Cymulate

Full Kill-Chain APT Simulation Module

Solution Brief

Are you APT-ready? Simulate. Evaluate. Remediate.

Cymulate makes it simple to continuously test, measure and improve the effectiveness of your security controls in defending against real-world advanced persistent threats.

Can you test controls across the kill chain?

Advanced persistent threats (APTs) attempt to bypass security controls across the cyber kill chain, from pre-exploitation through exploitation to post-exploitation.
As such, defending against an APT requires testing the effectiveness of multiple security controls within your infrastructure. Since the efficacy of one control may affect the next control in the security framework, ascertaining if your defenses work against a full-blown attack becomes a daunting proposition.

Challenging security with Cymulate's full kill-chain APT simulation

Cymulate's Full Kill-Chain APT simulation module solves the challenge of security effectiveness testing across the entire cyber kill chain by validating your security framework in a comprehensive and easy-to-use manner. Instead of challenging each attack vector separately, organizations can now run a simulation of a full-scale APT attack with a click of a button, and gain a convenient, single-pane view of gaps across their security arsenal.

Simulate high-profile APT groups

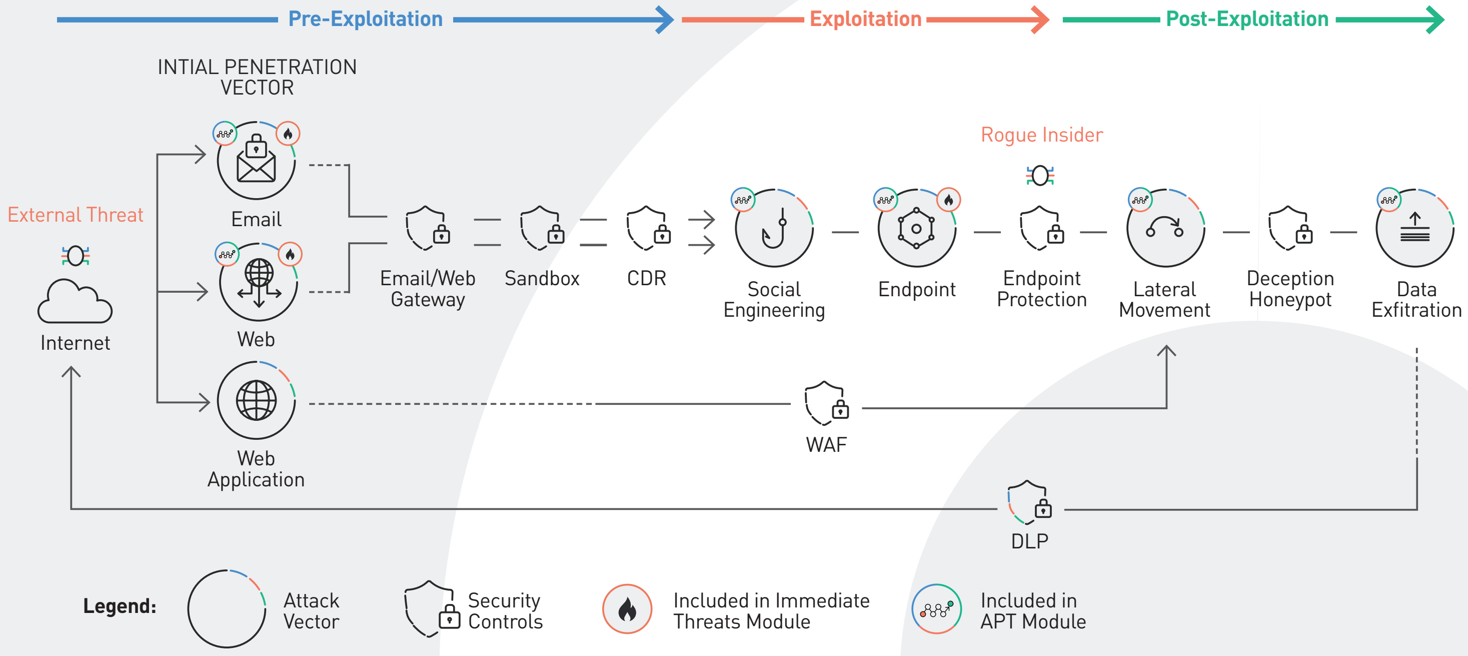
Organizations can select among eight different APT attack templates that mimic the modus operandi of real-world APT attacks launched by well-known APT groups, such as Fancy Bear, OilRig, Lazarus Group, Ocean Lotus and Dragonfly 2.0.

True-to-life APT attack flow

As with a real APT, the different vectors are launched sequentially, starting from a simulated attack delivered through email or web browsing, followed by execution of code and evasion techniques that challenge endpoint security mechanisms. Depending on the template chosen, the module may then challenge network configuration and policies by attempting to move laterally. It then attempts to exfiltrate predefined sets of data, for example mock PII, health records, card details etc., to test DLP controls. For the most true-to-life simulation of an APT, launch it in agentless mode with a simulated phishing email.

Validating SOC readiness and detection capabilities

By launching pinpointed APT attack simulations, organizations can run blue-team tests to challenge and evaluate the effectiveness of their current detection tools, and take corrective measures to remediate any gaps.



