Guia do comprador de segurança de APIs

Evoluir para cumprir o desafio de segurança de APIs

À medida que as organizações se tornam cada vez mais centradas na nuvem e digitais, suas APIs crescem em escopo e escala, aumentando seu valor. Agora, as APIs:

- Operam no núcleo de aplicativos e serviços que atendem seus clientes e parceiros, incluindo as mais recentes inovações de IA
- São incorporadas em ambientes de nuvem, desde os serviços que seus desenvolvedores usam até as cargas de trabalho que seus engenheiros migram
- Representam os fluxos de receita, ajudando a expandir seus negócios e a construir um ecossistema de desenvolvedores

No entanto, se você é como os 78% dos profissionais de TI e segurança que experimentaram incidentes de segurança de APIs[1], você também viu em primeira mão que as APIs são um risco crescente. APIs expostas ou mal configuradas são predominantes, desprotegidas e fáceis de violar. Em muitos casos, as organizações sequer têm conhecimento de todas as suas APIs, deixando-as sem gerenciamento. Essas APIs adormecidas, ou zumbi, são importante vetores de ataque.

Os riscos são altos. Os ataques às suas APIs podem comprometer a receita, a resiliência e a conformidade regulatória de uma empresa. A maioria das organizações ainda não tem os controles e recursos certos para evitar ataques às APIs. Certamente, muitas empresas têm ferramentas de API em sua pilha existente, incluindo gateways de API e firewalls de aplicativos da Web. No entanto, embora essas ferramentas possam oferecer alguma proteção, elas não são projetadas para fornecer o grau de visibilidade, segurança em tempo real e testes contínuos para defender contra ataques modernos a APIs.

1. Akamai Technologies, “API Security Disconnect Report,” 2023

O que é preciso para proteger totalmente seu patrimônio de APIs? Embora uma série de produtos de segurança de APIs tenha surgido nos últimos anos, navegar pelo crescente escopo dos fornecedores e seus recursos pode ser difícil.

As ameaças atuais exigem uma solução completa de segurança de APIs, abrangendo quatro áreas críticas: descoberta de APIs, gerenciamento de postura, detecção e correção de ameaças e testes de segurança. Este guia do comprador descreve os principais recursos que uma solução abrangente de segurança de APIs precisa ter, definindo os recursos e controles de segurança de que você precisa para desenvolver e manter APIs seguras, ao mesmo tempo em que localiza e protege todas as APIs em seu ecossistema.

Principais recursos para a segurança abrangente de APIs

Para determinar os recursos de segurança de APIs de que você precisa, é importante entender a natureza dos desafios que você enfrenta.

As APIs são frequentemente distribuídas em vários ambientes, desde no local até na nuvem híbrida. Além da complexidade, seu ecossistema de APIs provavelmente se estende muito além de sua própria presença de rede e nuvem. Pense na infinidade de conexões que suas APIs estabeleceram com aplicativos, serviços e sistemas pertencentes a terceiros, que podem ou não priorizar a segurança de APIs.

Além disso, é difícil receber insights em tempo real sobre:

- Onde suas APIs são roteadas
- Como elas estão configuradas
- Que dados confidenciais elas movem
- Quais riscos elas representam

À medida que as empresas desenvolvem e implementam rapidamente novos aplicativos e APIs, a superfície de ataque cresce exponencialmente. Quanto às APIs mais antigas, sua organização pode ter um cluster delas, criado e produzido anos atrás, antes que a segurança de APIs se tornasse uma necessidade crítica.

A falta de visibilidade leva a descobertas preocupantes: apenas 4 em cada 10 profissionais de segurança com inventários de API completos sabem qual de suas APIs retorna dados confidenciais quando chamadas. Muitas dessas chamadas de API vêm de agentes mal-intencionados que testam vulnerabilidades e, uma vez que identificam uma lacuna, os ataques costumam ser implacáveis.

Quando você está avaliando fornecedores de segurança que alegam ser capazes de proteger totalmente sua API, é importante garantir que eles tenham controles e recursos estabelecidos e em produção em quatro áreas críticas.

