cymulate

SOLUTION BRIEF

Red Teaming

New Threats Don’t Wait for Your Next Red Team Exercise

Red teams simulate real-world cyber attacks to identify threat exposure, so security can be strengthened before adversaries exploit those weaknesses. However, traditional one-off tests using open-source tools often lack comprehensive coverage and a well-structured red team exercise typically takes up to two months. Red teams struggle to:

- Scale testing to cover more threats and attack surfaces
- Quickly convert new threat intelligence into custom attack chains
- Map results and findings to actionable security enhancements
- Minimize disruption to production systems while testing defenses

Scale Red Team Testing with AI & Automation

Cymulate Exposure Validation automates and scales red teaming with production-safe security assessments that include custom attack chains, network penetration testing and 100% MITRE ATT&CK coverage backed by a library of more than 100,000 attack actions.

Red teamers rely on Cymulate to identify and fix the most critical security gaps because the findings include MITRE ATT&CK mappings, remediation guidance, recommended IoCs and custom detection rules that can be directly applied to EDR, SIEM, XDR and more.

With AI-powered analysis of threat intel and industry-leading attack simulation, Cymulate gives red teams the automation to build new tests faster, test more environments and repeat testing to confirm remediation and identify security drift.

> **With Cymulate, I can quickly see top MITRE techniques not prevented or not detected, so I can give my detection engineering team more specific data on what needs to be improved.**
>
> – Lead Red Team Engineer, Financial Services

Solution Benefits

Scale offensive testing

Assess more threats and cover more of the attack surface with automation.

Build custom attack scenarios

Customize testing with simple workflows and options to create new attack scenarios.

Deliver actionable results

Support purple teaming and provide clear guidance for the security team to remediate, close gaps and reduce exposure.

Cymulate Offering

- Exposure Validation
- Custom Attacks
- Attack Path Discovery

Red Teaming Solution Features

Customize and scale attack chains and attack scenarios

Simple no-code workflows to build attack chains from a library of more than 100,000 attack actions, with options to upload and create custom threat scenarios. Additionally, the attack scenario library is updated daily based on new threat intelligence, so red teamers can focus on building custom attacks and spend less time investigating new threats.

Test new threats faster with the power of AI

Automate threat assessments with an AI-assisted dynamic attack planner that converts threat intel into custom threat assessments on demand.

Automate attack path discovery

Simulate an attacker who has compromised a single workstation and is moving laterally in search of additional assets. The process uncovers lateral movement gaps, privilege escalation paths and exposed data or credentials that attackers can exploit.

Map to MITRE ATT&CK framework

Visualize emulation coverage with the MITRE ATT&CK heatmap to quickly understand coverage and evaluate if there are specific techniques or sub-techniques that are not covered by assessments.

Evaluate employee awareness

Create an internal security awareness campaign to measure employee resilience against phishing attacks. Identify employees in need of additional awareness training and highlight users who are not following policies.

Provide actionable findings

Go beyond identifying security gaps and support purple teaming by providing control and system owners with the precise actions to remediate and improve threat resilience.

Why choose Cymulate?

Depth of attack simulations

Over 100,000 attack simulation resources from real-world attack scenarios for comprehensive testing of your security controls.

Production safe

Live-data test scenarios are production-safe and will not disrupt or cause harm to production systems.

Automated validation

The attack simulations are fully automated, enabling continuous validation of security controls against immediate threats.

About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. For more information, visit www.cymulate.com.

Get a Demo