



How To Continuously Validate Security Posture

Table of Contents

| | |
|---|----|
| Understanding Security Posture, at a Glance | 3 |
| Scenarios | 4 |
| • Immediate Threats Intelligence | 4 |
| • Email Gateway | 5 |
| • Web Gateway | 6 |
| • Web Application Firewall (WAF) | 7 |
| • Endpoint Security | 8 |
| • Data Exfiltration | 9 |
| • Full Kill-Chain Scenarios..... | 10 |
| Advanced Scenarios | 11 |
| Campaigns | 12 |
| • Attack Surface Management (ASM) | 12 |
| • Phishing Awareness | 13 |
| • Lateral Movement | 14 |
| • Full Kill-Chain Campaigns | 15 |
| Analyzing Security Posture In-Depth | 15 |
| Dynamic Dashboards | 16 |
| ABVM – Optimizing Vulnerability Patching Prioritization | 17 |

With the constantly evolving threat landscape, the compliance requirements getting more stringent all the time, and the business imperatives leading to the constant new deployments that are the hallmarks of agile development, preventing security posture drift can seem a pipe dream. Yet, continuous security validation technologies are keeping up with the times and provide solutions designed to ensure that the integrity of an organization's infrastructure is secure against threats and its system is resilient.

Understanding Security Posture, at a Glance

The demo dashboard below shows the result of Cymulate's scoring system applied to an organization's security posture, both overall and at every point in the kill-chain. The scores displayed number from 0 to 100 and reflect the results of the assessments ran on an infrastructure. In the Cymulate language, the higher the number, the higher the risk to an organization. In the sample above, that for the email gateway segment, the score is a low 1, which validates that the endpoint security controls are functioning at a very high efficacy level, whereas the Attack Surface Management segment scores a dangerously high 89, indicating that a potential attacker could easily find unmonitored exposed assets.

The Cymulate security score is calculated by correlating industry-recognized standards; the NIST Risk Management Framework, CSVSS v3.0 Calculator, Microsoft's DREAD and the MITRE ATT&CK™ Framework with the resilience of an infrastructure to the set of production-safe attacks launched by the Cymulate platform. Resilience is measured by evaluating the percentage of attacks detected, preempted, or mitigated by the existing security infrastructure.

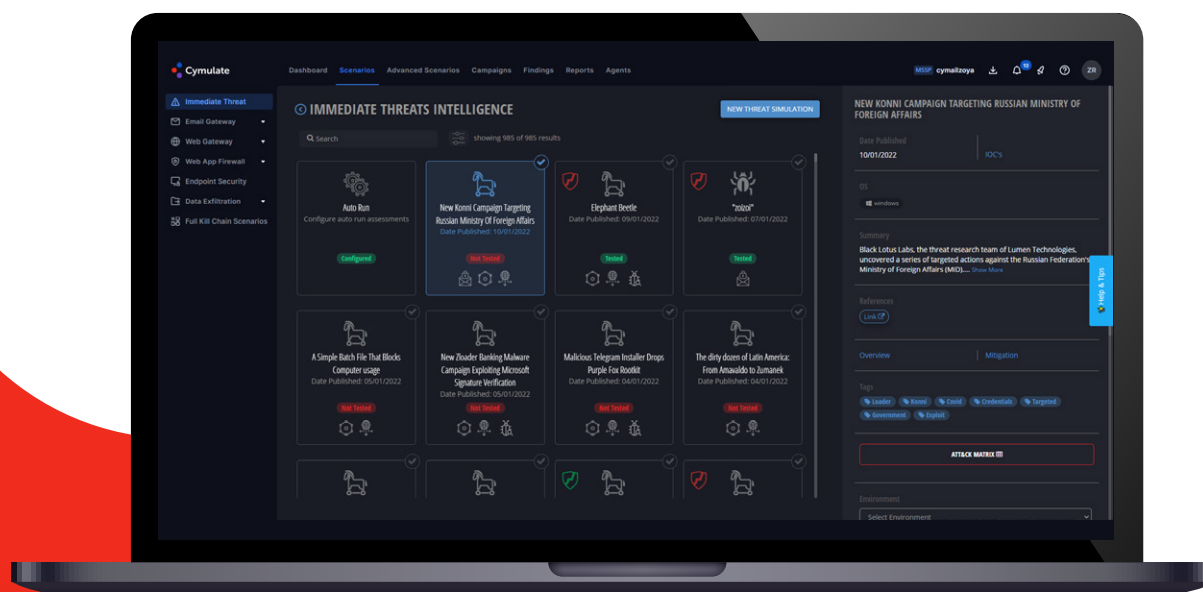


Scenarios

Agent based production-safe attacks are designed to assess the efficacy of security controls. These are divided into modules:

Immediate Threats Intelligence

Every day, numerous new payloads and attacks emerge in the wild making it nearly impossible to validate that an organization's security controls are protecting against each threat as they appear. If these threats succeed in bypassing an organization's security controls, they can eventually cause serious damage to an organization. These new attacks (such as Emotet, Dridex, Ryuk, Trickbot, and others), orchestrated by known and unknown hostile entities, come in different forms such as email attachments or a downloadable links appearing on legitimate or compromised websites. Cymulate's analysts continuously monitor the web for new threats, adding the most recent and relevant ones, usually within 24 hours after discovery. Simulations of new threats are created daily by the Cymulate Research Lab and made available for customers on the Cymulate platform.

