figura 2. *Estágios da maturidade da automação da segurança*

Estágio 1: Oportunidade

Neste estágio, o foco é automatizar as operações de segurança para economizar tempo. Os objetivos comuns incluem padronizar as ações de segurança em tecnologias e dispositivos similares, além de otimizar as tarefas manuais realizadas em soluções de fornecedores diferentes.

Estágio 2: Sistemático

Neste estágio, o foco é adotar um conjunto coeso de serviços e ferramentas de operações de segurança para aprimorar os processos e aumentar a eficiência. Os objetivos comuns incluem a construção de processos de segurança em fluxos de trabalho de nível superior e a centralização dos processos de resposta de segurança.

Estágio 3: Institucionalização

Neste estágio, o foco é impulsionar a colaboração e integrar a segurança na organização. Os objetivos comuns incluem criar fluxos de trabalho automatizados e programáticos que envolvam todos os aspectos da segurança, além de integrar as tecnologias de TI e proteção.

Leia o blog post

Integrações e casos de uso

Defina seu caminho para a automação da segurança

Casos de uso comuns e de alto nível para a automação da segurança

Cada um destes casos de uso pode servir como ponto de partida para sua jornada de automação da segurança. O segredo é começar aos poucos, com simplicidade, e aumentar a intensidade ao longo do tempo.

Aprimorar a investigação de incidentes

Investigar incidentes e alertas de segurança envolve a coleta de informações de vários sistemas de proteção para avaliar se algum evento real ocorreu. Geralmente, você coleta as informações por meio de diversas interfaces de usuário, emails e ligações telefônicas. A ineficiência desse processo pode atrasar as medidas de correção de ameaças. Isso deixa sua empresa vulnerável e aumenta os possíveis prejuízos associados a uma violação. Com a automação, você coleta informações programaticamente nos sistemas de segurança. Além disso, ela oferece suporte ao aprimoramento sob demanda das atividades de triagem realizadas por meio de sistemas de gerenciamento de eventos e informações de segurança (SIEM). Assim, os alertas e os incidentes são avaliados e respondidos com mais rapidez.

À procura de ameaças

A procura de ameaças envolve a identificação e investigação de ameaças potenciais à segurança de forma proativa. Assim como no processo de investigação de incidentes, as equipes coletam e enviam informações entre muitos sistemas de forma manual. Com a automação, você personaliza e otimiza o controle de assinaturas, as pesquisas de correção e os alertas para avaliar mais rapidamente as possíveis ameaças. Também é possível criar e atualizar automaticamente as regras de sistema de detecção de invasões (IDS) e as consultas de correlação de SIEM, aprimorando a descoberta de ameaças. Assim, é possível atualizar os recursos de segurança da organização com mais frequência e eficiência para oferecer mais proteção aos negócios.

Resposta a incidentes

Responder aos incidentes é interromper a continuação de uma violação. Depois de descobrir uma violação, a equipe de segurança precisa responder a ela com rapidez e em escala para poder contê-la. No entanto, as atividades de resposta costumam incluir muitas tarefas manuais, o que diminui o tempo de correção e deixa sua organização vulnerável por mais tempo. Com a automação, você codifica as ações em playbooks reproduzíveis e pré-aprovados para acelerar a resposta. É possível agilizar tarefas como o bloqueio de domínios ou endereços IP invasores. Isso possibilita o tráfego seguro, interrompe credenciais corrompidas e isola cargas de trabalho suspeitas para futura investigação, diminuindo o dano associado ao incidente.

A integração é essencial

Abordagens unificadas exigem a integração da plataforma de automação e das tecnologias de segurança. Tipos essenciais de integração incluem:

- **Firewalls:** controlam o tráfego entre as redes, protegendo as aplicações expostas à Internet. Com a automação, você acelera as alterações em configurações de registros e políticas.
- **Sistemas de prevenção e detecção de invasões (IDPS):** Monitoram o tráfego de rede para encontrar atividades suspeitas, emitir alertas de ameaça e bloquear as invasões. Com a automação, você simplifica o gerenciamento de registros e regras.
- **Sistemas de gerenciamento de eventos e informações de segurança:** coletam e analisam eventos de segurança para detectar ameaças e responder a elas. Com a automação, você tem acesso programático a fontes de dados.
- **Ferramentas de gerenciamento de acesso privilegiado (PAM):** Monitoram e gerenciam as contas e os acessos que têm privilégios. Com a automação, você otimiza o gerenciamento de credenciais.
- **Sistemas de proteção de endpoints:** monitoram e gerenciam os dispositivos para aumentar a segurança deles. Com a automação, você simplifica as tarefas comuns de gerenciamento de endpoints.

