DATA SHEET

Cymulate

Cymulate Breach and Attack Simulation: Advanced Scenarios

Automated Testing for Blue and Red Teams

Cymulate Breach and Attack Simulation (BAS) Advanced Scenarios provides an open framework for customizing chained cybersecurity assessments and automating testing.

To meet the needs of specific applications, environments, and infrastructure testing, Cymulate BAS Advanced Scenarios provides red teams with thousands of out-of-the-box resources and templates. An integrated template editor allows red teams to modify built-in resources or create new assets from executions to entire testing protocols. With coverage for Windows, MacOS, Linux, cloud infrastructure, Kubernetes, and more, Cymulate BAS Advanced Scenarios applies the latest threat intel and primary research from the Cymulate Threat Research Group with updates on emerging threats and new simulations.

On-demand and scheduling systems allow for both ad hoc checks and automated testing, so blue teams can independently run customized assessments to validate security controls against emergent threat activity, confirm remediation, or prepare for audits and penetration tests.

How it Works

Cymulate BAS Advanced Scenarios is a SaaS-based solution that uses a single lightweight agent per environment to run automated assessments of on-prem, cloud, or hybrid environments.

Cymulate BAS Advanced Scenarios operates on the concept of resources and templates, which serve as the foundation for assessments.

- Resources include executions (commands, scripts, or other action objects) and files (binaries, zip files, and other objects that executions can use).
- Templates are one or more resources linked together to form scenarios simulating different forms of attack.
- Each template can be as simple as a single execution or as complex as a series of chained scenarios tailored to meet an organization's specific assessment requirements and its data systems, applications, and infrastructure.

Advanced Scenarios Benefits

Realistic Testing

Offensive chained attack simulations based on threat actor tactics and techniques

Extensive Customization

Thousands of modifiable built-in resources and templates and the ability to build new assessments with custom executions, files, and Sigma rules

Automated Assessments

Scheduled and automated testing for blue teams to independently repeat assessments, validate mitigations, and identify drift without distracting red teamers from their own assignments

Cyber Framework Mapping

Simulated real-world behavior of malware and APT groups mapped to the MITRE ATT&CK and NIST 800-53 frameworks

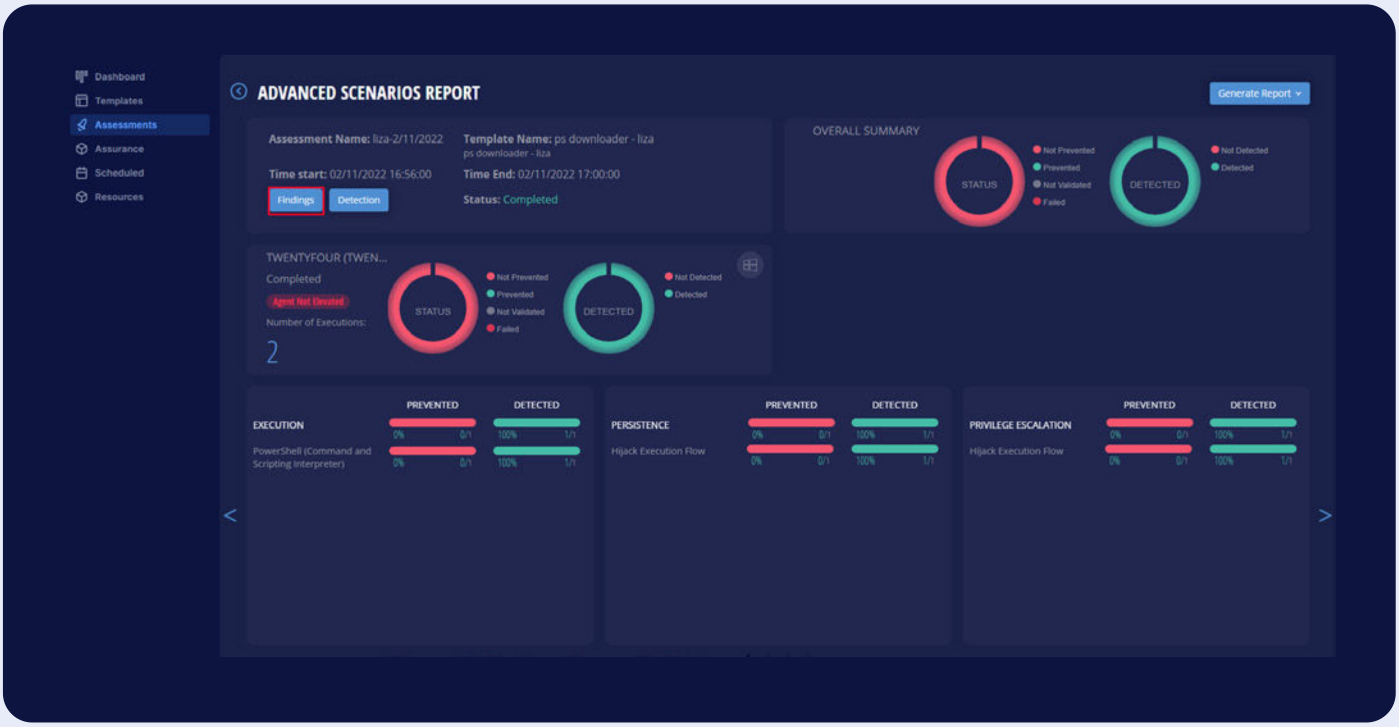
Cymulate BAS Advanced Scenarios Template Examples

