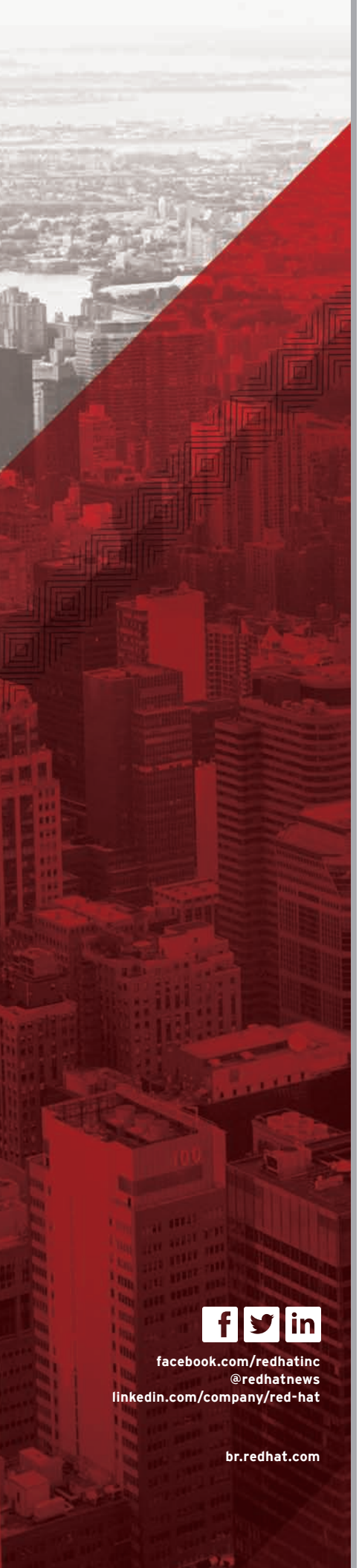

WHITEPAPER

COMO A SEGURANÇA E A INOVAÇÃO SE ENCONTRAM NA RED HAT

Gordon Haff

RESUMO EXECUTIVO

A Red Hat desenvolve softwares em colaboração com clientes de uma grande variedade de setores, incluindo serviços financeiros e governamentais. Isso não resulta somente em inovação, mas também fornece uma orientação valiosa para as decisões relacionadas à segurança de processos, serviços ou recursos de produtos. Essa abordagem torna o software de infraestrutura da Red Hat®, como o Red Hat Enterprise Linux®, e as plataformas de aplicativos, como o Red Hat JBoss Enterprise Application Platform, partes fundamentais dos negócios em alguns dos setores mais regulados e sensíveis.

O ambiente de ameaças dos dias atuais, significa que a segurança e a operacionalização por toda a sua infraestrutura de TI, incluindo ambientes de cloud híbrida, está mais importante do que nunca.

Neste whitepaper, abordaremos o cenário atual de segurança e como você pode se tornar um parceiro da Red Hat para atender às metas de segurança, gerenciamento de risco e conformidade. Este documento também inclui a abordagem de exigências comuns para mitigação de vulnerabilidades, implementação de gerenciamento de configuração e estabelecimento de controles de acesso. Embora essas exigências não sejam novidade, no mundo digital de hoje, elas são amplificadas em um número maior e mais rápido de ameaças, arquiteturas de TI que são abertas ao mundo e para infraestrutura que é tanto heterogênea quanto híbrida.

Assim, discutiremos a abordagem da Red Hat quanto à segurança e ao trabalho realizado em comunidades upstream para que, de maneira proativa, as vulnerabilidades possam ser corrigidas antes mesmo de se transformarem em problemas. Falaremos também sobre o Red Hat Insights, um serviço de gerenciamento de subscrição que, proativamente, identifica e soluciona os possíveis problemas técnicos que possam ocorrer em seus sistemas. Discutiremos o papel da automação na operacionalização da segurança e da documentação de processos em códigos com o uso de produtos como o Ansible Tower e o Red Hat Satellite. Abordaremos a função do DevOps na habilitação de um processo de TI mais moderno e ágil para a aplicação de atualizações de código. Veremos, também, como o Red Hat CloudForms fornece um ponto centralizado de controle baseado em políticas sobre ambientes de TI híbridos.