Continue lendo para conferir uma série de listas de verificação do comprador que você pode usar para avaliar os recursos dos fornecedores.

01

Descoberta de APIs

É comum ter APIs que ninguém conhece. No entanto, sem um inventário preciso, sua empresa está exposta a uma série de riscos. Para fazer um inventário eficaz de suas APIs, você precisa ser capaz de:

- ☑ Localizar e fazer o inventário de todas as suas APIs, independentemente da configuração ou tipo
- ☑ Detectar APIs inativas, legadas e zumbi
- ☑ Identificar domínios esquecidos, negligenciados ou de sombra desconhecidos
- ☑ Eliminar pontos cegos e revelar possíveis caminhos de ataque

02

Gerenciamento de postura de APIs

Configurações erradas de API simples podem abrir a porta para invasores. Uma vez lá dentro, eles podem acessar e exfiltrar rapidamente seus dados confidenciais. Para entender como todas as suas APIs estão configuradas, você precisa ser capaz de:

- ☑ Verificar automaticamente a infraestrutura para descobrir configurações incorretas e riscos ocultos
- ☑ Criar fluxos de trabalho personalizados para notificar as principais partes interessadas sobre vulnerabilidades
- ☑ Identificar quais APIs e usuários internos podem acessar dados confidenciais
- ☑ Atribuir classificações de gravidade aos problemas detectados para priorizar a correção

03

Detecção e correção de ameaças a APIs

Os ataques a APIs estão se tornando inevitáveis. Para detectar e corrigir ameaças de forma eficaz, você precisa ser capaz de:

- ☑ Monitorar a violação e o vazamento de dados, violações de políticas, comportamento suspeito e ataques a APIs
- ☑ Analisar o tráfego de APIs de todas as fontes e integrar-se a fluxos de trabalho existentes (emissão de tíquetes, informações de segurança e gerenciamento de eventos etc.) para alertar as equipes de operações de segurança
- ☑ Evitar ataques e uso indevido em tempo real com correção parcial ou totalmente automatizada

04

Teste de segurança de APIs

A velocidade é essencial cada aplicativo que seus desenvolvedores criam, mas isso facilita que uma vulnerabilidade ou falha de design não seja detectada. Para testar adequadamente suas APIs, você precisa ser capaz de:

- ☑ Executar diversos testes automatizados que simulem tráfego mal-intencionado e sigam a lógica de negócios da API subjacente
- ☑ Descobrir vulnerabilidades antes que as APIs entrem em produção para reduzir o risco de um ataque bem-sucedido
- ☑ Inspecionar suas especificações de API em relação às políticas e regras de governança estabelecidas
- ☑ Executar testes de segurança com foco em API sob demanda ou como parte de um pipeline de CI/CD

Descoberta de APIs: aprofunde-se nos principais recursos

Muitas organizações operam APIs novas e legadas. Não é incomum ter APIs não gerenciadas em produção que ninguém nas equipes de operações ou segurança sabe, expondo os negócios a uma série de riscos de cibersegurança e dificuldades operacionais. APIs não autorizadas podem surgir de fatores como atalhos e falhas de processo, ou então quando não são desligadas quando desativadas. Na próxima página, mostraremos os principais exemplos para você ficar de olho.

APIs comerciais

Alguns pacotes de software comercial incluem APIs para se conectar com outros aplicativos e fontes de dados externas. Essas APIs podem ser ativadas sem que ninguém perceba.

Falha em desativar

As APIs também podem ser oficialmente desativadas, mas permanecerem em operação devido a descuidos operacionais. Essas APIs às vezes são chamadas de zumbi.

Versões antigas de APIs

Em alguns casos, uma versão mais antiga de uma API nunca é desativada. Uma versão antiga pode ter que coexistir com uma nova versão por um determinado período enquanto o software é atualizado. Mas e se a pessoa responsável por desativar a API sair da empresa, for realocada ou simplesmente se esquecer de desligar a versão antiga?

