SOLUTION BRIEF

Cymulate

Cloud Detection Engineering

Challenge

Today, nearly every company uses cloud computing. However, insufficient cloud expertise, lack of visibility in the cloud, and multi-cloud and dynamic workloads make it difficult to fully secure cloud environments. Studies show that more than one-third of organizations experienced a data breach in their cloud (IBM, Cost of a Data Breach Report, 2023).

While breach prevention is an important strategy, organizations need to shift gears and adopt an assumed breach mindset when it comes to protecting the cloud. Assuming breach enables security teams to build up their cloud defenses with detection engineering to identify attacks accurately and contain threats before they can spread.

Adopt an Assume Breached Mindset

Cymulate enables organizations to implement a cloud detection engineering approach by providing advanced detection assessments to validate detection rate and response. The faster an organization can detect a threat, the quicker it can contain it, minimizing the damage and protecting the organization's reputation. This focus on detection is only possible with visibility and analysis most frequently provided with log collection and Security Incident and Event Management (SIEM). The challenge is to make sure you have the right logs and the SIEM analysis provides meaningful alerts.

Cymulate tests the effectiveness of a SIEM setup by simulating high-privileged activities that a cyber attacker would typically execute on various cloud environments during a breach. This detection engineering exercise aims to gauge which activities trigger SIEM events and whether those events correctly lead to alerts.

How it Works

Assess the Detection Rate with Assume Breach Simulations for the Cloud

Cymulate provides an open framework for streamlined simulations of high-privileged activities within various cloud environments, enabling you to effortlessly monitor their detection via your SIEM system, all within one unified platform. In addition to providing out-of-the-box assume breach simulations for testing AWS, Google Cloud, and Azure, the solution provides a repository of executions for fully customizable assessments.

Benefits

Validate Log Collection

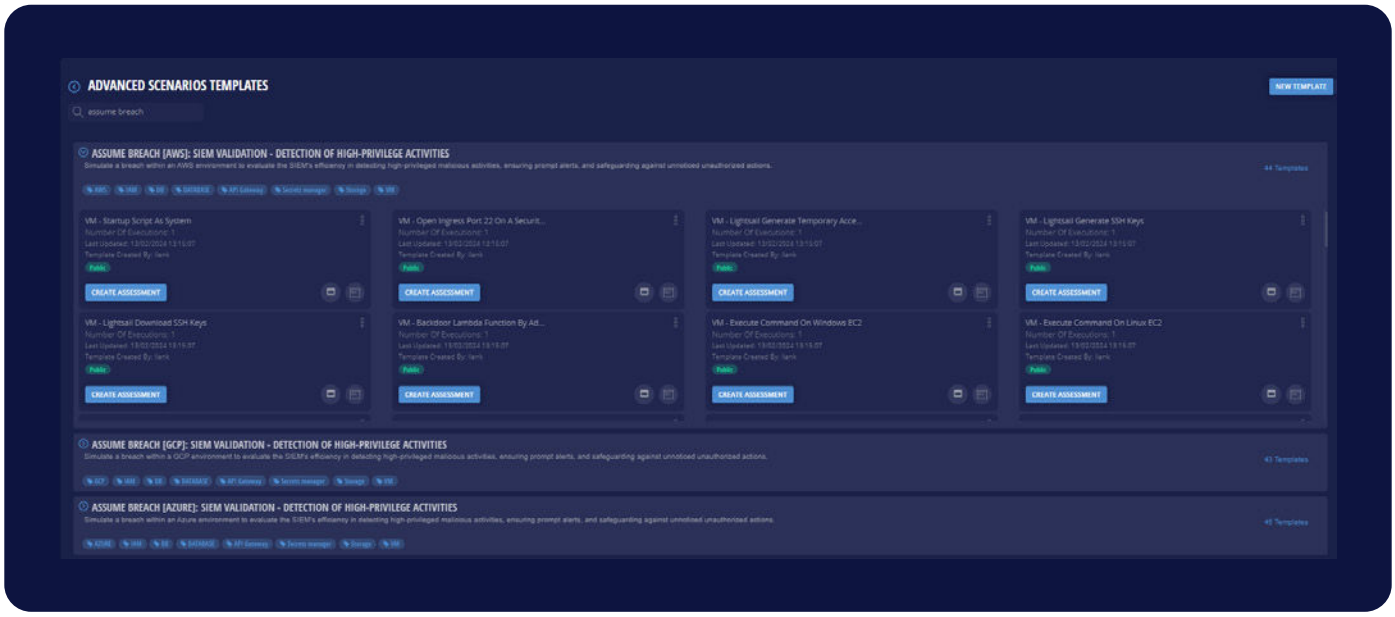
Test and validate that cloud platforms generate the right logs and the SIEM receives them.