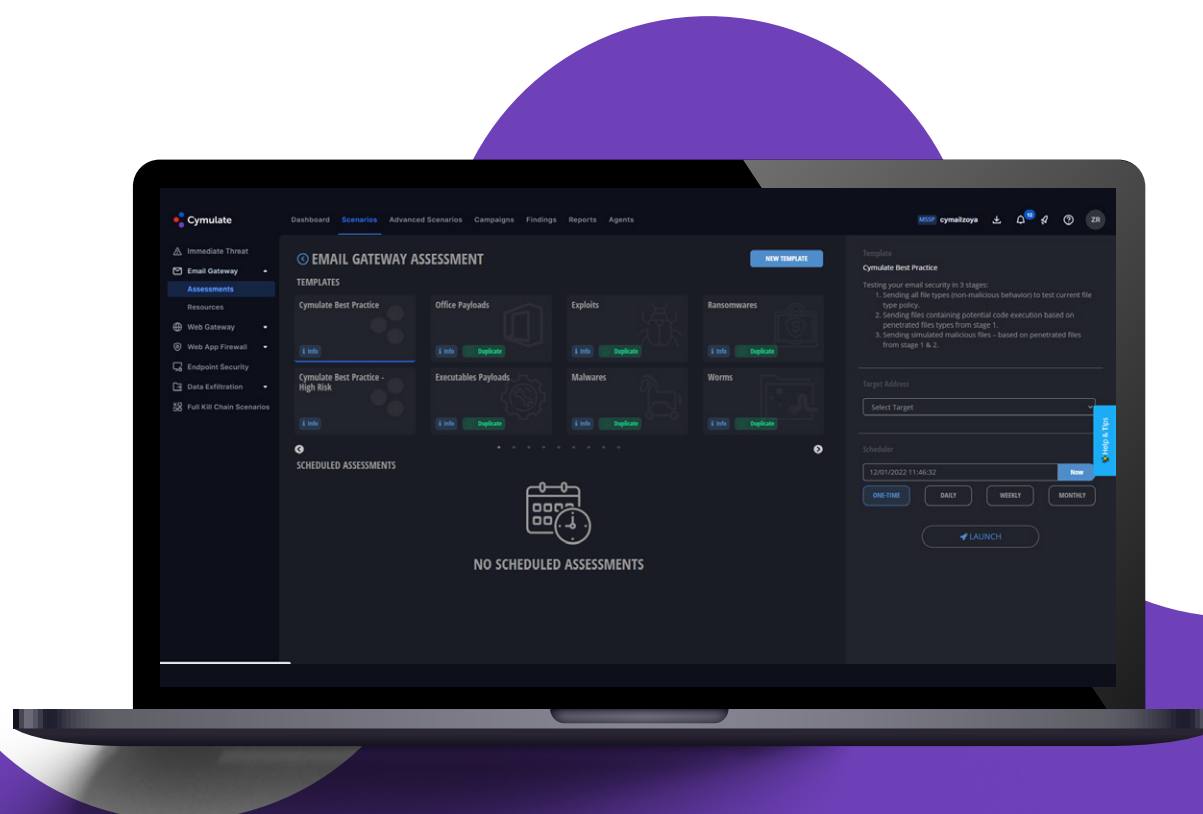




Email Gateway

Email is the most frequently used delivery method of attack for exploiting security weaknesses and compromising an organization's environment. Organizations deploy different email security solutions and services to protect themselves from email attacks but incorrect implementation and misconfigurations often allow malicious emails to penetrate.

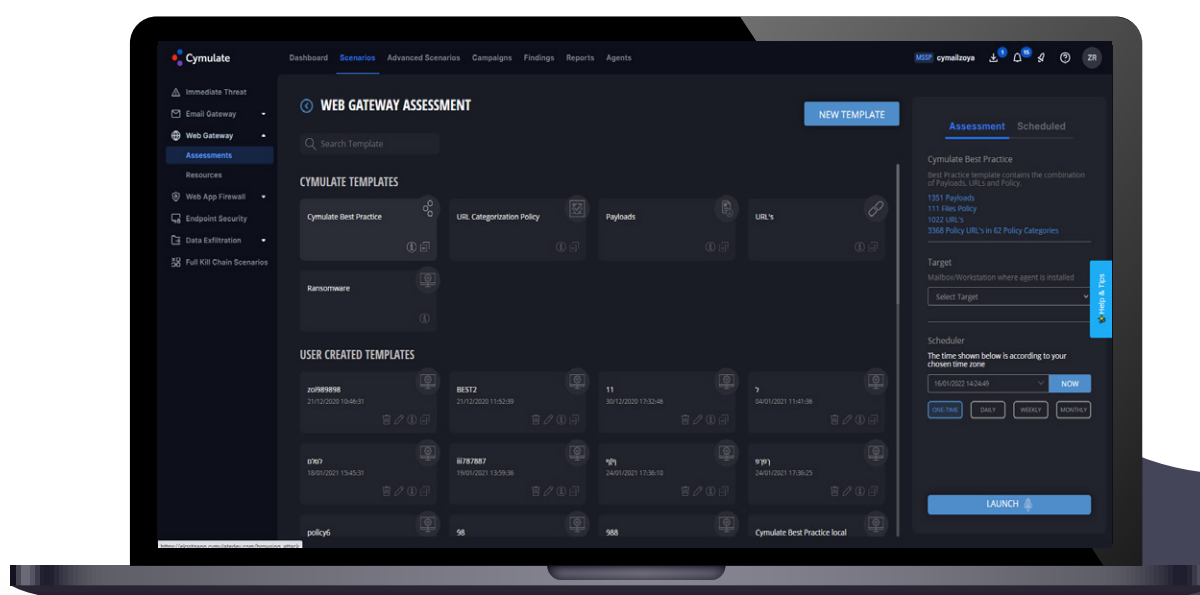
The Email Gateway module allows organizations to test their email security solutions against a comprehensive set of simulated attacks. This module allows them to send thousands of different types of simulated malicious emails containing threats such as ransomware, worms, trojans, and exploits.



Web Gateway

Malicious and compromised websites are commonly used by cyber-criminals to gain a foothold or steal information. These include websites that infect browsers with drive-by downloads and phishing websites that mimic legitimate sites to steal user credentials. A growing proportion of websites use HTTPS encryption to convey a false sense of security to the end-user.