Atalhos e falhas de processo

Algumas APIs não autorizadas são resultado de não se comunicar com as pessoas certas. Por exemplo, uma equipe de linha de negócios (LOB) pode criar APIs para atender a necessidades específicas sem informar à equipe de TI, ou os desenvolvedores podem estar mais preocupados com a execução do que com o procedimento. APIs que foram “herdadas” como parte de uma aquisição também são frequentemente negligenciadas. Esses tipos de APIs não autorizadas muitas vezes são chamadas de APIs sombra.

Ao falar com fornecedores, peça para explicarem como fazem para garantir que as APIs não autorizadas, legadas, zumbi e sombra sejam identificadas e resolvidas antes que possam ser exploradas. Muitas vezes, APIs legadas e zumbi são o elo mais fraco na segurança de APIs. Portanto, é fundamental identificar APIs que não são gerenciadas por um gateway de API e localizá-las, fazer inventário delas e determinar se precisam ser corrigidas ou desativadas.

Principais recursos de descoberta de APIs

Uma solução de segurança de APIs deve incorporar os seguintes recursos de descoberta

Descoberta de ativos de API e inventário granular

Uma ferramenta de descoberta de APIs deve ser capaz de localizar e identificar as APIs que você tem, independentemente da configuração ou tipo, incluindo RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC e gRPC. Também deve criar um inventário que é atualizado automaticamente para evitar que fique obsoleto, além de fornecer a capacidade de pesquisar, marcar, filtrar, atribuir e exportar APIs com base em qualquer atributo.

Detecção de APIs inativas, legadas e zumbi

APIs legadas e zumbi podem minar as iniciativas de segurança de APIs da sua organização. Essas APIs normalmente não possuem propriedade e função, não tendo nenhum controle de visibilidade ou segurança. É fundamental que uma ferramenta de descoberta de APIs seja capaz de localizar essas APIs.

Descoberta de domínio sombra

Além das APIs sombra, você pode ter domínios sombra inteiros: nomes de domínio de API dos quais você não tem conhecimento. As ferramentas de descoberta de APIs devem conseguir identificar domínios sombra esquecidos, negligenciados ou desconhecidos que possam representar um risco de segurança.

Varreduras automáticas

Varreduras são essenciais para eliminar pontos cegos e identificar problemas críticos, incluindo:

- Credenciais e chaves de API vazadas
- Exposição de esquema e código de API
- Configurações incorretas da infraestrutura
- Vulnerabilidades na documentação, repositórios GitHub, espaços de trabalho Postman etc.

Identificar essas e outras fontes de inteligência explorável também pode ajudar as equipes a entender possíveis caminhos de ataque que podem ser explorados pelos cibercriminosos.

Desenvolvimento personalizado limitado

Por fim, com a ferramenta certa de descoberta de APIs, você não deve precisar de desenvolvimento personalizado para fontes de tráfego. Essas ferramentas devem vir com integrações incorporadas para os principais componentes de infraestrutura. O desenvolvimento personalizado normalmente consome muito tempo e, se houver mudanças na origem da fonte, uma integração provavelmente precisaria ser reformulada, o que não é viável para equipes de segurança de TI.

Gerenciamento de postura de APIs: aprofunde-se nos principais recursos

As ameaças ao seu patrimônio de APIs estão crescendo rapidamente devido a tendências como a mudança da TI centralizada para operações LOB descentralizadas, o aumento do uso de recursos em nuvem e a transição para arquiteturas baseadas em microsserviços.

A descoberta robusta (conforme descrito na seção anterior) é o primeiro passo para proteger seu patrimônio de APIs. Você precisa descobrir e fazer o inventário de APIs de todos os tipos que estão em uso.

Existem vários recursos adicionais essenciais para gerenciar a postura de segurança de suas APIs. Você precisa conseguir identificar quais APIs acessam e transmitem dados confidenciais e classificar essas APIs de acordo, pois as APIs que lidam com dados, como informações do cliente, precisam obrigatoriamente ser autenticadas. Também é importante identificar vulnerabilidades de infraestrutura que tornarão qualquer API mais vulnerável.

