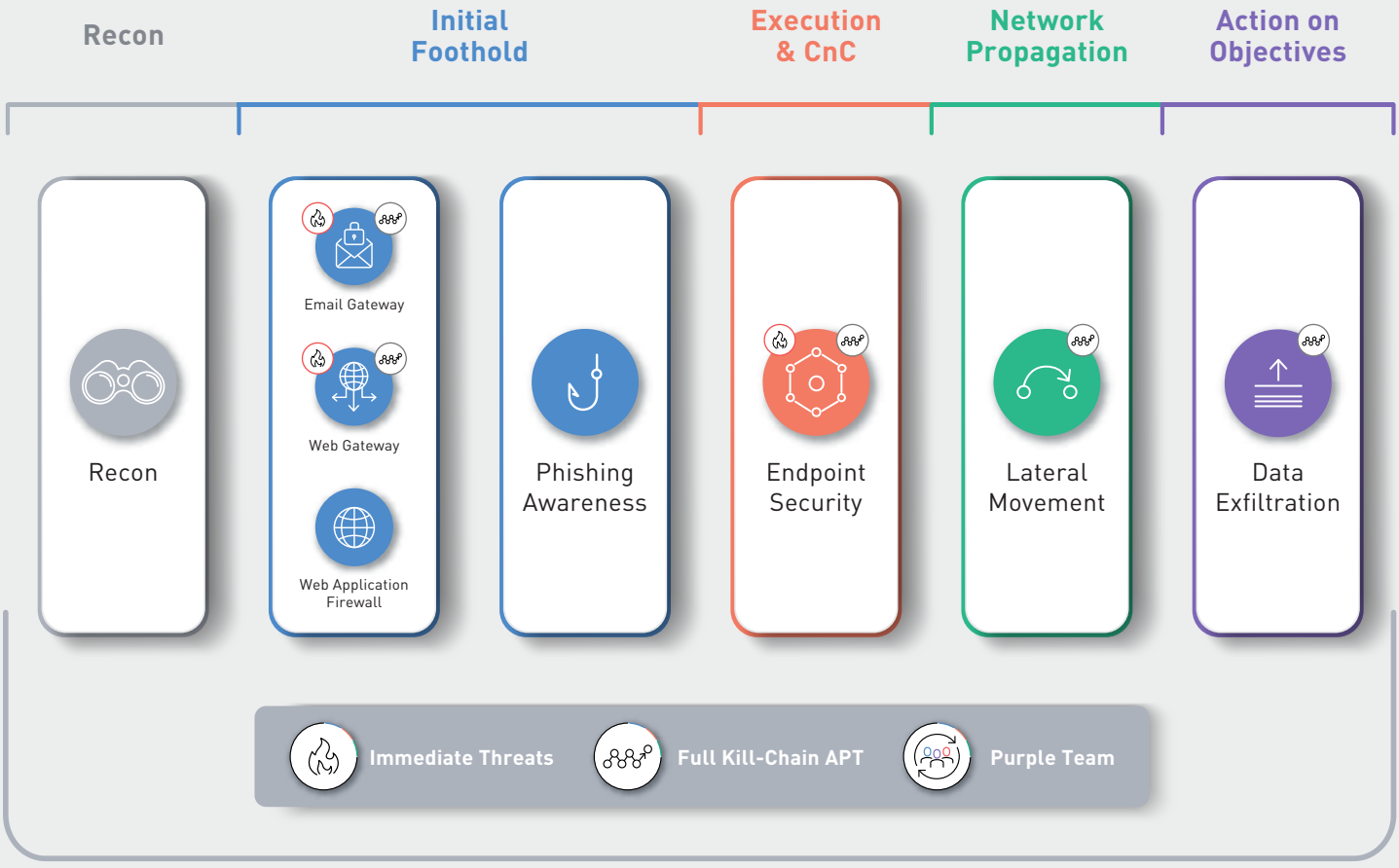
End-to-end security validation

Cymulate SaaS-based Breach and Attack Simulation (BAS) enables companies to assess, optimize and validate the effectiveness of their security controls and processes based on life-like attacks across the full cyber kill chain. It provides a threat-oriented approach to continuous security validation, necessary considering the changing attack surface, changes in the security architecture and constantly evolving cyber-threats.
The platform operationalizes the MITRE ATT&CK framework from reconnaissance to impact. It proactively challenges security controls by mimicking the tactics and techniques of an adversary, in addition to assessing the external attack surface (reconnaissance), lateral movement and phishing awareness.
Simple to use, Cymulate is based on the expertise of professional and seasoned security practitioners and penetration testers. Out-of-the-box, best-practice assessments launch a broad spectrum of attacks that discover misconfigurations and security gaps that would otherwise go unnoticed.
It enables security validation anytime, anywhere, on the production environment without interruption to the business.

