As 10 melhores empresas de testes de penetração em 2025 - Against Inva

Data: 2025-09-23 18:36:12

Autor: Inteligência Against Invaders

Melhores empresas de teste de penetração

As empresas de testes de penetração desempenham um papel vital no fortalecimento das defesas das organizações de segurança cibernética, identificando vulnerabilidades em seus sistemas, aplicações e redes.

Essas empresas simulam ataques cibernéticos do mundo real para descobrir fraquezas que podem ser exploradas por atores maliciosos, ajudando as empresas a implementar medidas proativas de segurança. Eles fornecem serviços adaptados a vários setores, incluindo segurança de aplicativos da Web, testes de aplicativos móveis, avaliações de segurança em nuvem e muito mais.

- **Teste manual e automatizado:** Combinando a experiência humana com ferramentas automatizadas para identificação abrangente de vulnerabilidades.
- **Suporte de conformidade:** Garantir a adesão aos padrões regulatórios como ISO 27001, GDPR, HIPAA e PCI DSS.
- **Serviços especializados:** Oferecendo soluções de nicho, como testes de segurança da API, testes de penetração da IoT e exercícios de equipes vermelhas.
- **Integração com oleodutos de desenvolvimento:** Integração perfeita nos fluxos de trabalho de CI/CD para monitoramento contínuo e gerenciamento de vulnerabilidades.

Exemplos de serviços de teste de penetração

As empresas de teste de penetração geralmente oferecem uma ampla gama de serviços:

- **Teste de penetração de rede:** Avaliando a segurança de redes internas e externas para identificar riscos como configurações incorretas ou pontos de acesso não autorizados.
- **Teste de aplicativo da web:** Detectar vulnerabilidades em aplicativos da Web, incluindo injeção de SQL, scripts cruzados (XSS) e falhas de autenticação.
- **Teste de aplicativo móvel:** Avaliando a segurança de aplicativos móveis em plataformas como iOS e Android.
- **Avaliações de segurança em nuvem:** Identificando riscos na infraestrutura da nuvem e garantindo a configuração adequada dos ambientes de nuvem.
- **Exercícios de equipes vermelhas:** Simulando ameaças persistentes avançadas para testar os recursos de detecção e resposta de uma organização.

Por que os testes de penetração são importantes?

Como as organizações devem ser capazes de identificar e reparar vulnerabilidades antes de os atacantes explorá -las, o teste de penetração é essencial.

Como resultado, as empresas podem reduzir a chance de violações de dadosinfecções por malware e outros problemas de segurança cibernética.

O teste de penetração também é importante porque ajuda as empresas a garantir que seus controles de segurança sejam eficazes. As empresas podem examinar suas configurações para ver se precisam ser atualizadas ou substituídas.

O procedimento de teste de penetração é o seguinte:

A primeira etapa em qualquer teste de penetração é coletar informações sobre o sistema de destino. Fontes públicas, como o site de uma empresa, sites de mídia social e mecanismos de pesquisa, podem ser usados ??para obter essas informações.

Uma vez que o testador entende o Arquitetura do sistema e componentes, eles procurarão vulnerabilidades em potencial.

O próximo estágio é utilizar qualquer vulnerabilidade descoberta. Pode ser realizado manualmente ou usando ferramentas automatizadas.

Se o testador puder obter acesso a dados sensíveis ou executar código malicioso, eles tentarão escalar seus privilégios para obter mais controle sobre o sistema.

Finalmente, o testador documentará e apresentará suas descobertas ao cliente. Eles aconselharão como corrigir quaisquer problemas que foram descobertos, além de fornecer recomendações para mais mitigação.

Como escolher as melhores empresas de teste de penetração?

Ao selecionar os melhores serviços de teste de penetração, é importante avaliar cuidadosamente vários fatores para garantir que o provedor de serviços atenda aos seus requisitos e objetivos de segurança exclusivos. Aqui estão algumas dicas para ajudá-lo a tomar uma decisão bem informada:

Reconheça seus requisitos de segurança: Obtenha uma compreensão clara dos aspectos específicos da sua infraestrutura de TI que requerem testes. Possíveis áreas de foco podem ser segurança de rede, aplicativos da Web, aplicativos móveis ou redes sem fio. Compreender seus requisitos permitirá que você escolha uma empresa especializada nessas áreas.

