

Cyclone for Pen-testing Service Providers

Introduction

As your customers advance in cybersecurity maturity and attack resiliency, they are looking for help to develop blue team skills and actively protect their network. They want to develop their threat hunting capabilities, optimize threat-detection technology and exercise incident response playbooks.

With the pervasive cybersecurity skills shortage and wide range of expertise required, the human element in penetration testing services is a limiting factor to address this growing need. In addition to the high cost of retaining skilled penetration testers, the challenges faced by security service providers are:

Lack of Scalability:

Manual, non-repetitive processes, difficult to scale expertise, time-consuming reporting, and analysis.

Lack of Security Control Integration:

Current auto pen-testing tools only address the red-team side of an exercise; they lack security control visibility and the blue team perspective.

Cymulate Cyclone: Purple teaming for red teamers

Cymulate Cyclone enables pen-testing service providers to craft, automate and deliver purple teaming exercises that help their customers actively protect their network. Cyclone-based services optimize SOC detection, hone threat hunting skills and improve incident response processes, and its openness enables the creation of many other unique revenue-generating service offerings. Cyclone is a customizable, template-driven platform that scales existing pen-testing expertise. Cyclone purple teaming auto-correlates blue team detections to red team adversarial tactics, and it provides remediation and detection guidance, including Sigma rules. The attack scenarios are aligned to the MITRE ATT&CK framework, as are the executive and technical reports that the platform generates.



Automate purple teaming

- Craft, automate and launch attack scenarios.
- Automate reconnaissance A-Z penetration campaigns
- Correlate security-control findings and validate their effectiveness.



Scale Expertise

- Create reusable and modifiable template-based assessments.
- Automate routine and base-line assessments.
- Upskill junior team members.



Differentiate

- Offer unique and new revenue generating purple-team services.
- Create custom scenario-based services with flexibility to focus on a specific stage of an attack or recreate full kill chain APT flows.



Gain immediate value

- Leverage the rich repository of resources, including out-of-the-box assessment templates, executions, payloads, tools, and Sigma rules.

Rapid value creation

In addition to a rich repository of attack resources, Cymulate Cyclone is loaded with out-of-the-box assessments that can be deployed immediately as service offerings. These can be used as-is or can be modified and expanded to reflect in-house expertise or specific customer requirements.

These include, among many others:

- 01** APT group simulations
- 02** MDR and EDR efficacy testing efficacy testing
- 03** SOC validation
 - MTTD
 - MTTR
 - Tuning
- 04** Automated security assurance assessments

Deliver efficient and effective Purple Team services, provide actionable remediation and improvement guidance and help them to actively protect their networks with Cymulate Cyclone.



Efficient

- Auto-correlate security-control findings to attacks.
- Auto-generate reports mapped to MITRE ATT&CK®.
- Easily generate Sigma rules with the platform based on findings.
- Export findings to MITRE ATT&CK Navigator.



Human adaptive

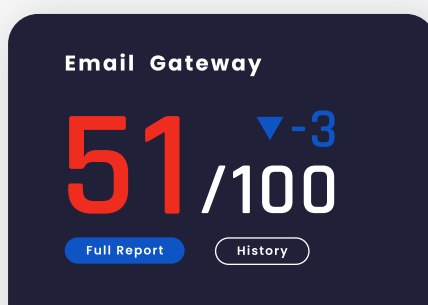
- Create both fully automated and interactive attack sessions.
- Upload or create your own assessments, payloads, executions, tools and Sigma rules.

How it works


Cymulate facilitates managing your security posture 24X7X365 within minutes and based on facts, in just three simple steps:



1 Simulate
Simulate attacks across any vector.



2 Evaluate
Know where your company is exposed.



3 Remediate
Fix your security gaps.

About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their CyberSecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company-and every company-will be.

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

[Start Your Free Trial](#)