With the Purple team module, Cymulate provides an open framework for red-teams and penetration testers to create sophisticated and meaningful attack scenarios and assessments. These can include atomic and chained executions that emulate a life-like attack flow. The assessments can be created using an extensive library of built-in executions, tools, and payloads in addition to custom resources.
Integrations with security systems, such as SIEM, EDR and vulnerability management systems augment existing security programs. They improve SOC and blue-team performance by validating threat detection and alerting capabilities, reducing false positives, and providing attack context to vulnerabilities.
Technical and executive reports show you exactly where you are exposed and provide you actionable remediation guidance.
Cymulate deployment takes less than an hour, requiring one software agent on a standard corporate endpoint per environment, and the licensing model is modular to the individual vector.
Please find hereunder a brief description of the currently available vectors and modules.



Test with Intelligence

The Cymulate **Recon module** discovers what a hacker can find out about your company during the initial information gathering phase of an attack. The module identifies and fingerprints externally accessible assets to discover internet facing weaknesses and vulnerabilities. It also looks for Open Source Intelligence (OSINT) to uncover leaked credentials and organizational information that can be used in an attack.

Email Security Validation

The Cymulate **Email Gateway vector** enables you to test and optimize your email security posture.
This vector challenges your email security controls, including sandbox and content disarm & reconstruction, against a comprehensive set of attacks.
The vector sends to the Cymulate agent emails with attachments containing malicious payloads, for example ransomware, worms, trojans, or links to malicious websites. The simulation reveals which malicious emails, file types and embedded files could potentially reach your employees' inbox.

Securing Your Web Gateway

The Cymulate **Web Gateway vector** validates your organization's web security controls.
This vector challenges the controls that protect employees from accessing and/or downloading malware from malicious and compromised websites.
The vector tests inbound protection against thousands of different simulated malicious files and exploits, and outbound protection against a feed of known compromised or malicious web sites, which are updated daily.

Testing Your WAF Security

The Cymulate **Web Application Firewall (WAF)** vector enables you to test and optimize your web security controls. This vector first identifies all the forms and other means of data import available on the target domain and then challenges the WAF against thousands of attacks, including OWASP top payloads, command injection and file inclusion attacks to assess the integrity of the WAF configuration and its blocking capabilities.

Endpoint Security Testing

The Cymulate **Endpoint Security Assessment vector** enables you to test and optimize the effectiveness of your endpoint security. The vector challenges your endpoint security controls against a comprehensive set of attacks that simulate malicious behavior of ransomware, worms, trojans and other types of malware. Integrations with endpoint detection and SIEM systems will correlate the events and alerts created by these systems to the attacks in order to validate their accuracy.

Improving Phishing Awareness

The Cymulate **Phishing Awareness vector** enables you to evaluate employee security awareness. It provides all the resources required to create, customize, launch and measure phishing campaigns.
Each campaign is tracked for 5 different actions (opening, clicking, entering credentials, reporting and completing a quiz) providing the full picture of employee security awareness levels, enabling the organization to focus on those that require more education and monitoring than others.

Safeguarding Your Internal Network

The Cymulate **Lateral Movement** (Hopper) vector challenges your internal network configuration and segmentation policies against different techniques and methods used by attackers to propagate within the network and control additional systems.
The vector simulates an adversary that has control over a single workstation and attempts to move laterally within the organization.
The result of the assessment is a visualization of all the endpoints that the hopper was able to reach with a detailed description of the attack and spreading methods used for each hop. The assessment identifies infrastructure weaknesses, network misconfigurations and weak passwords, and provides guidance to remediate them. Integrations with vulnerability management systems will identify vulnerabilities present on machines along the attack path.
The assessment does not exploit vulnerabilities and is safe to use in production environments.

Challenging Your DLP Controls

The Cymulate **Data Exfiltration vector** enables you to test the effectiveness of your Data Loss Prevention (DLP) security controls and optimize them.
This vector challenges your DLP controls with a broad range of synthetic regulatory, company confidential, and custom data sets. The vector packages the data into different file types including images and office files and attempts to exfiltrate them using multiple exfiltration methods. The results allow organizations to understand their DLP-related security gaps and take the appropriate measures to remediate.

Defending Against the Latest Attacks

The Cymulate **Immediate Threats Intelligence module** enables you to safely validate your organization's security controls against specific new threats found in the wild. The module is updated almost daily and can be configured to automatically launch assessments upon availability. The module validates email, web gateway, and endpoint security control efficacy but does not require these vectors to be individually licensed. Integration with vulnerability management systems will identify machines vulnerable to the specific exploits used by each threat, helping to prioritize remediation efforts.