Avaliação de configuração

Muitos ataques cibernéticos são bem-sucedidos devido a simples erros de configuração das redes, gateways de API ou firewalls que gerenciam e protegem o tráfego de API.

Uma solução de segurança de APIs deve ser capaz de fazer a varredura da infraestrutura e das configurações de software regularmente, incluindo arquivos de registro, reproduções de tráfego histórico, arquivos de configuração e muito mais. Isso permite que você descubra falhas de configurações e vulnerabilidades e elimine o risco de desvios na configuração.

Gravidade personalizável

À medida que a solução identifica novas vulnerabilidades em seu ambiente, ela também deve atribuir um nível de gravidade aos problemas que foram descobertos para que possam ser priorizados para correção. Os níveis de gravidade devem ser personalizáveis para se alinhar à tolerância ao risco, requisitos regulamentares e políticas internas da sua organização.

Fluxos de trabalho personalizados

Além da gravidade personalizável, a ferramenta ideal de gerenciamento de postura deve permitir que você crie fluxos de trabalho personalizados para agir imediatamente quando identificar vulnerabilidades. Esses fluxos de trabalho podem variar desde a criação de tíquetes até a notificação das principais partes interessadas e a atualização das configurações de rede.

Documentação gerada automaticamente

A documentação da API informa aos consumidores o que ela faz e como usá-la. As organizações devem avaliar se as APIs seguras estão em conformidade com especificações e documentação precisa. Documentação incompleta ou inexistente torna os testes de segurança mais difíceis, aumentando o risco de uma API entrar em produção com uma vulnerabilidade não detectada. Muitas vezes, esse problema acaba ganhando uma proporção maior devido à terceirização do desenvolvimento de APIs. Independentemente da origem do problema, a documentação desatualizada, incompleta e ausente é inaceitável se você quiser que seu programa de segurança de APIs seja bem-sucedido.

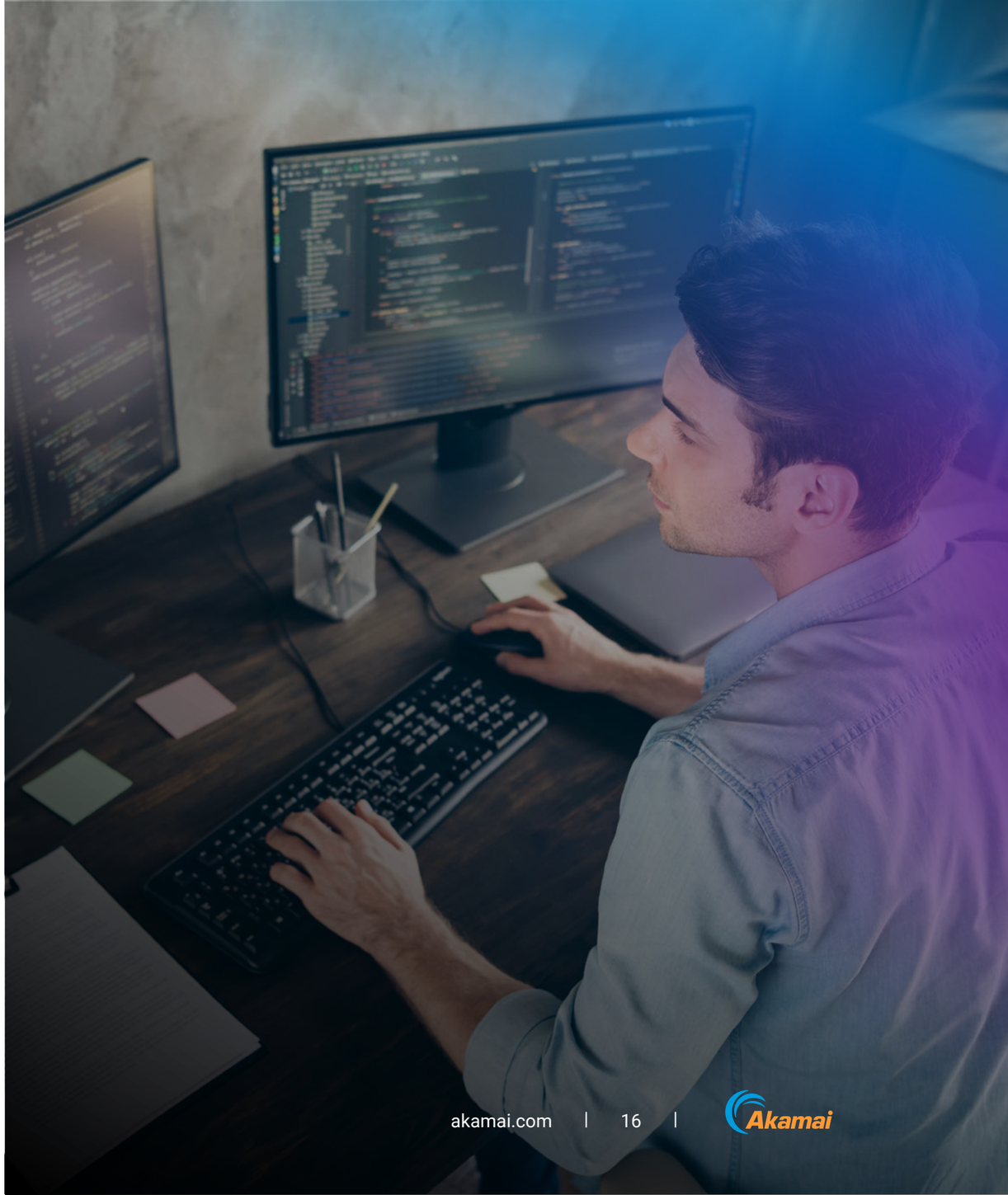
A especificação da OpenAPI define descrições de interface padrão. Uma solução de segurança de API deve ser capaz de:

