cymulate

DATA SHEET

Cymulate Threat Studio

Validate Defenses Against Relevant Threats

Custom threat assessments have long depended on open-source tools – with complexity, limited reliability and no formal support. While commercial red team tools brought stability and automation, these tools limited testing to out-of-the-box attack scenarios.

Cymulate Threat Studio removes the complexity of attack customization and streamlines the creation of both single-action scenarios and advanced, multi-stage attack chains.

With a user-intuitive solution to craft custom threat scenarios, Cymulate Threat Studio gives security teams the expertise and flexibility to prove prevention and detection against organization-specific threats – all without requiring the expertise of an experienced red teamer.

Streamline Custom Attack Creation and Validation

Cymulate Threat Studio streamlines the creation, customization and reuse of sophisticated attack simulations without requiring advanced expertise. With an intuitive attack scenario workbench, Cymulate guides users to combine custom scenarios with the extensive library of pre-built actions that can be easily tailored to specific attack tactics and techniques.

Beyond simplifying creation of custom attack scenarios, Cymulate enables seamless configuration and execution of assessments at scale. Security teams are equipped to rapidly close identified security gaps from assessments by generating detection rules and automatically pushing mitigation of IoCs.

Customize and Manage Attack Scenario Library

Cymulate Exposure Validation provides security teams with a robust attack resource library that includes prebuilt files, execution methods and URLs. With Cymulate Threat Studio, users can seamlessly expand this library by adding and configuring new resources, including custom files, URLs, execution methods, payloads and even phrases. Cymulate makes managing custom resources simple by allowing users to easily view resources and modify, as necessary.

Each new resource configured can be tailored to specific operating system platforms and assigned a custom risk level to reflect its criticality. Assessments map to MITRE ATT&CK tactics and techniques and assigned custom tags. This flexible and extensible approach allows organizations to continuously adapt to evolving attack surfaces and organizational needs

> **Cymulate makes advanced security testing fast and easy. When it comes to building custom attack chains, it's all right in front of you in one place. You can access the full Cymulate library or build your own attack actions."**
>
> – Mike Humbert, Cybersecurity Engineer at Darling Ingredients Inc.

Benefits

Scale offensive testing

Assess more threats in your environment and ensure tests are realistic and comprehensive.

Create custom attacks in minutes

Easily create individual custom attack scenarios in minutes with no advanced technical expertise required.

Centrally manage custom resources

Easily store and access organization-level resources for custom attack scenarios.

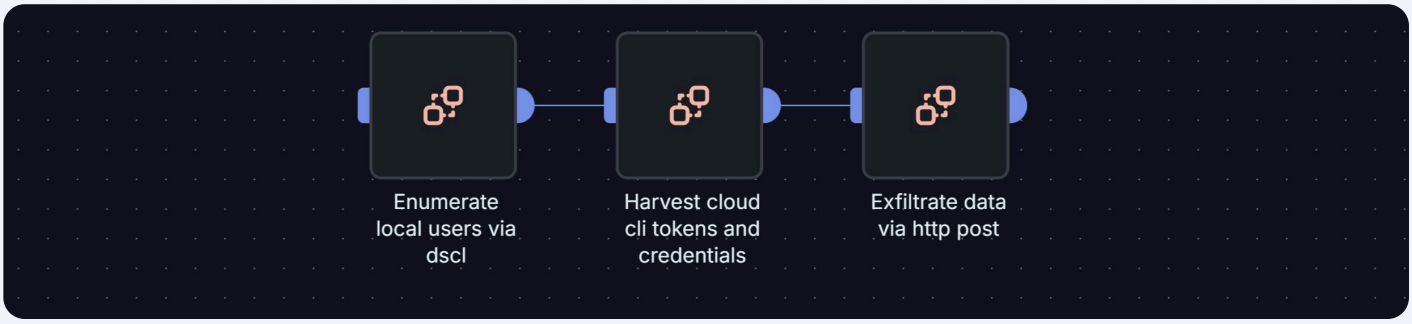
Prove defenses against relevant attacks

Execute relevant custom attack scenarios to validate security controls.

Build and Orchestrate Attack Flows with Ease

Cymulate Threat Studio empowers security teams with flexible, easy-to-use tools for building and customizing single or multi-chained attack simulations that reflect real-world adversarial behavior. Cymulate makes it easy to customize individual attack actions as well as create and visualize complex, multi-step attack chains through an intuitive interface. Key capabilities include:

- **Scenario creation –** Create new attack chains with a simple workflow that guides you through each stage and option to include choose from more than 100,000 actions.
- **Scenario customization –** Select custom resources when fine-tuning attack scenario action configurations such as files, URLs, scripts and email content to mirror the exact conditions you want to test.
- **Resource library expansion –** Upload and tag custom resources including payloads, URLs, files and phrases. Assign risk levels and map to MITRE ATT&CK tactics and techniques and assign custom tags.



The example chained attack above mimics an attacker enumerating local user accounts, discovering plaintext credentials and validating lateral movement by attempting password-based authentication against the discovered hosts.

Why Choose Cymulate?

Complete threat coverage

The most comprehensive threat library that enables validation across the full attack lifecycle – plus daily updates for the latest threats.

AI-powered environment and context mapping

Autonomous, AI-driven usability and workflows customize validation for your environment with intent-aware execution of what comes next.

Cyber defense engineering control plane

Closed-loop system that turns validation into continuous improvement across controls and threat detection.

About Cymulate

Cymulate is the leader in proactive, AI-powered security that continuously proves, prioritizes and adapts against real attacker behavior – before incidents occur. More than 1,000 enterprise security teams rely on Cymulate for autonomous threat validation and cyber defense engineering. Founded and led by experienced red teamers who know that testing alone does not deliver better security, Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.