DATA SHEET

mysecsimulation
Attack Surface Management (ASM)
Cymulate

Elimine a Lacuna entre ASM Tradicional e Gerenciamento de Vulnerabilidades

O Cymulate Attack Surface Management (ASM) descobre vulnerabilidades e configurações incorretas para identificar ativos expostos a acessos não aprovados, explorações e outros ataques. Ele verifica domínios, subdomínios, IPs, portas, plataformas de nuvem, configurações, dispositivos e privilégios e mapeia possíveis caminhos de ataque que poderiam ser usados por agentes de ameaças para acessar sistemas sensíveis e dados.

O Cymulate ASM inclui mapeamento de caminhos de ataques unificados e análise para demonstrar como um invasor pode atravessar da rede local para a nuvem e vice-versa. Visualizando a combinação de lacunas e fraquezas do início ao fim, fornece uma imagem mais completa e detalhada, para que as organizações possam avaliar com precisão os riscos dos ativos.

Capacidades do Cymulate

Minimize a Exposição à Ameaças Externas

O Cymulate inclui recursos externos de ASM para mapear a superfície de ataque externo emulando reconhecimento e métodos de investigação de atores de ameaças para identificar ativos digitais (como domínios da web, endereços IP, aplicativos e muito mais) e avaliar a explorabilidade. Com descobertas mapeadas para o MITRE Táticas, técnicas e procedimentos (TTPs) da estrutura ATT&CK®, as empresas podem tomar as medidas de mitigação necessárias.

Os clientes só precisam instalar um agente leve no ambiente para executar as avaliações. O agente facilita a comunicação entre os dispositivos do cliente e a plataforma Cymulate, garantindo atualizações oportunas e transferência eficiente de dados operacionais.

Como Funciona

- Scan nos ativos voltados para a Internet (externos)
- Identificação e mapeamento dos ativos mais importantes
- Execução de verificações de vulnerabilidades e configurações incorretas em todos os ativos externos encontrados
- Priorização das vulnerabilidades e configurações incorretas descobertas de acordo com a probabilidade de exploração e a importância do ativo
- Correção priorizada das lacunas de segurança exploráveis

Benefícios do Cymulate Attack Surface Management

VISIBILIDADE ABRANGENTE	MAPEAMENTO E ANÁLISE DOS CAMINHOS DE ATAQUES UNIFICADOS	PRIORIZAÇÃO MELHORADA	PONTUAÇÃO DE RISCO
Identificar configurações incorretas, vulnerabilidades, sistemas acessíveis externamente e as lacunas de segurança, local e na nuvem	Apresentação das informações em contexto para uma melhor visão do potencial de ataque viável	Seguir com as correções para fechar lacunas em sistemas, recursos e dados críticos	Rastreamento e análise das tendências das pontuações de risco para melhoria contínua e comparação com pares

Descubra Ativos Internos de Alto Risco

O Cymulate inclui recursos internos de ASM para mapear a superfície de ataque interna com varreduras autenticadas usando credenciais de usuário para identificar ativos exploráveis que um adversário pode aproveitar para se propagar de um ponto de apoio até as joias da coroa. Um único agente leve facilita a comunicação perfeita entre os dispositivos do cliente e a plataforma, garantindo atualizações oportunas e transferência eficiente de dados operacionais.

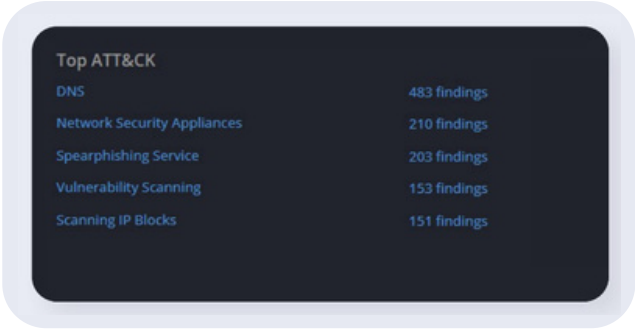
Como Funciona

- Scan dos ativos internos
- Execução de verificações de vulnerabilidade e configurações incorretas (local e na nuvem) nos ativos internos identificados
- Realização das análises profundas dos problemas de segurança e relacionamento entre ativos
- Identificação de vulnerabilidades e lacunas de segurança com mitigações recomendadas e detalhadas

