Red Team/Pen Test Automation

Solution Brief

Challenges

Traditional penetration testing and red teaming limitations can hinder an organization's ability to comprehensively and continuously assess their security posture. Penetration tests are expensive, time-consuming, and provide only a snapshot of an organization's security at a specific moment in time. In-house red teams, responsible for creating attack simulations with new tactics, techniques, and processes often spend a disproportionate amount of time on labor-intensive, repetitive and administrative tasks.

Red teams also often work separately from blue teams, which opens the door for misalignments and increased time to remediation. Furthermore, limited resources hamper the validation of the effectiveness of remediation measures, which can accelerate security drift.

Red teams also are required to dedicate a considerable part of their time, sometimes over half of it, generating summary reports instead of focusing on crafting advanced attack simulations.

Overview

Cymulate provides Red Teams a platform to increase their operational efficiency and scale up their adversarial activities in a production-safe environment. Assessments are easily customized, automated, and scheduled. Blue Teams that want to run offensive campaigns can also benefit from these capabilities with easy-to-use, out-of-the-box assessments.

Off-the-shelf attack simulations available on-demand, 24/7, operationalize the possibility to continuously assess an organization's defenses. This ensures that an organization's controls configurations and security resilience stay up to date with both the latest threats and the frequent new deployments that modify the organization's infrastructure.
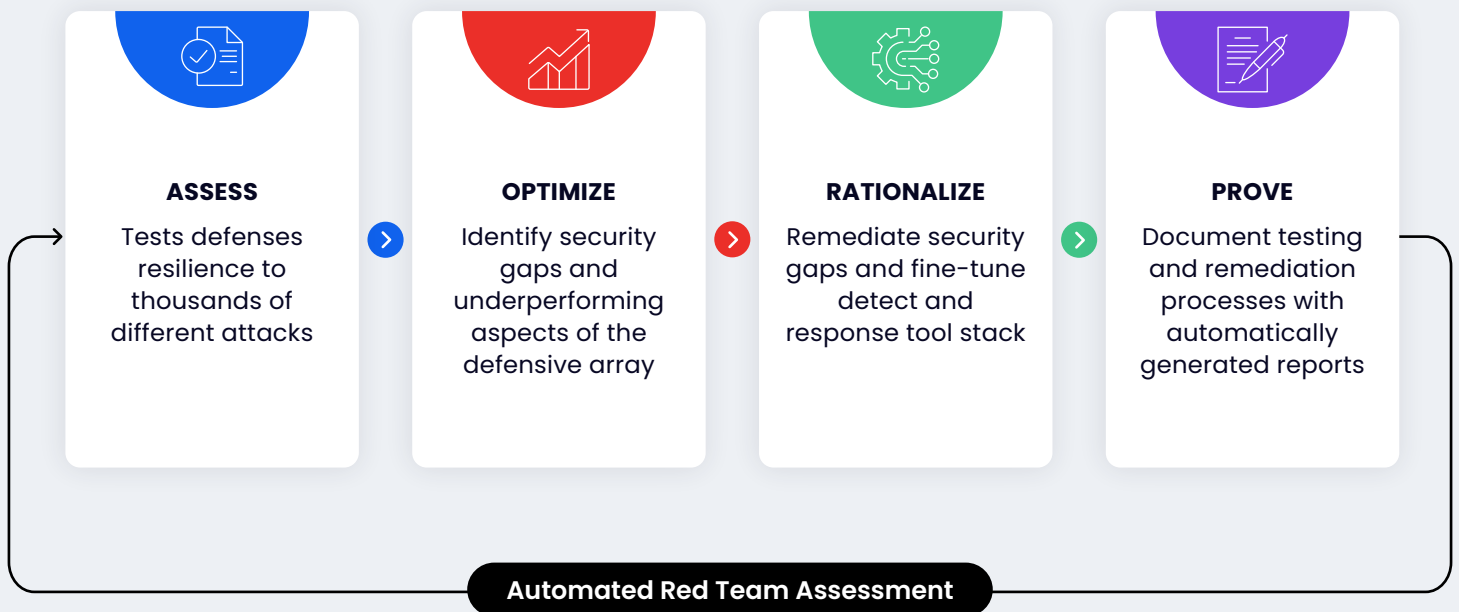
Automated report generation and drag-and-drop attack simulations customization wizard free skilled security team members time, enabling them to focus their efforts on high value tasks.

In addition, the Cymulate Platform integrates seamlessly with leading security technology partners through out-of-the-box APIs, enhancing collaboration and streamlining the security process.

Benefits

- > Continuous attack simulations, available on-demand 24/7
- > Ability to challenge and probe security controls across the cyber kill chain
- > Ensuring controls are up to speed on the latest threats
- > Repeatable system to test and retest security controls
- > Rapid assessment and remediation of detected vulnerabilities
- > Integration with leading security technology partners via out-of-the-box APIs

Automating Red Teaming and Pen Testing with Cymulate

ASSESS
Tests defenses resilience to thousands of different attacks

OPTIMIZE
Identify security gaps and underperforming aspects of the defensive array

RATIONALIZE
Remediate security gaps and fine-tune detect and response tool stack

PROVE
Document testing and remediation processes with automatically generated reports

Automated Red Team Assessment

Main Features

Simulated Phishing Attacks
With real production-safe payload, links to fake malicious websites identify employees who need additional phishing awareness training.

Full-Scale APT Attack Campaigns
Simulates a real APT attack by launching different vectors sequentially, starting with email or web browsing, followed by code execution and evasion techniques that challenge network configuration and segmentation policies, and attempts to progress vertically and laterally to exfiltrate data or execute command and control.

Enhanced Threat Mitigation
Identify real-world threats and accelerate mitigation with actionable guidance and integrated ticketing for streamlined mitigation management.

Case Study

### Persistent Systems Gains Visibility & Control of its Security Posture

Persistent Systems is a digital engineering and enterprise modernization partner, with over 22,000 employees located across 18 countries.

> **Use Case: Red Team Automation and Customization**
> Persistent's red team uses Advanced Scenarios to automate their assessments, as well as scale their adversarial activities with pro-active threat hunting and health checks. Most recently, the team used this module to test a golden ticket attack. Any gaps that are found during these assessments are automatically documented in a mitigation report so they can be remediated immediately, before an attacker can exploit them.

Read more

Additional Resources
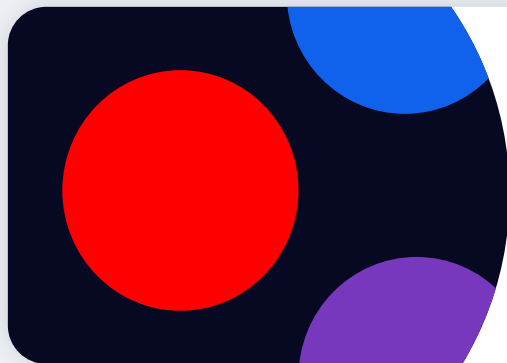
Cymulate

Automated Pen Testing Breach & Attack Simulation

Read more

Backed by the Industry

Awards and Accolades

About Cymulate

Cymulate provides organizations with comprehensive security control validation and in-depth insights into breach feasibility. This modular solution addresses a wide variety of business and technical use cases and scales from out-of-the-box simulations to full customization for advanced attack simulations. With Cymulate, companies assess, optimize, rationalize, and prove their security program with minimal resource investment. Security professionals and business stakeholders leverage these insights to reduce cyber risk, justify investments, provide proof of security resilience to executive leadership, and gain evidence for compliance and regulatory purposes.

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

info@cymulate.com | www.cymulate.com