

# Cymulate Breach and Attack Simulation

# Validate, Measure & Optimize Security Controls

Cymulate Breach and Attack Simulation (BAS) validates cybersecurity controls by safely conducting threat activities, tactics, techniques, and procedures in production environments. With automation and a library of realistic attack scenarios and simulations, Cymulate BAS gives security teams an easy-to-use interface to test security architecture, people, and processes for continuous assessment of cyber resilience.

Cymulate BAS applies the latest threat intel and primary research from the Cymulate Threat Research Group with daily updates on emerging threats and new simulations – all mapped to the MITRE ATT&CK framework. On-demand and scheduling systems allow for both ad hoc checks and automated testing to validate security controls against emergent threat activity, confirm remediation, or prepare for audits and penetration tests.

# **How it Works**

Cymulate BAS enables customers to securely simulate real-world cyber attacks, thoroughly testing their organization's resilience against known and emerging threats. Cymulate BAS is cloud based and easily deployed with minimal installation and maintenance efforts.

Customers only need to install one lightweight agent per environment to run assessments. The agent facilitates seamless communication between customer devices and the Cymulate platform, ensuring timely updates and efficient transfer of operational data.

# **Validate Security Controls**

Security is built upon a layered defense that needs continuous testing to assess if controls are working effectively. Cymulate BAS tests for detection and alerting on threats to confirm that controls are functioning correctly or if threats can evade them.

Each vector is scored independently and aggregated for an overall risk score based on industry-standard frameworks. Cymulate BAS integrates with many SIEM, SOAR, GRC, EDR, firewall, and ticketing systems via API to validate and improve security tool detection and response capabilities

# **Cymulate BAS Benefits**



# REALISTIC CONTROL TESTING

Offensive testing based on threat actor techniques & tactics, simulated safely



#### MITIGATION GUIDANCE

Clear steps to remediate, close gaps & reduce exposure



#### CONTINUOUS VALIDATION

Repeat assessments to validate mitigations & identify drift



#### **RISK SCORING**

Benchmarking against peers & continuous improvement with tracked & trending risk scores

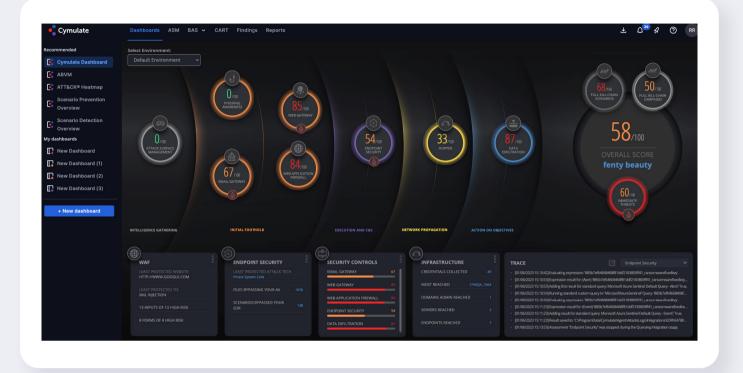


#### AUTOMATION

Scheduled & automated assessments for testing on demand or upon threat updates



# **Cymulate Dashboard**



The Cymulate dashboard presents an at-a-glance view of threat vectors, their scores, and the overall Cymulate risk score.

#### Test Email Security Controls

The **email gateway** capability challenges email security controls (both native and third-party) by sending emails with attachments containing ransomware, worms, trojans, or links to malicious websites to explicitly defined email addresses within the organization. Cymulate BAS validates control effectiveness for each threat and escalates the email threats that bypass the first line of defense and reach inboxes without being altered or removed.

### Assess Web Gateway Protection

The **web gateway capability** tests employee access to malicious websites through coercion or purposely performing dangerous activities. Cymulate BAS includes tests for both inbound protection against thousands of simulated malicious files and exploits and outbound protection against a daily feed of comprised URLs.

#### Challenge Web Application Firewall (WAF) Configurations

The **WAF capability** simulates attacks against web applications that the WAF protects to discover exploitable vulnerabilities in web applications and infrastructure, preventing potentially sensitive information from being stolen. This capability uses payloads such as command injection, XML injection, SQL injection, NSQL injection, and file inclusion. The results of the simulations are mapped to MITRE ATT&CK tactics, techniques, and procedures (TTPs) and Open Web Application Security Project (OWASP) security risks.