Experiência e experiência: Procure empresas com um forte histórico e extenso histórico em testes de penetração. Veja seus estudos de caso, depoimentos de clientes e reputação do setor. A experiência da equipe, demonstrada através de certificações como OSCP, CEH ou CISSP, também é crucial.

Metodologia e ferramentas: Gostaria de saber mais sobre as metodologias e ferramentas empregadas para testes de penetração. As empresas de primeira linha geralmente aderem a estruturas estabelecidas, como a OWASP para a segurança dos aplicativos da Web, e empregam uma mistura de ferramentas automatizadas e métodos de teste manual.

Personalização e escopo dos serviços: A empresa deve ser capaz de personalizar seus serviços para atender aos seus requisitos específicos. Certifique -se de ter a experiência para conduzir os

tipos específicos de testes de penetração necessários, como caixa preta, caixa branca ou teste de caixa cinza.

Garantir a conformidade legal e ética: A empresa precisa aderir às diretrizes de segurança cibernética e operar dentro de limites legais. Seria ideal se eles estivessem abertos a assinar um Contrato de não divulgação (Nda) para garantir a segurança de seus dados.

Relatórios e suporte completos: Após a realização dos testes, os melhores testes de penetração devem oferecer um relatório detalhado que descreve as vulnerabilidades identificadas, seu nível de gravidade e sugestões para resolvê -las. Descubra se eles ajudam a lidar com essas vulnerabilidades.

Comunicação e gerenciamento de projetos: O sucesso de qualquer empreendimento depende fortemente de comunicação eficaz e gerenciamento de projetos. A empresa precisa fornecer atualizações regulares durante o processo de teste e abordar prontamente quaisquer perguntas ou preocupações que você possa ter.

Custo e valor: Considerando o custo é importante, mas não deve ser o único fator a considerar. Leve em consideração a experiência da empresa, a qualidade do serviço e a potencial economia de custos que vêm da prevenção de violações de segurança.

Referências e revisões do cliente: Para avaliar a satisfação do cliente e o histórico da empresa, é aconselhável solicitar referências ao cliente ou realizar pesquisas on -line para ler críticas e depoimentos.

Engajamento e suporte contínuos: A seleção de uma empresa que fornece suporte contínuo mesmo após a fase de teste é importante. Isso inclui o reteste após a vulnerabilidades terem sido abordados e oferecer conselhos e atualizações valiosos de segurança.

Melhores empresas pentesting: nossas principais escolhas

Raxis

Soluções de teste de penetração de especialistas

- Teste de penetração como um serviço
- Equipe Raxis Red
- Teste de infraestrutura
- Teste de aplicativo da web
- Pentesting em rede
- Serviços de equipe roxa
- Avaliação de segurança pré-aquisição
- Serviços de resposta a incidentes

Laboratórios de ameaças

Serviço gerenciado primeiro para pentesting

- Ameakspike azul
- Ameakspike vermelho
- Exercícios da equipe vermelha
- Teste de infraestrutura
- Teste de aplicativo da web
- Teste de API
- Varredura de vulnerabilidade
- Pentesting em rede

Cobalto

Pentesting mais rápido, mais inteligente e mais forte

- Aplicativo da web PENTEST
- API Pentest
- Aplicativo móvel PENTEST
- Pentest de rede externa
- Pentest de rede interna
- Revisão da configuração da nuvem
- Teste de penetração da AWS
- Pentesting ágil

Melhores empresas de teste de penetração: principais recursos e serviços

Principais empresas de teste de penetração	Principais recursos	Serviços
1. Raxis	PTAAs (rede de rede e web) Pentesting em rede Aplicação e API Pentesting Dispositivo/IoT/Scada Pentesting Equipe vermelha	Teste de penetração como um serviço Simulações de ataque da equipe vermelha Teste de segurança de aplicativos da web Avaliações de vulnerabilidade da API Teste de penetração de infraestrutura de rede

