

Podemos Integrar Segurança ao DevOps e à Infraestrutura como Pipelines de Código?

Por Fernando Cardoso

Está é pergunta mais questionada pelas equipes de segurança, uma vez que elas adentram o mundo do DevOps depois que o pipeline de CI/CD já está construído e os clientes perguntam sobre compliance, segurança e regulamentos internos da empresa. Sem o background do processo de construção do pipeline, pode ser complicado para as equipes de segurança compreender todas as etapas do processo. Convencionalmente, o foco das equipes de DevOps não é a segurança, mas sim, a criação de aplicações e a entrega delas no prazo, mas quem disse que isso não pode ser feito de forma segura? Vamos mergulhar nos principais desafios.



O “**Grande**” Desafio de Integrar a Segurança e Dominá-la



De um modo geral, se você mencionar palavras como Ruby, Go, Node, JS, Java ou Python, as equipes de segurança não poderão necessariamente participar da conversa - sem terem culpa alguma. Quando o DevOps estava se tornando popular, as equipes de segurança não eram consideradas responsáveis pela verificação do pipeline de desenvolvimento. Naquela época, e mesmo agora, o código de segurança no pipeline dependia do conhecimento dos desenvolvedores e das práticas recomendadas em que eles se apoiavam para o processo de desenvolvimento. **Agora, com a introdução mais recente do DevSecOps, um novo conjunto de ferramentas foi introduzido para automatizar a segurança e a resposta a incidentes. Isso fornece mais um incentivo para a segurança aprender o idioma do DevOps e trabalhar em conjunto.**

Não vai demorar muito até que as equipes de segurança começem a se adaptar e aceitar essa nova realidade. Trabalhar junto começa com a compreensão dos processos uns dos outros. Se as equipes de segurança entenderem o processo do pipeline, poderão começar a planejar a segurança nos estágios iniciais de qualquer nova aplicação. A aplicação da segurança diretamente no ambiente de desenvolvimento integrado e no pipeline de CI / CD levará à detecção e resposta mais rápidas de novas falhas de segurança que podem ser introduzidas e fornecerá aos desenvolvedores feedback em tempo real para corrigi-lo.

Para adotar uma cultura DevSecOps, a empresa precisa dar atenção ao treinamento cruzado de suas equipes, por exemplo, ensinando desenvolvedores sobre segurança e instruindo profissionais de segurança em processos de desenvolvimento e como criar novas aplicações em prazos mais exigentes. Quando nos entendemos melhor, podemos aprender a falar a língua um do outro e a trabalhar melhor em equipe, sem ter muito atrito. Agora, a menção de linguagens de programação não fará com que as equipes de segurança olhem para você confusos e elas podem até entender como as APIs podem automatizar tarefas mundanas. Isso não seria legal?

Imagine se sua equipe de segurança tivesse o conhecimento necessário para escrever e entender um script de automação em Python, Node.JS ou qualquer outra linguagem de script que lhes permitisse manipular APIs para automatizar o trabalho normal do dia-a-dia. Muitas organizações estão automatizando processos e tecnologias de segurança a fim de obter uma segurança mais eficaz e eficiente. Isso incluiria o uso de APIs em pipelines de construção e plataformas e ambientes de tempo de execução, mas a segurança precisa entender como tudo funciona. Se sua empresa não estiver bem adaptada ao novo mundo, você poderá começar a enfrentar alguns desafios bem complicados.

Nove Recomendações de Segurança para Começar a Implementar Seu Pipeline de CI / CD

Os métodos abaixo podem ser empregados em aplicações monolíticas ou de microsserviços usando tecnologias como soluções nativas de contêiner, serverless ou em nuvem.

1

Teste de Unidade

Esse tipo de segurança verifica unidades individuais e pequenas de um software. Os desenvolvedores podem usar isso para testar se a função correta está fornecendo o retorno certo ou para garantir que uma alteração / atualização em uma função pequena não esteja afetando os resultados da aplicação.

2

Teste de Segurança de Aplicações Estáticas (SAST)

O SAST é mais conhecido como "teste de caixa branca". Esse tipo de teste de segurança oferece aos desenvolvedores a habilidade de encontrar vulnerabilidades de código-fonte no início do ciclo de vida de desenvolvimento de software (SDLC), o que pode ajudá-lo a corrigir o código mais rapidamente. As soluções SAST analisam uma aplicação de "dentro para fora" em um estado de não-execução.