- APT and TA Group Assessments
- LOLBins Assessments
- Web Application Simulation
- Cloud Security Validation
- Network Traffic Validation
- Windows, MacOS, and Linux Assessments
- Identity and Access Management Validation
- On-premise Assessments
- Industry Focused Assessments (Finance, Banking, Law, Energy, Government, Healthcare, etc)
- Kubernetes Assessments
- Supply Chain Assessments

Analyze Assessment Results and Generate Insights

Assessment Report and Dashboard

The assessment report provides an overall summary, agent details, efficacy of detections, and more. The report dashboard analyzes the findings that surfaced in each assessment. Users can view details about specific findings and whether the execution was validated, prevented, or detected.



ADVANCED SCENARIOS REPORT

Assessment Name: liza-2/11/2022

Template Name: ps downloader - liza
ps downloader - liza

Time start: 02/11/2022 16:56:00

Time End: 02/11/2022 17:00:00

Status: Completed

OVERALL SUMMARY

TWENTYFOUR (TWEN...
Completed
Agent Not Elevated
Number of Executions:
2

EXECUTION	PREVENTED		DETECTED	
EXECUTION	0%	0/1	100%	1/1
PowerShell (Command and Scripting Interpreter)	0%	0/1	100%	1/1

PERSISTENCE	PREVENTED		DETECTED	
PERSISTENCE	0%	0/1	100%	1/1
Hijack Execution Flow	0%	0/1	100%	1/1