2. Breachlock	Cobertura de ativo de pilha completa Relatórios e priorização em tempo real Especialista liderado, pentesting movido a IA Varredura contínua embutida DevOps Ticketing Integrações Garantia de conformidade Orientação/suporte de remediação de especialistas	Teste de penetração como um serviço (PTAAs) Validação da exposição adversária (Aev) Ataque de superfície de ataque (ASM) Pentesting contínuo Equipe vermelha Gerenciamento contínuo de exposição a ameaças (CTEM)
3. Laboratórios de ameaças	Prevenção de perda de dados forense Filtragem na web Inventário de ativos Proteção de vazamento de dados Firewall da rede	Monitoramento de segurança de rede Detecção de ameaças Resposta de incidentes Gerenciamento de vulnerabilidades Relatórios de conformidade
4. Segurança da roda dentada	Teste de penetração contínuo (CPT) Ataque de superfície de ataque (ASM) Simulações adversárias Relatório sob demanda e executivo Suporte ilimitado de reteste e remediação	Descoberta automática de novos ativos Ferramenta de gerenciamento de superfície de ataque Análise e painel em tempo real Scoping & Recon Work Flows ATOR ATOR / simulação adversária
5. UnderDefense	Simulação avançada de ameaças Relatórios e análises em tempo real Compromissos liderados por especialistas Verificações de conformidade regulatória Orientação de suporte e remediação pós-teste	Teste de penetração de aplicativos Teste de penetração de infraestrutura Teste de segurança da IoT Teste de rede sem fio Operações da equipe vermelha
6. ACUnetix	Testes aprimorados da AI-Ai Cobertura de pilha completa Cenários de teste personalizados Análise de especialistas manuais Relatórios e suporte contínuos	Teste de penetração de aplicativos da web Teste de penetração de rede Segurança da nuvem Teste de penetração baseado em conformidade Teste de penetração de aplicativos móveis
7. Rapid7	Gerenciamento e avaliação de vulnerabilidade Detecção de incidentes e resposta Aplicativo e segurança em	Soluções avançadas de gerenciamento de vulnerabilidades Serviços de resposta a incidentes em tempo real

	nuvem Gerenciamento e teste de conformidade Serviços abrangentes de teste de penetração	Recursos robustos de teste de penetração Teste abrangente de segurança de aplicativos Proteção eficaz de segurança em nuvem
8. Pentera	Testes de penetração automatizados Validação de segurança contínua Relatórios detalhados Escalabilidade Garantia de conformidade	Exercícios de equipes vermelhas Simulações de phishing Teste de penetração de rede Teste de aplicativo da web Avaliação de vulnerabilidade
9. Intruso	Scanner de vulnerabilidade Varredura contínua de rede Suporte ao cliente Digitalizações automatizadas Detecção de App Web App/API	Gerenciamento de vulnerabilidades Teste de penetração Digitalização do servidor de perímetro Segurança da nuvem Segurança de rede
10. Invicti	Teste de segurança de aplicativos da web WAF (Web Application Firewall) Gerenciamento Testes abrangentes de penetração Soluções de teste de conformidade robustas Detecção automatizada de vulnerabilidades	Serviço de varredura de vulnerabilidade automatizada Teste de segurança de aplicativos da web Gestão de firewall de aplicativos da web Serviço de teste de penetração automatizado Serviço de teste de conformidade abrangente

8 benefícios que você pode obter com testes regulares de penetração

1. Encontrar vulnerabilidades de maneira rápida e fácil.
2. É menos provável que ataques cibernéticos e violações de dados aconteçam.
3. Melhor proteção contra ameaças.
4. Tenha mais fé na segurança de seus processos.
5. Prova de que a empresa está seguindo as regras estabelecidas pelos reguladores.
6. Melhor descoberta de eventos e resposta a eles.
7. As operações de segurança agora são mais eficientes e bem -sucedidas.
8. Mais informações sobre os prós e contras de suas configurações de segurança.

10 melhores empresas de teste de penetração 2025

1. **Raxis**
2. **Breachlock**
3. **Laboratórios de ameaças**
4. **Segurança da roda dentada**
5. **UnderDefense**
6. **Avenetix**

7. **Rapid7**
8. **Pentera**
9. **Intruso**
10. **Invicti**

À medida que o mundo muda seu foco para a transformação digital, garantir que seus sistemas e dados sejam seguros se tornassem mais importantes do que nunca. Um dos melhores métodos a fazer isso é o teste de penetração.

Mas existem tantas empresas pentesting disponíveis que decidir o que é apropriado para você pode ser difícil. Portanto, aqui está uma visão detalhada das 10 principais empresas de teste de penetração que podem tornar sua experiência digital melhor do que nunca.

1. Raxis

Raxis Começou como uma loja de testes de penetração de boutique, conhecida por testes completos e uma forte equipe de teste de penetração que possui várias certificações de segurança cibernética de elite, eles também cresceram para se tornar um provedor líder de PTAAs (teste de penetração como serviço).

