DATA SHEET

Cymulate

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

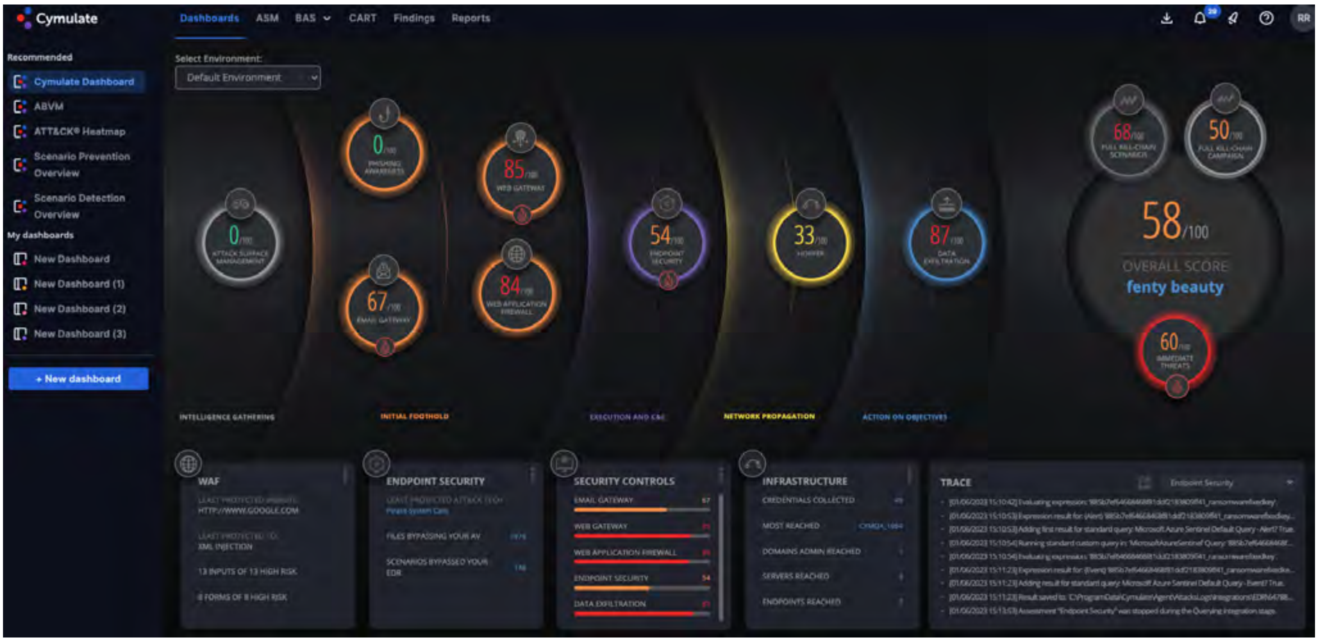
MITIGATION GUIDANCE
Clear steps to remediate, close gaps & reduce exposure

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



WAF
LEAST PROTECTED WEBSITE
HTTP://WWW.GOOGLE.COM
LEAST PROTECTED TOI
XML INJECTION
13 INPUTS OF 13 HIGH RISK
8 FORMS OF 8 HIGH RISK

ENDPOINT SECURITY
LEAST PROTECTED ATTACK TECH
Private System Calls
FILES BYPASSING YOUR AV 1976
SCENARIOS BYPASSED YOUR EDR 116

SECURITY CONTROLS
EMAIL GATEWAY 67
WEB GATEWAY 85
WEB APPLICATION FIREWALL 84
ENDPOINT SECURITY 54
DATA EXFILTRATION 87

INFRASTRUCTURE
CREDENTIALS COLLECTED 49
MOST REACHED CYMDA_1664
DOMAINS ADMIN REACHED 1
SERVERS REACHED 8
ENDPOINTS REACHED 7

