Custom Attack Scenarios

Solution Brief

Cymulate

Challenges

Ready-made attack scenarios do not always fully address all unique aspects of an organization's infrastructure or business processes. Ensuring that data access, segmentation policies, and security controls configuration are efficient sometimes necessitates customized validation assessments. This might even be required to adhere to regulatory compliance requirements.

Yet, developing contextual security validation scenarios is resource-intensive, and requires in-depth scripting or coding knowledge. Though frameworks such as MITRE ATT&CK are invaluable resources, manually operationalizing their TTPs is resource-consuming, prone to errors and needs further customization to cater to various operating systems, applications, and security controls

As a result, in-house security teams commonly lack the knowledge or resources to create and execute the required sophisticated, customized attack simulation scenarios.

Overview

Cymulate's Advanced Scenarios provides organizations with a drag-and-drop wizard containing over 2000 customizable pre-encoded executions that can be run atomically or chained together to easily create complex customized attack scenarios. The wizard also enables chaining with parameters from previous executions or external sources. The wizard's resources significantly reduce manual, labor-intensive tasks, which allows skilled cyber professionals to focus on high-value tasks.

Individual executions can be further customized by with the hundreds of files and Sigma rules in the wizard repository.

Customizable advanced scenario templates classified by industry sectors, APT groups, attack tactics and more can either be run as is, or further customized as required.
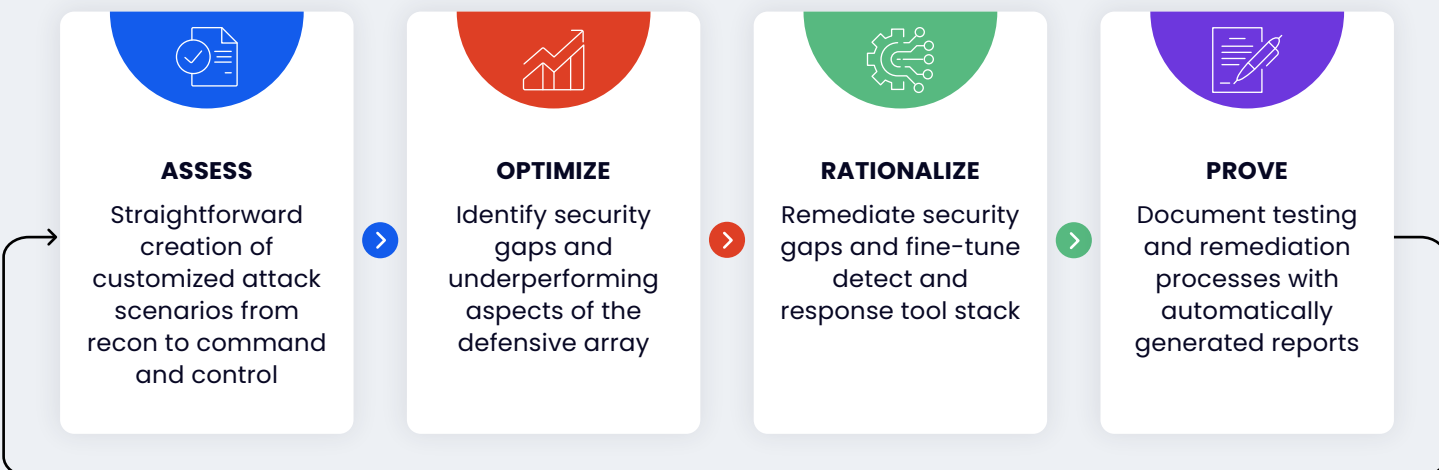
Automatically generated reports that include mitigation guidance accelerate mitigation efforts and access to a detailed analysis of the attack simulation penetration reach.

All templates, ready-made and saved customized attack scenarios can be run at any time or scheduled to run at a specific time or at time intervals.

Benefits

- Customization wizard
- Ability to challenge and probe security controls across the cyber kill chain
- Saving customized attacks, making them repeatable and schedulable
- Integrations with leading security technology partners via out-of-the-box APIs
- Automated report generation

Customizing Attack Scenarios with Cymulate

ASSESS
Straightforward creation of customized attack scenarios from recon to command and control

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

Main Features

Drag-and-Drop executions repository with over 2000 customizable pre-encoded executions to create attack simulation or customize templates, including the possibility to chain execution to create multi-step attacks.

Simulated real behavior of APT groups and malware mapped to the MITRE ATT&CK and the NIST framework.

Automatically generated reports including in depth analysis of the assessment results.

Enhanced Threat Mitigation accelerate mitigation with actionable guidance and integrated ticketing for streamlined mitigation management.

Case Studies and Customer Success Stories

Persistent Systems
UK Pension Management and Consulting Firm

A digital engineering and enterprise modernization partner, with over 22,000 employees located across 18 countries.

Use Case
Red team automation and customization

Persistent 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.
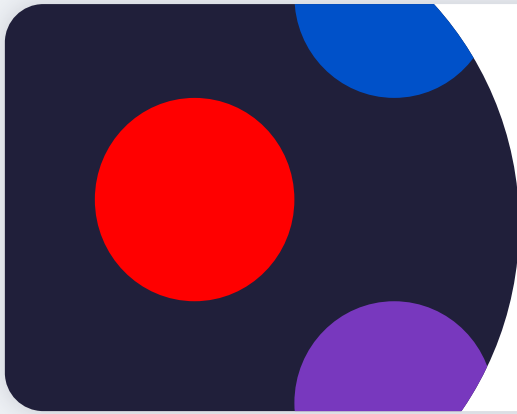
Read more

"
Working with Cymulate is like having a complete red team on board — without the added expense.
"

Mor Asher, Infosec Manager, Telit (Global leader in Internet of Things)

Read more

Additional Resources

Cymulate

Automated Pen Testing vs Breach & Attack Simulation

Ask the Right Questions, Get the Best Answers

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