Enquanto outras opções do PTAAs se concentram em soluções automatizadas ou testadores de nível júnior, sua solução, Raxis Attack, combina ferramentas automatizadas com a mesma equipe de pentesting que executa seus testes tradicionais de penetração.

Os clientes desta solução também obtêm acesso à equipe de teste de penetração do RAXIS por meio de bate-papo ou videoconferência para discutir perguntas sobre as descobertas manuais testadas pelo sexo e automatizadas.

Sua oferta de greve de Raxis ainda oferece uma variedade de testes tradicionais de penetração no tempo. Seus pentests de rede interna podem ser executados remotamente usando seu dispositivo transportador personalizado, no local nos locais dos clientes e também em ambientes em nuvem.

Eles realizam pentestes de rede externa para empresas de todos os tamanhos e afirmam que as empresas que solicitam seu primeiro teste de penetração geralmente escolhem essa opção.

Eles também realizam testes especializados, incluindo pentestes de aplicativos da web para sites de todos os tamanhos, incluindo SaaS, API Pentests e aplicativos móveis e pentests de dispositivos.

A oferta da equipe Raxis Red tem uma alta taxa de sucesso para obter acesso a edifícios, redes internas e informações confidenciais.

Prós e contras

Prós	Contras
Testadores de penetração de elite certificados	Pode ser caro comparado às soluções automatizadas ou de nível júnior
Atende aos requisitos de conformidade	Preços não listados em seu site; deve entrar em contato com Raxis para receber uma cotação
Soluções PTAAs manuais de teste humano	
Plataforma Raxis One personalizada	

Melhor para

- **Detecção de vulnerabilidade especializada**: Identifica as fraquezas ocultas do sistema.
- **Conformidade e segurança**: Garante padrões regulatórios de conformidade.
- **Simulação em tempo real de ameaças**: Simula os cyberattacks do mundo real.

2. Breachlock

Breachlock entrega testes de penetração como um serviço (PTAAS) que combina a automação movida a IA com testes liderados por especialistas, dando às organizações a flexibilidade de testar o que desejam, quando desejam e sempre que necessário, seja periódico ou até contínuo.

Cobrindo aplicativos, APIs, redes, ambientes em nuvem, modelos de IA e IoT, o Breachlock oferece visibilidade de pilha completa através da superfície de ataque em uma plataforma unificada.

A metodologia e modelo de entrega exclusivos da Breachlock permitem que as empresas identifiquem vulnerabilidades em tempo real, priorizem-as com base no risco real e remedie mais rapidamente com orientação clara de remediação e relatórios apoiados por evidências.

A plataforma Unified Breachlock, onde sua solução PTAAS está alojada, consolida Serviços de teste de penetraçãoAtaque o gerenciamento da superfície (ASM), pentesting contínuo, validação de exposição adversária (AEV) e uma união vermelha em uma única solução, reduzindo os silos e a complexidade do gerenciamento das soluções de pontos, fornecendo informações baseadas em riscos que ajudam as equipes de segurança a identificar rapidamente as vulnerabilidades que mais importam e focam os esforços de remediação onde o ROI é mais alto.

Breachlock é um fornecedor de testes de penetração confiável para mais de 1.000 clientes em mais de 20 países, incluindo algumas empresas da Fortune 500.

Prós e contras

Prós	Contras
Acelera a identificação, priorização e remediação de vulnerabilidades	Não há testadores de crowdsourcing, apenas especialistas internos.
Relatórios em tempo real e apoiados por evidências	
Cobertura de ativo escalável e de pilha completa	
Programação e execução mais rápidas	
Fornece informações contextuais aprimoradas da AI-i-i	
Pentesting flexível em tempo, sob demanda e contínuo	

Melhor para

Organizações que desejam testes de penetração flexíveis, sob demanda ou contínuos com integrações de relatórios prontos para conformidade e DevOps.

Empresas e empresas de rápido crescimento que precisam de testes de penetração escaláveis,

flexíveis e eficientes com cobertura unificada de pilha completa em aplicativos, APIs, redes e nuvem.

As equipes de segurança se esforçam para aumentar a frequência ou continuidade de testes de penetração.

3. Laboratórios de ameaças

Laboratórios de ameaças é uma empresa de segurança cibernética que oferece uma plataforma de segurança de endpoint 7 em 1 e serviços de segurança totalmente gerenciados.

