10 melhores ferramentas de simulação de violação e ataque (BAS) em 202

Data: 2025-09-12 17:13:49

Autor: Inteligência Against Invaders

Melhores ferramentas de violação e ataque (BAS)

Em 2025, o cenário da cibersegurança é definido por sua complexidade e velocidade das ameaças modernas.

As equipes de segurança estão impressionadas com uma variedade fragmentada de controles de segurança e a falta de visibilidade clara do que realmente está funcionando.

As plataformas de simulação de violação e ataque (BAS) resolvem esse problema, validando de maneira contínua e segura as defesas de segurança contra o mundo real cenários de ataque.

Essas ferramentas automatizam o processo de um teste de penetração manual ou exercícios da equipe vermelha, fornecendo às equipes de segurança insights orientados a dados para identificar e remediar proativamente as fraquezas antes que possam ser exploradas por um adversário.

Por que escolhemos a simulação de violação e ataque (BAS)

Os métodos tradicionais de validação de segurança, como testes de penetração manual, geralmente são lentos, caros e fornecem apenas um instantâneo de ponto de vista da postura de segurança de uma organização.

As plataformas BAS, por outro lado, oferecem validação contínua de segurança em escala.

Ao simular uma ampla gama de técnicas de ataque e matar as cadeias do acesso inicial aos dados da Exfiltração de Dados, pode avaliar automaticamente a eficácia dos controles de segurança de uma organização, priorizar os riscos mais críticos e fornecer orientação clara de remediação.

Isso é crucial para manter uma postura de segurança proativa e resiliente em um mundo de alterações constantes.

Como escolhemos as melhores empresas de simulação de violação e ataque (BAS)

Para compilar esta lista das principais empresas da BAS, avaliamos -as com base nos seguintes critérios:

Experiência e experiência (EE): Focamos em empresas com um forte histórico, um profundo entendimento das metodologias de atacantes e um fluxo contínuo de novos cenários de ataque relevantes.

Autoridade e confiabilidade (AT): Consideramos liderança de mercado, reconhecimento da indústria de empresas como Gartner e Forrester e sua capacidade de fornecer informações precisas e acionáveis.

Riqueza de recursos: Avaliamos a amplitude e a profundidade de suas plataformas, procurando recursos principais em:

Validação contínua: A capacidade de correr testes automatizados em uma base contínua.

Integração de inteligência de ameaças: A capacidade de se integrar à mais recente inteligência de ameaças do mundo real.

Orientação de remediação: Fornecendo etapas claras e priorizadas para corrigir vulnerabilidades identificadas.

MITRE ATT & CK Alinhamento: Mapeamento de simulações de ataques diretamente para a estrutura do Mitre ATT e CK padrão do setor.

Comparação dos principais recursos (2025)

1. Cymulate

Cymulate é uma plataforma de BAS líder que fornece uma ampla gama de ataque automatizado Simulações para validar controles de segurança em toda a cadeia de mortes.

A plataforma oferece uma abordagem modular, permitindo que as organizações testem tudo, desde a segurança de phishing e gateway da web até o movimento lateral e a exfiltração de dados.

O foco da Cymulate em fornecer uma pontuação clara de segurança e os relatórios acionáveis ??ajudam as empresas a entender rapidamente sua postura de risco e priorizar os esforços de remediação.

Por que você quer comprar:

A plataforma da Cymulate é altamente escalável e fornece uma pontuação de segurança clara e orientada a dados, fácil para entender as partes interessadas técnicas e não técnicas.

Seu design modular permite que as organizações comecem com avaliações específicas e se expandam conforme necessário.

Recurso	Sim/não	Especificação
Validação contínua	? Sim	Avaliações automatizadas para todos os vetores de ataque.
Inteligência de ameaças	? Sim	Emula os mais recentes ataques baseados na inteligência de ameaças.
Orientação de remediação	? Sim	Recomendações acionáveis ??para ajuste de controle de segurança.

Recurso	Sim/não	Especificação
MITRE ATT & CK	? Sim	Mapas todos os resultados da simulação para a estrutura ATT & CK.

? **Melhor para:** Empresas de todos os tamanhos que precisam de uma plataforma BAS abrangente e fácil de usar para avaliar continuamente sua postura de segurança e medir a eficácia de seus investimentos em segurança.

`Try Cymulate here ?` [`Cymulate Official Website`]

2. Attackiq

O ataques é uma plataforma BAS de nível empresarial que oferece uma solução de validação de segurança poderosa e flexível.

É conhecido por sua extensa biblioteca de conteúdo alinhada à Mitre ATT e CK, que fornece às equipes de segurança milhares de cenários de ataque realistas.

