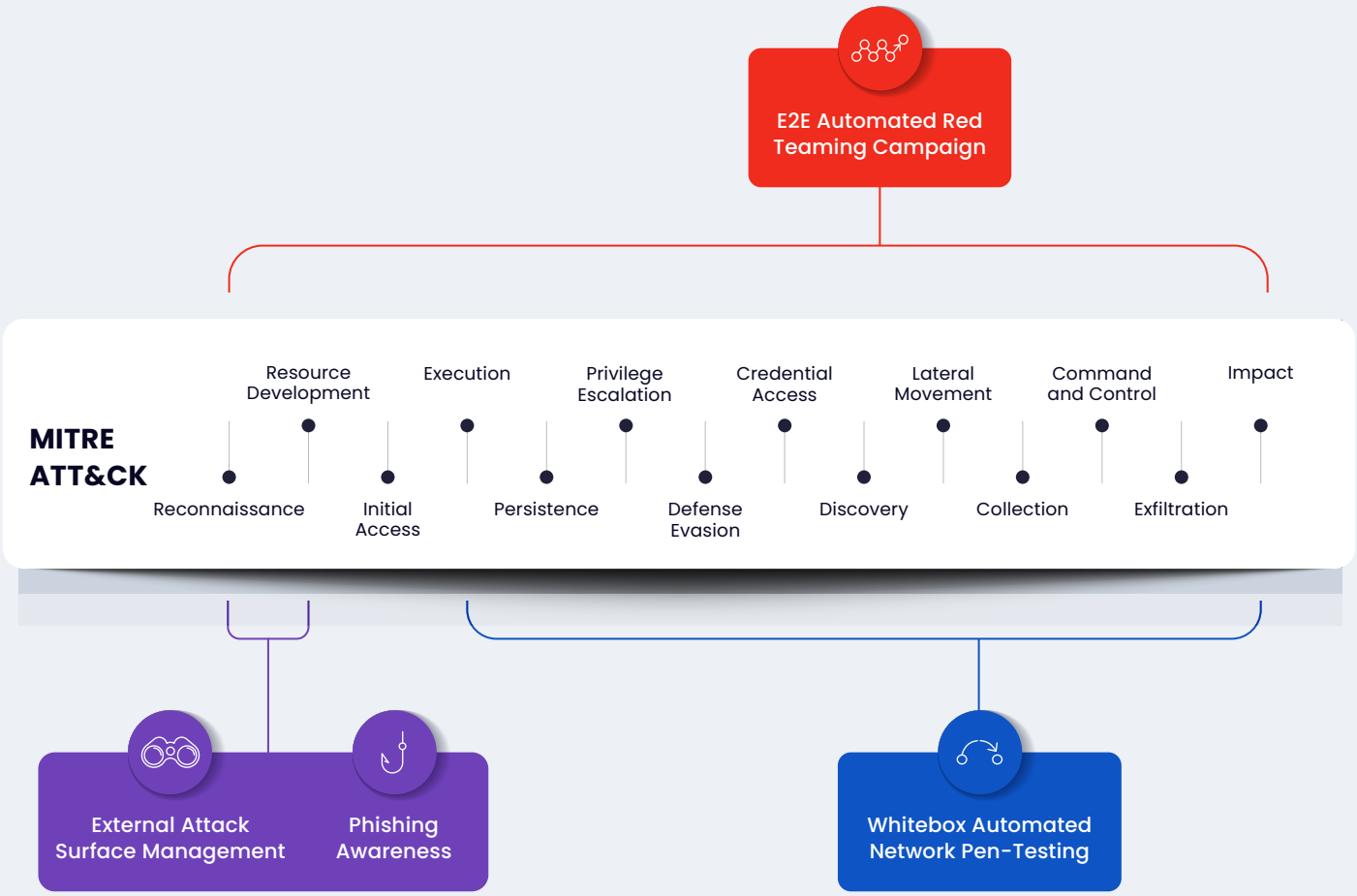
APT/Full Kill-Chain Security Validation

Solution Brief

Ensure End-to-End Protection

Advanced persistent threats (APTs) attempt to bypass security controls across the cyber kill-chain, from pre-exploitation through exploitation to post-exploitation. Defending against an APT requires testing the effectiveness of multiple security controls within a company's infrastructure. Since the efficacy of one control may affect the next control in the security framework, checking each security control separately is not enough to know if a company is protected from APTs.