TRACE
Endpoint Security

```
- [01/06/2023 15:10:42] Evaluating expression: '[illegible]_ransomwarefixedkey'.
- [01/06/2023 15:10:53] Expression result for: (Alert) '[illegible]_ransomwarefixedkey...
- [01/06/2023 15:10:53] Adding first result for standard query: Microsoft Azure Sentinel Default Query - Alert? True.
- [01/06/2023 15:10:54] Running standard custom query in: 'MicrosoftAzureSentinel' Query: '[illegible]...
- [01/06/2023 15:10:54] Evaluating expression: '[illegible]_ransomwarefixedkey'.
- [01/06/2023 15:11:23] Expression result for: (Event) '[illegible]_ransomwarefixedke...
- [01/06/2023 15:11:23] Adding result for standard query: Microsoft Azure Sentinel Default Query - Event? True.
- [01/06/2023 15:11:23] Result saved to: 'C:\ProgramData\Cymulate\Agent\AttacksLogs\Integrations\EDR\[illegible]...
- [01/06/2023 15:13:53] Assessment "Endpoint Security" was stopped during the Querying integration stage.
```

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.

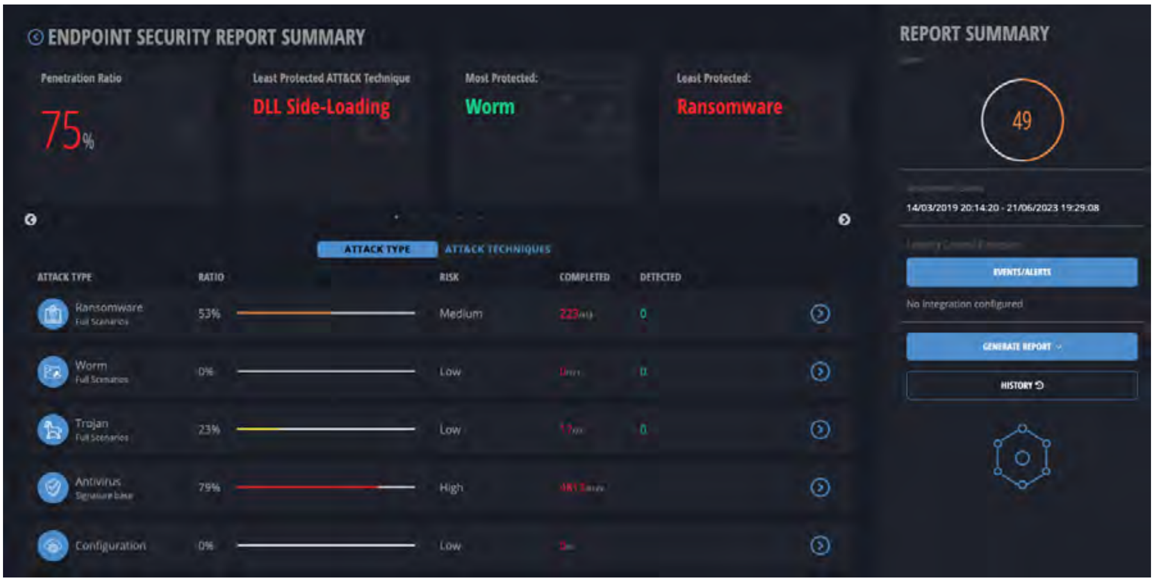
Validate Security Architecture Against APT Attacks

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 SECURITY REPORT SUMMARY

Penetration Ratio: 75%

Least Protected ATT&CK Technique: DLL Side-Loading

Most Protected: Worm

Least Protected: Ransomware

ATTACK TYPE	RATIO	RISK	COMPLETED	DETECTED
Ransomware Full Scenarios	53%	Medium	223 [illegible]	0
Worm Full Scenarios	0%	Low	[illegible]	0
Trojan Full Scenarios	23%	Low	[illegible]	0
Antivirus Signature base	79%	High	[illegible]	
Configuration	0%	Low	[illegible]	