A plataforma aberta e as integrações da Aactiq com uma ampla gama de fornecedores de segurança o tornam uma pedra angular para organizações que desejam criar um programa de segurança orientado a dados e medir o ROI de suas ferramentas de segurança.

Por que você quer comprar:

A plataforma do ATTILIQ é construída sobre a estrutura do Mitre ATT & CK padrão do setor, fornecendo um idioma comum para a validação de segurança.

Sua arquitetura aberta e extensa biblioteca de conteúdo o tornam uma ferramenta poderosa para criar um programa de segurança proativo e orientado a dados.

Recurso	Sim/não	Especificação
Validação contínua	? Sim	Teste contínuo de controles de segurança.
Inteligência de ameaças	? Sim	Emula os ataques com base na mais recente inteligência.
Orientação de remediação	? Sim	Fornece orientações passo a passo para corrigir lacunas de segurança.
MITRE ATT & CK	? Sim	Biblioteca de conteúdo extensa alinhada com a estrutura ATT & CK.

? **Melhor para:** Grandes empresas e agências governamentais que precisam de uma plataforma altamente personalizável e orientada a dados para validar continuamente seus controles de segurança e medir a eficácia de suas defesas.

`Try AttackIQ here ?` [`AttackIQ Official Website`]

3. SafeBreach

O SafeBreach fornece uma plataforma de simulação de violação e ataque que cria um “gêmeo digital” do ambiente de segurança de uma organização.

Ao implantar simuladores leves em toda a rede, o SafeBreach pode executar simulações contínuas e não-discretas para testar Controles de segurança de uma maneira realista.

A extensa biblioteca de “manual de hackers” da plataforma, que contém milhares de cenários de ataque, garante que as organizações estejam sempre testando as últimas ameaças.

Por que você quer comprar:

A abordagem “gêmea digital” do SafeBreach fornece uma visão altamente realista e abrangente da postura de segurança de uma organização.

A capacidade da plataforma de simular ataques em toda a cadeia de mortes ajuda as equipes de segurança a priorizar os riscos mais críticos e entender o verdadeiro impacto de uma violação.

Recurso	Sim/não	Especificação
Validação contínua	? Sim	Simulações contínuas e não-disruptivas.
Inteligência de ameaças	? Sim	“Hacker’s Playbook” com milhares de cenários de ataque.
Orientação de remediação	? Sim	Recomendações acionáveis ??para ajuste de controle de segurança.
MITRE ATT & CK	? Sim	Mapas todos os cenários de ataque para a estrutura ATT & CK.

? **Melhor para:** As equipes de segurança que desejam testar continuamente suas defesas contra uma ampla gama de ataques e ver como as vulnerabilidades podem ser acorrentadas para criar uma cadeia de mortes.

`Try SafeBreach here ?` `SafeBreach Official Website`

4. Segurança do Picus

A Picus Security é uma plataforma líder de BAS que fornece uma abordagem orientada a dados para a validação de segurança.

Sua plataforma, a plataforma de validação de segurança completa do PICUS, testa de maneira contínua e automaticamente os controles de segurança em relação a uma vasta biblioteca de ameaças do mundo real.

O PICUS é particularmente forte no fornecimento de orientação de remediação específica do fornecedor, ajudando as equipes de segurança rapidamente a ajustar suas ferramentas de segurança para maximizar sua eficácia.

Por que você quer comprar:

O foco da PICUS em fornecer recomendações específicas de fornecedores é um grande diferencial.

Ajuda as equipes de segurança a tirar o máximo proveito de seus investimentos de segurança existentes, fornecendo um caminho claro e automatizado para a remediação.

Recurso	Sim/não	Especificação
Validação contínua	? Sim	Validação de segurança automatizada contínua.
Inteligência de ameaças	? Sim	Uma vasta biblioteca de ameaças do mundo real.
Orientação de remediação	? Sim	Recomendações específicas do fornecedor para ajustar os controles de segurança.
MITRE ATT & CK	? Sim	Mapeamento completo para a estrutura ATT & CK.

? **Melhor para:** As equipes de segurança que precisam medir a eficácia de seus produtos de segurança em tempo real e desejam orientações claras específicas para o fornecedor sobre como melhorar suas defesas.

`Try Picus Security here ?` [`Picus Security Official Website`]

5. XM Cyber

O XM Cyber ??fornece uma plataforma BAS que se concentra no gerenciamento de caminhos de ataque.

Sua plataforma identifica e prioriza automaticamente os caminhos de ataque mais críticos, ajudando as equipes de segurança a entender como um invasor poderia se mover por sua rede.