Entretanto, a história da segurança dos dias atuais não é referente a recursos específicos de segurança ou de soluções que fornecem um resultado mágico. Mas sim, sobre uma visão mais ampla da segurança (que realmente significa gerenciamento de risco, conformidade e governança) e sua operacionalização, de maneira que faça sentido aos negócios. E esse será o verdadeiro foco.

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

br.redhat.com

"Os projetos de software open source que incentivam testes de desenvolvimento, estão constantemente aprimorando a qualidade do software, e consequentemente, aumentando o nível de qualidade de todo o setor."

ZACK SAMOCHA
DIRETOR SÊNIOR DE PRODUTOS
COVERITY

AS CONSTANTES MUDANÇAS NA SEGURANÇA

O muro e o fosso de um castelo medieval significavam uma barreira formidável a possíveis invasores. Porém, era uma barreira que seria eficiente somente se os possíveis invasores não conseguissem violar um ponto fraco ou aplicar uma nova tática. A segurança tradicional de TI é, primariamente, baseada na criação e proteção de um perímetro de hardware, aplicativos e dados locais. Ela não ignora ameaças internas que surgem de malícias ou erros. Ela se baseia, quase totalmente, em firewalls, sistemas de detecção de invasores e controles de acesso, visando manter o "vilão" do lado de fora dos portões.

Hoje em dia, a segurança da informação deve adaptar-se ao cenário em constante mudança. Seja ao fornecer a clientes e parceiros acesso a determinados sistemas e dados, permitir que funcionários utilizem seus próprios smartphones e notebooks, utilizar aplicativos de provedores de software como serviço (SaaS) ou obter vantagem de modelos de preço do tipo pague o que usar de provedores de cloud pública. Não há mais um perímetro único. Fazer o uso máximo dos ativos de informações de uma organização, poderá exigir que tais informações sejam compartilhadas com partes terceirizadas autorizadas. A conformidade regulatória e a alta intensidade e sofisticação de ataques cibernéticos, destacam ainda mais a necessidade de uma estratégia de segurança de TI mais profunda e multifacetada do que a norma tradicional na maioria das organizações.

Observamos essa tendência tanto na pesquisa de analistas quanto nas conversas com os clientes. Por exemplo, o fato de que a segurança está quase sempre no topo da lista de preocupações das pesquisas realizadas sobre a adoção da cloud pública, não é uma novidade para ninguém. Porém, não são os aspectos familiares à segurança do sistema, como acesso e controle ou firewalls configurados inapropriadamente, que causam tal preocupação. Em vez disso, jurisdição de dados, auditabilidade, conformidade regulatória e criptografia verificável de ponta a ponta, estão no topo da lista. E essas são exatamente as áreas sobre as quais o provedor de cloud tem alguma responsabilidade direta.

A organização responsável por executar a carga de trabalho, também tem um papel importante a desempenhar no estabelecimento da origem do software, na compreensão dos regulamentos e das certificações, no fornecimento de controles e acesso apropriados com base na política, no gerenciamento das relações com o fornecedor e, em geral, no estabelecimento de processos formais e reproduzíveis para segurança e resposta a incidentes.

PENSANDO SOBRE A SEGURANÇA

Este documento menciona várias tecnologias e recursos relacionados à segurança da informação. Porém, a implementação de defesa, detecção e dissuasão eficazes não significa utilizar um produto ou componente em particular. Mas sim, estabelecer uma base sólida que permita a automação dos processos dos negócios, institucionalização de boas práticas e resolução de problemas de maneira eficiente, quando estes ocorrerem. Como observado pelo especialista em segurança, Bruce Schneier: "A segurança não precisa ser perfeita, porém os riscos devem ser gerenciáveis".[1]

O CIA Triad, um modelo conceitual comum de práticas de segurança, foca em três aspectos de proteção (primariamente, de dados):

1. Confidencialidade – restringir o acesso aos dados, disponibilizando-os somente aos indivíduos autorizados
2. Integridade – garantir que os dados não sejam alterados ou excluídos por uma parte não autorizada
3. Disponibilidade – garantir que os dados estejam disponíveis quando necessário

1 https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

"A crença de que os provedores de cloud são totalmente responsáveis pela segurança de seus clientes desencoraja as organizações a garantir aos seus funcionários o uso apropriado dos serviços de cloud".

