Fornecedores de detecção de ameaças cibernéticas desistem do teste de

Data: 2025-09-22 14:00:00

Autor: Inteligência Against Invaders

Três grandes fornecedores de soluções de segurança cibernética decidiram não participar da edição

de 2025 do teste anual de solução de detecção e resposta de endpoint (EDR) do MITRE.

Depois que a Microsoft anunciou que não participaria do MITRE Engenuity ATT&CK Evaluations: Enterprise 2025 em junho, a SentinelOne e a Palo Alto Networks confirmaram em 12 de setembro que também estavam se retirando do teste para este ano.

Essas decisões levantaram preocupações entre a comunidade de segurança cibernética sobre o futuro e a relevância do programa. Esses movimentos são especialmente surpreendentes, pois as três empresas são grandes fornecedores de segurança cibernética e todas tiveram um bom desempenho no teste de 2024, no qual a solução da Microsoft superou os testes do MITRE, o SentinelOne ficou em quinto lugar e Palo Alto em 12º.

É uma decisão particularmente surpreendente para a Microsoft, que usou sua classificação no teste para promover sua solução, Microsoft Defender XDR, em dezembro de 2024.

Curiosamente, todas as três empresas justificaram a mudança dizendo que queriam priorizar o desenvolvimento e a inovação de produtos.

No entanto, especialistas sugeriram que outros fatores também podem estar em jogo, incluindo os testes se tornando cada vez mais vistos como promocionais, em vez de obter ganhos reais de segurança.

Segurança da informação conversou com Charles Clancy, CTO do MITRE e vice-presidente sênior do MITRE Labs, que compartilhou elementos-chave da evolução do teste de avaliação que poderiam explicar as decisões antes dos resultados do teste deste ano em dezembro de 2025.

História de fundo das avaliações da ATT&CK: Enterprise

A MITRE Corporation é uma organização sem fins lucrativos com sede nos EUA que executa muitos programas de segurança cibernética, incluindo alguns em nome do governo dos EUA.

O MITRE introduziu sua estrutura ATT&CK em 2015, que rapidamente se tornou a ferramenta

padrão no setor de segurança cibernética para mapear técnicas, táticas e procedimentos (TTPs) de adversários cibernéticos do mundo real.

Em 2019, a MITRE ATT&CK lançou seu primeiro programa de avaliações para “preencher uma lacuna no mercado de testes de segurança”, argumentou Clancy.

“Havia muitos tipos de testes de terceiros para produtos de segurança cibernética, mas cada um deles tinha seu próprio processo e metodologia de pontuação, levando a resultados inconsistentes e falta de rigor que não estava impulsionando o setor”, explicou.

Avaliações MITRE Engenuity ATT&CK: Enterprise é o mais regular de todos os testes de avaliação, ocorrendo todos os anos desde o seu lançamento.

Em uma postagem no LinkedIn, Igal Gofman, diretor de engenharia da CrowdStrike e ex-pesquisador de segurança da Microsoft e da Tenable, chamou o teste de “Olimpíadas da segurança cibernética”.

Entre as 1000 pessoas que trabalham na prática de segurança cibernética da MITRE, 133 são dedicadas à MITRE ATT&CK, das quais 12 a 15 pessoas estão trabalhando na Testes de avaliações , Clancy disse *Segurança da informação*.

A cada ano, a equipe por trás do programa de testes escolhe um dos vários adversários da vida real e/ou cadeias de ataque com base em seus TTPs mapeados no ATT&CK.

Em seguida, eles testam as soluções EDR dos fornecedores participantes em ataques simulados usando o Caldera, a própria plataforma automatizada de emulação de adversários do MITRE, de acordo com vários critérios, incluindo resultados de detecção, falsos positivos e verdadeiros negativos.

Embora esse teste possa ser usado para comparar a eficácia das soluções de EDR, Clancy observou que ele não deve ser visto como uma referência longitudinal porque cada teste anual difere muito do anterior.

“O ethos que estamos tentando impulsionar nos testes é a comparação de um produto individual para detectar um determinado agente de ameaça. Simular diferentes adversários ano após ano é realmente importante para entender as diferentes classes de ameaças emergentes”, disse Clancy.

Por dentro das edições 2024 e 2025 do teste

Em 2024, o MITRE ATT&CK Evaluations: Enterprise emulou 14 técnicas em 7 táticas de hackers conhecidos afiliados à Coreia do Norte, 16 técnicas em 7 táticas do grupo de ransomware CL0P e 31 técnicas em 11 táticas do grupo de ransomware LockBit.

A CrowdStrike, um dos principais fornecedores de EDR, não participou da edição daquele ano, com um membro do subreddit da CrowdStrike – que alegou estar trabalhando para a empresa – Sugerindo que a avaliação foi definida para ocorrer logo após a interrupção global de 19 de julho que afetou o produto EDR da empresa.

Naquele ano, a Microsoft, ESET e Cybereason lideraram o ranking, seguidos por ThreatDown, SentinelOne e Bitdefender.