## Confirm Endpoint Security Tools

The **endpoint security capability** tests endpoint security platforms and native tools against behavioral and signature-based attacks, lateral movement, and MITRE ATT&CK methods and commands to discover security gaps and misconfigurations.

### Analyze Data Loss Prevention (DLP) Controls

The **data exfiltration capability** tests the effectiveness of DLP security controls and native controls with exfiltration methods such as HTTP & HTTPS, DNS, DNS tunneling, ICMP tunneling, Telnet, email, removable hardware, cloud services, and more. Cymulate BAS packages the data into different file types, including images and office files, and attempts to exfiltrate them using multiple exfiltration methods.

#### Identify Exposure to the Latest Active Threats

The **immediate threat intelligence capability** tests security controls against new and emerging threats observed in the wild. The Cymulate Threat Research Group updates Cymulate BAS daily with attack simulations of these latest threats that require urgent attention and action. Threat and simulation updates include insights into threat actors, attack vectors, techniques mapped to MITRE ATT&CK, and indicators of compromise.

#### Validate Security Architecture Against APT Attacks

The **full kill-chain** scenarios capability simulates end-to-end attack scenarios of known advanced persistent threat (APT) groups. These attack simulations deliver and execute production-safe ransomware, trojan, worm, or custom payload via web or email attack vectors. In addition to challenging each attack vector separately, Cymulate BAS tests the effectiveness of various security controls across the entire cyber kill-chain-from attack delivery to exploitation and post-exploitation.

### **Analyze Assessment Results & Generate Insights**

#### Control Validation Dashboards

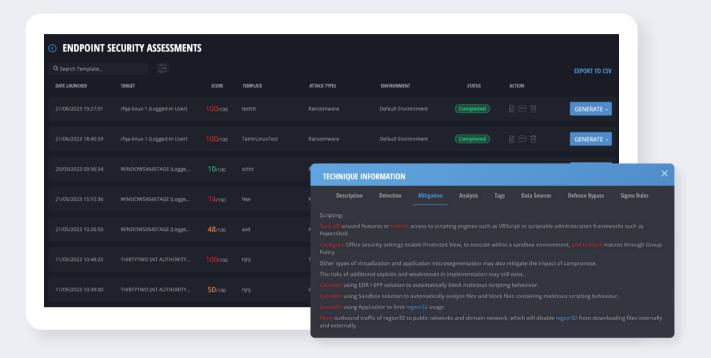
Dashboards and detailed reports summarize results for each Cymulate BAS Scenarios capability and threat vector with both at-a-glance metrics and details (payload/URL/site) from recent tests.

© ENDPOINT SECUR	RITY RE	PORT SUMMARY					
Penetration Ratio		Least Protected ATT&CK Technique DLL Side-Loading	Most Protected: Worm		Least Protected		49
0			ATT&CK TECHNIQUES			Ø	Assessment dates 14/03/2019 20:14:20 - 21/06/2023 19:29:08 Security Control Detection
ATTACK TYPE	RATIO	ATTACK TYPE	RISK	COMPLETED	DETECTED		EVENTS/ALERTS
Ransomware Full Scenarios			Medium			$\odot$	No integration configured
Worm Full Scenarios						⊚	GENERATE REPORT ~ HISTORY つ
Trojan Full Scenarios						$\odot$	
Antivirus Signature base						$\odot$	
Configuration						⊘	



#### Assessment History & Mitigation Guidance

Customers can view the history of all assessments and drill down further per assessment to view results and mitigation guidance mapped to the MITRE ATT&CK framework.



#### Dynamic Dashboards & Reports

Dynamic dashboards and reports provide organizations with the ability to gather insights based on findings from across the Cymulate platform. Organizations can choose from out-of-the-box templates or create customized dashboards and reports tailored to meet their specific needs and goals. Included in the dynamic reports is an up-to-date view of the latest critical and high-risk security gaps across security controls and policies in the organization Customers use this report as a base for discussion with IT and security engineering teams to prioritize remediation efforts and further investigate the best course of action.