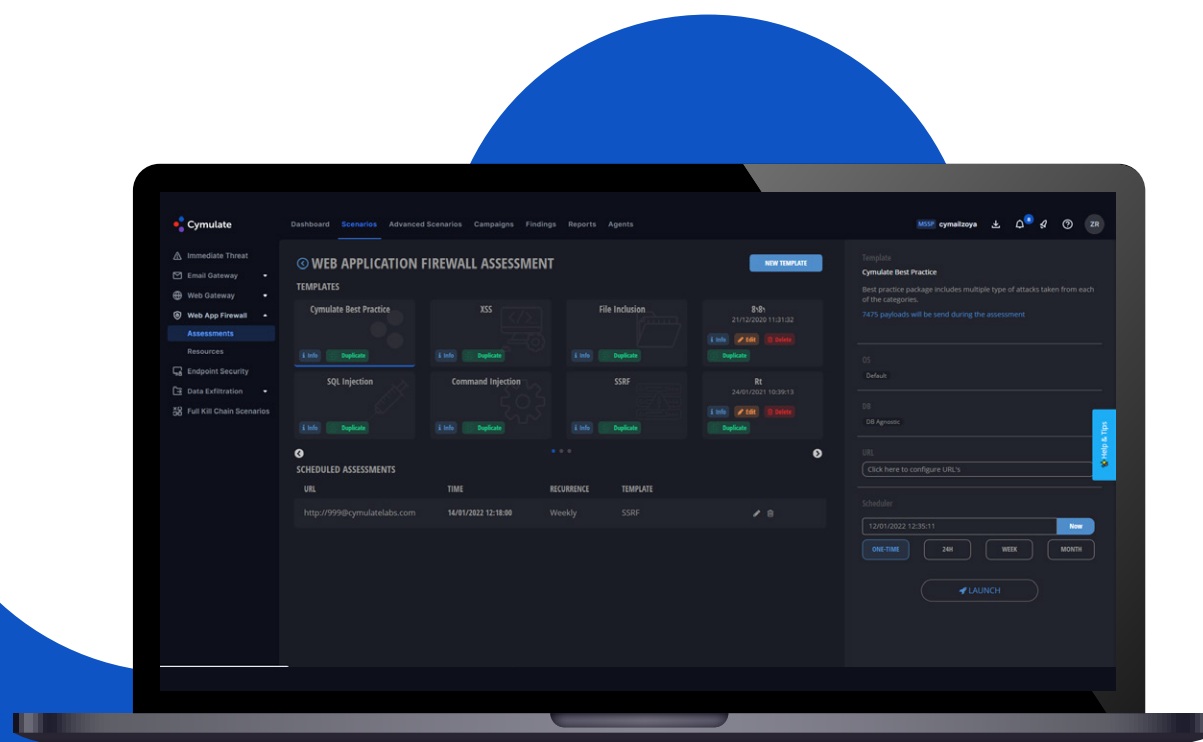
The Web Gateway module simulates an employee accessing malicious websites. The tests are performed over HTTP and HTTPS by the Cymulate Agent to validate the effectiveness of the organization's web security from a controlled endpoint on the production network. Security assessments are performed against a large, continuously growing database of malicious websites that are updated daily. Continuous testing verifies that web security controls are set up correctly and maintained at optimal effectiveness.



Web Application Firewall (WAF)

Web application attacks are frequently used by threat actors to steal information or penetrate an organization through its externally facing web applications. Attacks such as SQL injection (SQLi) and other forms of command injections are used to exploit web application and web infrastructure vulnerabilities that can lead to a breach. Web application security measures often fall short through misconfiguration and lack of optimization. In addition, evolving hacker tools and techniques can cause even the best web application firewall implementation to be ineffective within a few months, or even weeks.

The Cymulate WAF module simulates the behavior of an adversary attacking the web application and web infrastructure of an organization. It tests the effectiveness of the web security controls against these attacks and is constantly updated with new tactics and techniques.



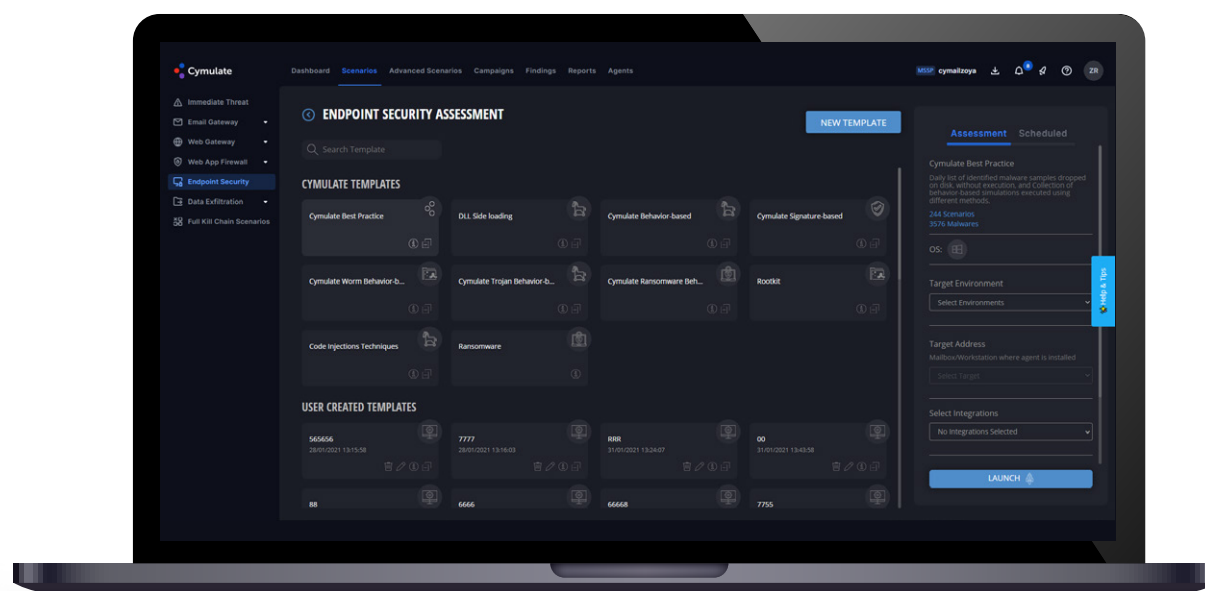
Endpoint Security

User workstations and endpoints are the most common target for gaining initial foothold in cyber-attacks and a base for lateral movement within a compromised network. Therefore, organizations often invest heavily in Endpoint Protection Platforms (EPP) and Endpoint Detection and Response solutions (EDR).