- Comparar as especificações da API com o tráfego observável real e identificar diferenças, permitindo que as organizações vejam quais das suas APIs implantadas não cumprem as especificações e, potencialmente, representam um risco.
- Gerar automaticamente a documentação completa da OpenAPI com base no estado atual e futuro da API. Assim, garante que todas as APIs estejam devidamente documentadas e que a documentação esteja atualizada. Identificar essas e outras fontes de inteligência explorável também pode ajudar as equipes a entender possíveis caminhos de ataque que podem ser explorados pelos cibercriminosos.

Detecção e correção de ameaças a APIs: aprofunde-se nos principais recursos

Os ataques que tentam explorar vulnerabilidades de APIs agora são reais. Não é mais uma questão de “se” sua organização será atacada, mas sim de “quando” e “como”. Tornou-se imprescindível detectar ataques rapidamente e bloqueá-los antes que possam causar danos significativos, como a exfiltração de dados privados de clientes. Mesmo que suas APIs sejam tão seguras quanto possível, você precisa de proteção de tempo de execução ativa para detectar vazamentos de dados, adulterações de dados, violações de políticas de dados, comportamento suspeito e ataques à segurança de APIs. Isso deve incluir registro do tráfego de APIs, monitoramento do acesso a dados confidenciais, detecção de ameaças e bloqueio ou correção de vetores de ataque.

Nas duas páginas seguintes, explicaremos os principais recursos que uma solução de segurança de API deve incluir.



Monitoramento fora de banda em tempo real

O monitoramento de segurança de APIs não deve afetar ou retardar o tráfego de APIs. Procure fornecedores que possam oferecer uma abordagem sem agentes que permita que as empresas implantem com mais rapidez e recebam mais tráfego. No entanto, em circunstâncias em que é apropriado (por exemplo, ambientes complexos no local), a solução deve ter flexibilidade suficiente para oferecer suporte aos agentes também.

Uma solução de segurança de APIs deve espelhar o tráfego de fontes de dados identificadas e realizar análises sobre os dados desse tráfego em segundo plano, com alertas em tempo real de quaisquer problemas descobertos.

Detecção de anomalia e exploração de APIs

A coleta passiva de dados não é suficiente, especialmente porque o número de APIs e o volume total de tráfego de APIs continuam a crescer. A atividade da API deve ser analisada continuamente para detectar eventos anômalos e alertar equipes de segurança e operações.

