cymulate

SOLUTION BRIEF

Cloud Security Validation

Adversaries Exploit Cloud Platforms

Adversaries are increasingly targeting cloud platforms running business-critical applications and workloads. With containers lacking properly configured security protections and cloud environments using insecure default settings, threat actors are taking advantage with an increase in cloud data breaches.

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:

- **Cloud Hosted Applications**
- **Cloud Containers and Kubernetes**
- **Cloud Workloads**
- **Cloud Infrastructure & Services**

Cymulate breach and attack simulations for cloud, rigorously test the effectiveness of the security controls protecting each layer of the cloud architecture. The simulation assessments evaluate the ability of cloud security controls to prevent and detect a wide range of cyber threats by utilizing threat intelligence, red teaming, penetration testing, and the MITRE ATT&CK framework.

The Cymulate platform automates the execution of a range of malicious and sensitive privileged activities in your cloud environment to determine if they are prevented and detected by your cloud runtime security controls.

The assessments are fully automated, production-safe (not harmful to your cloud platforms) and can be run weekly for continuous validation and to measure performance and drift over time.

Cymulate automates the security testing of leading cloud providers (Azure, AWS, GCP) and their native cloud security tools including Azure Defender for Cloud, AWS GuardDuty, and Google Cloud Security Command Center.

This comprehensive approach identifies areas for improvement and ensures ongoing readiness to face potential cloud-based threats.

Solution Benefits

Continuous validation

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

Identify gaps and weaknesses

Find the gaps and weaknesses in your cloud controls and policies that could lead to a cloud data breach.

Optimize security controls

Configure and tune your cloud runtime controls with mitigation guidance to prevent and detect high privileged threat activity in your cloud containers.

Reduce 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 Breach and Attack Simulations rigorously test the effectiveness of security controls used to protect different layers of your cloud architecture. Each layer uses different controls to secure the cloud environment.

<table>
<tr><th>Cloud Layer</th><th>Security Controls</th><th colspan="3">Tested Layer</th><th>Cymulate Simulations</th></tr>
<tr><td>Cloud Hosted Applications</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>WAF: OWASP</td></tr>
<tr><td>Cloud Containers & Kubernetes</td><td>CNAPP, CWPP, SIEM, FW/IPS</td><td colspan="3">Container Engine / Kubernetes</td><td>K8S: Kubernetes, Azure, AWS, GCP, On-Premise</td></tr>
<tr><td>Cloud Workloads</td><td>EDR, SWG, SEG, DLP, SIEM, FW/IPS</td><td colspan="3">Virtual Machines / Operating Systems / Container Host</td><td>CWPP: Runtime Protection
EDR: VMs, DLP: Data Loss</td></tr>
<tr><td>Cloud Infrastructure & Services</td><td>CNAPP, CSPM, SIEM</td><td colspan="3">Infrastructure and Services
Azure / AWS / GCP / On-Prem</td><td>CDR: Cloud Detections</td></tr>
</table>

Cloud Hosted Applications

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

Cloud Containers and Kubernetes

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

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

Cloud Infrastructure & Services

Using an “assume breach” post-exploitation approach, simulate an attacker executing high-privilege activities to validate detections within your SIEM platform.

Why choose Cymulate?

Depth of attack simulations

Leverage nearly 8,000 attack scenarios to simulate high-privilege actions with an “assume breach” mindset to test and validate cloud security controls and policies.

Production safe

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

Automated validation

The assessment is fully automated, enabling continuous validation and performance optimization of your cloud security control effectiveness.

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 500 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.

Get a Demo