However, endpoint security measures often fall short due to misconfigurations and lack of optimization. Even the best implementation will not be optimal within a few months or even weeks and will miss evolving variants of worms, ransomware, and trojans while failing to detect new hacker tools and techniques.

Testing endpoints against behavior and signature-based attacks, lateral movement, and MITRE ATT&CK methods and commands is crucial to expose gaps that may exist. By simulating scenarios that mimic adversary behavior, the Endpoint Security module identifies security gaps and provides guidance to remediate them.

Endpoint Security assessments can also be used to validate an organization's security tools (EDR, SIEM, SOAR). By integrating security tools into the Cymulate platform, the Cymulate Agent will check if events were detected and whether an alert was triggered.



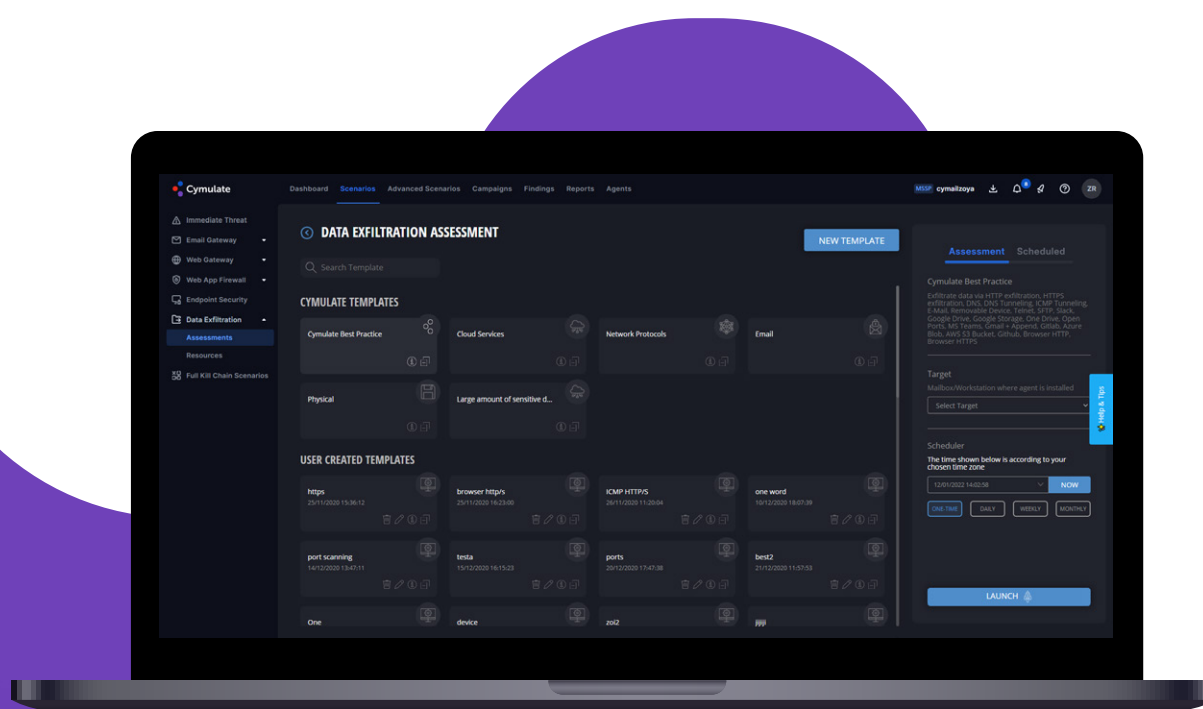
Data Exfiltration

Cymulate's Data Exfiltration module enables an organization to test the effectiveness of its Data Loss Prevention (DLP) security controls and optimize them as necessary. This module challenges DLP controls with a broad range of regulatory or custom data sets and exfiltration methods.

DLP solutions are designed to protect against both malicious and unintentional data exfiltration. Corporate confidential data such as financial reports prior to publication, source code, and other intellectual property must be protected from corporate espionage. In addition, companies must comply with strict laws and regulations (GDPR, HIPAA, PCI-DSS, etc.) when handling sensitive data or PII (personally identifiable information).

DLP solutions also aim to protect organizations from employees inadvertently storing or sharing sensitive information on unsanctioned cloud services (shadow IT).

Organizations should be able to test their DLP controls frequently in the face of regulatory revisions, updates to corporate data security policies, and new exfiltration methods. The Data Exfiltration module allows organizations to test their DLP solution in a non-disruptive manner and continuously validate that confidential and sensitive assets remain secure on an ongoing basis.