Ele combina tecnologias avançadas como IA e aprendizado de máquina com análise especializada para fornecer detecção de ameaças em tempo real, resposta a incidentes, monitoramento de conformidade e serviços de segurança ofensivos.

Principais recursos

- **Segurança do endpoint**: Inclui filtragem na Web, prevenção de perda de dados, heurísticas de ransomware, controle de aplicativos e zoneamento de rede.
- **Detecção de ameaças em tempo real**: Análise movida a IA e monitoramento 24/7 por malware, phishing, ameaças internas e tentativas de hackers.
- **Resposta de incidentes**: Resposta rápida a ameaças com recursos forenses, como gravação de tráfego e forense de disco.
- **Suporte de conformidade**: Garante a adesão a padrões como CIS, GDPR e PCI-DSS com verificações de conformidade do dispositivo.
- **Gestão de ativos**: Rastreia a atividade do endpoint, as configurações e o status do antivírus, enquanto apoia o gerenciamento de inventário.
- **Escalabilidade**: Adequado para empresas de todos os tamanhos com preços de custo fixo.

Prós e contras

Prós	Contras
Suíte abrangente de segurança 7 em 1 em 1	A configuração inicial pode exigir tempo e recursos
Detecção de ameaças em tempo real movida a IA	Recursos avançados podem ser complexos para equipes menores
Forte suporte ao cliente com respostas rápidas	Impacto potencial de desempenho durante o uso pesado
Preços de custo fixo para escalabilidade	Alguns usuários relatam desafios com documentação
Monitoramento de conformidade e relatórios detalhados	Opções de integração limitadas em comparação aos concorrentes

Melhor para

AmeansSpike é ideal para organizações que buscam:

1. Proteção abrangente de endpoint com detecção de ameaças em tempo real.
2. Serviços gerenciados para monitoramento de segurança cibernética e resposta a incidentes.
3. Garantia de conformidade para padrões regulatórios como GDPR ou PCI-DSS.

4. Segurança da roda dentada

A Sprocket Security fornece testes de penetração contínua (CPT) que combinam monitoramento automatizado da superfície de ataque com testadores humanos especializados para validar o risco e reduzir os ciclos de remediação.

A abordagem centrada na plataforma continua testando ligadas a mudanças reais em seu ambiente, para que você seja validado e achados acionáveis ??o ano todo, em vez de um instantâneo único.

Serviços -chave:

Testes de penetração contínua (externa e interna), gerenciamento de superfície de ataque (ASM), simulações de adversário, engenharia social.

Por que escolher a sprocket:

O modelo híbrido da Sprocket desencadeia testes humanos quando as alterações de ativos são detectadas, reduzindo os falsos positivos e garantindo que os testadores validem riscos exploráveis. A empresa enfatiza os fluxos de trabalho orientados a plataformas e os relatórios sob demanda, para que as equipes de segurança e engenharia possam rastrear a remediação com menos atrito.

Credenciais notáveis:

A Sprocket anunciou publicamente a certificação Crest para seus serviços de teste de penetração-um sinal de processo e padrões técnicos verificados independentemente.

Melhor para: Equipes nativas de SaaS e Cloud, no meio do mercado para organizações corporativas que precisam de validação contínua de ativos em rápida mudança e desejam testes de penetração integrados a uma única plataforma.

5. UnderDefense

UnderDefense é uma empresa proeminente de segurança cibernética que oferece serviços especializados em detecção e resposta gerenciada (MDR), teste de penetração, resposta a incidentes e automação de conformidade.

Ele atende às organizações do mercado intermediário e corporativo, fornecendo ferramentas e conhecimentos avançados para proteger contra ameaças cibernéticas.

Principais recursos

- **Serviços MDR**: Monitoramento 24/7, caça proativa de ameaças e tempos de resposta rápidos (até 20 minutos) para detectar e mitigar ameaças.
- **Teste de penetração**: Realiza mais de 160 simulações ofensivas anualmente para identificar vulnerabilidades em sistemas e aplicações.
- **Resposta de incidentes**: Oferece mitigação rápida dos ataques cibernéticos para minimizar o tempo de inatividade e os danos.
- **Automação de conformidade**: A plataforma Maxi simplifica requisitos regulatórios como SOC 2, HIPAA e Compliance GDPR.

- **Monitoramento de superfície de ataque externo**: Identifica vulnerabilidades em ativos voltados para a Internet para evitar a exploração.