Dashboard do Cymulate Attack Surface Management

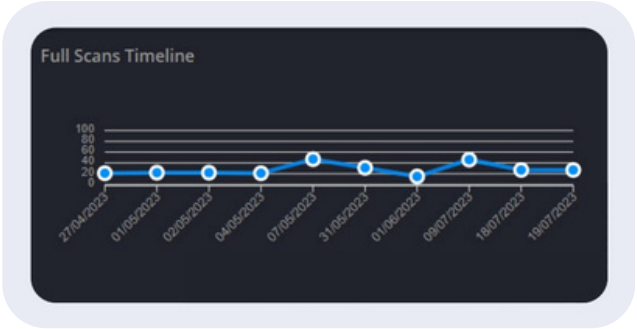
Pontuação Geral
Pontuação de segurança baseada na taxa de sucesso de ataque simulado correlacionada com os padrões do setor

Principais Descobertas
Visão rápida e expansível dos principais ataques, principais ativos e principais descobertas



Distribuição de Descobertas
Compreensão imediata das distribuições de descobertas por categoria, gravidade ou status dos ativos

Tendência
Acompanhamento fácil da evolução da segurança da superfície de ataque em uma linha do tempo que reflete a pontuação do módulo ASM em intervalos de tempo selecionados



Mapeie Caminhos de Ataque em Toda a Organização

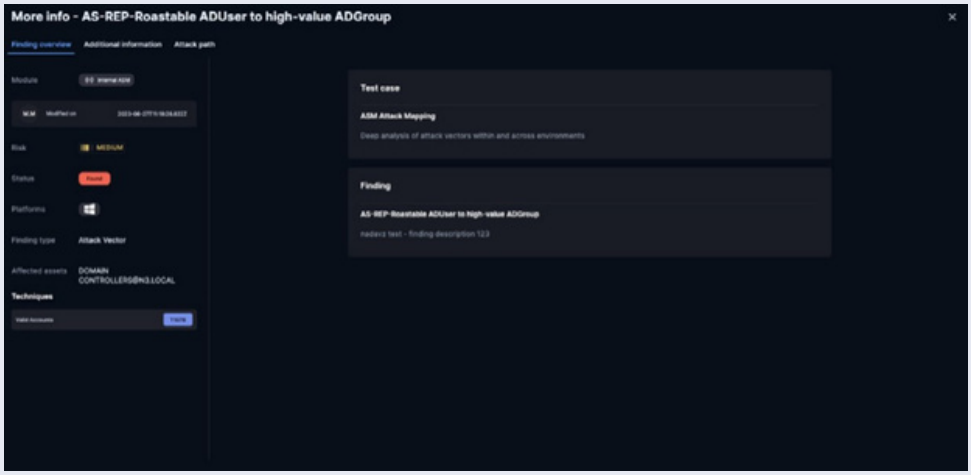
Com descobertas da superfície de ataque interna, o **Cymulate ASM unified attack path mapping and analysis** mapeia caminhos de ataque em redes, plataformas de nuvem (AWS, Azure e GCP) e sistemas de identidade, incluindo serviços do Active Directory. Interconexões, relações de confiança, permissões e outros fatores podem mudar o caminho de um invasor de maneiras inesperadas, e ter a capacidade de identificar e ver claramente esses caminhos permite que a organização identifique e feche rapidamente as lacunas sem interromper as operações comerciais.

Como Funciona

- Mapeamento dos caminhos de ataque em redes, plataformas de nuvem, sistemas de identidade e serviços do Active Directory
- Avaliação dos caminhos de ataque mais cruciais por grau de exploração
- Identificação das mudanças nos processos e na tecnologia que teriam o maior impacto na redução de riscos

Visão Geral das Descobertas

Veja as descobertas relacionadas por verificação. Em cada descoberta, visualize o risco, o status, a plataforma e o ativo afetado para identificar áreas de risco potencial.

