

# Red Team Automation & Customization to Scale Adversarial Activities

It can be difficult for red teams to scale their adversarial testing activities. Their daily responsibilities are time-consuming and labor-intensive, leaving less opportunity for high value tasks. Budget cuts and the shortage of security professionals only add to the obstacles preventing red teams from scaling successfully.

Cymulate provides red teams a platform to increase their operational efficiency and optimize their adversarial activities in a production-safe environment. Cymulate's red team capabilities include the modules Attack Surface Management (ASM), Phishing Awareness, Lateral Movement, Full-Kill Chain Campaign, and Advanced Scenarios.

## Automate

Automate assessment scripts and repetitive, labor-intensive manual tasks

## Scale

Simultaneously run hundreds of attacks at the level of a team's most seasoned expert

## Customize

Gain the freedom to create, modify, and run chained or atomic attack campaigns

## Red Team Automation Capabilities



### External Attack Surface Management (ASM)

The reconnaissance phase entails a comprehensive analysis of an organization which can mean days or months before red teamers even begin an attack. Cymulate's External Attack Surface Management (ASM) technology emulates real attackers to automatically identify externally accessible digital assets (such as domains and IP addresses) and assess their exploitability against an organization's security policies and solutions.

Saving time and resources, this module only needs a domain to begin its automatic assessment; red teamers can easily utilize the ASM findings to begin their chain of attacks without any additional research. With findings mapped to the MITRE ATT&CK® framework's TTPs (tactics, techniques, and procedures) and detailed remediation guidance, red teamers no longer need to spend time analyzing results and writing reports. Additionally, blue teams can remediate based on the automated reports and then independently run ASM again to ensure mitigation.



## Phishing Awareness

Testing phishing awareness is an important aspect of assessing an organization's security posture but manually running phishing campaigns is labor intensive and time consuming. Pen testers may only resort to a phishing attack if they can't find any other way into an organization so this aspect of an attack is not always evaluated. The Phishing Awareness module provides the resources to create an automated internal phishing campaign.

Pen testers and red teams can customize each campaign by deciding who to send it to, payload delivery method, design, and the content of the email. Customization makes it more challenging for employees to recognize phishing emails, creating a realistic situation to test how they might act in real-life. The module enables red teams to send numerous phishing emails at once, and the continuous feedback provided by automated reports helps organizations focus on employees that may require more education and monitoring than others.



## Lateral Movement

Continuously assessing network configuration and segmentation policies through escalating privileges and exploiting misconfigurations on multiple machines can be time-consuming for red teams when done manually. The Lateral Movement module emulates a real-life hacker that has gained an initial foothold in a company's network and shows how the hacker can move laterally from the originating workstation in search of valuable assets. It runs automatically and applies "living off the land" non-destructive hacking tactics and techniques to continuously uncover infrastructure misconfigurations and weaknesses.

Continuous testing helps red teams identify loose privileges or changes in the IT infrastructure and network misconfigurations that may open new paths for lateral movement. Because Lateral Movement is automated and utilizes different types of tactics and techniques simultaneously, it helps red teams scale their capabilities and increase chances to find a security gap, without any additional manpower. Blue teams can utilize the module's remediation guidance following each assessment and run the same assessment again, without the red team, to ensure their actions had a positive impact.



## Full Kill-Chain Campaign

Cymulate's Full Kill-Chain APT (advanced persistent threat) module enables organizations to test security effectiveness across the entire cyber kill chain. In addition to challenging each attack vector separately, organizations can run a full-scale APT attack simulation to understand the overall effectiveness of their security control configuration and detect and response tools. Red teams can use this module to automate APT attacks instead of running them on their own. Following each campaign, Cymulate provides mitigation guidance so that blue teams can remediate controls and independently run the same campaign to see the impact of their actions.

