cymulate

DATA SHEET

Cymulate Auto Mitigation

Go Beyond Validation to Mitigate Threat Exposure

Security teams know they are in a daily race to stay ahead of advanced cyber threats. Cymulate helps organizations move beyond identifying gaps to actively closing them. By combining continuous threat validation with automated control updates, Cymulate enables teams to strengthen detection and prevention before attackers exploit weaknesses.

The Cymulate Platform continuously tests security controls using real-world attack techniques mapped to MITRE ATT&CK. When exposures are identified, Cymulate Auto Mitigation deploys targeted updates to security controls, transforming validation into measurable resilience.

Through this closed-loop approach, Cymulate automates:

- Daily testing of new threats
- Updating security controls to block or detect validated threats
- Proving threat resilience and the current state of security posture

Close the Risk-to-Fix Gap with Auto Mitigation

With daily updates of the latest threats and a cyber defense engineering control plane, Cymulate closes the loop between validation and threat-informed defenses.

When validation identifies a security gap, Cymulate Auto Mitigation generates appropriate mitigation guidance, including vendor-specific behavioral detection rules and indicators of compromise (IoCs). Cymulate pushes these updates directly to connected security controls and re-validates the threat to confirm control effectiveness.

Cymulate also provides control over deployed mitigations directly from the platform. EDR detection rules and IoCs generated and pushed by Cymulate and managed directly from the Cymulate console. For supported controls, IoCs can be configured with expiration dates, enabling automatic removal after a defined period.

> **Cymulate integrates with our XDR to improve our threat detection and response. Cymulate automatically uploads critical threat data directly to our XDR to ensure that potential threats are identified and addressed quickly, without manual intervention."**
>
> – Senior Security Manager, Singapore Bank

Benefits

Accelerate mitigation

Reduce manual tasks with automation that converts exposure validation to immediate threat resilience.

Optimize prevention

Push threat updates directly to security controls to detect and prevent threats that have been proven to bypass security controls.

Reduce MTTR

Develop self-improving defenses that adapt and minimize mean time to remediation.

Save time

Eliminate manual workflows and free up SecOps resources for higher-value priorities.

How It Works

Cymulate continuously validates security controls by executing safe, real-world attack simulations across the environment. When a simulation identifies a security gap, such as a missed detection, misconfigured control or insufficient protection, Cymulate analyzes the results and determines the appropriate mitigation action.

1. Gap identification: Each simulation highlights where prevention or detection controls fail to block or detect attacker techniques aligned to MITRE ATT&CK.

2. Mitigation generation: Based on the identified exposure, Cymulate automatically generates the relevant mitigation.

- For control gaps that require updated threat intelligence, Cymulate extracts and prepares relevant IoCs, such as file hashes, IP addresses, domains or registry keys.
- When simulations reveal behavioral detection gaps at the endpoint, Cymulate generates vendor-specific detection rules formatted for EDR platforms. These rules are derived from the observed malicious behavior and mapped to the relevant attack techniques.

3. Automated deployment: Mitigation updates, whether IoCs or behavioral detection rules, are deployed directly to integrated security controls, eliminating the need for manual rule creation, translation and deployment.

4. Automated validation: After deployment, Cymulate automatically re-runs the relevant simulations to confirm that the mitigation effectively blocks or detects the attack. This closed-loop validation ensures that exposures are not only identified, but measurably reduced.

5. Optional prevention enforcement: Once detection rules are validated, security teams can confidently promote them from detection to prevention mode within their endpoint platform, further strengthening resilience.

Integrate with Security Controls to Harden Defenses

The Cymulate option for auto mitigation includes control integrations for:

Carbon Black. · CROWDSTRIKE · cybereason · FORTINET · Microsoft · SentinelOne

cisco SECURE · paloalto NETWORKS · SOPHOS · TREND MICRO · zscaler

Why Choose Cymulate?

Complete threat coverage

The most comprehensive threat library that enables validation across the full attack lifecycle – plus daily updates for the latest threats.

AI-powered environment and context mapping

Autonomous, AI-driven usability and workflows customize validation for your environment with intent-aware execution of what comes next.

Cyber defense engineering control plane

Closed-loop system that turns validation into continuous improvement across controls and threat detection.

About Cymulate

Cymulate is the leader in proactive, AI-powered security that continuously proves, prioritizes and adapts against real attacker behavior – before incidents occur. Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.