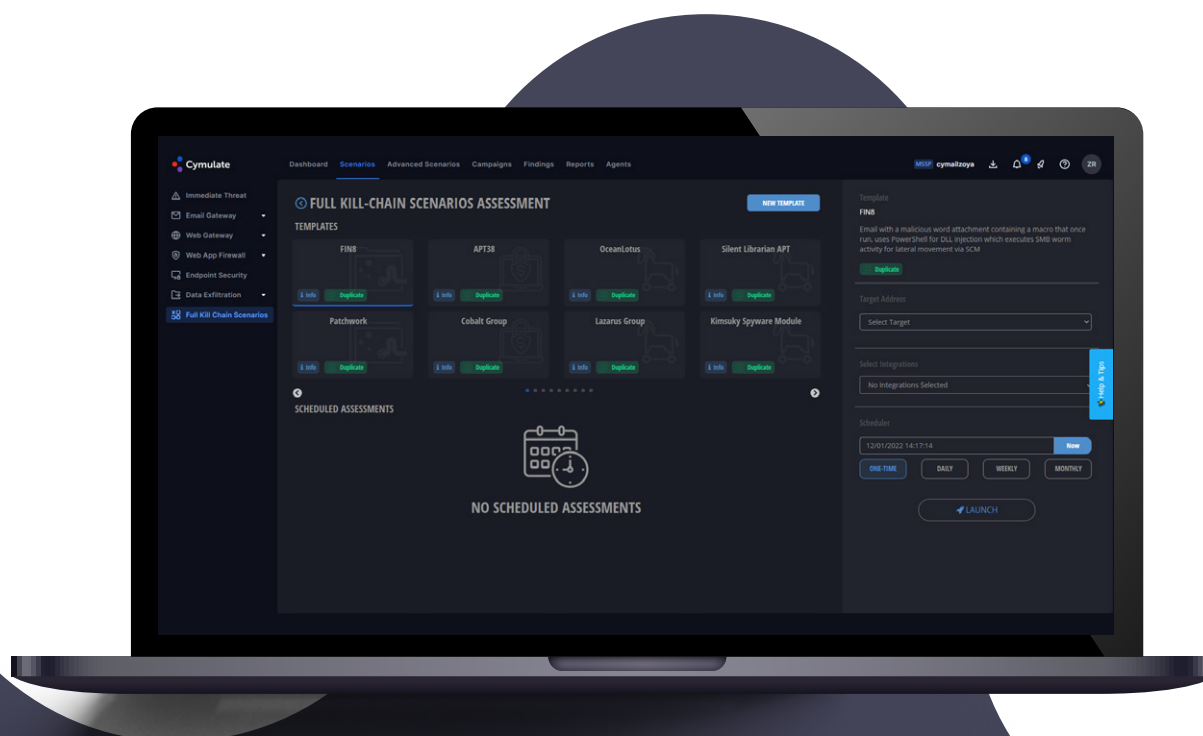
Full Kill-Chain Scenarios

Cymulate's Full Kill-Chain Scenarios module allows organizations to measure and improve the effectiveness of their security controls in defending against real-world Advanced Persistent Threats (APTs).

While other Cymulate Scenarios modules such as Email Gateway and Web Gateway assess specific security controls, the Full Kill-Chain Scenario module tests the effectiveness of multiple security controls within an infrastructure from pre-exploitation through exploitation to post-exploitation.

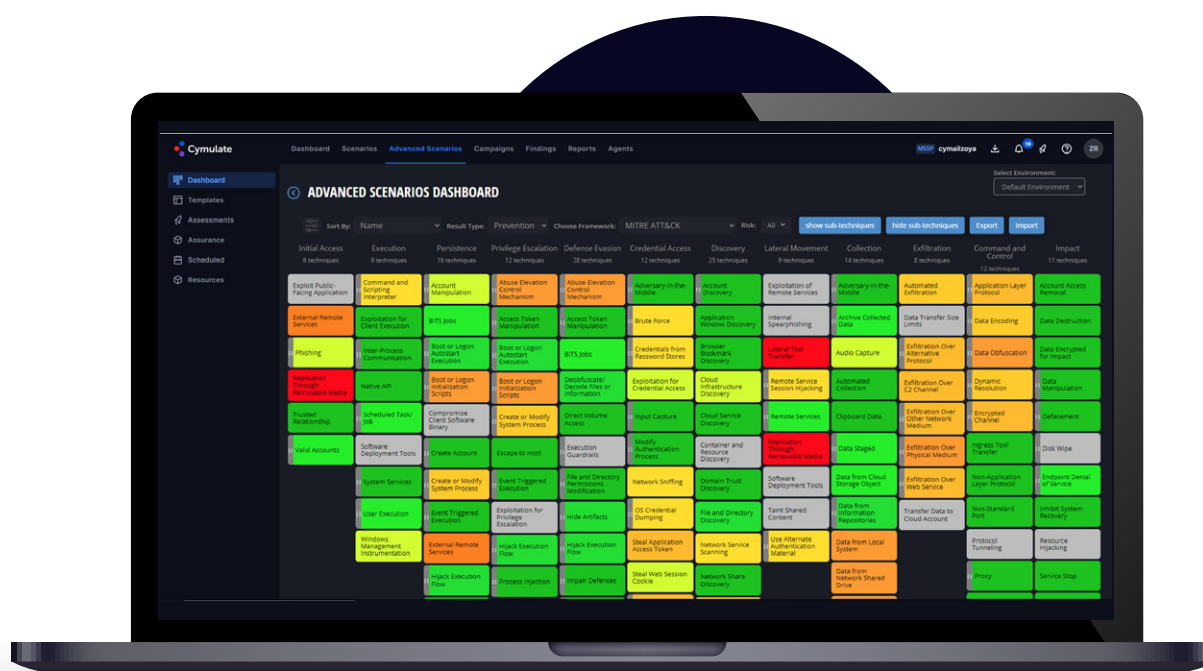
By simulating APTs that attempt to bypass security controls across the cyber kill-chain, an organization can challenge and evaluate the effectiveness of its current detection tools and take corrective measures to remediate any gaps.

From a blue team perspective, these automated off-the-shelf attack scenarios can be used continuously to provide detailed visibility and understanding of the security controls and how the changes made in their configuration, or with new deployments, affect the security posture.



Advanced Scenarios

The Cymulate Advanced Scenarios module enables an organization to create highly customized assessments to test, validate, and assure security solution protection and resilience to the Full Kill-Chain of an Advanced Persistent Threat (APT) or a subset of such tactics. Tactics and techniques are mapped to the MITRE ATT&CK framework and can be tested for both red teams and blue teams.



Assessments are based on templates, either Cymulate or user created, and are comprised of built-in or customized executions, payloads, programs, and tools. Advanced Scenarios assessments can perform chained and atomic executions of tactics and techniques used by threat actors worldwide. Assessments can be set up in two ways:

- **Atomic manner** - To validate security solution protection
- **Chained manner** (Real attack simulation) - To create and build real-world scenarios by chaining executions to help red teams and test blue teams

Advanced Scenarios assessments can be highly customized and allow users to create their own attacks via Cymulate and user supplied executions, files, and Sigma rules. Users can then simulate these attacks to test their detection and response solutions with specific test cases and customized attack scenarios.