A plataforma Maxi da UnderDefense integra ferramentas de segurança existentes com recursos como detecção de ameaças automatizadas, avaliações de prontidão para conformidade, análise de comportamento do usuário e monitoramento de superfície de ataque externo. Ele foi projetado para ambientes em nuvem, híbrido e local, fornecendo recursos abrangentes de visibilidade e resposta.

Prós e contras

Prós	Contras
24/7 de caça de ameaças proativas com tempos de resposta rápidos	Pode não ser econômico para pequenas empresas
Serviços abrangentes, incluindo MDR, teste de penetração e conformidade	Configuração e integração iniciais podem levar tempo
A plataforma Maxi simplifica os fluxos de trabalho de conformidade e segurança	Recursos avançados podem exigir planos de nível superior
Reconhecido globalmente por especialização (por exemplo, Bill & Melinda Gates Foundation)	A forte dependência da automação pode perder informações manuais diferenciadas

Melhor para

UnderDefense é ideal para:

- Organizações que exigem monitoramento contínuo para ameaças avançadas.
- Empresas que precisam de automação de conformidade para regulamentos como SOC 2 ou GDPR.
- Empresas que buscam testes de penetração de especialistas para descobrir proativamente as vulnerabilidades.

6. Acunetix

Acunetix é um poderoso scanner de vulnerabilidade da web projetado para identificar e remediar falhas de segurança em aplicativos, sites e APIs da Web.

Ele detecta mais de 6.500 vulnerabilidades, incluindo injeção de SQL e XSS, e suporta tecnologias da Web modernas, como spas e sites pesados ??de JavaScript.

Com os recursos de integração para pipelines de CI/CD e relatórios detalhados, é uma ferramenta essencial para organizações que desejam aprimorar sua postura de segurança na Web.

O Acunetix fornece opções de implantação local e de implantação em nuvem, tornando-o flexível para vários casos de uso. Sua tecnologia avançada de varredura garante resultados precisos com baixos falsos positivos, mas seus preços premium e suporte limitado de testes manuais podem representar desafios para organizações menores ou para aqueles que exigem mais testes práticos.

Prós e contras

Prós	Contras
Alta precisão com baixas taxas falsas positivas	Caro para organizações menores

Prós	Contras
Suporta tecnologias da web modernas como spas	Suporte de teste manual limitado
Integra -se perfeitamente com ferramentas de CI/CD	As varreduras intensivas em recursos podem afetar o desempenho do servidor
Atualizações regulares para abordar ameaças emergentes	Requer configuração adequada para obter melhores resultados

Melhor para

O Acunetix é o melhor para organizações de médio a grande porte, testadores de penetração e equipes DevSeCops que desejam automatizar a detecção de vulnerabilidades na Web com recursos e integrações avançados.

7. Rapid7

Rapid7 é uma empresa líder em segurança cibernética que oferece uma plataforma unificada para gerenciamento de vulnerabilidades, detecção e resposta, segurança em nuvem e segurança de aplicativos.

Ele combina ferramentas avançadas, automação e serviços especializados para ajudar as organizações a gerenciar riscos, evitar violações e proteger seus ambientes de maneira eficaz.

Principais recursos

- **Plataforma Insight**: Uma solução unificada para gerenciamento de vulnerabilidades (InsightVM), detecção e resposta (insightIdr), testes de segurança de aplicativos dinâmicos (InsightAppSec) e gerenciamento de riscos em nuvem (InsightCloudSec).
- **Detecção e resposta gerenciadas (MDR)**: Monitoramento 24/7, detecção de ameaças e resposta a incidentes com especialistas do SOC.
- **Gerenciamento de vulnerabilidades**: O InsightVM fornece visibilidade contínua sobre riscos entre os ambientes locais, nuvem e híbridos com orientação de remediação priorizada.
- **Segurança de aplicativos**: O InsightAppPsec usa o Dynamic Application Security Testing (DAST) para identificar vulnerabilidades em aplicativos da Web.
- **Segurança da nuvem**: O InsightCloudsec oferece riscos abrangentes em nuvem e gerenciamento de conformidade para ambientes de várias nuvens.
- **Automação e orquestração**: Simplina os fluxos de trabalho com inteligência de ameaças automatizadas, rastreamento de remediação e integrações com ferramentas como Jira e Slack.
- **Ferramentas de código aberto**: Mantém as comunidades de metasploit e velociraptor para testes de penetração e forense digital.