REPORT SUMMARY

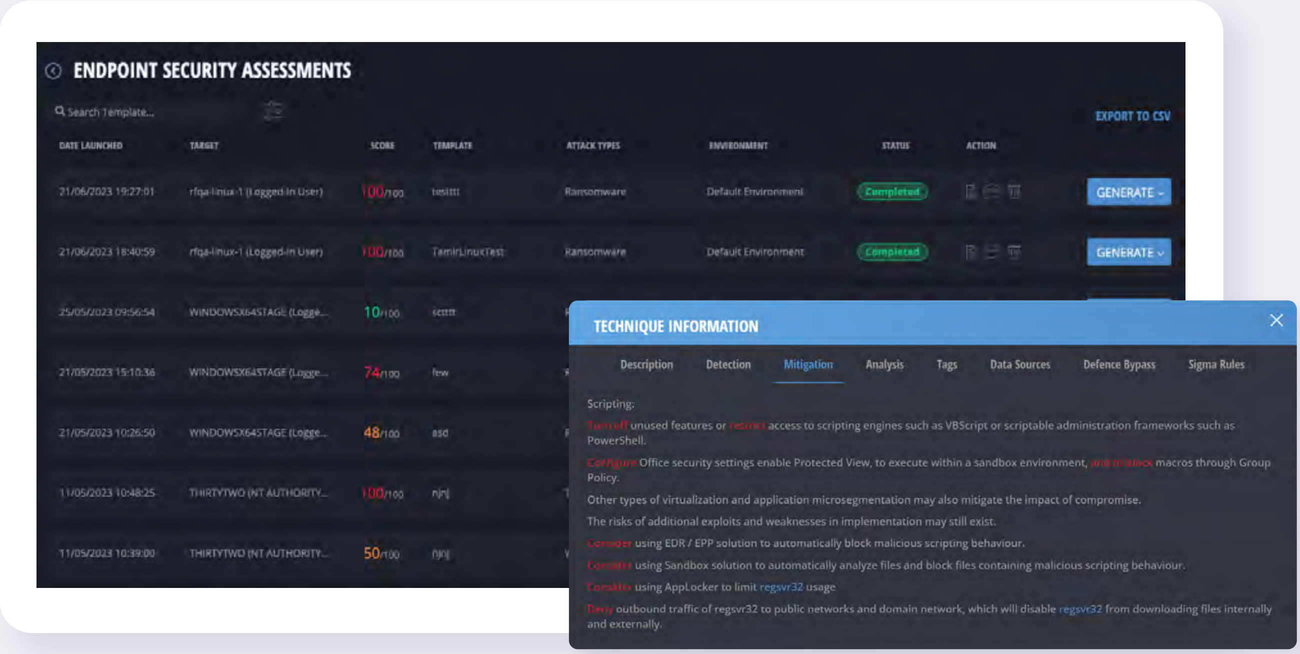
49

14/03/2019 20:14:20 - 21/06/2023 19:29:08

No integration configured

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.



ENDPOINT SECURITY ASSESSMENTS

DATE LAUNCHED	TARGET	SCORE	TEMPLATE	ATTACK TYPES	ENVIRONMENT	STATUS	ACTION	
21/06/2023 19:27:01	rfqa-linux-1 (Logged-in User)	100/100	tesittt	Ransomware	Default Environment	Completed		GENERATE
21/06/2023 18:40:59	rfqa-linux-1 (Logged-in User)	100/100	TamirLinuxTest	Ransomware	Default Environment	Completed		GENERATE
25/05/2023 09:56:54	WINDOWSX64STAGE (Logge...	10/100	scttt					
21/05/2023 15:10:36	WINDOWSX64STAGE (Logge...	74/100	few					
21/05/2023 10:26:50	WINDOWSX64STAGE (Logge...	48/100	asd					
11/05/2023 10:48:25	THIRTYTWO (NT AUTHORITY...	100/100	njnj					
11/05/2023 10:39:00	THIRTYTWO (NT AUTHORITY...	50/100	njnj					

TECHNIQUE INFORMATION

Scripting:

Turn off unused features or restrict access to scripting engines such as VBScript or scriptable administration frameworks such as PowerShell.

Configure Office security settings enable Protected View, to execute within a sandbox environment, and to block macros through Group Policy.

Other types of virtualization and application microsegmentation may also mitigate the impact of compromise.