3

Varredura de licença

Essa ferramenta de varredura ajuda a encontrar quais licenças o seu projeto usa em suas dependências e decide se deve ou não permiti-las.

4

Teste de Segurança de Aplicações Dinâmicas (DAST)

O DAST é mais conhecido como "teste de caixa preta". Esse tipo de teste de segurança permite encontrar vulnerabilidades e pontos fracos de segurança nas aplicações da web sem uma visão do código-fonte interna.

5

Varredura de Dependência

Muitas aplicações usam bibliotecas ou pacotes externos de projetos de código aberto. Essa técnica ajuda a encontrar automaticamente vulnerabilidades em suas dependências enquanto você está desenvolvendo e testando aplicações.

6

Varredura de contêineres

Essa técnica analisa imagens de contêiner em busca de vulnerabilidades, segredos, listas de verificação de compliance e malware conhecidos. Você vai querer executar isso em todos os estágios do SDLC para ajudar as equipes de operações a obterem uma imagem mais clara das preocupações com a segurança dentro do contêiner antes de serem enviadas para o ambiente de produção.

7

Proteção de Tempo de Execução

Essa camada de segurança é usada em máquinas físicas ou virtuais para proteger o SO e / ou os mecanismos de contêiner. Se o SO fosse comprometido, poderia causar uma Denial of Service (DoS) de todos os contêineres em execução no host ou no noite desse contêiner. Essa solução pode ajudá-lo a se proteger contra malware e vulnerabilidades, além de ajudar no processo de auditoria usando recursos como monitoramento de integridade de arquivos, inspeção de log e controle de aplicações.

8

Segurança Privilegiada de Contêiner

É aqui que o uid 0 do contêiner é mapeado para o uid 0 do host. Nesses contêineres, a proteção do host e a prevenção de fuga são feitas inteiramente por meio do Controle de Acesso Obrigatório, filtros seccomp, queda de recursos e namespaces. Essas tecnologias combinadas normalmente evitam danos acidentais ao host. Existem algumas preocupações com esse recurso de segurança. Se você estiver dando ao contêiner privilegiado acesso total ao host, isso poderá impactar todos os contêineres em execução, se algo der errado.

9

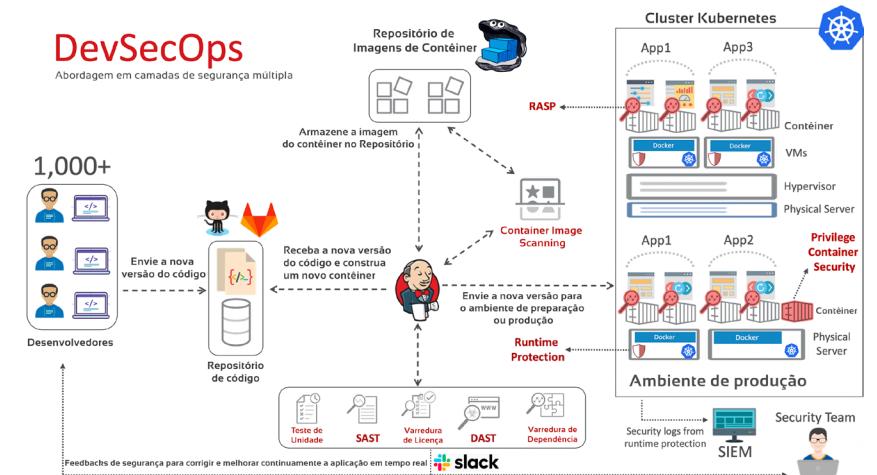
Autoproteção de Aplicação de Tempo de Execução (RASP)

A RASP trabalha dentro da aplicação como um framework de segurança que monitora e inspeciona continuamente o tráfego da aplicação. A RASP intercepta dinamicamente o tráfego considerado malicioso, protegendo-o contra injeção de SQL, cross-site scripting (XSS), vulnerabilidades, bots e muitos outros ataques a aplicações da Web. Um framework de segurança RASP é anexado no início do SDLC, tornando a aplicação segura por padrão. Esse conceito de segurança pode ser usado em aplicações da web, contêineres e serverless.



Essas são apenas algumas das muitas camadas de segurança que você pode integrar ao seu pipeline de DevOps. Com uma abordagem estratégica, você pode começar lentamente a implementar as camadas de segurança apropriadas para obter garantia de que seu pipeline está seguro, enquanto continua a se mover rapidamente.