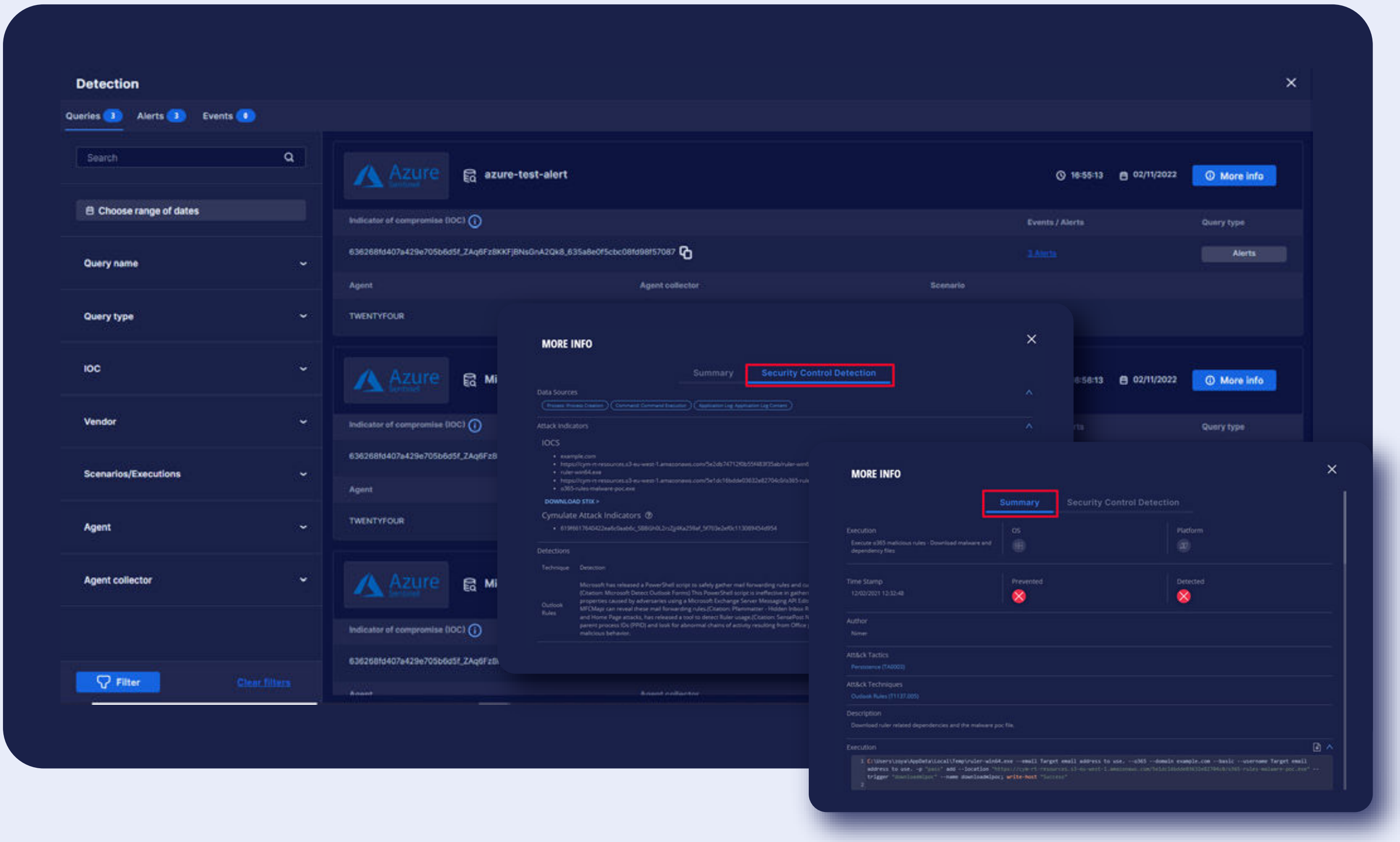
PRIVILEGE ESCALATION	PREVENTED		DETECTED	
PRIVILEGE ESCALATION	0%	0/1	100%	1/1
Hijack Execution Flow	0%	0/1	100%	1/1

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

Detection Results, Mitigation Guidance, Attack Indicators, and Sigma Rules

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

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.



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

The Cymulate Platform

Cymulate BAS Advanced Scenarios is available both as a standalone SaaS offering and as an integrated offering within the Cymulate Exposure Management and Security Validation Platform. The Cymulate platform provides a comprehensive and scalable solution for security leaders, regardless of their security posture maturity, to drive their continuous threat exposure management program and support both the technical and business requirements of scoping, discovery, prioritization, validation, and mobilization.

About Cymulate

Cymulate, the leader in exposure management and security validation, provides a modular platform for continuously assessing, testing, and improving cybersecurity resilience. More than 500 customers worldwide rely on the Cymulate platform to drive their threat exposure management programs from scoping through discovery, prioritization, validation, and mobilization. The Cymulate platform automates the attacker's perspective to help organizations understand threat exposure, how controls and processes respond to threats, and the improvements they can make to mitigate exposure risk. For more information, visit www.cymulate.com.

Contact us for a live demo

Start Your Live Demo

info@cymulate.com | www.cymulate.com