cymulate

SOLUTION BRIEF

Red Teaming

Where Traditional Red Teaming Falls Short

Red teams simulate real-world cyberattacks to uncover vulnerabilities and strengthen security before adversaries can exploit gaps. However, traditional one-off tests using open-source tools often lack comprehensive coverage. Red teams frequently 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

Exposure Validation Built for Red Teams

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 the most critical security gaps that they know will be addressed 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.

> **Before, the red team had to validate our outsourced SOC services with manually executed attacks, which is time-consuming and limited in scope.**
>
> **My team is about 60% more efficient with Cymulate. Our security team quickly runs assessments that extensively cover TTPs and IOCs with significantly less effort. The platform also generates SIEM-specific queries based on Sigma rules, making mitigation more streamlined and reducing the team's mean time to detect (MTTD) and mean time to prevent (MTTP).**
>
> – CISO, 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 actions and complex attack chains.

Automate live-data exercises

Collaborate with SecOps for purple teaming with realistic testing that integrates with SIEM, EDR, XDR and SOAR.

Deliver actionable results

Provide clear guidance for the security team to remediate, close gaps and reduce exposure.

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.

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 network pen testing
Simulate an attacker that has gained an initial foothold by taking control of a single compromised workstation and is moving laterally in search of additional assets that can be compromised.

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 provide control and system owners the precise action to remediate – including automated control updates for new IoCs.

> **Cymulate allows us to scale our red team activities extensively with only one teamer. Our testing is more extensive and efficient, with zero code assessments, automated reporting and easy-to-digest mitigation guidance.**
>
> – Assistant Information Security Manager, Financial Services

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
The full suite of attack simulations and test scenarios are completely production-safe and will not cause harm to your 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 and security validation. More than 1,000 customers worldwide rely on the Cymulate platform for continuous discovery, validation, prioritization and guided remediation of security gaps before attackers can exploit them. For more information, visit www.cymulate.com.

Get a Demo