🔹 Cymulate		rts			∓ <mark>₀</mark> එ <u></u> % @			
ecommended C, Cymulate Dashboard C, ABVM	Constroard / Security Controls Efficacy Security Controls Efficacy Lait updated pat new							
ATT&CK® Heatmap G* Overall Security	Security Controls Prevention		Security Controls Prevention Trend	: Unprevented Scenarios by Control				
Construction     Scenario Prevention     Overview     Scenario Detection     Overview     Drift Detection     Advanced Scenarios     Overview	62.3% • Not Presented			* Web Application * Web Cateway * Ensil Cateway				
Leteral Movement Security Posture y dashboards	Security Control Detection		Security Controls Detection Trend	Undetected Scenarios by Control				
Security Controls Efficacy     Efficacy     EDR Efficacy     Risk Overview     Remediation     Guidance     Modules - Shekel - Sahar     CVE dashboard	• 0.22% • Not Detected		There is nothing to show by string as situation of flows for white means	* Immediate Three_ is flat Kith-Chain Sc_ is first Calencery				
New Dashboard     Detection Dashboard     Example	Top 10 Possible Techinques	Hazardous Scenarios by Risk						
Rxample				$\bigcirc$				



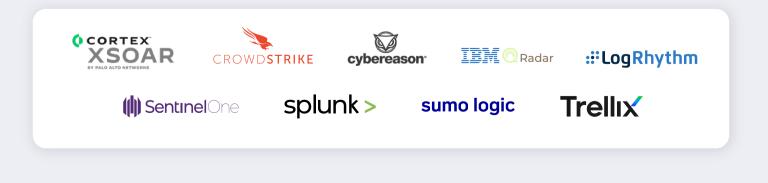
## Map Assessments to the MITRE ATT&CK® Framework

**The MITRE ATT&CK® Heatmap** provides a detailed view of the current state of cyber resilience by visualizing the exposure to each technique. The heatmap correlates all findings from across the Cymulate platform, including filtering and drill-downs into the assessment details for test results and recommended mitigations.

Dashboards ASM	BAS ✔ CART Findi	ings Reports								¥.	ц <del>,</del> % ©
3 MITRE ATT&	CK® HEATMAP										
										Show sub tee	chniques Export
Initial Access 12 techniques	Execution 35 techniques	Persistence 70 techniques	Privilege Escalation 40 techniques	Defense Evasion 88 techniques	Credential Access 30 techniques	Discovery 31 techniques	Lateral Movement 20 techniques	Collection 17 techniques	Exfiltration 11 techniques	Command and Control 26 techniques	Impact 18 techniques
Drive-by Compromise	AppleScript	Accessibility Features	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	II Adversary-in-the- Middle	II Account Discovery	Application Access Token	Adversary-in-the- Middle	II Automated Exfiltration	Application Layer Protocol	Account Access Remova
Exploit Public-Facing Application	CMSTP	II Account Manipulation	Access Token Manipulation	II Access Token Manipulation	Bash History	Application Window Discovery	Application Deployment Software	II Archive Collected Data	Data Compressed	Commonly Used Port	Data Destruction
External Remote Services	Command and Scripting Interpreter	AppCert DLLs	Accessibility Features	Application Access Token	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Audio Capture	Data Encrypted	Communication Through Removable Media	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppInit DLLs	AppCert DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Infrastructure Discovery	Exploitation of Remote Services	Automated Collection	Data Transfer Size Limits	Custom Command and Control Protocol	Data Manipulation
Phishing	Component Object Model and Distributed COM	Application Shimming	Appinit DLLs	Binary Padding	Credentials from Password Stores	Cloud Service Dashboard	Internal Spearphishing	Browser Session Hijacking	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	II Defacement
Replication Through Removable Media	Container Administration Command	Authentication Package	Application Shimming	Build Image on Host	Credentials from Web Browsers	Cloud Service Discovery	Lateral Tool Transfer	Clipboard Data	Exfiltration Over C2 Channel	II Data Encoding	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	BITS Jobs	Boot or Logon Autostart Execution	Bypass User Account Control	Credentials in Files	Cloud Storage Object Discovery	Pass the Hash	II Data Staged	Exfiltration Over Other Network Medium	II Data Obfuscation	Disk Structure Wipe
Spearphishing Link	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Initialization Scripts	CMSTP	Credentials in Registry	Container and Resource Discovery	Pass the Ticket	Data from Cloud Storage	Exfiltration Over Physical Medium	Domain Fronting	II Disk Wipe
Spearphishing via Service	Dynamic Data Exchange	Boot or Logon Initialization Scripts	Bypass User Account Control	Clear Command History	Exploitation for Credential Access	Debugger Evasion	Remote Desktop Protocol	Data from Configuration Repository	Exfiltration Over Web Service	Domain Generation Algorithms	Endpoint Denial of Service
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Create or Modify System Process	Code Signing	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking	Data from Information Repositories	Scheduled Transfer	Dynamic Resolution	Firmware Corruption
Trusted Relationship	Graphical User Interface	Browser Extensions	DLL Search Order Hijacking	Compile After Delivery	II Forge Web Credentials	File and Directory Discovery	Remote Services	Data from Local System	Transfer Data to Cloud Account	Encrypted Channel	Inhibit System Recovery
Valid Accounts	InstallUtil	Change Default File Association	Domain Policy Modification	Compiled HTML File	Hooking	Group Policy Discovery	Replication Through Removable Media	Data from Network Shared Drive		Fallback Channels	Network Denial of Service
	Inter-Process Communication	Component Firmware	Dylib Hijacking	Component Firmware	II Input Capture	Network Service Discovery	SSH Hijacking	Data from Removable Media		Ingress Tool Transfer	Resource Hijacking
	LSASS Driver	Component Object Model Hijacking	Elevated Execution with Prompt	Component Object Model Hijacking	Input Prompt	Network Share Discovery	Shared Webroot	Email Collection		Multi-Stage Channels	Runtime Data Manipulation