GARTNER
"AS CLOUDS SÃO SEGURAS: VOCÊ ESTÁ UTILIZANDO-AS DE MANEIRA SEGURA?"
SETEMBRO DE 2015
G00281279

Profissionais de segurança e organizações, como o Instituto Nacional de Padrões e Tecnologia dos EUA (US National Institute of Standards and Technology)[2], desenvolveram modelos mais complexos que incluem aspectos adicionais de segurança, como avaliação de risco, adequação, posse física, legalidade e utilidade. Um tratamento completo das melhores práticas de segurança vai além do escopo deste documento. Neste documento, iremos focar em novas e relevantes tecnologias e práticas relacionadas a arquiteturas híbridas, infraestruturas nativas na cloud, desenvolvimento de aplicativos por meio de abordagens DevOps e respostas às vulnerabilidades de segurança de software open source corporativo.

É uma questão da seriedade e sofisticação dos ataques, em que posições como a de diretor estratégico de segurança da informação (chief information security officer), estão se tornando cada vez mais comuns e, portanto, os planos de resposta a incidentes estão começando a se parecer mais com aqueles associados ao combate real. E há diversos motivos para isso.

O primeiro é que a segurança deve ser abordada no contexto dos negócios, e não somente como um problema de tecnologia. Isso significa, por exemplo, definir a propensão dos negócios aos riscos em termos de tolerância de perda. Um emissor de cartões de crédito sabe que terá perdas em razão de fraude. A prevenção completa de fraudes tornaria o uso de cartões de crédito em algo tão oneroso que ninguém faria seu uso. Em vez disso, o emissor do cartão aplica controles suficientes para manter as perdas em um nível aceitável, enquanto minimiza o impacto geral sobre a experiência dos usuários.

Outro motivo para a segurança ser levada mais a sério é que, assim como em casos de incêndios ou acidentes de carro, cada minuto é crítico. Funções, responsabilidades e processos devem ser estabelecidos com antecipação. A especialidade técnica é importante, mas ter planos de comunicação claros, visando o compartilhamento de informações com os indivíduos possivelmente afetados pelo incidente e com grupos mais amplos, como a imprensa, é tão importante quanto.

INTRODUÇÃO À SEGURANÇA

A segurança começa com um sonho de ser estável e seguro, mas é, geralmente, impulsionada pelo medo, preocupação e necessidade de evitar que os ativos sejam comprometidos durante seu ciclo de vida. Quaisquer que sejam as complexidades que podem ser impostas pelas arquiteturas de TI e pelo ambiente de ameaça externa dos dias de hoje, ainda é apropriado começar com o uso de tecnologias e práticas que vem sendo testadas ao longo do tempo e que podem ser estendidas para a realidade atual.

Open source é um exemplo disso. O modelo de desenvolvimento aberto permite que setores inteiros cheguem a um comum acordo sobre os padrões a serem utilizados, além de incentivarem seus melhores desenvolvedores a continuamente testarem e aprimorarem as tecnologias. O desenvolvimento de software em colaboração com usuários de diferentes setores, incluindo serviços governamentais e financeiros, fornece um feedback valioso que guia as discussões relacionadas à segurança e implementações de recursos de produtos. Ninguém pode resolver problemas de segurança de TI sozinho. A colaboração junto às comunidades para solução de problemas é o futuro da tecnologia.

O Linux tem sido o beneficiário de uma ampla variedade de tecnologias relacionadas à segurança e desenvolvidas a partir do modelo open source. Entre elas, estão:

- Um firewall gerenciado dinamicamente.
- SELinux para controles de acesso obrigatórios.
- Uma ampla variedade de recursos do espaço do usuário e fortalecimento do kernel.
- Gerenciamento de identidade e controle de acesso.
- Hashes de senha baseado em SHA-512.
- Criptografia do sistema de arquivos.

2 Publicação especial NIST 800-27 Revisão A

Além disso, o processo de desenvolvimento open source significa que, quando vulnerabilidades são encontradas, toda a comunidade de desenvolvedores e fornecedores podem trabalhar em conjunto e de maneira coordenada para a atualização do código, comunicados de segurança e documentação.