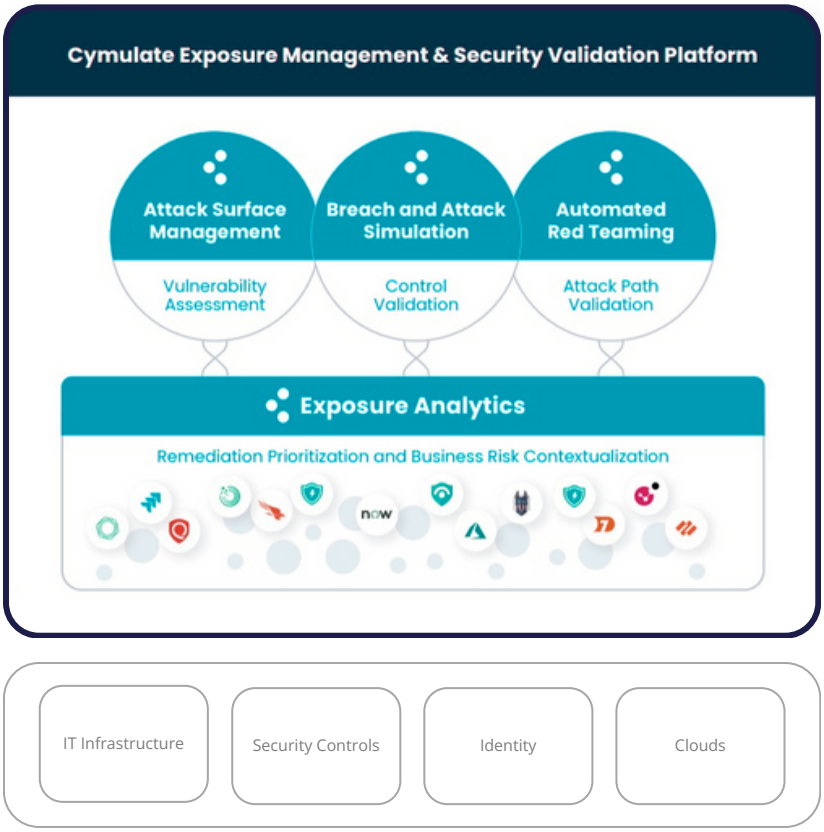


Mapeamento do Caminho de Ataque

Visualize as interconexões entre os ativos descobertos, considerando tanto relacionamentos legítimos quanto relacionamentos resultantes de vulnerabilidades e configurações incorretas. A pontuação de cada relacionamento mostrado no caminho de ataque corresponde ao seu nível de risco e probabilidade de exploração – quanto maior a pontuação, maior o risco.
Obtenha uma compreensão clara e prática da postura de segurança interna de uma organização, permitindo a priorização e resolução imediata de vulnerabilidades.

A Plataforma Cymulate

O **Cymulate Exposure Analytics** está disponível como uma oferta SaaS independente e como uma oferta integrada na plataforma Cymulate Exposure Management e Security Validation. A plataforma Cymulate fornece uma solução abrangente e escalonável para líderes de segurança, independentemente de sua maturidade de postura de segurança, para conduzir seu programa contínuo de gerenciamento de exposição a ameaças e apoiar os requisitos técnicos e de negócios de definição de escopo, descoberta, priorização, validação e mobilização.



Sobre a Cymulate

Cymulate, líder em gerenciamento de exposição e validação de segurança, fornece uma plataforma modular para avaliar, testar e melhorar continuamente a resiliência da segurança cibernética contra ameaças emergentes, ambientes em evolução e transformações digitais. A solução tem um impacto quantificável em todos os cinco pilares do programa de gerenciamento contínuo de exposição a ameaças (CTEM) e na capacidade de uma empresa de reduzir riscos ao compreender, rastrear e melhorar sua postura de segurança. Os clientes podem escolher entre seu produto Attack Surface Management (ASM) para criação de perfil de ativos com base em risco e validação de caminho de ataque, Breach and Attack Simulation (BAS) para testes simulados de ameaças e validação de controle de segurança, Continuous Automate Red Teaming (CART) para avaliação de vulnerabilidades, testes personalizados e baseados em cenários e Exposure Analytics para ingestão de dados do Cymulate e de terceiros para compreender e priorizar exposições no contexto de iniciativas de negócios e comunicações de resiliência cibernética para executivos, conselhos e partes interessadas.
Para mais informações, visite www.cymulate.com.