Validate SIEM Detection

Assess and validate SIEM detection rules for attack tactics and techniques across the kill-chain with a special focus on the actions of privileged users and privilege escalation.

Tune Alerting

Optimize SIEM analysis and rules for meaningful alerts and audit trails that provide essential information to security analysts.

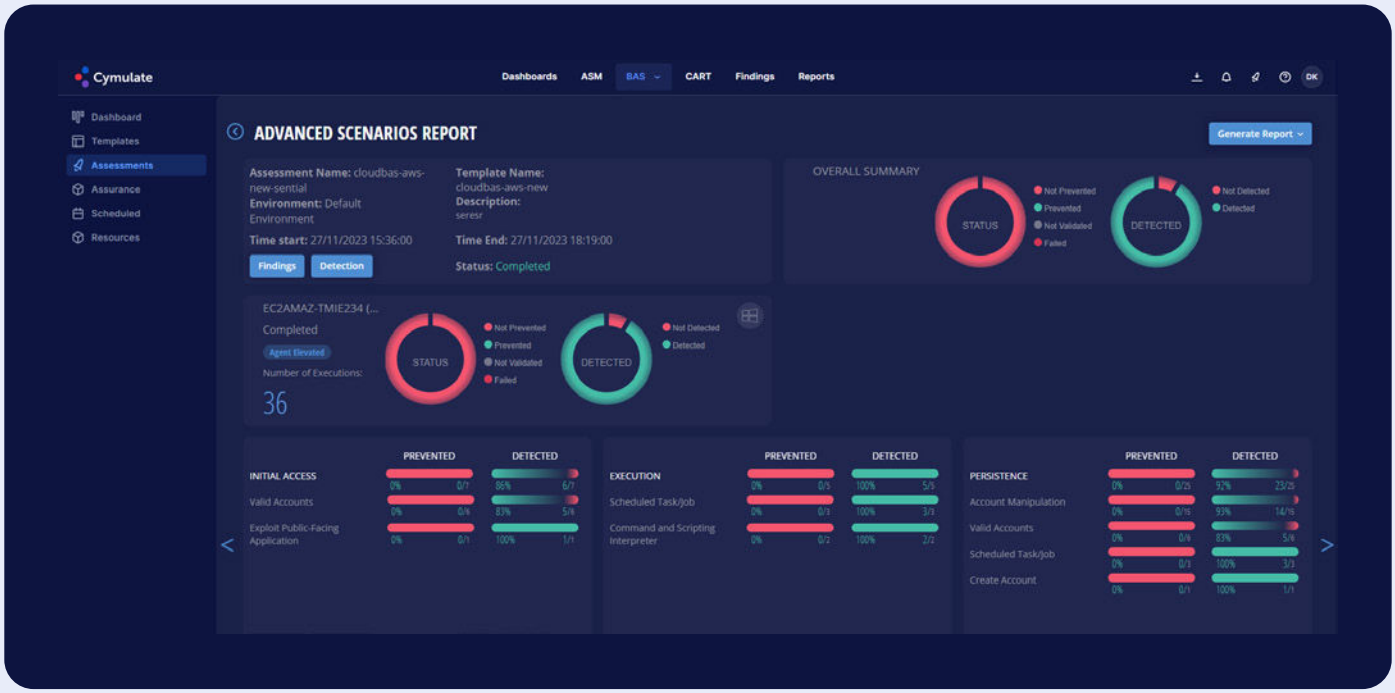


The Cymulate assume breach in the cloud templates are specifically designed to simulate high-privileged activities in various cloud environments.

Analyze Assessment Results, Generate Insights, and Fine-Tune Detection

The Cymulate assessment report provides an overall summary of detection results to assess the SIEM's performance. The report dashboard analyzes the findings and whether the execution was detected.

