cymulate

DATA SHEET

Cymulate Continuous Automated Red Teaming (CART)

Test and Validate Security Across the Full Kill-Chain

Cymulate Continuous Automated Red Teaming (CART) provides the automation and scale for ongoing security validation with advanced testing for active campaigns and custom threats that target users, systems and networks. The implementation is easy, and the assessments can test any technique at any stage of the attack kill-chain independently or as part of complex attack chains.

Cymulate CART simulates attacks that propagate within the network in search of critical information or assets. The solution is cloud-based and easily deploys with minimal installation and maintenance. Installing one lightweight agent per environment facilitates seamless communication between customer devices and the Cymulate platform, ensuring timely updates and efficient transfer of operational data.

> **Cymulate allows us to extensively scale our red team activities with only one red teamer.**
> - Assistant Information Security Manager, Financial Services

Cymulate CART Capabilities

Map attack paths

The network penetration testing capability simulates an attacker that has gained an initial foothold by taking control of a single compromised workstation, escalating privileges to disguise as legitimate users, and moving laterally in search of any additional assets that can be compromised. It safely applies threat tactics and techniques to uncover infrastructure misconfigurations and weaknesses in permissions, validating attack paths against security controls.

This independent capability allows the organization to segregate network-level defenses from endpoint-level defenses for a more accurate analysis of both layers of controls. Continuous testing with the network penetration testing capability helps identify changes in IT infrastructure and network misconfigurations that may provide new avenues for lateral movement. At the end of the assessment, the system also removes any components distributed to other machines.

Cymulate CART Benefits

Increase team efficiency

Automate assessments to reduce labor-intensive, manual testing.

Scale adversarial activities

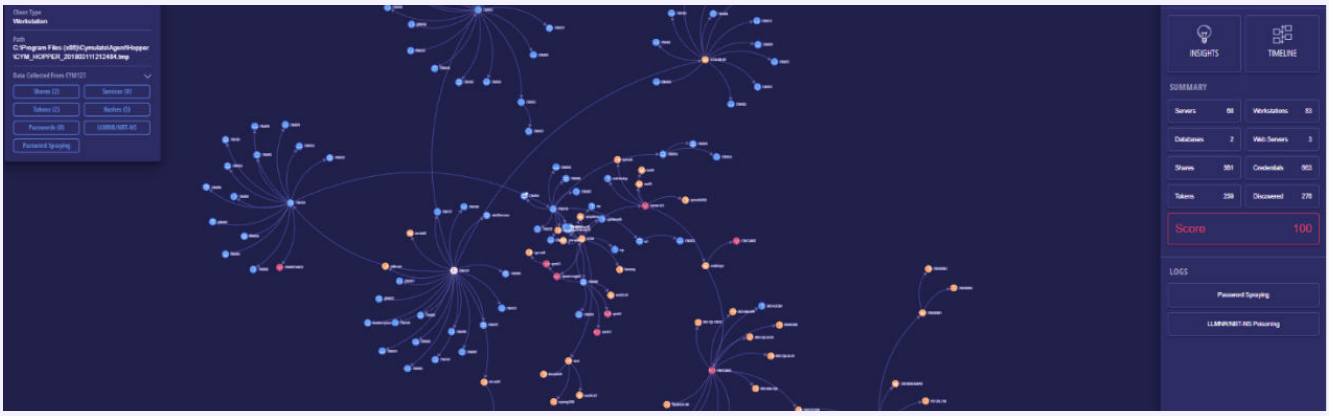
Create, modify and run chained or atomic attack campaigns.

Monitor security drift

Repeat assessments to validate mitigations and identify drift.

Optimize security

Clear steps to remediate, close gaps and reduce exposure.

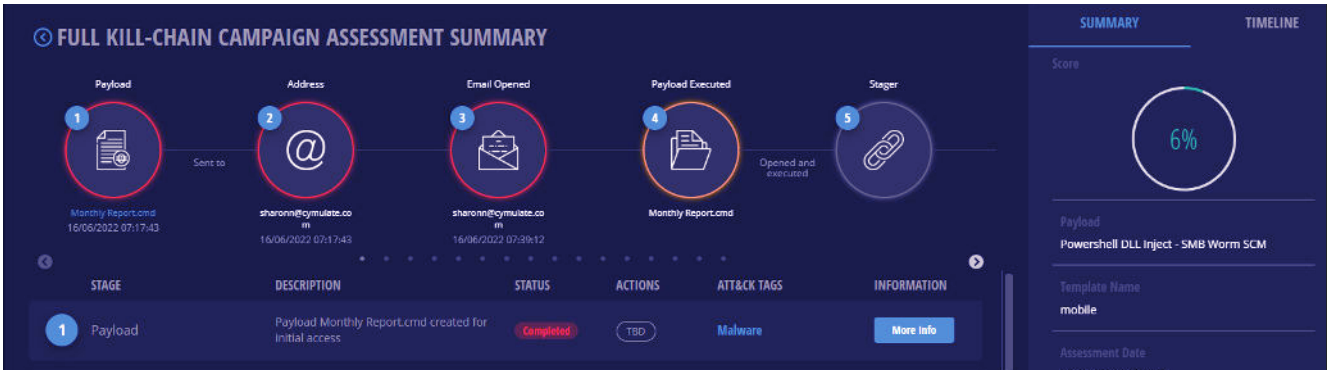


Each network penetration testing assessment visualizes the attack path, including all the endpoints reached and the methods used, providing insight into the weaknesses in the network infrastructure.

Test APTs and campaigns

The full kill-chain campaign capability validates an organization's security stack against real-world cyberattacks that attempt to bypass security controls and execute techniques from across the kill-chain, from attack delivery to exploitation and post-exploitation. The full kill-chain campaign begins with one or more production users interacting with targeted attack emails that pose no real risk to the organization but provide the initial foothold for the simulated attack chain.

Once the recipient clicks and executes the payload, follows a link to download and run a payload, or performs other user actions to initiate the attack, production-safe code execution and defense evasion techniques challenge endpoint security resilience with ransomware, trojans, worms, advanced scenarios or lateral movement. The cybersecurity team controls each attack step and technique, and Cymulate code components are used to ensure safety.



The full kill-chain campaign assessment summary visually represents the attack stages at the top of the screen. Each stage in the attack that was executed successfully is circled in red, and the stage that is circled in orange is when the attack was thwarted. The full kill-chain stages are listed below, each row displaying the stage, its description, status, actions and ATT&CK tags.

Evaluate employee awareness

The phishing awareness capability provides all the resources to create an internal phishing campaign and measure employee resilience against phishing attacks. Creating a customized assessment is quick and easy. Employee interactions with the mock phishing emails are automatically recorded, logging hazardous behaviors such as clicking links or entering credentials. These assessments identify employees needing additional phishing awareness training and highlight users who are not following proper policies and procedures.

About Cymulate

Cymulate is the leader in exposure management and security validation. More than 500 customers worldwide rely on the Cymulate platform for continuous discovery, validation, prioritization, and guided remediation of security gaps before attackers can exploit them. For more information, visit www.cymulate.com.