O Red Hat Enterprise Linux é a base da TI em alguns dos setores mais regulados e sensíveis. A sua segurança open source incorporada avança de maneira previsível e consumível. Esses mesmos processos e práticas se aplicam a infraestruturas da cloud híbrida, conforme a função do sistema operacional evolui e se expande para incluir novos recursos, como o container Linux. Além disso, os componentes são reutilizados na forma de microsserviços e outras arquiteturas com baixo acoplamento que interagem por meio das interfaces de programação de aplicativos (APIs). Assim, a manutenção da confiança sobre a origem desses componentes e suas dependências (ao criar aplicativos) se torna ainda mais importante.

OPERACIONALIZAÇÃO DA SEGURANÇA

Historicamente, a segurança era frequentemente abordada como uma função centralizada. Uma organização pode ter estabelecido uma única fonte confiável para usuário, máquina e identidades de serviço sobre todo um ambiente e descrito quais informações estão autorizadas para serem acessadas e quais ações podem ser realizadas.

Hoje em dia, a situação é mais complicada. Ainda é importante ter políticas de controle de acesso que governam as identidades do usuário, delegando autoridade conforme apropriado e estabelecendo relações de confiança com outros repositórios de identidade conforme necessário. Porém, os componentes de aplicativos que são executados no Linux ou em outros ambientes operacionais podem ser submetidos a múltiplos sistemas de autorização e listas de controle de acesso.

Conhecimento e controle sobre tais ambientes complexos, híbridos e heterogêneos, são importantes. Por exemplo, o monitoramento em tempo real e a aplicação de políticas não podem somente abordar questões de desempenho e confiabilidade antes de os problemas se tornarem sérios, mas também devem detectar e mitigar possíveis questões de conformidade. Uma automação realizada dessa maneira, reduz a quantidade de carga de trabalho exigida de um administrador de sistemas. Porém, também é uma maneira de documentar processos e reduzir procedimentos manuais propensos a erros. Erro humano é constantemente citado como a maior causa de brechas de segurança e interrupções.

O monitoramento operacional e a remediação devem ser mantidos durante todo o ciclo de vida de um sistema. Isso começa a partir do provisionamento. Assim como com outros aspectos do gerenciamento contínuo de sistemas, é importante manter um histórico completo de relatórios, auditorias e alterações.

A necessidade de políticas e planos de segurança não termina quando um aplicativo é descontinuado. A propriedade e as políticas pertencentes aos dados associados a um aplicativo devem ser bem compreendidas, de maneira que as etapas apropriadas possam ser seguidas para atender às exigências de retenção e de sanitização das informações de identificação pessoal (PII).

Com as instâncias de aplicativos tradicionais de longa duração, a manutenção de uma infraestrutura segura também significava analisar e corrigir manualmente desvios de configuração para aplicar o estado final do host desejado. Em geral, essa ainda é uma exigência importante. Entretanto, com o aumento do papel desempenhado pelos altos números de instâncias "imutáveis" de curta duração em ambientes nativos da cloud, é igualmente importante estabelecer a segurança em primeiro lugar. Por exemplo, você pode estabelecer e aplicar políticas baseada em regra sobre serviços habilitados nas camadas de um conjunto de software baseado em containers.

A adoção de uma abordagem de gerenciamento de risco de segurança, vai além da aplicação de um conjunto eficaz de tecnologias. Também exige a consideração da cadeia de fornecimento do software e a implementação de um processo de rápida resposta aos problemas.

Por exemplo, é importante validar que os componentes do software são originados de uma fonte de confiança. O container, um modelo ágil e simplificado de entrega de aplicativos, é um exemplo em questão. O container é uma maneira simples e eficiente de montar, distribuir e implantar o software. Essa mesma simplicidade poderá se tornar em um problema se o departamento de TI não garantir que o software seja originado de uma fonte de confiança e que o mesmo atende aos mais altos padrões de segurança e capacidade de suporte.

Como descrito anteriormente, a reposta a incidentes vai além do código de patches. Porém, uma plataforma de desenvolvimento de software ágil e um processo com testes integrados, ainda é uma parte importante da rápida resolução de problemas (bem como a redução da quantidade de código com bugs que entra em produção). Um canal de integração contínua/entrega contínua (CI/CD) que faz parte de um processo de entrega de software DevOps iterativo e automatizado, significa que elementos de código modular podem ser sistematicamente testados e liberados em tempo hábil. Além disso, o desdobramento explícito do processo de segurança sobre o fluxo de trabalho de implantação do software, torna a segurança uma parte constante do desenvolvimento do software—e não somente um bloqueio no caminho de produção.