Em 2025, a equipe de avaliações da ATT&CK selecionou dois cenários:

- Um cenário de aranha dispersa: intrusão multifacetada em um ambiente híbrido que apresenta engenharia social, exploração de infraestrutura em nuvem, abuso de identidade e técnicas de viver da terra (LOTL)
- Um cenário de ciberespionagem alinhado com a China: intrusão evasiva destacando o uso hábil de engenharia social pelo adversário, abuso de aplicativos e serviços legítimos, estabelecimento de mecanismos persistentes e emprego de malware personalizado para evitar a detecção

Embora ele tenha admitido que os fornecedores podem variar ano após ano, Clancy garantiu que eles podem contar com “muitos clientes recorrentes”.

Por que os fornecedores estão saindo do MITRE’s Test

No entanto, a edição deste ano, cujos resultados são esperados para dezembro, não terá três grandes players: Microsoft, SentinelOne e Palo Alto Networks.

A Microsoft anunciou que não participará do teste deste ano em 13 de junho, alegando que essa decisão “nos permite concentrar todos os nossos recursos na Secure Future Initiative e no fornecimento de inovação de produtos aos nossos clientes”.

Em 12 de setembro, SentinelOne e Palo Alto divulgaram declarações semelhantes.

O primeiro disse que queria “priorizar nossos recursos de produto e engenharia em iniciativas focadas no cliente enquanto acelera nosso roteiro de plataforma”, enquanto o último explicou que essa decisão “nos permite acelerar ainda mais as inovações críticas da plataforma que abordam diretamente os desafios de segurança mais urgentes de nossos clientes e respondem ainda mais rápido ao cenário de ameaças em evolução”.

Quando contatado por *Segurança da informação*, a SentinelOne e a Palo Alto Networks se recusaram a fornecer mais comentários. A Microsoft não respondeu a um pedido de comentário.

No entanto, Clancy, do MITRE, disse que está em contato próximo com os três fornecedores e acredita que conhece os motivos que os fizeram desistir do teste deste ano.

Primeiro, como os fornecedores disseram em suas declarações, participar do programa de avaliações MITRE ATT & CK requer um compromisso intensivo de recursos, sugerindo que o tempo e o pessoal dedicados a ele são perdidos em outros projetos.

Então, Clancy disse que a equipe por trás do teste se esforça para torná-lo mais difícil a cada ano e admitiu que pode ter ido longe demais este ano.

“A cada ano, queremos projetar um teste mais difícil do que no ano anterior, a fim de impulsionar toda a indústria, já que o teste pode oferecer uma oportunidade para os fornecedores atualizarem seus produtos em preparação para o teste e assim que obtiverem os resultados. E às vezes, não

conseguimos o equilíbrio certo", explicou.

Falando com *Segurança da informação*, Vishal Santharam, gerente sênior de produtos de segurança de endpoint da ManageEngine, elaborou o ponto de Clancy.

"Em 2024, o MITRE começou a registrar o volume de alertas nas avaliações, o que é sempre um desafio para um fornecedor sintonizar. Mais alertas significam maior fadiga de alerta", disse ele, referindo-se a um estudo da Forrester decodificando as avaliações MITRE de 2024: empresa com base no volume de alertas.

Além disso, Santharam observou que o teste Avaliações: Empresas de 2025 incluiu o ambiente de nuvem, "que é um território não testado e requer ainda mais atenção dos fornecedores".

Finalmente, Clancy disse *Segurança da informação* que sua equipe costumava realizar um fórum de fornecedores a cada ano para se preparar para o teste MITRE ATT&CK Evaluations: Enterprise.

"Este fórum, que foi útil para trabalhar com a indústria para definir os objetivos do teste a cada ano, caiu nos últimos dois anos", admitiu Clancy.

No LinkedIn, Gofman, da CrowdStrike, argumentou que os testes MITRE Evaluations foram inicialmente uma ótima iniciativa para comparar soluções de segurança, mas se transformaram em "teatro de fornecedores" nos últimos anos.

"Os fornecedores investem enormes recursos para vitórias de relações públicas, não para melhorias reais de segurança. Com o MITRE e a CISA sob pressão de cortes e mudanças no orçamento, alguns fornecedores provavelmente viram uma oportunidade de recuar", disse ele.

"O conceito de teste baseado em TTP ainda é valioso, mas a maneira como ele evoluiu, está desatualizado, excessivamente focado em endpoints, separado das ameaças do mundo real, é muito menos", acrescentou.

Patrick Garrity, pesquisador de vulnerabilidades da VulnCheck, corroborou essa visão: "[It] Parece que essa atividade de benchmarking se tornou um gigante distração para construir produtos melhores em troca de publicidade", disse ele em outra postagem do LinkedIn.

Apesar dessas preocupações, Clancy confirmou que uma dúzia de fornecedores de segurança cibernética ainda estavam participando da edição de 2025 do teste.

MITRE reiniciará o fórum de fornecedores em 2026

Clancy disse *Segurança da informação* que sua equipe pretendia restabelecer o fórum de

fornecedores antes das avaliações do MITRE ATT&CK: Enterprise 2026.

“Isso é algo que já estamos trabalhando para restabelecer para a edição de 2026”, disse ele.

Mais tarde, ele tornou essa ambição pública em um post no LinkedIn publicado em 18 de setembro, depois que SentinelOne e Palo Alto anunciaram que não participariam da edição de 2025.