Prós e contras

Prós	Contras
Plataforma unificada para segurança de ponta a ponta	A configuração inicial pode ser complexa para alguns usuários
Serviços de MDR 24/7 com suporte especial	Recursos avançados podem exigir uma curva de aprendizado acentuada
Fortes recursos de gerenciamento de vulnerabilidades	Os preços podem ser altos para organizações menores

Prós	Contras
Ferramentas nativas da nuvem para ambientes de várias nuvens	Algumas ferramentas podem gerar falsos positivos
Contribuições de código aberto como metasploit	Personalização limitada em determinados fluxos de trabalho

Melhor para

Rapid7 é ideal para:

1. As organizações que precisam de uma plataforma de segurança abrangente que cobre gerenciamento, detecção, resposta e segurança em nuvem de vulnerabilidades.
2. Empresas que exigem serviços gerenciados como o MDR para descarregar operações de segurança diárias.
3. Empresas que procuram automação para otimizar os esforços de detecção, remediação e conformidade de ameaças.

8. Pentera

Pentera é uma empresa de segurança cibernética especializada em validação de segurança automatizada ™. Sua plataforma permite que as organizações testem continuamente suas defesas, simulando ataques do mundo real, identificando vulnerabilidades e priorizando os esforços de remediação.

Fundada em 2015 como PCYSYS e renomeada em 2021, a Pentera é confiável por mais de 950 empresas em 45 países.

Principais recursos

- **Validação de segurança automatizada ™**: Emula o comportamento adversário para testar superfícies de ataque internas e externas, incluindo ambientes em nuvem, sem a necessidade de agentes ou manuais.
- **Simulação de ataque abrangente**: Testes vulnerabilidades usando técnicas como movimento lateral, exploração de credenciais, simulação de ransomware e exfiltração de dados.
- **Priorização baseada em risco**: Fornece orientação de remediação acionável com base na gravidade e no impacto potencial das vulnerabilidades.
- **Produtos modulares**:
    - *Pentera Core*: Valida os controles internos de segurança da rede.
    - *Superfície pentera*: Concentra -se na segurança de rede externa.
    - *Nuvem pentera*: Protege ambientes em nuvem.
    - *Módulo Ransomwareready*: Testes a resiliência contra ataques de ransomware.
    - *Módulo de exposição de credenciais*: Identifica os riscos de credenciais vazadas.
- **Pentera Labs**: Equipe de pesquisa que atualiza continuamente a plataforma com as mais recentes técnicas de inteligência e ataque de ameaças.

Prós e contras

Prós	Contras
O design sem agente garante fácil implantação	A configuração inicial pode exigir experiência

Prós	Contras
Validação contínua de controles de segurança	Recursos avançados podem ser caros para equipes menores
Simulações de ataque do mundo real com correntes de matança completas	Personalização limitada para casos de uso específicos
Orientação de remediação baseada em risco	Pode não substituir o teste de penetração manual totalmente
Aumenta a produtividade da equipe (até 5x)	Requer atualizações regulares para se manter eficaz

Melhor para

Pentera é ideal para:

1. Empresas que buscam validação contínua de segurança em ambientes internos, externos e em nuvem.
2. As organizações que desejam identificar e remediar proativamente as vulnerabilidades antes de os atacantes as exploram.
3. As equipes de segurança que desejam automatizar o pentesting e melhorar a produtividade.

9. Intruder

Intruso é uma plataforma de gerenciamento de vulnerabilidades baseada em nuvem projetada para ajudar as organizações a identificar, priorizar e remediar as fraquezas de segurança cibernética.

Oferece monitoramento contínuo, detecção de ameaças em tempo real e digitalização proativa de segurança para sistemas voltados para a Internet, tornando-a uma ferramenta valiosa para empresas com o objetivo de reduzir sua superfície de ataque e impedir que as violações de dados.

Principais recursos

- **Varredura de vulnerabilidade**: Detecta e prioriza questões como injeção de SQL, scripts de sites cruzados (XSS), falhas de criptografia e equívocas.
- **Monitoramento contínuo**: Digitaliza automaticamente as vulnerabilidades e fornece alertas sobre novas ameaças ou mudanças na superfície de ataque.
- **Digitalização do perímetro**: Monitora ativos voltados para a Internet para identificar exposição desnecessária e reduzir os riscos.
- **Gerenciamento de patches**: Identifica os patches ausentes em software, estruturas e hardware.
- **Suporte de integração**: Funciona perfeitamente com ferramentas como Jira, Slack, Microsoft Teams, AWS, Azure e Google Cloud.
- **Suporte de conformidade**: Ajuda a atender a padrões como GDPR e PCI-DSS, fornecendo relatórios detalhados.
- **Facilidade de uso**: Plataforma baseada em SaaS com configuração simples e interface intuitiva.

