DATA SHEET

Cymulate

Cymulate Continuous Automated Red Teaming

Validate Attack Paths Across the Full Kill-Chain

Cymulate Continuous Automated Red Teaming (CART) provides cybersecurity teams a platform to increase operational efficiency and optimize their adversarial activities with production-safe methodologies. The implementation is easy, and the assessments can test any technique at any stage of the attack kill-chain independently – start with a well-crafted phishing email or begin from inside the network and move laterally in stealth, using a variety of exploits. The Cymulate CART solution supports automated testing for vulnerability validation, what-if scenario, targeted-, and custom-testing within a flexible framework for repeatable and scalable testing.

How it Works

Cymulate CART simulates attacks that propagate within the network in search of critical information or assets. The solution is cloud-based and easily deployed with minimal installation and maintenance efforts. For some capabilities, customers only need to install one lightweight agent per environment to run assessments. The agent facilitates seamless communication between customer devices and the Cymulate platform, ensuring timely updates and efficient transfer of operational data.

Cymulate CART Capabilities

Network Pen Testing

The **network penetration testing capability** simulates an attacker that has gained an initial foothold by taking control of a single compromised workstation, moving laterally in search of any additional assets that can be compromised. It safely applies threat tactics and techniques to uncover infrastructure misconfigurations and security weaknesses, 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 cleans up after itself to remove any components that were distributed to other machines.

Cymulate CART Benefits

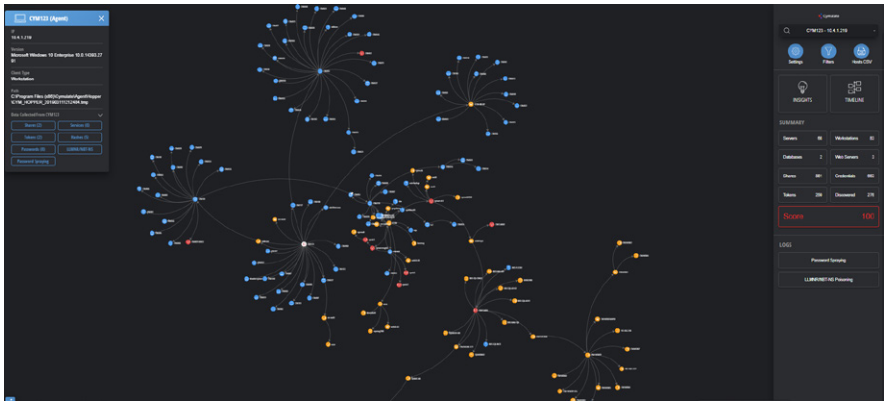
AUTOMATED TESTING
Scheduled and automated assessments for testing on demand and reducing repetitive, labor-intensive manual tasks

CUSTOMIZATION
The ability to create, modify and run chained or atomic attack campaigns

CONTINUOUS VALIDATION
Repeat assessments to validate mitigations and identify drift

REDUCED RISK
Clear steps to remediate, close gaps, and reduce exposure

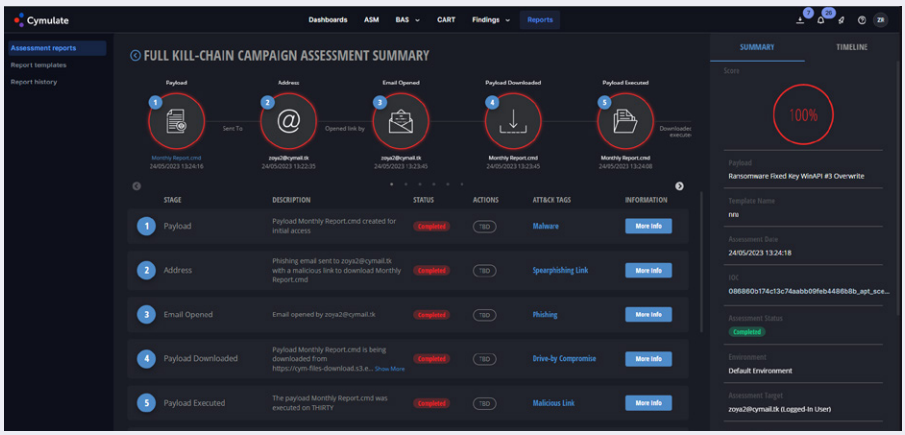
Network Pen Testing: Validated Attack Paths