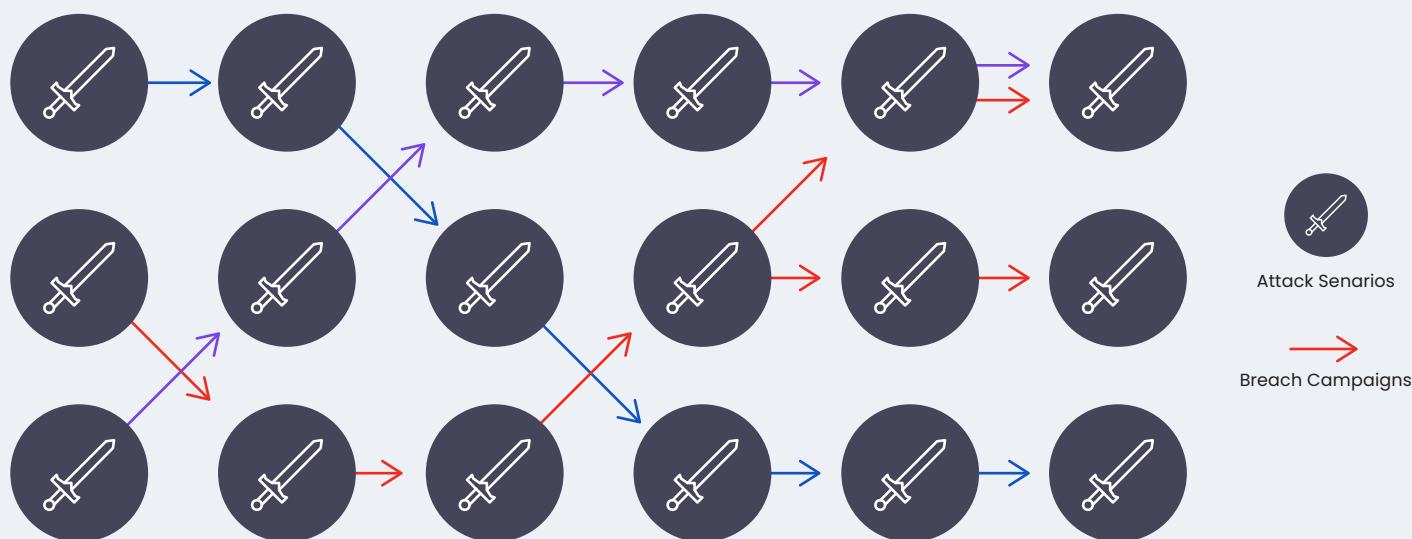
As with a real APT, the different vectors are launched sequentially, starting from a simulated attack delivered through email or web browsing, followed by execution of code and evasion techniques that challenge security endpoint mechanisms. Depending on the chosen template, the module can challenge network configuration and policies by attempting to move laterally and continues its attack by seeking to exfiltrate predefined sets of data (for example mock PII, health records, card details etc.) to test DLP controls. To create a true-to-life simulation of an APT, this module can be launched in agentless mode, beginning with a simulated phishing email.



## Advanced Scenarios

Cymulate’s Advanced Scenarios is an open purple teaming framework for the creation and automation of offensive security assessments. The module extensively leverages the MITRE ATT&CK® and NIST 800-53 Revision 5 framework, enabling red teams to create complex scenarios from pre-built resources and custom binaries and executions, without any limits or restrictions. Each step in the scenario is connected, so a previous assessment output can be used as part of the upcoming assessment input.

Custom scenarios can be used for pro-active threat hunting and health checks. It is also an effective way for blue teams to continuously test mitigation efforts following a pen test; by automating pen test assessments to see if the blue team’s remediation reduced risk, red teams don’t need to spend their time manually running the same assessments. Additionally, the framework launches attacks and correlates them to security control findings through API integrations to provide actionable detection and mitigation guidance for security analysts.



\* Figure: Create and customize end-to-end red teaming campaigns




## Cymulate’s Extended Security Posture Management (XSPM)

Knowing how an attacker can penetrate and propagate into an organization only provides partial visibility of a company’s security posture. It might answer the question “how can I be breached?” but certainly does not answer “how well are my security controls performing?”




A comprehensive security posture assessment requires security control validation and prioritized vulnerability patching. This is essential to maximize operational efficiency while minimizing risk exposure. Cymulate’s Extended Security Posture Management (XSPM) framework provides an end-to-end overview of an organization’s security posture.

## Benefits

### Red Team

-  More time for sophisticated red team exercises
-  Less time spent on coding & tedious tasks
-  Auto-generated reports & analytics

### Blue Team

-  Improve adversarial skills on the job
-  Increased collaboration
-  Quick time to mitigation

## Why Cymulate



Deploys  
in Minutes



Comprehensive  
In-Depth Validation



End-to-End  
Visibility



Vulnerability  
Prioritization Technology



Red & Purple  
Teaming Framework



Immediate  
Threat Intelligence

## About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness. **Measuring your cybersecurity performance is fundamental towards creating a more secure organization!**

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

[Start Your Free Trial](#)