As ferramentas avançadas incorporam recursos de IA e aprendizado de máquina para analisar o tráfego em tempo real e aproveitar insights contextuais para identificar atividades anômalas que possam indicar vazamento de dados, adulteração de dados, violações de políticas de dados e outros ataques de segurança de APIs.

Prevenção a ataques de APIs

Uma vez que uma anomalia ou outro problema foi identificado e um alerta gerado, o tempo é essencial. O movimento não autorizado de dados confidenciais por meio de APIs ou outro uso indevido suspeito de APIs deve ser detectado e bloqueado. Uma solução de segurança de APIs não deve apenas bloquear o uso indevido por meio da integração com seus firewalls e gateways de API: ela deve automatizar a correção de forma parcial ou total. A correção semiautomatizada deve estar disponível para tratar alguns tipos de alertas. Para problemas recorrentes e identificados anteriormente, você deve ter a opção de fornecer uma resposta totalmente automatizada.

Pontuação para confiança de ataque

Algumas soluções no mercado usam algoritmos de aprendizado de máquina treinados para avaliar sinais externos e internos, incluindo comportamento de API, padrões de tráfego de rede, dados de geolocalização e feeds de inteligência de ameaças. Usando fatores contextuais como esses, uma solução pode determinar o nível de confiança de que um incidente de tempo de execução detectado é o resultado de atividades mal-intencionadas.

Integrações para resposta a incidentes

Quando um incidente ocorre, uma solução de segurança de APIs deve incluir as integrações necessárias para garantir que as tarefas de correção sejam atribuídas às equipes apropriadas. Se forem detectados erros de configurações, violações de políticas de dados ou comportamentos suspeitos, eles devem ser reportados ao gateway da API, sistema SIEM e outros mecanismos de segurança da informação para garantir o nível certo de conscientização.

Como regra geral, uma solução de segurança de APIs deve se integrar facilmente com as outras ferramentas de segurança, monitoramento e gerenciamento que sua organização usa.

Teste de segurança de APIs: aprofunde-se nos principais recursos

Um erro que muitas equipes de desenvolvimento cometem é esperar muito tempo para iniciar o teste de API, fazendo com que os testes se tornem um gargalo. As equipes precisam adotar uma abordagem "shift-left" para garantir que os testes comecem o mais cedo possível no processo de desenvolvimento e que sejam abrangentes. Os benefícios dos testes eficazes de segurança das APIs são significativos:

- **Prevenção contra ataques**
  - Ao descobrir vulnerabilidades antes que as APIs entrem em produção, é possível reduzir o risco de um ataque bem-sucedido
- **Conformidade aprimorada**
  - Testes abrangentes ajudarão você a garantir a conformidade e evitar multas e danos à reputação
- **Maior confiança**
  - Testes rigorosos e eficazes podem aumentar a confiança da sua organização nas APIs e ajudar a garantir que os lançamentos dos seus desenvolvedores aconteçam dentro do prazo

Alguns fornecedores no mercado podem oferecer recomendações às empresas sobre como corrigir problemas em seus ambientes, além de habilitar configurações abrangentes de teste de API. As recomendações podem incluir etapas de ação para configurar autenticações adequadas ou corrigir dependências de API. O benefício: se você puder resolver problemas de lógica de negócios em seu ambiente, poderá aumentar o número de APIs otimizadas para testes, resultando em maior cobertura de testes.

Todo o conceito de testes de segurança de API, no entanto, permanece um pouco nebuloso. As equipes de desenvolvimento podem não entender completamente o que isso implica. O teste de API "shift-left" é um processo em três etapas:

1. **Entender a API:** entender o caso de uso da API embasa os testes, especialmente para problemas complicados de lógica de negócios.
2. **Certificar-se de que você pode interagir com a API corretamente:** certifique-se de que você pode usar a API do jeito que ela foi concebida. Isso é essencial para validar que sua compreensão da API corresponde à forma como a API funciona.
3. **Enviar tráfego de ataque para a API:** isso pode incluir a manipulação manual de solicitações para a API, a inserção de cadeias de Fuzzing em solicitações ou o uso de uma ferramenta automatizada para realizar testes de segurança de APIs. Como acontece com tudo na TI moderna, a automação costuma ser a melhor maneira de fazer o trabalho em escala sem comprometer a velocidade.