GOVERNANÇA E CONFORMIDADE SOBRE CLOUD HÍBRIDAS

Embora o medo em relação à falta de segurança em cloud pública possa ser ingênuo, as clouds públicas e híbridas introduz riscos, considerações de conformidade e desafios que são diferentes das preocupações sobre datacenters locais tradicionais. É importante compreender sobre quais áreas você ainda tem responsabilidade ao usar clouds públicas. Por exemplo, no caso de infraestrutura como serviço (IaaS), é preciso desempenhar os mesmos cuidados quanto ao fornecimento e manutenção do sistema operacional e de aplicativos que seriam aplicados quando executados localmente.

Uma variedade de estruturas pode ajudar os executivos e arquitetos de TI a avaliar e eliminar o risco associado ao uso de provedores de cloud pública. Um bom exemplo é o Cloud Controls Matrix (CCM), da Cloud Security Alliance (CSA).[3]

O CSA CCM fornece uma estrutura de controles entre 16 domínios, incluindo:

- Gerenciamento da continuidade dos negócios e resiliência operacional.
- Gerenciamento de chave e criptografia.
- Gerenciamento de identidade e acesso.
- Segurança mobile.
- Gerenciamento de ameaças e vulnerabilidade.

O CCM v3.0.1 define 133 controles e mapeia a relação entre cada controle e outros padrões, regulamentos e estruturas de controles de segurança aceitos no setor, como ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum e NERC CIP.

3 https://cloudsecurityalliance.org/group/cloud-controls-matrix/

Utilizando o CCM como estrutura de referência, as soluções e as parcerias da Red Hat são mais relevantes nesses domínios:

- Controle de alterações e gerenciamento de configuração.
- Segurança de dados e gerenciamento do ciclo de vida das informações.
- Gerenciamento de chave e criptografia.
- Gerenciamento de identidade e acesso.
- Segurança de virtualização e infraestrutura.
- Interoperabilidade e portabilidade.

A Red Hat também trabalha junto aos parceiros em todas essas áreas e fornece suporte a outros domínios, como gerenciamento de ameaças e incidentes e ao fornecer respostas eficientes e em tempo hábil às vulnerabilidades, conforme estas são descobertas.

O projeto de serviço para entrega através de arquiteturas híbridas também pode ser informado por metodologias de TI mais tradicionais. Por exemplo, a Estratégia de Serviço de Biblioteca de Infraestrutura de TI (ITIL) é um dos cinco módulos do ciclo de vida de ITIL. Ele pode guiar você pela projeção, desenvolvimento e implementação de uma estratégia de provedor de serviço que esteja alinhada à estratégia organizacional. Assim, as práticas de ITIL podem ser utilizadas para ajudar a projetar os serviços completos e apropriados para TI híbrida.

A partir de uma perspectiva de tecnologia, um componente essencial de governança e conformidade é uma plataforma de gerenciamento de cloud (CMP) híbrida baseada em política, como o Red Hat CloudForms. Uma CMP eficiente fornece acesso a catálogos de serviço com provisionamento automatizado de atribuição de funções, aplicação de cotas e chargeback por todas as plataformas de cloud e virtualização. Oferece suporte à orquestração de recursos, automação e tarefas complexas baseada em políticas para ajudar a garantir a disponibilidade e o desempenho do serviço. Tudo isso ajuda o departamento de TI a manter o controle dos aplicativos e a capacidade da infraestrutura.

DOMÍNIO	EXEMPLO DE PRODUTO E CARACTERÍSTICAS
Segurança da interface e do aplicativo	A Red Hat fornece APIs que seguem os padrões do setor. Por exemplo, os produtos do Red Hat JBoss Middleware oferecem suporte a APIs padrão de Java™ SE e Java EE, SAML 2.0 para logon único web e WS-Security para proteção dos serviços web.
Garantia de auditoria e conformidade	Os recursos de auditoria do Red Hat CloudForms, bem como os recursos de registro de uma variedade de produtos, oferecem suporte ao processo de auditoria. A Red Hat também é parceira de empresas que fornecem produtos de registro e análise.
Gerenciamento de configuração e controle de alterações	Tanto o Red Hat Satellite quanto o Ansible Tower fornecem ferramentas de gerenciamento de configuração e provisionamento.
Gerenciamento do ciclo de vida das informações e segurança de dados	Os recursos do Red Hat Gluster Storage, como o arquivamento ativo, ajudam a oferecer suporte ao gerenciamento do ciclo de vida das informações. O Red Hat JBoss Data Grid utiliza autenticação por Java SE e recursos de criptografia para proteger dados confidenciais armazenados em seu datastore distribuído em memória.