Abaixo está uma arquitetura que mostra como colocar a segurança em camadas em diferentes etapas no pipeline do DevOps:



Três maneiras de adicionar segurança à sua Pipeline de Infrastructure as Code (IaC)

Agora que temos mais informações sobre como implementar a segurança no pipeline de CI / CD, vamos continuar discutindo como adicionar verificações de segurança para configurações incorretas em seu IaC.

De acordo com o Gartner, “até 2023, pelo menos 99% das falhas de segurança na nuvem serão culpa do cliente”.¹ O Gartner também declara: “Até 2024, as organizações que implementam uma oferta de CSPM e estendem isso ao desenvolvimento reduzirão os incidentes de segurança relacionados à nuvem devido a configuração incorreta em 80%.”¹

Essa estatística está principalmente associada a configurações incorretas na infraestrutura de nuvem. É muito importante ter visibilidade e um processo para feedback em tempo real, pois fornece aos desenvolvedores mais informações sobre o IaC antes de serem construídos. Sem as informações adequadas, um desenvolvedor pode começar, sem saber, a criar um novo ambiente de nuvem com falhas de segurança que podem gerar muitas dores de cabeça para sua empresa.

1

Plug-in de Segurança do Ambiente de Desenvolvimento Integrado

Esse tipo de plug-in foi projetado para fornecer feedback em tempo real aos desenvolvedores sobre o IaC e o desenvolvimento de aplicações. Os desenvolvedores podem verificar e corrigir problemas no espaço de trabalho do ambiente de desenvolvimento sem ferramentas de segurança adicionais para detectar problemas- deslocando a segurança o mais para a esquerda possível.

2

Scanner de Templates

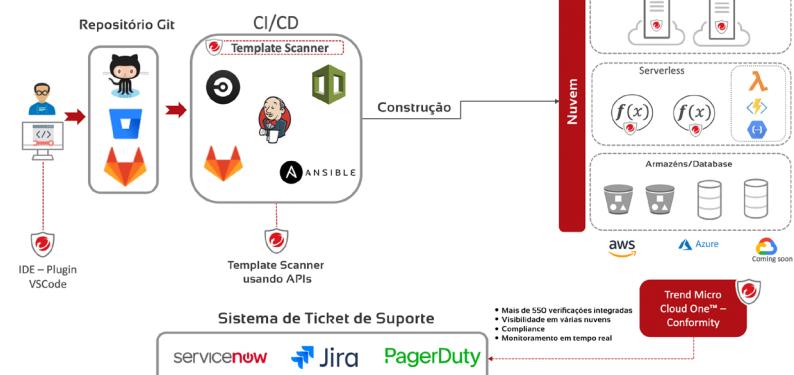
Esse scanner usa APIs diretamente na plataforma de segurança para integrar-se a ferramentas personalizadas ou casos de uso específicos em pipelines de CI / CD. As varreduras fornecem verificações em tempo real toda vez que você envia um novo código. Os resultados podem ser compartilhados com desenvolvedores e arquitetos em nuvem, fornecendo a eles as informações necessárias para monitorar quaisquer problemas antes de iniciar a produção.

3

Gerenciamento de Postura de Segurança em Nuvem (CSPM)

Uma ferramenta de segurança para detectar configurações incorretas em vários provedores de serviços em nuvem. Essa tecnologia pode se integrar aos recursos do DevSecOps para auxiliar nos recursos de correção automática em sua infraestrutura de nuvem. Também pode ajudar as organizações a obterem uma imagem coerente da segurança e riscos de compliance em ambientes com múltiplas nuvens.

Infrastructure as a Code - Pipeline



Conclusão

À medida que continuamos a evoluir, todas as empresas precisarão repensar sua atual estratégia de segurança cibernética para workloads em nuvem, contêineres e ambientes sem serverless.

No final do dia, a bem-sucedida integração da segurança no pipeline do DevOps se resume a garantir que as equipes de segurança estejam envolvidas nos estágios iniciais do projeto. A utilização dessa abordagem ajudará a facilitar a comunicação e a integração mais confiáveis entre o DevOps e as equipes de segurança, gerando resultados de maior qualidade e melhor segurança para as aplicações.



Securing Your Connected World

© 2020 Trend Micro Incorporated e / ou suas afiliadas. Todos os direitos reservados. Trend Micro e o logotipo da t-ball são marcas comerciais ou marcas registradas da Trend Micro e / ou de suas afiliadas nos EUA e em outros países. As marcas registradas de terceiros mencionadas são de propriedade de seus respectivos proprietários.

[Asset01_Integrate_Security_Into_DevOps_200520US]