O foco do XM Cyber ??em caminhos de ataque, em vez de apenas vulnerabilidades individuais, fornece uma maneira mais estratégica e eficaz de reduzir o risco e melhorar Postura de segurança.

Por que você quer comprar:

A plataforma da XM Cyber ??fornece uma visão única e baseada em gráficos da postura de segurança de uma organização.

Ao identificar e priorizar os caminhos de ataque, ajuda as equipes de segurança a concentrar seus recursos limitados nas fraquezas que mais importam.

Recurso	Sim/não	Especificação
Validação contínua	? Sim	Análise de caminho de ataque contínuo.
Inteligência de ameaças	? Sim	Emula as mais recentes técnicas de ataque.
Orientação de remediação	? Sim	Fornece orientações priorizadas para quebrar os caminhos de ataque.
MITRE ATT & CK	? Sim	Mapas atacam caminhos para a estrutura ATT & CK.

? **Melhor para:** As equipes de segurança que desejam ir além das vulnerabilidades individuais e se concentrarem nos caminhos mais prováveis ??de atacar que um adversário levaria para comprometer sua rede.

`Try XM Cyber here ?` [XM Cyber Official Website]

6. Scythe

A Scythe é uma plataforma de emulação de adversário que capacita as equipes vermelhas e os profissionais de segurança a conduzir exercícios realistas e roxos da equipe.

Ao contrário das plataformas BAS totalmente automatizadas, a Scythe se concentra em fornecer um kit de ferramentas flexível e poderoso para simular ataques sofisticados.

Sua plataforma permite que as equipes de segurança criem campanhas de ataque personalizadas, testem TTPs específicos (táticas, técnicas e procedimentos) e validem seus controles de segurança em um ambiente controlado.

Por que você quer comprar:

A Scythe fornece um poderoso kit de ferramentas para profissionais de segurança que desejam ir além das simulações pré-construídas.

Sua flexibilidade permite que as equipes simulem cenários de ataque altamente específicos e validem suas defesas contra as ameaças mais sofisticadas.

Recurso	Sim/não	Especificação
Validação contínua	? Sim	Testes contínuos e sob demanda.
Inteligência de ameaças	? Não	O foco está nos cenários de ataque personalizados.
Orientação de remediação	? Sim	Fornece orientações técnicas claras para remediação.
MITRE ATT & CK	? Sim	Uma vasta biblioteca de técnicas ATT e CK.

? **Melhor para:** Equipes de segurança avançadas, equipes vermelhas e MSSPs que precisam de

uma plataforma flexível e poderosa para realizar simulações de ataque realistas e personalizadas.

Try Scythe here ? Scythe Official Website

7. Randori (IBM Security Randori Recon)

Randori, agora parte da IBM Security, oferece uma abordagem única do BAS e do gerenciamento de superfície de ataque.

Sua plataforma combina descoberta contínua com simulações de ataque automatizado, fornecendo uma visão panorâmica de uma organização superfície de ataque externo.

A tecnologia de Randori investiga com segurança os ativos externos de uma organização, identificando fraquezas e fornecendo uma lista priorizada de vulnerabilidades que provavelmente serão direcionadas por um invasor real.

Por que você quer comprar:

A plataforma de Randori fornece uma perspectiva única e externa sobre a postura de segurança de uma organização.

Ao investigar continuamente a superfície de ataque externa, ajuda as equipes de segurança a descobrir e remediar vulnerabilidades antes de serem encontradas por um adversário.

Recurso	Sim/não	Especificação
Validação contínua	? Sim	Simulação contínua de sondagem e ataque.
Inteligência de ameaças	? Sim	Fornece uma visão panorâmica da superfície de ataque.
Orientação de remediação	? Sim	Lista priorizada de vulnerabilidades para remediar.
MITRE ATT & CK	? Sim	Mapas atacam simulações à estrutura ATT & CK.

? **Melhor para:** As equipes de segurança que desejam ter uma visão panorâmica de sua superfície de ataque externa e validar continuamente suas defesas contra ameaças do mundo real.

Try Randori here ? IBM Security Randori Recon Official Website

8. Firecompass

O Firecompass fornece uma plataforma de equipes de superfície de superfície vermelha automatizada contínua e de ataque.

Sua tecnologia descobre continuamente a pegada digital de uma organização e lança ataques automatizados de hackers éticos para encontrar vulnerabilidades exploráveis.

A plataforma da Firecompass foi projetada para fornecer uma abordagem contínua e proativa da segurança, ajudando as organizações a encontrar e a corrigir fraquezas antes de serem alavancadas por um invasor real.

Por que você quer comprar:

O FireCompass fornece uma única plataforma para o gerenciamento de superfície de ataque e a equipe automatizada de redes vermelhas.