Saiba mais

Simplifique seu centro de operações de segurança com o Red Hat Ansible Automation Platform

Há muitas soluções de automação disponíveis, mas nem todas incluem os recursos necessários para você realizar uma automação da segurança eficaz. Escolha plataformas de automação que ofereçam:

- **Linguagem de automação acessível e universal.** Com uma linguagem fácil de entender e escrever, é possível documentar e compartilhar informações entre membros da equipe de segurança que tenham níveis diferentes de especialização no domínio.
- **Abordagem open source e imparcial.** Para oferecer o máximo de eficiência, a plataforma de automação precisa ter interoperabilidade com todo o ecossistema do fornecedor e a infraestrutura de segurança.
- **Design modular e extensível.** Com uma plataforma modular, é possível implantar a automação em etapas. Além disso, a extensibilidade oferece suporte à adoção de ferramentas adicionais de outros fornecedores, agora ou futuramente, conforme necessário.

Aumente a segurança da sua organização com a Red Hat

O **Red Hat® Ansible® Automation Platform** é a base para criar e executar serviços de automação em escala. Ele oferece todas as ferramentas e funcionalidades necessárias para automatizar a segurança. A solução combina uma linguagem de automação simples e fácil de ler com um ambiente de execução confiável e agragável, além de recursos de compartilhamento e colaboração voltados para a segurança. Por se tratar de uma base open source, você conecta e automatiza quase tudo na infraestrutura de TI e segurança, criando uma plataforma comum que possibilita a participação e o compartilhamento em toda a organização. O Red Hat Ansible Automation Platform também gera resultados comprovados em outras áreas, como DevOps e operações de TI e rede.

A plataforma fornece **conjuntos Ansible compatíveis e voltados para a segurança**, como módulos, funções e playbooks. Com estes recursos, você coordena as atividades de várias classes de soluções de segurança para ter uma resposta mais unificada às ciberameaças e às operações de segurança:

- Encadeamento de fluxos de trabalho e playbooks para ter capacidade de reutilização modular.
- Consolidação e centralização de registros.
- Suporte a controles de acesso e serviços de diretório locais.
- Integração de aplicações externas usando interfaces de programação de aplicações (APIs) RESTful.

O Red Hat Ansible Automation Platform também inclui ferramentas e recursos para otimizar a automação. O **Automation Analytics** oferece insights sobre como a organização usa a automação. Com o **Automation Hub**, a equipe tem acesso a conteúdo certificado sobre automação por meio de um repositório centralizado. E o **Content Collections** otimiza o gerenciamento, a distribuição e o uso dos recursos de automação.

Obtenha ajuda dos especialistas

Com a Red Hat, você acelera a implantação da automação.

- O programa **Red Hat Services Journey: Automation Adoption** oferece um framework para gerenciar a jornada de adoção da automação por toda a organização.
- O **Red Hat Training and Certification** oferece certificação e treinamento prático para aumentar a eficiência da automação.
- O **Red Hat Support** trabalha com você para possibilitar o sucesso da sua jornada da TI. Nosso premiado serviço de suporte web[8] oferece acesso a práticas recomendadas, patches e alertas de segurança, documentações e atualizações. Você também pode trabalhar com um gerente técnico de contas ou engenheiro de suporte para solucionar problemas e receber orientações especializadas.
- As **coleções de conteúdo certificadas por parceiros** permitem que você automatize prontamente hardware e software de uma ampla seleção de fornecedores. Esse conteúdo confiável e pré-criado sobre automação está disponível pelo Automation Hub e é compatível com o parceiro e com a Red Hat.