## Validate and Improve Detection and Response with Security Control Integrations

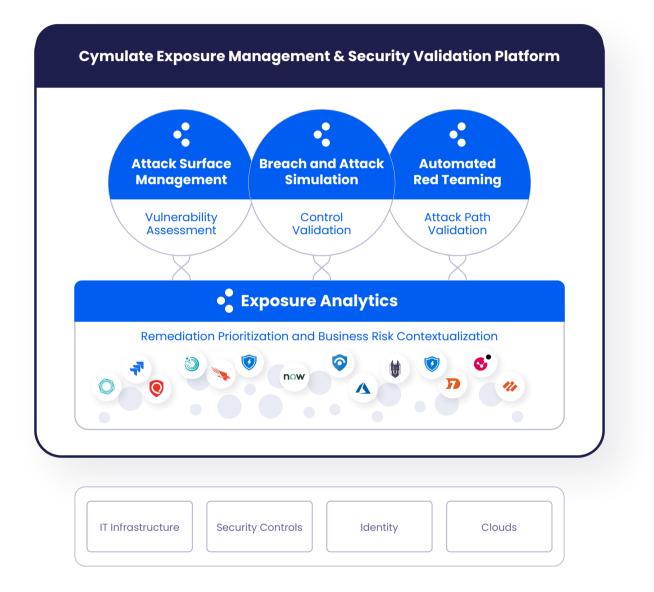
Cymulate BAS integrates with many SIEM, SOAR, GRC, EDR, and other tools via API to augment and benefit existing security solutions. With the API integrations, Cymulate identifies the specific policies that need to be tuned to improve security posture and mitigate control gaps. Cymulate remediation guidance integrates with IT service management to streamline workflows and security task management. Here is just a small sample of the available integrations.





## **The Cymulate Platform**

Cymulate BAS 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 against emergent threats, evolving environments, and digital transformations. The solution has a quantifiable impact across all five continuous threat exposure management (CTEM) program pillars and on a business's ability to reduce risk by understanding, tracking, and improving its security posture. Customers can choose from its Attack Surface Management (ASM) product for risk-based asset profiling and attack path validation, Breach and Attack Simulation (BAS) for simulated threat testing and security control validation, Continuous Automate Red Teaming (CART) for vulnerability assessment, scenario-based and custom testing, and Exposure Analytics for ingesting Cymulate and 3rd-party data to understand and prioritize exposures in the context of business initiatives and cyber resilience communications to executives, boards, and stakeholders. For more information, visit www.cymulate.com.

Contact us for a live demo



info@cymulate.com | www.cymulate.com