Cymulate

Recon Module Assessment

Solution Brief

Test with Intelligence

Cymulate's Recon module discovers what a hacker can find out about your company during the initial information gathering phase of an attack.
The Recon module scans your domains and sub domains for internet facing vulnerabilities and for Open Source Intelligence (OSINT) to discover leaked credentials and organizational information that can be used in an attack.

Attack Vector Overview

During the recon phase, an attacker performs a comprehensive analysis on their target organization. They scan multiple reconnaissance sources for intelligence they can exploit. This includes organizational, employee and technical information that can be used in a social engineering attack or to gain illicit network access.

Continuous Testing

The Cymulate Recon module continuously scans the internet for information that an adversary can find and use before launching an attack.
The module can scan for intelligence on your company, 3rd party supply chain or a target for a merger or acquisition. It scans domains and sub-domains for application and infrastructure vulnerabilities, web misconfigurations and open ports, it also searches open sources for leaked credentials, compromised passwords, darknet presence, employee emails, and other exploitable intelligence that an attacker may use to their advantage. The Recon module alerts the security operations team when newly found intelligence is discovered, enabling them to mitigate vulnerabilities and reduce their cyber exposure.

How It Works

Test Setup - The recon module requires the domain of your company or a third-party in order to begin the assessment process.

Test Execution – Once initiated the platform discovers and fingerprints the company's domain and sub-domains, and scans for application and infrastructure vulnerabilities and weaknesses. In parallel the platform searches the web for other intelligence that an attacker can use to their advantage.

Test Results – Results are provided in a report that includes the findings and, where applicable, the actionable steps that can be taken to remediate them. The report is continuously updated with new findings.

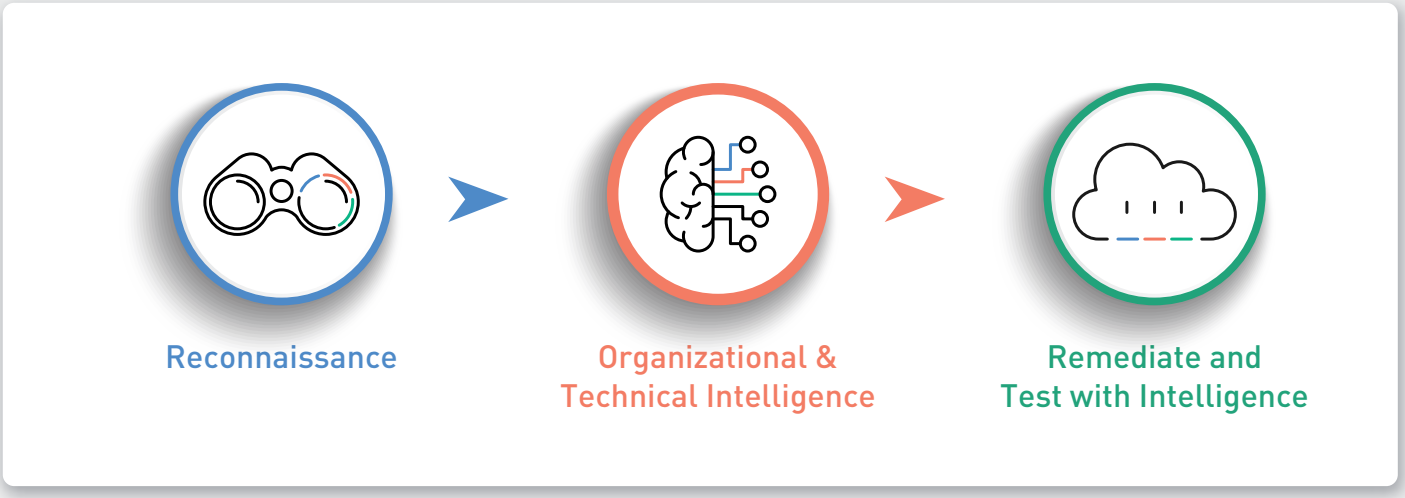
Cymulate

Key Features

- The Recon module is continuous, new findings trigger alerts for immediate attention.
- Findings include both technical and organizational findings.
- Third-Party Assessments–customers can assess potential business partners before engaging with them.
- Simple mitigation and remediation steps are provided together with a complete view of the findings.

Actionable Insights

Recon findings are presented in a comprehensive report listing a complete view of the findings discovered outside of your organization with a risk assessment score. Security teams may then take the appropriate measures to reduce their cyber exposure.



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: 31W 34th Street, 8th floor New York, 10001 | +1 212 6522632