8 Prêmios e reconhecimentos do Red Hat Customer Portal, **access.redhat.com/recognition**.

A automação na prática

Red Hat Ansible Automation Platform agrega comprovadamente valor aos negócios

O Red Hat Ansible Automation Platform oferece uma maneira mais eficiente e otimizada de automatizar seu centro de operações de segurança. O valor agregado aos negócios é comprovado por estudos de analistas feitos em organizações que usam o Red Hat Ansible Automation Platform. A IDC perguntou a diversos tomadores de decisões quais foram suas experiências com o Red Hat Ansible Automation Platform. As respostas indicam que todas as organizações obtiveram produtividade, agilidade e benefícios operacionais significativos por meio da automação.

de ganho em eficiência e produtividade das equipes de segurança de TI[9]

de ganho em eficiência na mitigação dos incidentes de segurança[9]

de ganho em eficiência na aplicação de patches de segurança[9]

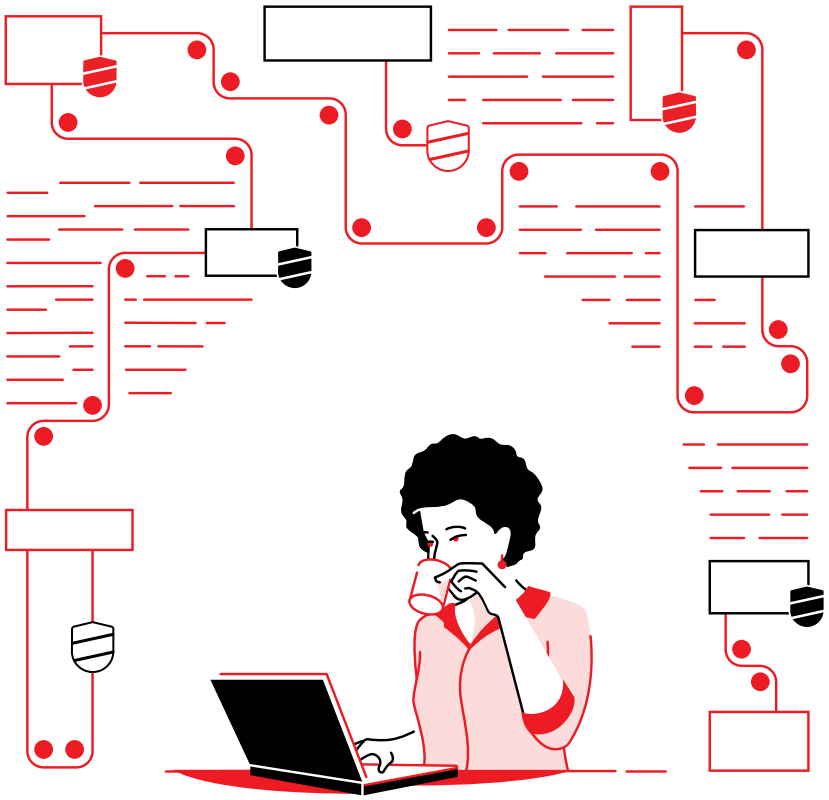
"O Red Hat Ansible [Automation Platform] é uma solução incrível que unificou nossas equipes de TI. As equipes de servidor, segurança, rede e banco de dados podem trabalhar em camadas separadas e usar o Red Hat Ansible Automation para criar os próprios playbooks."[9]

Leia o relatório de analistas

9 *Whitepaper da IDC patrocinado pela Red Hat. "Red Hat Ansible Automation Improves IT Agility and Time to Market", junho de 2019.* **https://www.redhat.com/pt-br/resources/business-value-red-hat-ansible-automation-analyst-paper.**

Pronto para simplificar seu centro de operações de segurança?

Com a automação, você identifica e responde às crescentes ameças de segurança em escala e com rapidez. A Red Hat ajuda você a proteger seus negócios ao conectar suas equipes de segurança, ferramentas e processos a uma plataforma de automação consistente e colaborativa.



Saiba como automatizar a segurança com o Red Hat Ansible Automation Platform: **red.ht/automate-security**

F24343_0720_KVM

Red Hat