Cymulate's Full Kill-Chain APT enables organizations to test security effectiveness across the entire kill-chain. They can run a full-scale APT attack simulation to understand the overall effectiveness of their security control configuration and detect and response tools. Organizations can select from out-of-the-box APT attack templates or customize their own. After each assessment, the platform provides remediation guidance so companies can take corrective measures to eliminate any gaps. This module can be launched with an agent as a Full Kill-Chain Scenario, or it can be launched in agentless mode as a Full Kill-Chain Campaign.

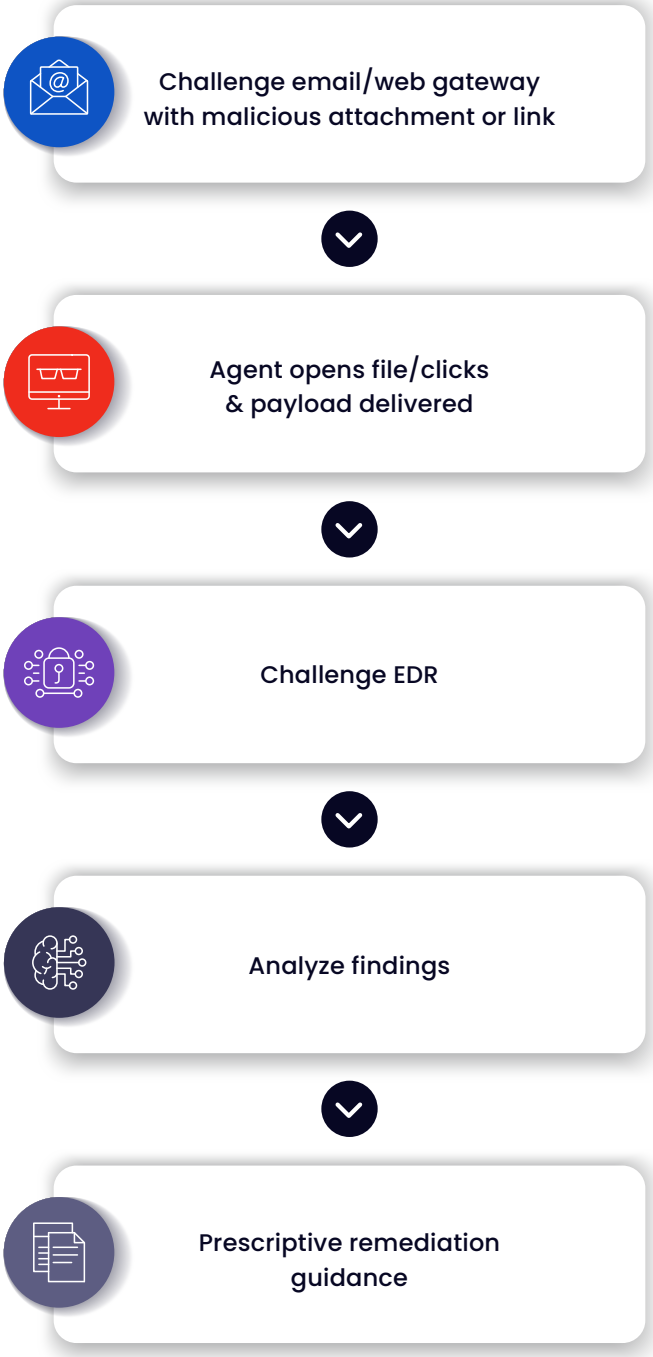


Cymulate

How Does it Work?

