Cymulate

Lateral Movement Assessment
Solution Brief

Safeguarding your Internal Network

Cymulate's Lateral Movement campaign challenges your internal network configuration and segmentation policies against different techniques and methods used by attackers to propagate within the network and control additional systems.

Following establishing an initial foothold within a network, an adversary's next step is lateral movement. The attacker will use different techniques to progress through a network in search of an objective. As threat actors move deeper into the network, they become harder to detect because they use evasion techniques to cloak their presence and actions, as well as escalate their privileges to impersonate authorized users in order to access high value assets.

The Cymulate Lateral Movement campaign simulates an adversary that has control over a single, compromised workstation and attempts to move laterally within the organization. The result of the assessment is a visualization of all the endpoints that the Cymulate Agent was able to reach with a detailed description of the methods used.

The assessment identifies infrastructure weaknesses and provides guidance to remediate them. Continuous testing helps to identify changes in the IT infrastructure and network misconfigurations that may open new paths for lateral movement.

How It Works

Phase 1: Discovery
The Cymulate Agent scans the system and internal network for potentially reachable systems and fingerprints them. In addition, relevant information is collected from the workstation itself such as network shares, user accounts, and services. Once critical areas to access are identified, the next step is gathering login credentials that will allow entry.

Phase 2: Credential Access
The Cymulate Agent will collect information from the workstation based on common credential dumping techniques which will later be used for spreading purposes. Credential dumping techniques can include dumping of tokens, hashes, and Kerberos tickets from memory and the collection of cleartext passwords.

Phase 3: Lateral Movement
Based on results from previous stages, the Cymulate Agent will try to spread laterally from the original workstation by leveraging one or more attack methods. If Crown Jewels have been defined in the template, the campaign will attempt to access these specifically.

Phase 4: Test Results and Actionable Insights
The Lateral Movement results are presented in an interactive graphic diagram that shows the attacker's lateral movement path and the methods used to achieve each hop, along with KPI metrics and actionable mitigation recommendations. By taking the appropriate countermeasures, IT and security teams can increase their internal network security. A technical and an executive report are also generated following each assessment and a risk score is calculated.

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