Essa abordagem integrada garante que as organizações possam descobrir e remediar continuamente suas vulnerabilidades mais críticas, fornecendo uma postura de segurança proativa e resiliente.

Recurso	Sim/não	Especificação
Validação contínua	? Sim	Equipes vermelhas automatizadas contínuas.
Inteligência de ameaças	? Sim	Usa técnicas de ataque do mundo real.
Orientação de remediação	? Sim	Fornece conselhos de remediação clara e priorizados.
MITRE ATT & CK	? Sim	Mapas Atacar os cenários da estrutura ATT & CK.

? **Melhor para:** As empresas que precisam descobrir continuamente sua pegada digital e validar seus controles de segurança contra cenários de ataque do mundo real.

`Try FireCompass here ?` `FireCompass Official Website`

9. Cronus

A Cronus Cyber ??Technologies oferece uma plataforma de teste de penetração automatizada que se concentra na identificação de vulnerabilidades na rede, aplicativos e aplicativos de uma organização e Ambientes em nuvem.

Sua plataforma, Cybot, fornece uma abordagem contínua e automatizada para a validação de segurança, ajudando as organizações a identificar e remediar as fraquezas antes que possam ser exploradas.

O foco de Cronus nos testes automatizados o torna uma solução escalável e econômica para uma ampla gama de organizações.

Por que você quer comprar:

A plataforma da Cronus Cyber ??fornece uma maneira altamente automatizada e eficiente de realizar testes de penetração.

Seu foco nos testes contínuos garante que as organizações possam identificar e remediar

rapidamente vulnerabilidades, melhorando sua postura geral de segurança.

Recurso	Sim/não	Especificação
Validação contínua	? Sim	Teste de penetração contínuo e automatizado.
Inteligência de ameaças	? Sim	Emula uma ampla gama de cenários de ataque.
Orientação de remediação	? Sim	Fornece orientação de remediação clara e acionável.
MITRE ATT & CK	? Sim	Mapas todas as descobertas para a estrutura ATT & CK.

? **Melhor para:** As organizações que precisam de uma plataforma escalável de teste de penetração automatizadas para testar continuamente sua rede e aplicativos para vulnerabilidades.

`Try Cronus Cyber Technologies here ?`
`Cronus Cyber Technologies Official Website`

10. Verodin

A Verodin, agora parte da Keysight, é um participante fundamental no espaço do BAS, conhecido por seu foco em fornecer uma abordagem orientada a dados para a validação de segurança.

A plataforma de operações de segurança Keysight (que inclui a tecnologia Verodin) foi projetada para ajudar as equipes de segurança a entender a verdadeira eficácia de seus controles de segurança.

Ao simular ataques e medir os resultados, a Verodin fornece uma visão clara e objetiva da postura de segurança de uma organização e ajuda a justificar os investimentos em segurança.

Por que você quer comprar:

A plataforma da Verodin fornece uma visão clara e objetiva da postura de segurança de uma organização.

Ao medir a eficácia dos controles de segurança, ajuda as equipes de segurança a tomar decisões orientadas a dados e a demonstrar o ROI de seus investimentos em segurança.

Recurso	Sim/não	Especificação
Validação contínua	? Sim	Validação de segurança automatizada contínua.
Inteligência de ameaças	? Sim	Integra -se à mais recente inteligência de ameaças.
Orientação de remediação	? Sim	Fornece orientações claras e priorizadas.
MITRE ATT & CK	? Sim	Mapas todas as descobertas para a estrutura ATT & CK.

? **Melhor para:** As grandes empresas que precisam de uma plataforma orientada a dados para medir a eficácia de seus controles de segurança e justificar seus investimentos em segurança.

`Try Verodin here ?` `Verodin Official Website`

Conclusão

Em 2025, a simulação de violação e ataque (BAS) é indispensável para qualquer organização sério sobre proativo segurança cibernética.

Eles fornecem uma camada vital de validação contínua que vai muito além das avaliações tradicionais e pontuais. As principais empresas desta lista oferecem pontos fortes únicos.

Cymulate, Attackiq e SafeBreach lideram com plataformas abrangentes e escaláveis ??para uma ampla gama de necessidades. XM Cyber ??e Randori se destacam por seu foco na visão panorâmica de um hacker, priorizando os caminhos de ataque e as ameaças externas.

Para organizações que precisam de uma ferramenta altamente técnica e personalizável, a Scythe fornece uma solução ideal.

Por fim, a melhor plataforma BAS para sua organização dependerá de seu tamanho, maturidade de segurança e metas específicas, mas qualquer uma dessas 10 principais opções melhorará significativamente sua capacidade de identificar e remediar fraquezas antes que um invasor real possa explorá -los.