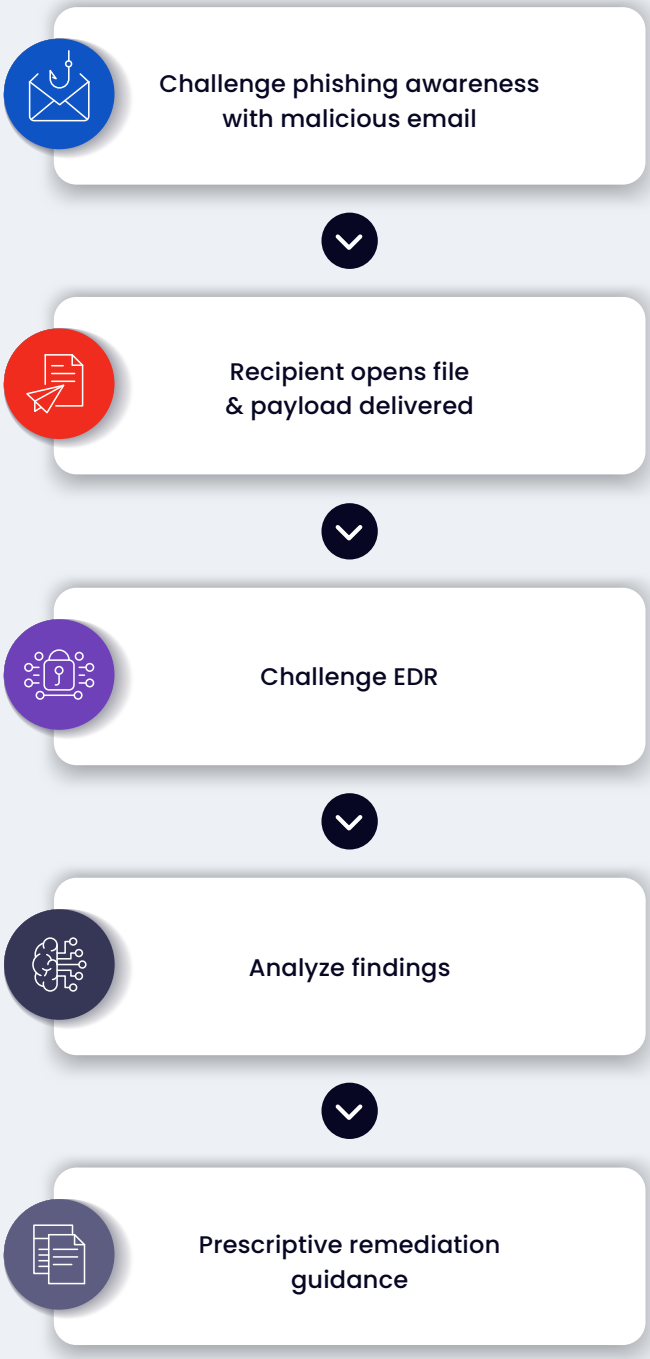
Full Kill-Chain Scenarios

As with a real APT, the different vectors are launched sequentially, starting from a simulated attack delivered by the Cymulate server through the email or web gateway. Once the payload is delivered, production-safe code execution and defense evasion techniques challenge endpoint security resilience with ransomware, trojans, worms, or advanced scenarios.



Full Kill-Chain Campaigns

This is an agentless assessment that begins with a phishing campaign and relies on users being manipulated to open the malicious files or link. Once the recipient clicks and executes the payload, production-safe code execution and defense evasion techniques challenge endpoint security resilience with ransomware, trojans, worms, advanced scenarios, or lateral movement.



Who Can Use Full Kill-Chain APTs?

Red Teams

Red teams use this module to automate and schedule APT attacks, instead of continuously running them manually.

Red and Blue Teams

Blue teams use Cymulate's mitigation guidance to remediate controls and independently rerun the campaign that the red team already created to assess the impact of their actions.

Blue Teams

For organizations without red teams, blue teams utilize both the out-of-the-box assessments and the mitigation guidance to continuously test their controls against APTs and improve their adversarial skills.

Benefits

Red Team

- More time for sophisticated red team exercises
- Less time spent on coding & tedious tasks
- Auto-generated reports & analytics

Blue Team

- Improve adversarial skills on the job
- Increased collaboration
- Quick time to mitigation

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness. **Measuring your cybersecurity performance is fundamental towards creating a more secure organization!**

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

Start Your Free Trial

Headquarters: Maze St 3, Tel Aviv 6578931, Israel | +972 3 9030732 | info@cymulate.com