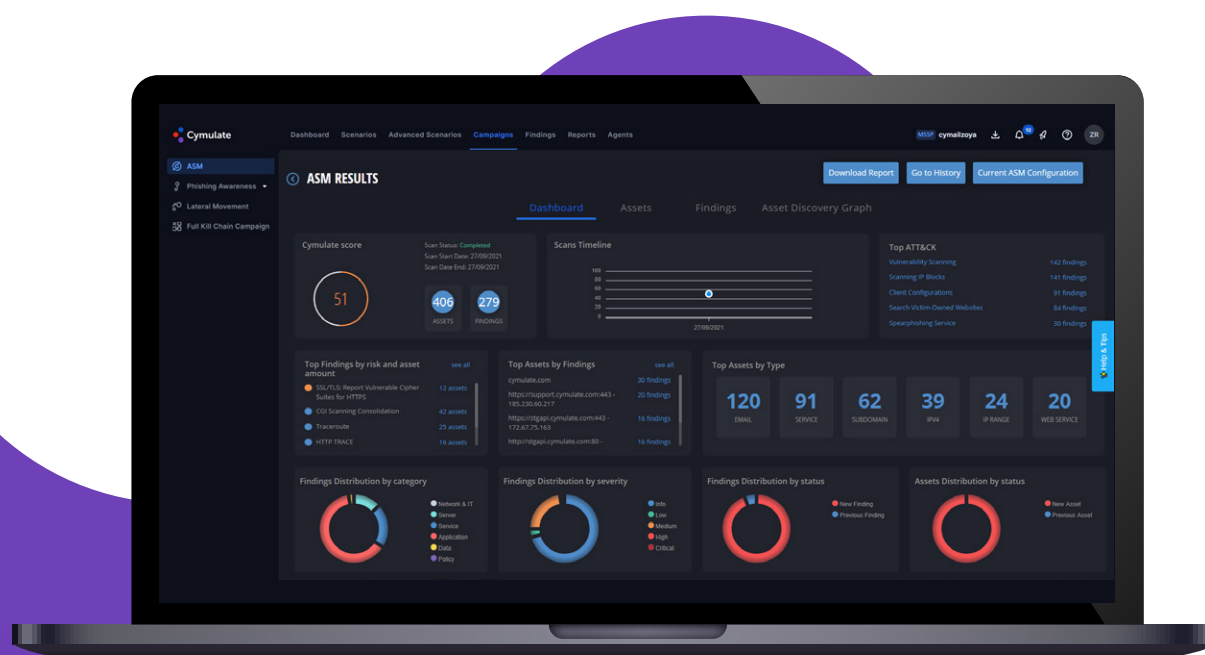
Campaigns

As opposed to the attack scenarios that validate the security controls efficacy, attack campaigns emulate the adversarial attempts of attackers from the outside-in. To facilitate the in-depth checking of the different stages of an attack, the types of campaigns are available in the following modules:





Attack Surface Management (ASM)

Cymulate's ASM (Attack Surface Management) Campaign module discovers which digital assets are exposed to adversaries that aim to access, exploit, and collect information during the reconnaissance phase of an attack. The module scans the domains, sub domains, IPs, ports, and more for internet facing vulnerabilities and Open-Source Intelligence (OSINT).

During the reconnaissance phase, an attacker performs a comprehensive analysis of the organization they are targeting. They scan multiple sources for intelligence they can later exploit including organizational, employee, and technical information that can be used in a social engineering attack or to gain illicit network access and initial foothold.



ASM Module Key Features

-  Continuous, automated checkups
-  Technical and informational findings
-  Mitigation and remediation plan
-  Actionable Insights