Principais recursos de teste de segurança de APIs

Os testes de segurança de APIs devem incluir testes estáticos, dinâmicos e de penetração. Uma solução de segurança de APIs deve incluir ferramentas para facilitar testes completos, automatizando os processos de teste na maior medida possível. Procure os seguintes recursos de teste de API em uma solução de segurança de APIs:

Testes de segurança de APIs automatizados e proativos

Os testes de segurança automatizados reduzem significativamente o risco e o custo ao identificar configurações incorretas, vulnerabilidades e não conformidade antes de uma API entrar em produção.

Governança de API

É essencial pensar em questões de governança, como funções, responsabilidades e políticas. Isso inclui responsabilidades de nível de execução para desenvolvedores, engenheiros de segurança e engenheiros de plataforma, bem como supervisão de políticas e decisões sobre riscos. Uma solução de segurança de APIs deve permitir que você inspecione as especificações da sua API em relação às políticas e regras de governança estabelecidas.

Pipeline de CI/CD e integração de repositório de código

DevSecOps é uma variante do DevOps que adiciona segurança ao fluxo de trabalho de desenvolvimento de software. A segurança de APIs precisa fazer parte das iniciativas do DevSecOps. Uma solução de segurança de APIs deve fornecer um conjunto de testes de segurança focados em APIs que são executados sob demanda ou como parte de um pipeline de CI/CD. A integração CI/CD é essencial, pois permite a testagem rápida e contínua de segurança de APIs necessária para acompanhar o desenvolvimento dos aplicativos.

Juntando tudo: identifique e resolva as lacunas de segurança das suas APIs

As APIs são um componente essencial da capacidade das organizações de atender clientes, gerar receita e operar de forma eficiente em uma economia cada vez mais digital e centrada na nuvem. No entanto, seu crescimento contínuo, a proximidade com dados confidenciais e a falta de controles de segurança tornam as APIs um alvo atraente para os invasores de hoje.

As ferramentas que muitas organizações usam para gerenciar APIs e ter proteção básica oferecem um grau de redução de risco, mas ainda são insuficientes para enfrentar as ameaças atuais a APIs. Não se pode confiar nelas como a única fonte de proteção.

Em vez disso, as organizações devem buscar uma solução abrangente de segurança de APIs que possa fornecer todos os quatro componentes discutidos neste guia do comprador: descoberta, gerenciamento de postura, detecção e correção de ameaças e testes de segurança. Você não precisa abandonar as ferramentas existentes que se mostraram eficazes em certas áreas; basta procurar uma solução capaz de se integrar sem problemas às suas ferramentas.

Começar a usar a segurança de APIs não significa que você precisa alocar recursos significativos. Você pode começar comprometendo-se com um piloto mensurável e de menor escala que aborda lacunas específicas em sua pilha de segurança. Ou você pode iniciar sua jornada de segurança de APIs com uma atualização abrangente. Cada organização é diferente.

Com o número cada vez maior de ataques focados em API, seu passo mais importante é a decisão de agir. Esperamos que este guia do comprador tenha sido útil para você.

Leia mais sobre métodos de ataque de APIs, vulnerabilidades comuns de APIs e como proteger sua organização.

Saiba como podemos ajudar agendando uma **demonstração personalizada do Akamai API Security**.

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem comprometer o desempenho ou a experiência do cliente. Ao aproveitar a escala de nossa plataforma global e sua visibilidade de ameaças, trabalhamos com você para evitar, detectar e mitigar ameaças, permitindo que você construa a confiança na sua marca e opere de acordo com a sua visão. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em **akamai.com** e **akamai.com/blog**, ou siga a Akamai Technologies no **X**, antigo Twitter, e **LinkedIn**. Publicado em 09/24.

Akamai