cymulate

SOLUTION BRIEF

Cloud Security Validation

Adversaries Exploit Cloud Platforms

Attackers increasingly target cloud platforms running business-critical applications and workloads. With containers lacking properly configured security protections and cloud environments using insecure default settings, cloud data breaches are at an all-time high.

Continuous Validation of Cloud Security Controls

To combat the increase in cloud attacks, security leaders need to test the efficacy of different security controls across the layers of their cloud architecture.

Cymulate provides both pre- and post-exploitation simulation assessments to test and validate security controls and policies for the different layers of a cloud architecture, including:

- **Applications**
- **Containers and Kubernetes**
- **Cloud Workloads**
- **Cloud Infrastructure**

Cymulate Exposure Validation applies industry-leading breach and attack simulation and automated red teaming to rigorously test the effectiveness of the security controls protecting each layer of the cloud architecture. The attack assessments evaluate the ability of cloud security controls to prevent and detect a wide range of cyber threats by using threat intelligence, red teaming, penetration testing and the MITRE ATT&CK framework.

Complete Exposure Validation for Cloud

With a library of cloud-focused attack techniques, Cymulate automates the execution of malicious and sensitive privileged activities in your cloud environment to determine if they are prevented and detected by your runtime security controls.

The assessments are fully automated, production-safe (not harmful to your cloud platforms) with options to schedule ongoing continuous validation and to measure performance and drift over time. Cymulate automates the security testing of leading cloud providers (Azure, AWS, Google Cloud) and their native cloud security tools including Microsoft Defender for Cloud, AWS GuardDuty and Google Cloud Security Command Center.

This comprehensive approach identifies areas for improvement and builds threat resilience to potential cloud-based attacks.

Solution Benefits

Continuous security validation

Automate continuous testing and validation of your cloud security runtime controls.

Identify gaps and weaknesses

Prove the exposures in your cloud controls and policies that could lead to a cloud data breach.

Optimize security controls

Configure and tune your cloud runtime environment with mitigation guidance to improve resilience.

Reduce threat exposure risk

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

Testing Layers of a Cloud Architecture

Cymulate automates exposure validation with the most complete library of cloud-based attack scenarios to validate cloud security across the architecture layers, security technologies and the controls to secure the cloud environment.

<table>
<tr><th>Cloud Layer</th><th>Security Control</th><th colspan="3">Tested Layer</th><th>Cymulate Simulations</th></tr>
<tr><td>Application Security Control</td><td>WAF</td><td>Business Application
App Binaries & Libraries</td><td>Business Application
App Binaries & Libraries</td><td>Business Application
App Binaries & Libraries</td><td>OWASP</td></tr>
<tr><td>Container & Kubernetes Security Controls</td><td>CWPP, CNAPP, SIEM, FW/IPS</td><td colspan="3">Container Engine / Kubernetes</td><td>K8: Azure, AWS, GCP, On-Premise</td></tr>
<tr><td>Cloud Workloads Security Controls</td><td>EDR, SWG, SEG, SIEM, DLP, FW/IPS</td><td colspan="3">Virtual Machines / Operating Systems / Container Host</td><td>MITRE ATT&CK</td></tr>
<tr><td>Cloud Infrastructure Security Controls</td><td>CNAPP, CSPM, SIEM</td><td colspan="3">Infrastructure</td><td>SIEM Detection (Assume Breach)</td></tr>
</table>

Application Security Control

Simulate OWASP threat models, web-based attacks and command injections to validate web application firewall protection for web applications running on cloud platforms.

Container & Kubernetes Security Controls

Test the effectiveness of container runtime security in a Kubernetes environment across the MITRE ATT&CK framework using malicious behaviors and privileged activities, such as container escaping, secrets listing and other persistent and evasive techniques.

Cloud Workloads Security Controls

Test the security of cloud workload runtime protection for AWS EC2 instances, Azure Virtual Machines, and Google Cloud compute instances. Execute common cloud attack scenarios like crypto mining, data exfiltration, endpoint threats and other malicious behaviors.

Cloud Infrastructure Security Controls

Using an “assume breach” post-exploitation approach, simulate an attacker executing high-privilege activities to validate detections within the SIEM platform and create new rules to enhance detection.

Why choose Cymulate?

Depth of attack simulations

More than 200 templates for cloud techniques, Kubernetes security and SIEM detections of malicious cloud behaviors.

Production safe

The full suite of test cases is completely production-safe and will not harm your cloud environment.

Automated validation

Offensive made testing for cloud made easy with automation and integration with cloud security controls.

About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to validate, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. For more information, visit www.cymulate.com.

Get a Demo