cymulate

DATA SHEET

Breach and Attack Simulation (BAS)

Are Our Cyber Defenses Secure?

Organizations invest significant time and money into their security defenses, but how do you know if your security controls and operational response can stop the latest sophisticated cyber attack?

The worst time to find weaknesses in your security defenses is during a cyber incident. By moving from a defensive position and adopting an offensive mindset, you can routinely test and validate that your security controls can prevent and detect the latest emergent threats.

Don't Speculate. Simulate.

When it comes to answering the above questions with conviction, don't speculate, simulate. Cymulate uses breach and attack simulation technology to create real-world attack scenarios that are executed in a production-safe mode to test and validate your security controls against the latest emergent threats and threat actors.

The attack scenario workbench provides a quick and easy way to create fully automated assessments from a rich library of attack scenarios. Security teams can use the workbench to compose attack simulations by selecting from the list of security controls, threats, platforms and operating systems that matter to them the most.

Validate Security Controls:

- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Web App Firewalls (WAF)
- Endpoint Security (AV / EDR)
- Network Security (IPS/IDS)
- Data Loss Prevention (DLP)
- Cloud Security (CWPP)
- Kubernetes/Containers (K8S)
- SIEM and SOAR

Validate Threats:

- APT Groups
- Vulnerabilities (CVEs)
- ATT&CK Tactics & Techniques
- Ransomware Threats
- Malware, Worms and Trojans
- Production Platforms
- Malware Families
- Daily Threat Feeds

Assessments can be saved as templates and launched on a regular schedule to monitor security posture and measure any drift away from a preset baseline. Security teams can also create smart templates which are automatically updated with the latest attack scenarios that match the template criteria when the assessment is launched.

Cymulate provides best-practice templates and pre-built assessments that use a wide range of attack types and methods to validate your individual security controls and cloud platforms using full kill-chain attacks and malicious behaviors used by well-known threat actor APT groups.

Cymulate BAS Benefits

Execute real-world attacks

Simulate the threats that concern you the most using a rich library of attack scenarios and malicious actions.

Identify security gaps

Find gaps and weaknesses in your security defenses that could result in a cyber breach.

Harden security defenses

Fine-tune your security controls with mitigation guidance, detection rules and automated IOC updates.

Reduce exposure risk

Continuously measure and improve your security posture to reduce the risk of a breach.

Gartner Peer Insights Customers' Choice 2024 ™

Control Optimization Made Easy with Automation and AI

The Cymulate Exposure Validation Platform applies breach and attack simulation to validate and optimize security controls with advanced testing and easy, repeatable automation in the industry's most deployed solution for exposure validation that includes:

- **Dashboards and executive reports –** Gain security posture insights and monitor for drift using risk scores, trends, prevention / detection ratios, top attack types and APT groups not prevented by your security controls.
- **Assessment templates –** Create your own assessment templates that validate your security posture and controls including dynamic **smart templates** that automatically include new attack scenarios at launch.
- **Best practice assessments –** Automated testing and validation of key security controls and threat scenarios using our best practice assessments and pre-built templates.
- **Attack scenario workbench –** Flexible workflows to build custom chained assessments from a rich library of the latest attack scenarios and malicious behaviors – or create your own attack actions and scenarios.
- **Daily threat feeds –** Validate controls against the latest threats and active campaigns with a daily update from the Cymulate Threat Research Team and optional auto-run capability to test immediately or at a user-defined time.
- **Integrations and connectors –** Integrate technologies from leading security vendors to optimize your investments in SIEM, SOAR, GRC, EDR, firewall and more via APIs to validate and improve detection and response capabilities.
- **AI-powered attack planner –** Privacy-focused artificial intelligence converts threat intel and plain language prompts into custom threat assessments and complex attack chains.
- **Automated control updates –** Integrate security controls and push new indicators of compromise (IOCs) to mitigate control gaps identified by the latest assessments.
- **Mitigation guidance and detection rules –** Remediation insights provide straightforward guidance to mitigate threats, fine tune controls and refine policies for better protection.
- **Full MITRE ATT&CK coverage –** Reports and findings are mapped to the MITRE ATT&CK® framework with heatmaps showing areas of strengths and weaknesses across the full range of MITRE tactics and techniques.
- **Extensible to Cloud, Windows, Mac and Linux –** Extensive attack simulation and immediate threat testing across on-premises, cloud (AWS, Azure, Google Cloud) and hybrid environments and operating systems (Windows, Mac, Linux).

Why Choose Cymulate?

Depth of attack scenarios

Out-of-the box templates and a library of more than 120,000 attack simulation resources from real-world attack scenarios for comprehensive testing of your security defenses.

Production-safe execution

The full suite of test cases is completely production-safe with no malicious payload or code execution that could impact your production environment.

Fully automated testing

The assessment is fully automated, enabling continuous validation and performance optimization of your web application firewall effectiveness every week.

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 1,000 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation. For more information, visit www.cymulate.com.