DOMÍNIO	EXEMPLO DE PRODUTO E CARACTERÍSTICAS
Gerenciamento de chave e criptografia	Os recursos de criptografia do Red Hat Enterprise Linux incluem hashes de senha baseado em SHA-512, criptografia do sistema de arquivos, além de certificações e melhorias em criptografia NSA Suite B. O OpenJDK, que é incluído, fornece algoritmos de criptografia e interfaces para o Red Hat JBoss Middleware, conforme padronizado pelo Java Community Process.
Gerenciamento de risco e governança	A automação baseada em políticas do Red Hat CloudForms é um exemplo de um recurso que pode ser utilizado pelas organizações para aplicar planos de governança.
Gerenciamento de identidade e acesso	O gerenciamento de identidade centralizado faz parte do Red Hat Enterprise Linux, assim como os controles de acesso obrigatórios fornecidos pelo SELinux. Recursos de autenticação, autorização e auditoria no nível do aplicativo estão disponíveis no Red Hat JBoss Middleware.
Infraestrutura e virtualização	O Red Hat Enterprise Linux, Red Hat Enterprise Virtualization, Red Hat OpenStack® Platform e Red Hat Enterprise Linux Atomic Host fornecem uma infraestrutura robusta e segura.
Interoperabilidade e portabilidade	As soluções da Red Hat seguem padrões abertos, bem como fornecem APIs abertas. Os containers fornecem uma nova abordagem para portabilidade da carga de trabalho entre os ambientes.
Segurança mobile	O Red Hat Mobile Application Platform fornece controle centralizado sobre o gerenciamento de segurança e políticas.
Gerenciamento de incidentes de segurança, e-disc e análise forense da cloud	Quando há vulnerabilidades de segurança, a Red Hat fornece aos clientes meios para uma rápida abordagem dessas vulnerabilidades e proteção de seus sistemas.
Gerenciamento da cadeia de fornecimento, transparência e responsabilidade	A Red Hat ajuda a proteger a cadeia de fornecimento ao assinar digitalmente todos os pacotes lançados (incluindo containers) e distribuí-los através de canais seguros.
Gerenciamento de vulnerabilidade e ameaças	O Red Hat Insights é um serviço hospedado que ajuda a identificar e solucionar, de maneira proativa, os problemas técnicos dos ambientes do Red Hat Enterprise Linux e do Red Hat Cloud Infrastructure. A Red Hat também cria e oferece suporte a definições de patch de Linguagem de Avaliação e Vulnerabilidade Aberta (OVAL), fornecendo versões em formato legível por máquina de nossos comunicados de segurança. O OpenSCAP permite verificar as configurações de segurança de um sistema e analisar o sistema quanto aos sinais de comprometimento por meio do uso de regras baseada em padrões e especificações.

Recursos específicos da Red Hat são mapeados para domínios de segurança CSA (exceto domínios como segurança de datacenter e segurança de recursos humanos, que são primariamente focados nas práticas de segurança física interna da organização).

"O Red Hat CloudForms é como um canivete suíço. Você pode fazer diversas coisas com ele no ambiente de TI, incluindo insights e inteligência na sua infraestrutura. Nós analisamos os números para ver quais recursos foram implantados e quanto tempo levou todo o processo. Percebemos que com a solução da Red Hat, economizamos praticamente dez anos na espera pela entrega dos recursos e quase cinco milhões de dólares em economia de custos desde 2014. Além disso, o Red Hat Insights, nos oferece a possibilidade detectar e solucionar problemas críticos antes que eles ocorram."

