Cymulate

Cloud Security Validation

Organizations that migrate their on-premise assets to the cloud, or those that begin developing new applications in the cloud, are faced with additional security requirements. A common practice is to combine already in-use security tools along with new cloud-specific tools, like CSPM or CIEM, that focus on misconfigurations or access management. However, this stack of cloud security tools needs to be carefully configured as well as continuously validated and optimized to prevent exposure.

Key considerations in security validation for cloud environments

- Cloud-specific security control validation
- Incident response (IR) playbooks & tabletop exercises
- SIEM & SOAR validation for events & alerts in the cloud
- Effective network segmentation for both virtual & on-prem networks

Comprehensive Cloud Security Validation

Cymulate's Extended Security Posture Management (XSPM) validates cloud security with a proactive and comprehensive approach. Simulated attacks enable companies to simultaneously assess their on-premise and cloud environments using the tactics and techniques of an adversary to uncover critical security gaps and misconfigurations. Following each assessment, easy-to-digest mitigation guidance enables teams to focus their remediation efforts.

A Complementary Approach

Cymulate provides organizations with visibility into their security controls, as well as insights into how they can be breached by malicious actors. With this in-depth assessment, companies gain an extensive overview of their security posture.

Security Control Validation

Security teams orchestrate continuous simulated attack scenarios that test the efficacy of their cloud-native or cloud-hosted security controls, such as web gateway, web application firewall (WAF), endpoint security (EDR), and data loss prevention (DLP). These assessments are available out-of-the-box or can be customized according to an organization's specific needs. Cymulate's Research Lab updates the platform daily with Immediate Threat Intelligence so that organizations can rapidly assess their resilience against the latest threats.

Organizations who employ an EDR in the cloud and/or a virtual firewall, use Cymulate to validate that it blocks malicious traffic and activity as expected.

Breach Feasibility Assessment

External Attack Surface Management

The External Attack Surface Management (EASM) module enables organizations to automatically discover externally accessible, internet-facing assets, including web applications, servers, cloud services and infrastructure connected to the internet, and even organizational and credential intelligence that a hacker can use in an attack. The EASM module performs continuous and quantitative technical analysis to look for vulnerabilities and exploitable misconfigurations in the assets it discovers, and then prioritizes them based on risk.

Many cloud workloads are public-facing, and this type of discovery provides organizations an understanding of where a malicious actor is likely to begin when attempting to attack a cloud environment.

Lateral Movement

The cloud introduces an exponential increase in interconnected virtual networks that are also connected to on-premise networks, creating a much larger attack surface. The Lateral Movement module assess what happens after an attacker gains an initial foothold so that security teams evaluate the attacker's ability to move from one workload to another, or to other networks—from the cloud or on-premise.

As many organizations keep their crown jewels on-premise, a hacker will try to move from a cloud network to the on-premise network via site-to-site VPNs and direct connectivity services.

The Lateral Movement module attempts to emulate this behavior to provide visibility into a hacker's potential attack path across the network so a company can add controls to block the movement.

Cymulate

Why Cymulate?

Migrating to the cloud provides organizations the opportunity for rapid development and release, but it also increases the risk of an expanded attack surface that hackers may try to exploit. To maintain both speed and security, blue and red cyber teams need to understand the paths an adversary can take and ensure their controls will block them. Cymulate enables organizations to continuously validate and optimize their cybersecurity program, both on-premise and in the cloud.

With Cymulate, organizations can:

Ensure security controls are blocking malicious behavior

Stay on top of the latest threats with threat intelligence

Emulate attacker behavior to discover an organization's footprint

Determine potential paths for an attacker to gain an initial foothold

Validate network segmentation both in the cloud and on-premise

Detect security drift with continuous, scheduled automated assessments

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness. **Measuring your cybersecurity performance is fundamental towards creating a more secure organization!**

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com