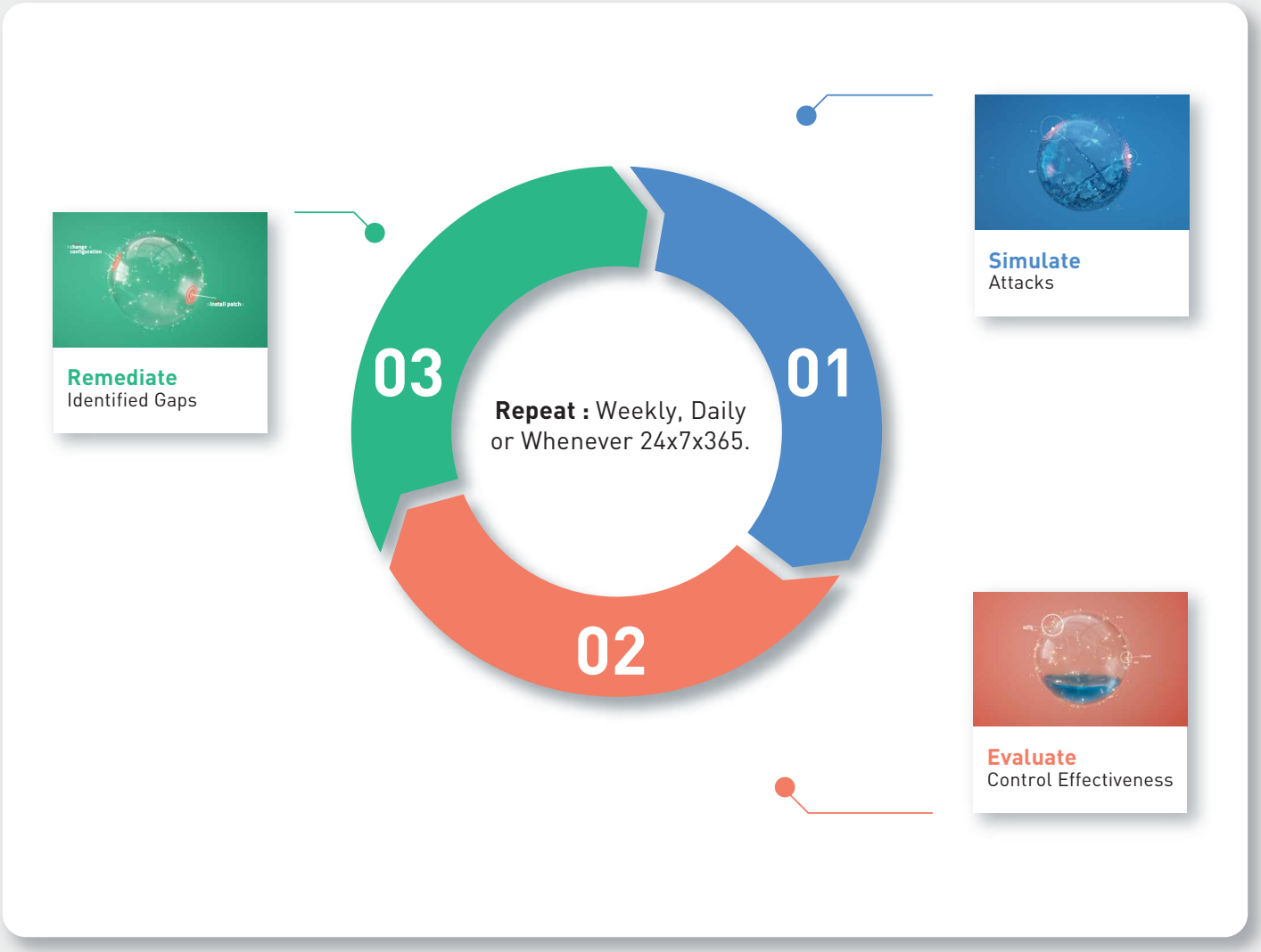
Full Kill-Chain APT Simulation

Cymulate **Full Kill-Chain APT module** enables you to test, measure and improve the effectiveness of your security controls against real-world advanced persistent threats. The module provides pre-defined templates for testing against well-known APT groups. It also enables you to create your own APT attacks from a rich repository of attack resources.
APT assessments execute across the entire kill chain, potentially including Email, Web, Phishing, Endpoint, Lateral Movement and Data Exfiltration.

Automate & Scale Adversarial Expertise

The Cymulate Purple Team module enables SOC/Blue Teams, along with professional Red Teams and pen testers to create, store, modify, and execute both simple and sophisticated assessments using custom built or out-of-the-box templates. It is an open framework, enabling the creation and use of custom payloads and executions. The module can be used to automate Purple team exercises, for example to exercise incident response playbooks. It can also automate security assurance activities and create assessments that validate an organizations unique security policy.
The module leverages the MITRE ATT&CK framework and its taxonomy, mapping both assessments and results to the framework. In addition to providing the result of each individual assessment, the Purple Team dashboard aggregates the results of all the combined assessments on a timeline. This enables you to assess and track your organization's resilience to specific tactics or techniques or to particular APT groups and the TTPs they use.

Cymulate



Who We Are

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security controls against the full attack kill chain, enabling organizations to avert damage and stay safe.
Cymulate is trusted by companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision - to make it easy for anyone to protect their company with the highest levels of security. Because the easier cybersecurity is, the more secure your company - and every company - will be.

Contact us for a 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