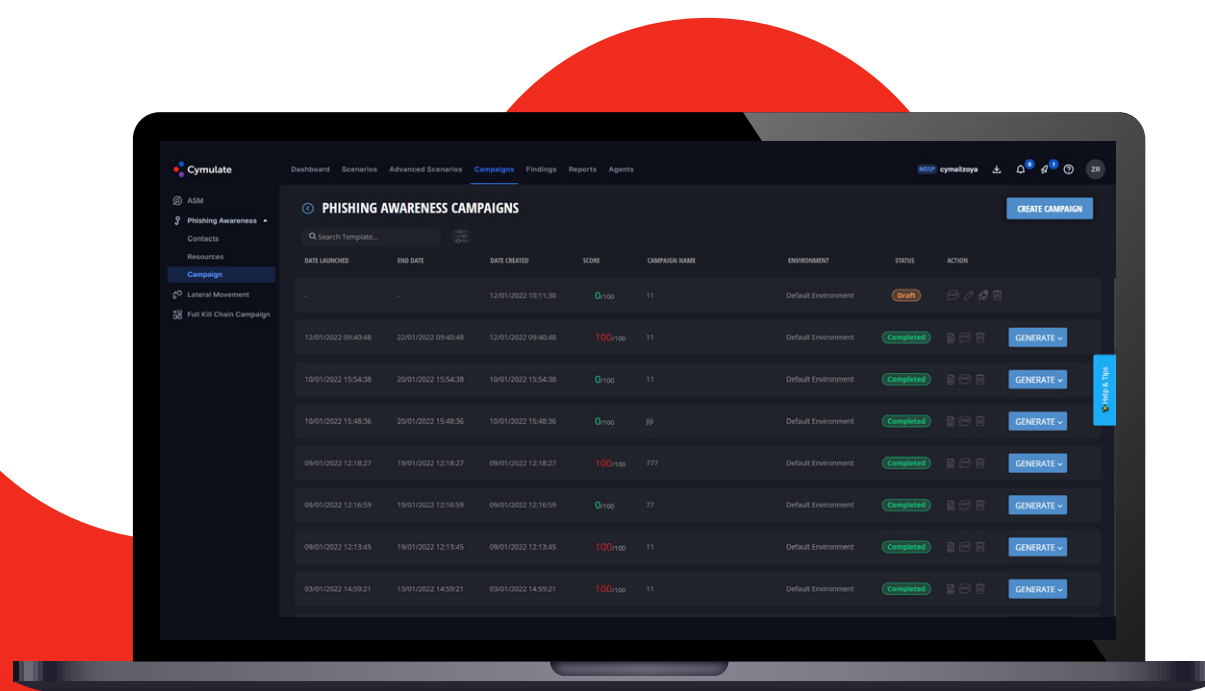
Phishing Awareness

Cymulate's Phishing Awareness Campaign module enables organizations to evaluate employee security awareness. It simulates phishing campaigns to easily detect which employees open the simulated malicious content that can place an organization at risk. The continuous feedback given from the simulated tests helps focus on employees that may require more education and monitoring than others.

Phishing attacks use social engineering to mimic trusted entities and increase the likelihood of the recipient to act, such as clicking on a malicious attachment or link and unwittingly entering sensitive information such as a password or bank account details.

A successful phishing attack enables the adversary to infiltrate and compromise corporate and production environments. That's why it is important to raise awareness among employees regarding cyber-attacks using social engineering methods since they are constantly evolving and becoming increasingly harder to detect.

Increasing employee awareness and vigilance will reduce cyber exposure and help prevent data breaches, minimize malware-related downtime, and avoid incident costs.





Lateral Movement

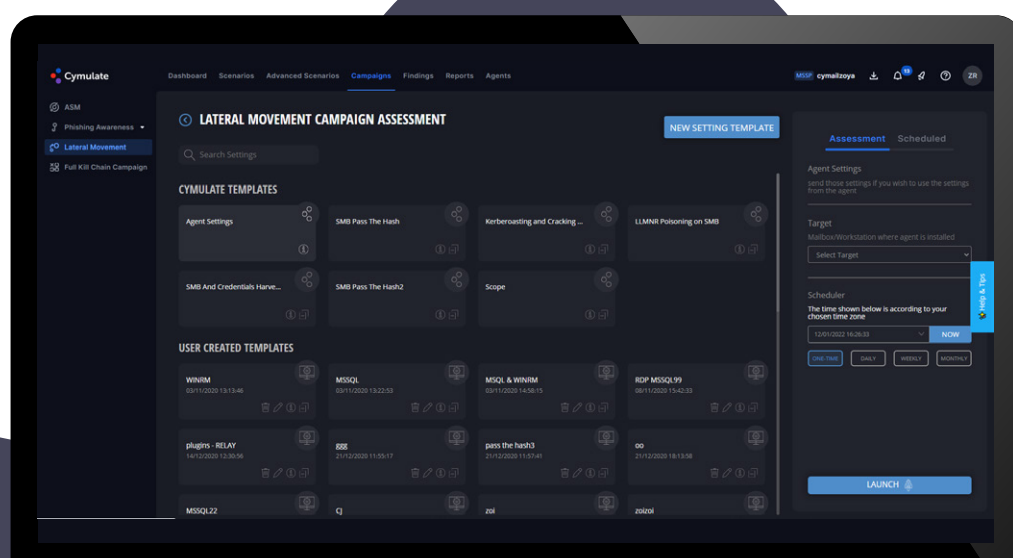
Cymulate's Lateral Movement campaign challenges internal network configuration and segmentation policies against different techniques and methods used by attackers to propagate within the network and control additional systems.

Once an adversary establishes an initial foothold within a network, their next step is lateral movement where they use various techniques to progress through the network to reach their objective.

As threat actors move deeper into the network, they become harder to detect. They use evasion techniques to cloak their presence and actions and escalate their privileges to impersonate authorized users to access high value assets.

Cymulate's 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 assessment 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.

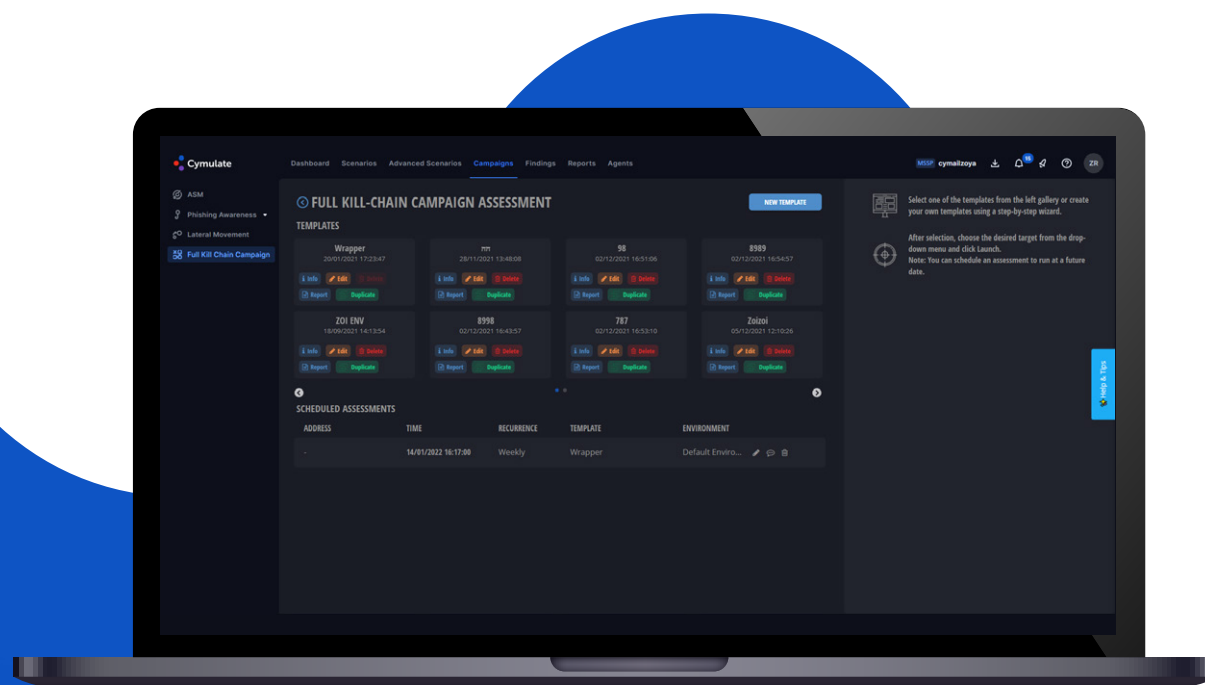




Full Kill-Chain Campaigns

Cymulate's Full Kill-Chain Campaigns module allows organizations to measure and improve the effectiveness of their security controls in defending against real-world Advanced Persistent Threats (APTs).