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

Validate Security Against Advanced Persistent Threats

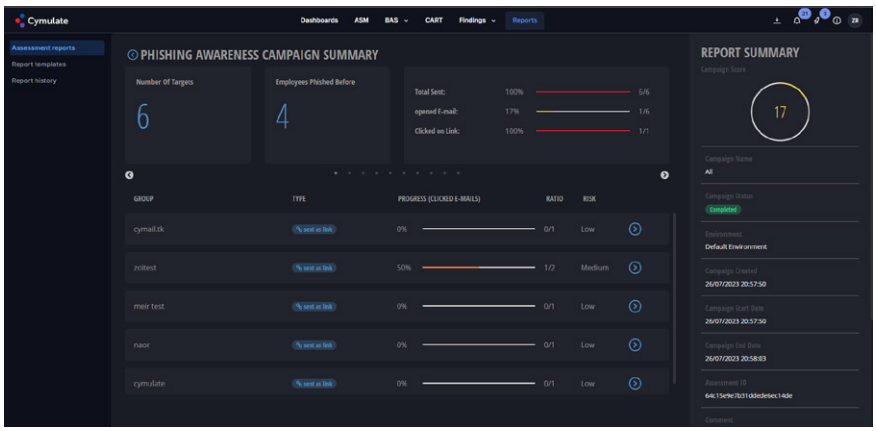
Cymulate CART includes the **full kill-chain campaign capability** to validate an organization's security framework against real-world cyber attacks attempting to bypass security controls across the cyber kill-chain, from attack delivery to exploitation and post-exploitation. The full kill-chain capability begins with one or more production users interacting with targeted attack emails that pose no real risk to the organization. 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. Each step of the attack and each technique used is controlled by the cybersecurity team and uses Cymulate code components to ensure safety.



The full kill-chain campaign assessment summary provides a graphical representation of 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 the stage the attack was thwarted. The full kill-chain stages are also listed below, each row displaying the stage, its description, status, actions, and ATT&CK tags.

Evaluate Employee Security 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 with Cymulate CART is quick and easy, and 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.