Pre-Exploitation

Exploitation

Post-Exploitation

INTIAL PENETRATION VECTOR

External Threat

Internet

Email

Web

Web Application

Email/Web Gateway

Sandbox

CDR

Social Engineering

Endpoint

Rogue Insider

Endpoint Protection

Lateral Movement

Deception Honeypot

Data Exfitration

WAF

DLP

Legend: Attack Vector; Security Controls; Included in Immediate Threats Module; Included in APT Module

Actionable mitigation insights and reporting

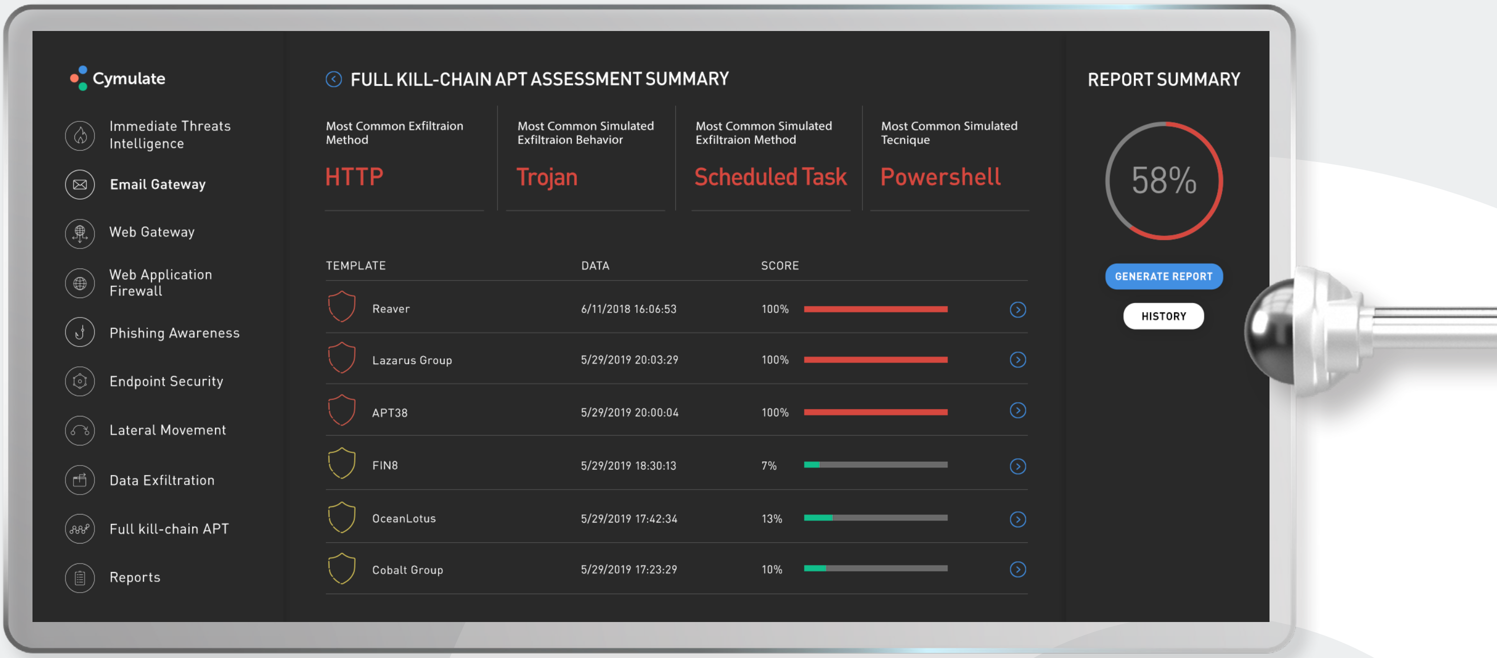
An attack simulation is only as effective as the corrective steps taken to remediate identified gaps. Therefore, at the end of each APT simulation, the following actionable insights are automatically generated and delivered:

- **The outcome of each step of the APT** simulation is shown, e.g. Success, Failure or Partial Success, showing you where you're most vulnerable and where your controls are already optimized against a potential attack.
- **An exposure score** is generated, taking into account the APT's potential asset impact, its infection success rate and probability of encounter.
- **Remediation and mitigation guidelines** are provided to enable IT and security teams to implement the appropriate countermeasures. Guidelines are based on industry best practices, and are also mapped to the MITRE ATT&CK™ framework to offer additional context.
- **KPI Metrics** calculated at the end of each simulated APT deliver quantifiable security posture benchmarks, and enable prioritizing remediation efforts and resources. They also provide a way to measure security effectiveness over time, and enable comparing your organization's cyber stance to others in your industry.
- **Executive and technical-level briefs** summarize simulation results for the board, or delve into details for your security team so that it has the information it needs to reduce your attack surface.

Deploys in minutes | Simple to use | SaaS-based platform | Automated or on-demand | Covers the full attack kill chain

Who we are

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security controls, allowing hyper-connected 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 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.



FULL KILL-CHAIN APT ASSESSMENT SUMMARY

Most Common Exfiltraion Method	Most Common Simulated Exfiltraion Behavior	Most Common Simulated Exfiltraion Method	Most Common Simulated Tecnique
HTTP	Trojan	Scheduled Task	Powershell

TEMPLATE	DATA	SCORE
Reaver	6/11/2018 16:06:53	100%
Lazarus Group	5/29/2019 20:03:29	100%
APT38	5/29/2019 20:00:04	100%
FIN8	5/29/2019 18:30:13	7%
OceanLotus	5/29/2019 17:42:34	13%
Cobalt Group	5/29/2019 17:23:29	10%

Full Kill-Chain APT Simulation Module - Executive Summary Dashboard

Are you APT-ready? Find out with a free trial or contact us for a live demo at www.cymulate.com