cymulate

DATA SHEET

Cymulate Custom Attacks

Stay Ahead of Sophisticated Threats

Why validate your cyber defenses with manual, infrequent testing when you could automate real-world TTPs? Traditional approaches are resource-intensive and can't scale to support the complexity of multiple environments and constantly evolving threats.

To build and scale custom offensive testing, you need a modern solution that's easy-to-use and allows you to quickly create customized attack scenarios, execute continuous validation and prove resilience against threats unique to your organization.

Accelerate Custom Attack Creation

Cymulate Exposure Validation includes an option for **Custom Attacks** that streamlines the creation of relevant, sophisticated attack simulations. With a user-friendly platform, security teams can quickly build, customize and reuse advanced individual or chained attack simulations. The platform delivers a user-friendly workbench that simplifies scenario design and enables continuous validation and rapid response. For missed detections, tailored SIEM, EDR and XDR detection rules are provided for fast and easy integration into security technologies

Expand Attack Resource Library

The Cymulate platform empowers security teams with a robust attack resource library that includes prebuilt files, execution methods and URLs. This allows for rapid customization of attack simulations to mirror real-world threats. Users can seamlessly expand this library by adding and configuring new resources, including custom files, URLs, execution methods, payloads, and even phrases.

Each new resource can be tailored to specific operating system platforms and assigned a custom risk level to reflect its criticality. Furthermore, the attack can be mapped to relevant MITRE ATT&CK tactics and techniques. This flexible and extensible approach allows for highly granular threat emulation that adapts to evolving attack surfaces and organizational needs.

Benefits

Scale offensive testing

Assess more threats and ensure tests are realistic and comprehensive.

Streamline customized assessments

Easily create custom attack scenarios for testing without requiring extensive technical expertise.

Validate relevant threats

Ensure attack simulations are context-aware, threat-relevant and actionable.

Accelerate threat detection

Simulate custom threats and easily add and fine-tune detection rules for undetected threats.

"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.

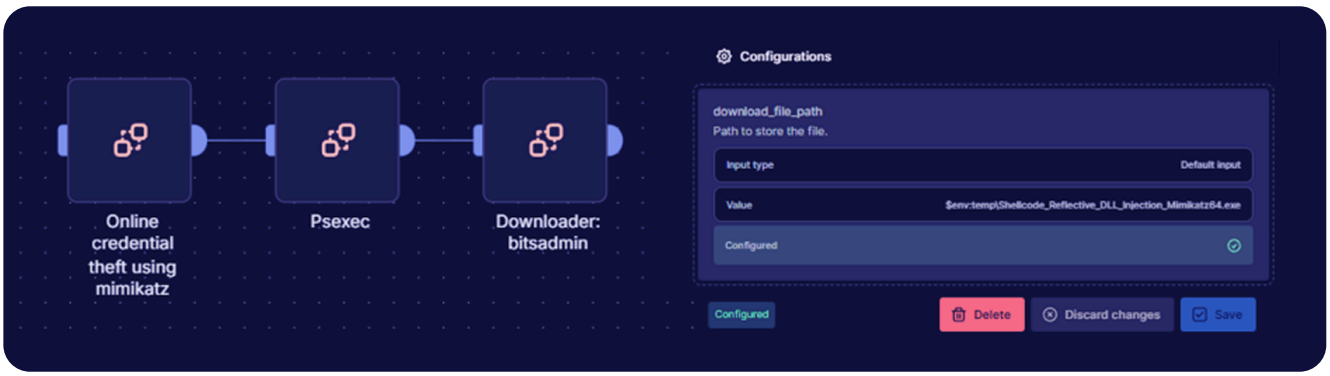
Easily Create and Customize Attacks

Cymulate empowers security teams with flexible, easy-to-use tools for building and customizing chained attack simulations that reflect real-world adversarial behavior. Whether starting from scratch or modifying existing scenarios, the platform enables rapid creation and deployment of tailored attack sequences aligned with your specific validation goals. The Cymulate platform makes it easy to visualize and understand complex, multi-step attack chains through an intuitive interface.

Key capabilities include:

- **Refine Existing Attack Scenarios –** Easily use existing attack scenarios to modify configuration variables to ensure relevant to specific environment
- **Create New Custom Attacks –** Easily create new attack chains with a user-intuitive interface guiding you through each stage and allowing you to choose from over 100,000 actions.
- **Customize Attack Chains –** Fine-tune chained attacks by easily modifying configuration for timing, file downloads, URLs and email content to mirror the exact conditions you want to test. In addition, add or remove actions from our extensive action library.

Here's an example that represents the rapid creation of an advanced chained attack scenario, comprised of three configured actions with custom resources. Running this advanced chained threat simulation assesses an organization's threat resilience for the specific attack configurations and validates cybersecurity defenses across identity management and endpoint policies.



- Mimikatz Execution – Used to extract sensitive credentials, including usernames, domain names and passwords
- Remote Execution with PsExec – Leverages stolen credentials to remotely launch an application on a target system
- Malicious File Download – Delivers and executes a harmful payload on the compromised endpoint

Why choose Cymulate?

Depth of attack simulations

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

Production safe

The full suite of attack simulations and test scenarios are completely production-safe and will not cause harm to your production systems.

Fully automated validation

The attack simulations are fully automated, enabling continuous validation of security controls and emerging 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.