JASON CORNELL
GERENTE DE AUTOMAÇÃO DE INFRAESTRUTURA E CLOUD
COX AUTOMOTIVE

COMO A RED HAT PODE AJUDÁ-LO A CRIAR UMA CLOUD SEGURA

Abordamos algumas das áreas de funcionalidade que são importantes para proteger as infraestruturas de cloud híbrida que utilizam soluções Red Hat. Isso inclui:

- Criptografia, controles de acesso obrigatórios (SELinux) e gerenciamento de identidade no Red Hat Enterprise Linux 7.
- Registros granulares, baseado em políticas e alertas visíveis fornecidos pelo Red Hat CloudForms, que permitem uma rápida resposta automatizada entre cargas de trabalho heterogêneas e diferentes tipos de cloud.
- Provisionamento e gerenciamento automatizados fornecidos pelo Ansible Tower e Red Hat Satellite, os quais também monitoram os desvios de configuração e realizam correções conforme necessário.
- Capacidade de utilização do Red Hat JBoss BRMS e Red Hat JBoss BPM Suite para criar fluxos de trabalho que supervisionam e respondem a transações que violam regras de negócios específicas ao domínio.

Por exemplo, o Payment Card Industry (PCI) Data Security Standard (DSS) continua a se desenvolver e exige uma aplicação mais restrita de suas exigências. Conforme as empresas implantam novos aplicativos e soluções modernas de tecnologia, elas devem considerar as ramificações de conformidade dos ambientes compartilhados. O Red Hat CloudForms ajuda os clientes a obter controle do ambiente de virtualização ao criar ou gerenciar ambientes de cloud híbrida ou privada. O Red Hat CloudForms fornece mecanismos robustos para infraestrutura de cloud com controles de gerenciamento de virtualização avançados, recursos de gerenciamento de cloud híbrida ou privada e tecnologias de visibilidade operacional.[4] Isso inclui recursos de registro agregados que permitem segregar, registrar e alocar recursos por usuário, grupo, local ou outros atributos para granularidade de controle alinhada a políticas de Cgroups e SELinux.

Porém, o foco da Red Hat sobre a segurança é mais amplo e profundo do que os investimentos mais significativos em tecnologias de produtos. Ajudar os clientes a operar ambientes e processos seguros, também significa ter especialização contínua e envolvimento direto nos projetos upstream, implementar sistemas de criação e teste reproduzíveis, fornecer pacotes de maneira segura e responder de maneira rápida e eficiente a vulnerabilidades.

Diante do surgimento de vulnerabilidades de segurança, a Red Hat, por meio do Portal do Cliente, equipe de suporte técnico e equipe de segurança de produtos, oferece aos clientes diversas maneiras de rapidamente responder à essas vulnerabilidades e a proteger seus sistemas. Durante os incidentes de segurança Shellshock e Heartbleed, os clientes da Red Hat tiveram rápido acesso às informações, patches e aplicativos necessários para verificar sua exposição e solucionar possíveis problemas dentro de horas após a divulgação dos bugs.

Por exemplo, o Red Hat Insights pode ajudar você a identificar e solucionar, de maneira proativa, os problemas técnicos dos ambientes do Red Hat Enterprise Linux e do Red Hat Cloud Infrastructure. Esse serviço foca na segurança e em controles de implantação rigorosos, contando ainda com uma rede global de engenheiros e uma base de conhecimento extensa oferecida pela Red Hat com soluções técnicas e resolução de problemas anteriores. Ele analisa as informações do sistema e compara essas informações com nosso banco de dados de regras deterministas em constante desenvolvimento. Essas regras são o resultado do empenho de nossa equipe de Customer Experience and Engagement que trabalham para identificar e documentar as melhores práticas de otimização de cargas de trabalho e prevenção de problemas. O Red Hat Insights compartilha essas informações de maneira proativa e sugere etapas de remediação em um formato simples e de fácil entendimento. O Red Hat Insights pode ajudar você a simplificar as operações e evitar possíveis interrupções nos negócios.

4 Para obter mais detalhes sobre como o Red Hat Enterprise Linux, Red Hat Satellite e Red Hat CloudForms fornecem uma base que oferece suporte ao gerenciamento contínuo de controles PCI-DSS relevantes e à aplicação de políticas, consulte http://www.redhat.com/pt-br/resources/pci-dss-compliance-red-hat

"Nosso objetivo é garantir uma maior segurança e confiabilidade em nossos aplicativos de missão crítica, que incluem gerenciamento de dados para toda a rede pública de hospitais e clínicas, bem como informações de planos de seguro privados."