Prós e contras

Prós	Contras
Plataforma SaaS fácil de usar com configuração	Recursos avançados limitados em comparação

Prós	Contras
rápida	aos concorrentes
O monitoramento contínuo garante proteção atualizada	Não pode substituir testes de penetração manual detalhados
Forte priorização de vulnerabilidades	Planos de nível superior podem ser caros para pequenas empresas
Integração perfeita com ferramentas populares	Personalização limitada para necessidades específicas de varredura
Atualizações regulares para incluir as ameaças mais recentes	Concentra -se principalmente em vulnerabilidades externas

Melhor para

Intruder é ideal para:

1. Empresas pequenas e médias que precisam de gerenciamento de vulnerabilidade acessível, mas robusto.
2. Organizações que procuram monitoramento contínuo de sistemas voltados para a Internet.
3. Equipes que exigem fácil integração com os fluxos de trabalho e ferramentas existentes.

10. Invicti

Invicti é uma plataforma líder de segurança de aplicativos da Web, especializada em testes de segurança de aplicativos dinâmicos (DAST) e Teste de Segurança de Aplicativos Interativos (IAST).

Ajuda as organizações a proteger seus aplicativos e APIs da Web, automatizando a detecção, priorização e remediação de vulnerabilidades. A Invicti é confiável por milhares de organizações globalmente por sua precisão, escalabilidade e recursos de integração.

Principais recursos

- **Scanning ™ baseado em prova**: Verifica automaticamente vulnerabilidades explorando -as com segurança para eliminar falsos positivos e fornecer provas de exploração.
- **Teste de segurança abrangente**: Combina Dast e IAST para detectar vulnerabilidades, como injeção de SQL, XSS e muito mais em aplicativos da Web e APIs.
- **Automação e integração**: Integra -se aos pipelines CI/CD, rastreadores de emissão (por exemplo, JIRA, GitHub) e ferramentas de comunicação (por exemplo, Slack, Teams Microsoft) para fluxos de trabalho de devsecops sem costura.
- **Escalabilidade**: Projetado para proteger milhares de ativos da Web com recursos como varredura contínua, teste de API e rastreamento avançado.
- **Suporte de conformidade**: Ajuda a atender aos padrões como PCI-DSS, GDPR e SOC 2 com relatórios prontos para a auditoria.
- **Pontuação preditiva de risco**: Usa a IA para priorizar as vulnerabilidades com base em seu potencial impacto.

Prós e contras

Prós	Contras
Altamente preciso com o mínimo de falsos positivos	Recursos avançados podem exigir conhecimento técnico

Prós	Contras
A varredura baseada em prova economiza tempo na validação	Os preços podem ser altos para pequenas empresas
Combina Dast, IAST e SCA em uma plataforma	A configuração inicial pode demorar muito tempo
Integração perfeita nos fluxos de trabalho do SDLC	Personalização limitada para casos de uso de nicho
Escalável para grandes empresas	Concentra -se principalmente em aplicativos da web

Melhor para

Invicti é ideal para:

1. Empresas que precisam de segurança de aplicativos escaláveis ??para milhares de ativos da Web.
2. As equipes do DevSecops que buscam detecção automatizada de vulnerabilidades integradas aos pipelines de CI/CD.
3. Organizações que exigem suporte de conformidade com relatórios prontos para a auditoria.

Conclusão

Teste de penetração é um aspecto indispensável do sistema e segurança de dados. Ao selecionar um provedor respeitável e experiente, você pode ter certeza de que seus sistemas estão seguros e que quaisquer vulnerabilidades sejam encontradas e corrigidas antes que possam ser exploradas.

À medida que o mundo avança, mais empresas estão online, aumentando a vulnerabilidade a Ataques cibernéticos. Para proteger seus ativos e dados, é essencial investir em uma empresa de pentesting confiável que oferece uma gama abrangente de serviços.

Porque existem muitas alternativas, descobrir o melhor vale o esforço.