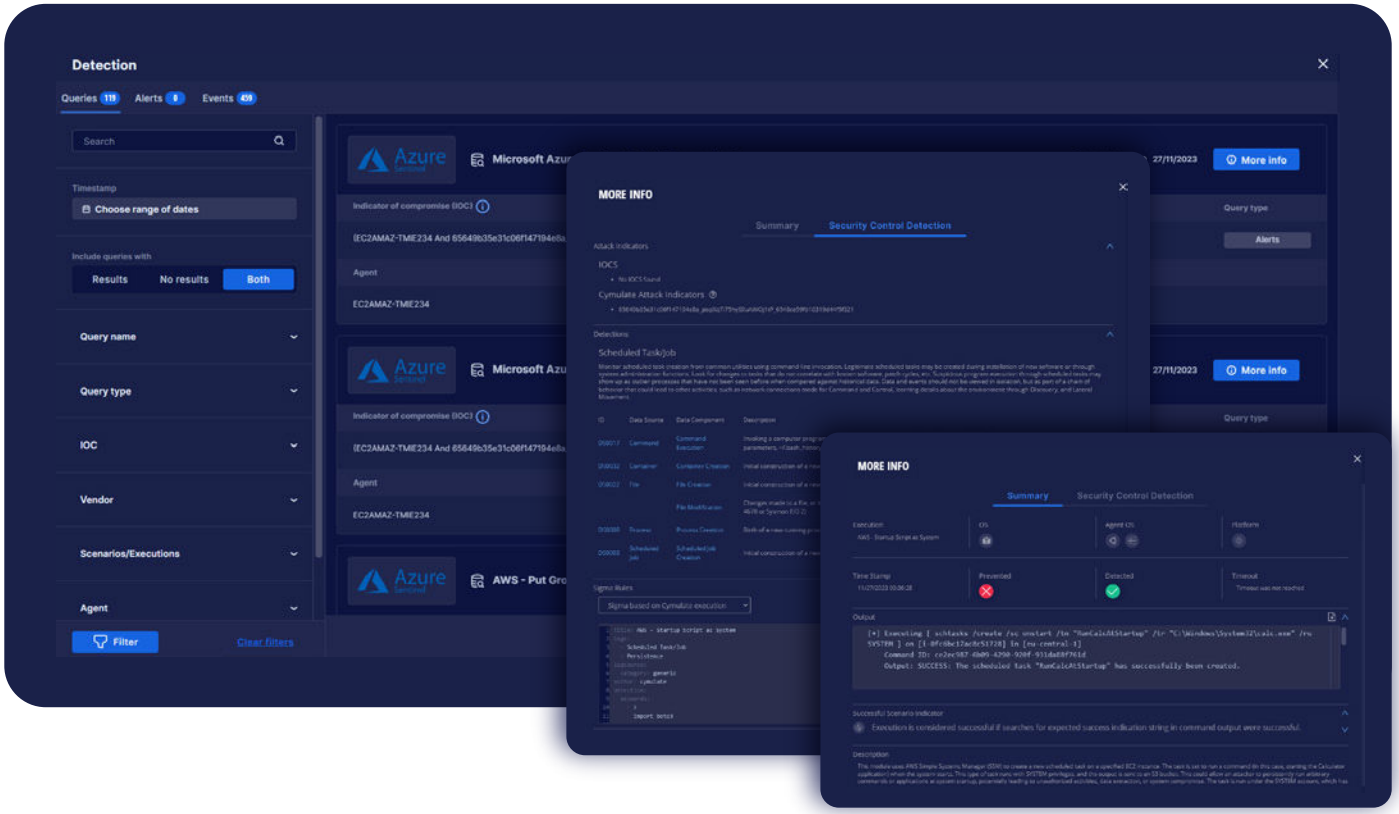
To determine the detection rate, Cymulate dashboards and reports include assessment details that include specific queries, threats detected, and events logged for both the assessment as a whole and for each corresponding MITRE ATT&CK tactic and technique.



The Cymulate report summarizes each assessment with metrics for threats and techniques detected mapped to MITRE ATT&CK.

Drilling down further, the assessment results also include a summary that provides easy-to-digest mitigation guidance. The security control detection tab includes information on attack indicators and Sigma rules, so users can refine queries and rules to improve SIEM detection before rerunning an assessment.

This capability is key for cloud detection engineering because it enables teams to continuously run assessments and validate whether the SIEM is accurately and fully detecting the relevant threats on the cloud and properly alerting SOC analysts. For every assessment, Cymulate provides Indicator of Compromise (IoC), Indicators of Behavior, Sigma Rules, and translation of the Sigma rules to vendor specific systems to help build new rules and fine tune existing rules to render accurate detection.



The detection results dashboard presents the queries and responses from integrated security tools, as well as mitigation guidance to improve SIEM detection.

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 of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.

Contact us for a live demo

Start Your Live Demo

info@cymulate.com | www.cymulate.com