SentinelOne

cymulate

SOLUTION BRIEF

Self-Healing Endpoint Security

A Joint Solution from SentinelOne and Cymulate

Maintain and Prove Protection against Evolving Threats

Security teams know they are in a daily race to stay ahead of advanced cyber threats, and advanced endpoint security provides the best defense against today's cyber threats.

Modern endpoint security combines behavioral and signature-based prevention with detection and response to provide full coverage of MITRE ATT&CK tactics. For this reason, it's essential for security teams to maintain this protection by:

- Adapting to new threats
- Identifying security drift (configuration changes and infrastructure updates that reduce threat coverage)
- Tuning detection rules

Continuous Security Optimization

SentinelOne and Cymulate combine to deliver self-healing endpoint security. The SentinelOne Singularity Endpoint combines next-gen prevention with real-time detection and response in a single platform with a single agent, empowering security teams to easily identify and secure every user endpoint on their network.

The Cymulate Exposure Validation Platform integrates with SentinelOne Singularity Endpoint to continuously test and validate security effectiveness with actionable and automated mitigations that boost prevention and detection for any identified gap. With breach and attack simulation and automated red teaming, the Cymulate platform tests known executions, malicious file samples and malicious behaviors to fully challenge SentinelOne's controls and policies. Through this integration, Cymulate provides SentinelOne users with:

- Automated updates of indicators of compromise (IoCs) for immediate prevention
- New custom detection rules formatted specifically for Singularity Endpoint
- Drift detection that identifies decreases in threat coverage
- Executive, technical and compliance reports backed by proof and evidence of security effectiveness
- MITRE ATT&CK heat maps that highlight the value of Singularity Endpoint and its coverage of tactics, techniques and sub techniques

Production-Safe, Automated Security Validation

The Cymulate platform includes SaaS-based threat emulation and a light-weight test point deployed on a sample endpoint. With coordination between SaaS and the test point, Cymulate validates the prevention and blocking of IoCs, vulnerability exploits and TTPs (tactics techniques and procedures). By integrating with the SentinelOne API, Cymulate validates threat detection by confirming both the alerts of attacks, and logging of the attacker's actions.

Solution Benefits

Optimize Prevention

Automate threat updates to block the latest threats in SentinelOne.

Optimize Detection

Configure, test and tune SentinelOne detection rules to optimize threat coverage.

Identify Drift

Detect changes to SentinelOne threat coverage from configuration or infrastructure updates.

Continuous Validation

Automate continuous testing to proves security effectiveness.

Optimize Threat Prevention

With a daily update of the latest threats, Cymulate continuously tests and proves the effectiveness of Singularity Endpoint to block advanced cyber attacks. To maintain and optimize threat prevention, Cymulate includes automated mitigation that pushes new IoCs directly to SentinelOne for immediate threat prevention. For speed and ease of use, Cymulate aggregates the recommended IoC updates and allows security teams to push the new IoCs in a single update. Alternatively, Cymulate provides security teams with the workflows to analyze every attack scenario and push the appropriate update.

Optimize Threat Detection and Response

For cyber attacks that require detection, Cymulate validates Singularity Endpoint to log and alert advanced TTPs. To maintain and optimize threat detection, Cymulate provides custom detection rules that can be directly applied via the SentinelOne management console or API.

More advanced cyber teams use Cymulate to build and test their own custom detection rules. Cymulate converts these detection rules into individual or chained attack scenarios that safely execute against Singularity Endpoint. Through its API integrations with SentinelOne, Cymulate validates the alerting of the rule and logging of all relevant threat actions.

Baseline Security Posture and Identify Security Drift

By continuously validating Singularity Endpoint against new threats, exploits and the latest techniques, Cymulate provides security teams and leaders with evidence-based metrics for threat prevention and detection with trending and baselining of those results over time. Dashboards and reports make this trending data easily accessible for security leaders to present in executive meetings, create board reports and share with auditors.

Because updates to control configurations and changes in IT infrastructure can impact security posture, security teams rely on Cymulate to identify security drift. With continuous validation and correlation of previous results, Cymulate highlights any decreases in threat coverage while providing the mitigation path in the form of new IoCs or detection rules.

Why choose Cymulate for validating and optimizing SentinelOne?

Automated Validation

More than 500 endpoint test scenarios using thousands of known malicious file samples and behaviors to simulate real-world attacks.

Production Safe

The full suite of test cases is completely production-safe and will not harm endpoint environments.

Adapt to New Threats

Actionable and automated findings to maximize threat prevention and optimize detection for the most effective threat coverage.

About Cymulate

Cymulate is the leader in exposure management and security validation. More than 1,000 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.

Get a Demo