JOSE MARQUES
COORDENADOR GERAL DE ANÁLISE E MANUTENÇÃO DO MINISTÉRIO DA SAÚDE DO BRASIL

A Red Hat também ajuda a proteger a cadeia de fornecimento ao assinar digitalmente todos os pacotes lançados e distribuí-los através de canais seguros. Informações de vulnerabilidade e erratas também são fornecidas em formato legível por máquina, de maneira que possam ser acessadas e aplicadas em escala—assim como através do uso de um scanner de Protocolo de Automação de Conteúdo Seguro (SCAP). O Red Hat Container Registry permite verificar se os componentes são originados de uma fonte segura, se os pacotes da plataforma não foram afetados, se a imagem do container não apresenta vulnerabilidades conhecidas nos componentes ou nas camadas da plataforma e se a pilha completa é comercialmente suportada.

O software open source corporativo também exige metodologias de testes e revisão de códigos. Por exemplo, o processo de lançamento do Red Hat Enterprise Linux 7 incluiu não somente a revisão de novos pacotes para bugs de segurança e problemas de pacote, mas também a garantia de que as correções anteriores foram resolvidas na base do código upstream ou, caso contrário, estes ainda estariam presentes. Um sistema de compilação reproduzível que registra todas as ações, permite que a Red Hat saiba onde, quando, por que e como uma determinada compilação ocorreu, de maneira que esta possa ser recriada futuramente, caso necessário— até mesmo depois de vários anos.

A Red Hat tem a capacidade de fornecer software dessa maneira não somente devido a sua experiência e à um processo que funciona consistentemente. Mas, também, porque os engenheiros da Red Hat mantêm sua especialização atualizada e fazem contribuições extensas em comunidades upstream associadas as nossas soluções de subscrição. Isso nos ajuda a aplicar alterações que são importantes aos nossos clientes, incluindo aquelas relacionadas à segurança.

A Red Hat mantém uma equipe dedicada à segurança de produtos, responsáveis por analisar diariamente as ameaças e vulnerabilidades que possam afetar qualquer uma de nossas soluções, e assim, fornecer informações e atualizações relevantes por meio do Portal do Cliente. Essa equipe é focada em identificar os problemas que realmente importam, ao contrário de problemas que são teóricos em sua grande parte. Os clientes confiam nessa especialização para garantir uma resposta rápida a esses problemas. A Red Hat trabalha com outras comunidades Linux e de software open source, bem como com outras empresas, visando reduzir os riscos sobre problemas de segurança através do compartilhamento de informações e revisão.

CONCLUSÃO

Segurança moderna significa migrar de uma estratégia baseada na minimização de alterações para uma que é otimizada para alterações. Um fluxo de trabalho orientado por insights deve fornecer visibilidade a múltiplos ambientes, agregar informações e gerar ações de remediação, mesmo para ativos que podem ter uma vida útil na ordem de minutos. A segurança deve ser um componente integrado ao canal de entrega de software, e não uma opção desconectada.

A Red Hat pode ser sua parceira nessa transformação. Nossas soluções fornecem as tecnologias e apresentam as certificações (como Common Criteria e FIPS)[5] que possivelmente serão necessárias à sua empresa. Estamos totalmente envolvidos na cadeia de fornecimento de software open source e possuímos a especialização e os processos para fornecer soluções open source inovadoras de maneira confiável, consistente e segura.

5 https://www.redhat.com/pt-br/technologies/industries/government/standards

SOBRE A RED HAT

A Red Hat é líder mundial no desenvolvimento e fornecimento de soluções de software open source, utilizando uma abordagem impulsionada pela comunidade para oferecer tecnologias confiáveis e de alto desempenho em nuvem, virtualização, armazenamento, Linux e middleware. A Red Hat também oferece serviços renomados de suporte, treinamento e consultoria. Como o principal conector de uma rede global de empresas, parceiros e a comunidade open source, a Red Hat contribui na criação de tecnologias relevantes e inovadoras, as quais oferecem os recursos necessários para o crescimento e a preparação de seus clientes para o futuro da TI.

PORTFÓLIO DA RED HAT Saiba mais em redhat.com.

AMÉRICA LATINA
+54 11 4329 7300
latammktg@redhat.com

BRASIL
+55 11 3629 6000
marketing-br@redhat.com

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

br.redhat.com
INC0374232_0416