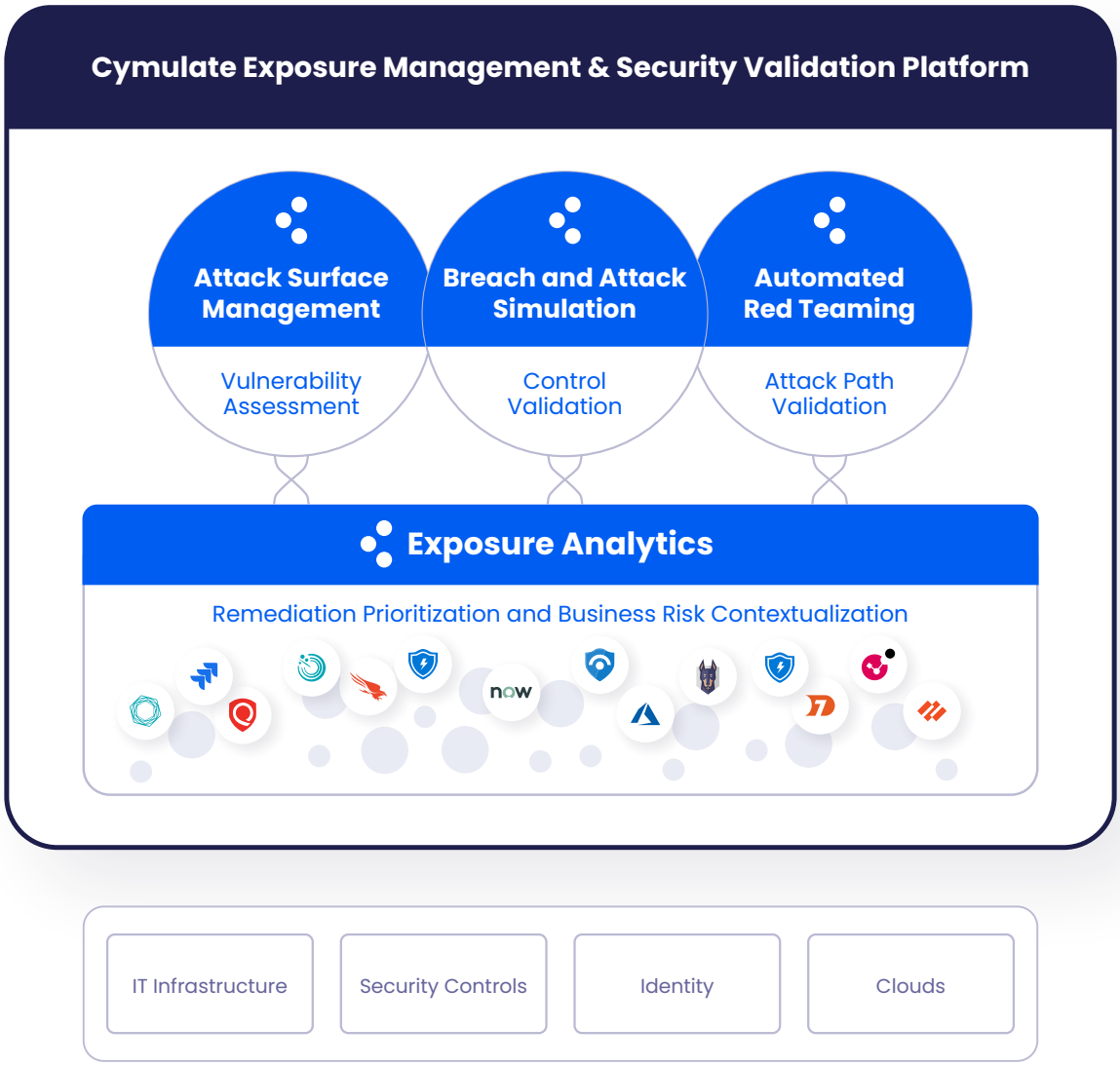
Phishing awareness summaries contain important, at-a-glance metrics such as the number of targets, employees phished before, total phishing emails sent, emails opened, links clicked, and more. The bottom half of the summary lists the groups targeted in the phishing campaign. Each row displays the group name, type of delivery, progress (clicked emails), ratio, and risk. Click on a group row to view more details, such as the recipient's email addresses, whether they have been phished previously, the current status of the sent payload (sent, opened, clicked), first and last name, and date sent.

Map Assessments to the MITRE ATT&CK® Framework

The MITRE ATT&CK® Heatmap provides a detailed view of the current state of cyber resilience by visualizing the exposure to each technique. The heatmap correlates all findings from across the Cymulate platform, including filtering and drill-downs into the assessment details for test results and recommended mitigations.

The Cymulate Platform

Cymulate CART is available both as a standalone SaaS offering and as an integrated offering within the Cymulate Exposure Management and Security Validation Platform. The Cymulate platform provides a comprehensive and scalable solution for security leaders, regardless of their security posture maturity, to drive their continuous threat exposure management program and support both the technical and business requirements of scoping, discovery, prioritization, validation, and mobilization.



About Cymulate

Cymulate, the leader in exposure management and security validation, provides a modular platform for continuously assessing, testing, and improving cybersecurity resilience against emergent threats, evolving environments, and digital transformations. The solution has a quantifiable impact across all 5 continuous threat exposure management (CTEM) program pillars and on a business's ability to reduce risk by understanding, tracking, and improving its security posture. For more information, visit www.cymulate.com.

Contact us for a live demo

Start Your Live Demo

info@cymulate.com | www.cymulate.com