Seis práticas recomendadas de DevSecOps para desenvolvedores

1 Reduzir riscos de dependência das aplicações

Talvez seja preciso gerenciar algumas possíveis vulnerabilidades nos componentes de software utilizados para criar aplicações. Ferramentas de análise de composição do software (SCA) podem ser usadas para reduzir os riscos da cadeia de suprimentos, especialmente na utilização de componentes de software open source. Busque ferramentas de SCA que possibilitem:

- Verificar as dependências da aplicação para conferir se não possuem vulnerabilidades conhecidas.
- Auxiliar na automação da conformidade de licenciamento de software, identificando os componentes e sinalizando as licenças possivelmente incompatíveis.
- Confirmar que as dependências das aplicações são atuais e tenham sido criadas por uma comunidade ainda ativa e produzindo atualizações.
- Ser uma parte automatizada do processo de criação de aplicações e do ambiente de desenvolvimento. Assim, os desenvolvedores podem solucionar problemas antes da integração, reduzindo o número de falhas na criação da aplicação.

2 Unificar o gerenciamento de código e configuração

O paradigma do GitOps, popular no Kubernetes e em ambientes de containers, inclui práticas que podem melhorar bastante sua postura de segurança, começando pelo desenvolvimento:

- Implemente as práticas recomendadas de desenvolvimento na configuração do gerenciamento de código-fonte (SCM). Ao utilizar os mesmos controles na verificação, mesclagem e aprovação, é possível rastrear quem fez as alterações na configuração da infraestrutura e quando elas foram realizadas.
- Em vez de depender das operações, os desenvolvedores devem realizar a configuração no início do processo e definir uma visão para o ambiente de produção pretendido para a aplicação. Usar os mesmos tipo de controle de ambiente e segurança para desenvolvimento, testes e produção facilita o gerenciamento da configuração ao longo do ciclo de vida.
- Utilize um pipeline de build automatizado para criar imagens de container e artefatos binários para integração e entrega contínuas (CI/CD). Não é preciso realizar nenhuma mudança ad-hoc na implantação dessas imagens na produção.
- Não armazene dados sensíveis no sistema de SCM. Use ferramentas para verificar a configuração e as imagens de container, garantindo que não tenham segredos integrados.

3 Proteger segredos das aplicações

É importante gerenciar identidades e segredos, como senhas, tokens e chaves, ao longo de todo o ciclo de vida da aplicação. O acesso aos sistemas de ACM, registros de containers e repositórios binários devem ser controlados. Também é preciso proteger as credenciais utilizadas pelas aplicações para acessar bancos de dados e serviços, assim como as necessárias para builds automatizados e processos de teste. Os segredos podem ser acidentalmente revelados se forem armazenados nos sistemas de SCM ou nos arquivos de configuração. Para proteger os segredos das aplicações:

- Defina uma infraestrutura de gerenciamento de idade e controle de acesso no início do ciclo de vida.
- Considere usar um cofre de segredos ou um módulo de segurança de hardware (HSM) para gerenciar e proteger os segredos em repouso ou trânsito. Em geral, os cofres de segredos são soluções de software, e os HSMs utilizam hardware especializado para oferecer níveis elevados de proteção. Ambos precisam ser integrados à infraestrutura de gerenciamento de identidade.

4 Usar imagens base confiáveis

Imagens base de containers são distribuições Linux® altamente minimizadas. Centenas de pacotes podem ser pré-instalados e conter possíveis vulnerabilidades. Para reduzir o risco das imagens de container:

- Escolha imagens confiáveis com atualizações seguras, frequentes e testadas. Investigue as fontes das imagens e as opções de suporte disponíveis.
- Utilize ferramentas de imagens para verificar vulnerabilidades conhecidas. Também é preciso fazer uma varredura nas imagens para verificar a segurança das configurações e se não há segredos integrados.
- Reduza os vetores de ataque removendo binários desnecessários, incluindo ferramentas de sistema operacional, que podem ser usados em uma falha.

5 Resolver problemas de conformidade e auditoria no início

Para reduzir atrasos na migração para a produção, é importante entender os frameworks de conformidade e controles técnicos que são necessários no início do desenvolvimento. É possível incluir verificações automatizadas no pipeline de build para aplicar os requisitos de conformidade e segurança.

Comece uma documentação proativa, uma vez que pode representar pelo menos 50% dos procedimentos e regras de uma auditoria. A documentação de regras deve incluir controles de acesso, controles de alteração, backups e retenção de dados. Verificações de segurança, como SCA e testes de segurança da aplicação, precisam ser incluídas na documentação dos procedimentos.

6 Começar com uma plataforma e um ecossistema robustos

Como as ameaças de segurança continuam a aumentar, é fundamental usar uma plataforma com um ecossistema de segurança abrangente que ofereça soluções integradas e com suporte. O Red Hat® OpenShift® é uma plataforma Kubernetes de nível empresarial com funcionalidades abrangentes para oferecer suporte a desenvolvimento e operações. Os pipelines de build e implantação robustos do Red Hat OpenShift oferecem um lugar ideal para implementar verificações e controles de segurança automatizados. As verificações de segurança podem ser incluídas em qualquer parte do processo, da criação do código-fonte e das imagens à implantação da produção.

A Red Hat tem um ecossistema de parceiros de segurança que aprimora e amplia os recursos de segurança do Red Hat OpenShift. Esses parceiros trabalham com a Red Hat parece oferecer soluções com suporte e integradas ao Red Hat OpenShift. Escolha entre várias opções para atender às suas necessidades organizacionais e de segurança específicas.

Para acelerar o desenvolvimento de aplicações baseadas em container, o Red Hat CodeReady Workspaces é um ambiente de desenvolvimento nativo do Kubernetes que pode ser executado no Red Hat OpenShift. O Red Hat Universal Base Images e o Red Hat Runtimes oferecem uma base sólida de uma fonte confiável para suas aplicações.

Framework de DevSecOps da Red Hat

Tenha uma visão holística do ciclo de vida da segurança e saiba como os recursos de segurança do desenvolvimento se encaixam no framework de DevSecOps da Red Hat. Acesse red.ht/DevSecOps.

Encontre soluções de segurança do desenvolvimento

Assista a webinars da Red Hat e dos parceiros de segurança da Red Hat para ver como incluir a segurança em todo o ciclo de vida da sua aplicação.

Sobre a Red Hat

A Red Hat ajuda os clientes a definir padrões entre diferentes ambientes e a desenvolver aplicações nativas em nuvem, além de integrar, automatizar, proteger e gerenciar ambientes complexos com serviços de consultoria, treinamento e suporte premiados.

facebook.com/redhatinc
@redhatbr
linkedin.com/company/red-hat-brasil

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

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

br.redhat.com
#F29682_0921