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 MSPs and consulting 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. It is a multi-tenant platform that supports role-based access controls (RBAC) enabling the service provider to engage customers on the platform. 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.
- 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:
1. APT group simulations
2. MDR and EDR efficacy testing
3. SOC validation
   • MTTD
   • MTTR
   • Tuning
4. 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.

Cymulate helps companies improve their security posture 24X7X365 within minutes, in just three simple steps:

01 Simulate Attacks across the full kill chain
02 Evaluate Controls to identify gaps
03 Remediate With actionable guidelines

About Cymulate
For companies that want to assure their security against the evolving threat landscape. Cymulate SaaS-based Continuous Security Validation automates security risk assessments end-to-end, enabling them to challenge, assess and optimize their cyber-security posture simply and continuously. Because security professionals need to know and control their dynamic environment.

Contact us for a live demo, or get started with a free trial
Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com
US Office: +1 212 6522632