By simulating APTs that attempt to bypass security controls across the cyber kill-chain, organizations can challenge and evaluate the effectiveness of their current detection tools and take corrective measures to remediate any gaps.

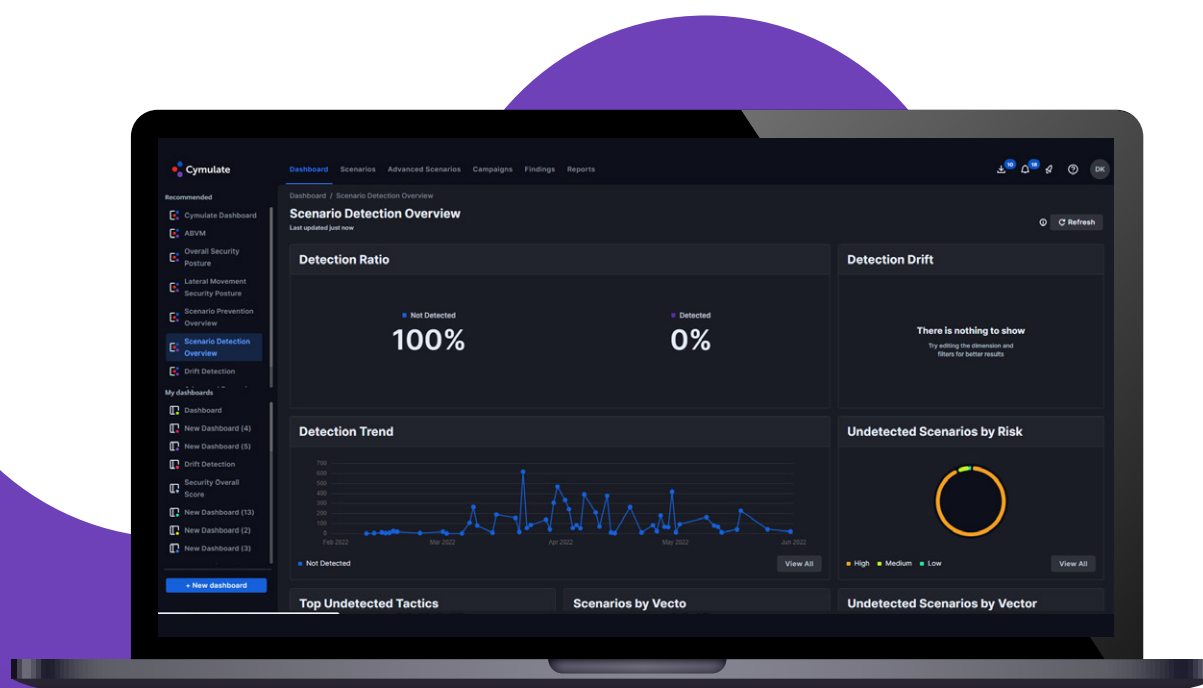


Analyzing Security Posture In-Depth





Cymulate's Dynamic Dashboards feature allows organizations to create dashboards that gather insights based on findings from across the platform according to the specific needs and goals of the organization.

Dashboards enable an organization to take full control of how it visualizes information by creating multiple, customized widgets. Widgets can be configured to display data according to the selected widget type, dimensions, and filters. Widgets are continuously updated with the latest assessment metrics so organizations can surface the most recent insights relevant to them.

Dynamic Dashboards



Key Benefits

-  Present findings to management in an easy-to-understand manner, without the need to present highly technical information
-  View specific data that is important to an organization, without any background noise
-  Create dashboards to do a deep dive into specific data and filter to a granular level
-  Display findings on a static and a timeline level for a useful reference

ABVM – Optimizing Vulnerability Patching Prioritization

One of the most common weaknesses in an organization's security posture is unpatched vulnerabilities. Many organizations know that the mix of legacy systems, old operating systems, open-source code, Mergers and Acquisitions, and uncontrolled partnerships with software providers leaves them vulnerable.

However, different vulnerabilities pose different risk levels and the impact they might have on an organization can vary. Patching methodologies based only on severity can lead to long and risky patching windows that are costly and unmanageable.

Instead of basing a patching plan on severity only, Cymulate's ABVM module enables organizations to prioritize patching by letting them know how likely a vulnerability can be exploited and accounts for the effectiveness of compensating security controls in an environment.

Cymulate's ABVM module integrates with various Vulnerability Management tools to provide organizations with the visibility and prioritization they need to create an action plan for risk reduction. Cymulate pulls data from the integrated Vulnerability Management (VM) tool and correlates known CVEs with the CVEs you are vulnerable to (based on the data from its VM tool). The results are displayed on the ABVM dashboard and offer a granular analysis of vulnerabilities found in the organization's system.

The ABVM dashboard helps organizations create a baseline action plan, by letting them know what is essential to patch first and what does not require immediate attention or resources. This will lead to a more robust cybersecurity posture and a better sense of control.

Key Benefits

- Simple integration with vulnerability management tools
- Granular analysis of vulnerabilities
- Baseline for action plan for remediation
- Reduction of patch management costs
- Recommendations for a shorter patching window
- Compliance Assurance

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](#)