The risks of additional exploits and weaknesses in implementation may still exist.

Consider using EDR / EPP solution to automatically block malicious scripting behaviour.

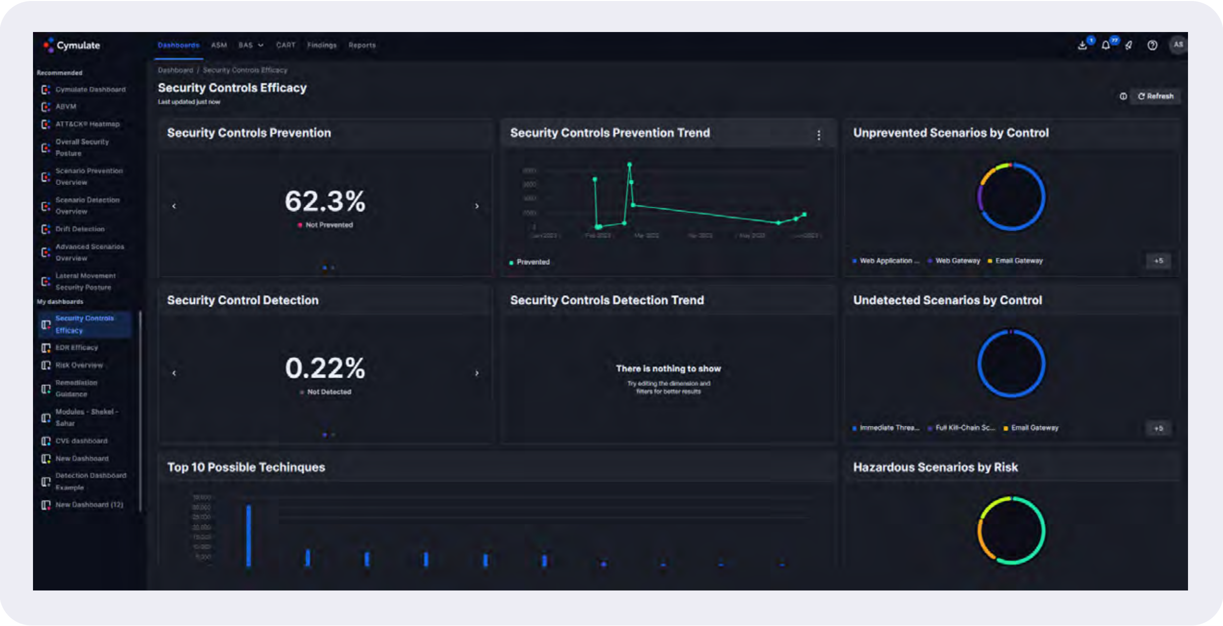
Consider using Sandbox solution to automatically analyze files and block files containing malicious scripting behaviour.

Consider using AppLocker to limit regsvr32 usage

Deny outbound traffic of regsvr32 to public networks and domain network, which will disable regsvr32 from downloading files internally and externally.

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
Dashboards
ASM
BAS
CART
Findings
Reports
Recommended
Cymulate Dashboard
ABVM
ATT&CK® Heatmap
Overall Security Posture
Scenario Prevention Overview
Scenario Detection Overview
Drift Detection
Advanced Scenarios Overview
Lateral Movement Security Posture
My dashboards
Security Controls Efficacy
EDR Efficacy
Risk Overview
Remediation Guidance
Modules - Shekel - Sahar
CVE dashboard
New Dashboard
Detection Dashboard Example
New Dashboard (12)
Dashboard / Security Controls Efficacy
Refresh
Security Controls Prevention
Security Controls Prevention Trend
Prevented
Unprevented Scenarios by Control
Web Application ...
Web Gateway
Email Gateway
+5
Security Control Detection
Security Controls Detection Trend
Undetected Scenarios by Control
Immediate Threa...
Full Kill-Chain Sc...
Email Gateway
+5
Top 10 Possible Techinques
Hazardous Scenarios by Risk

Security Controls Efficacy

Last updated just now

62.3% Not Prevented

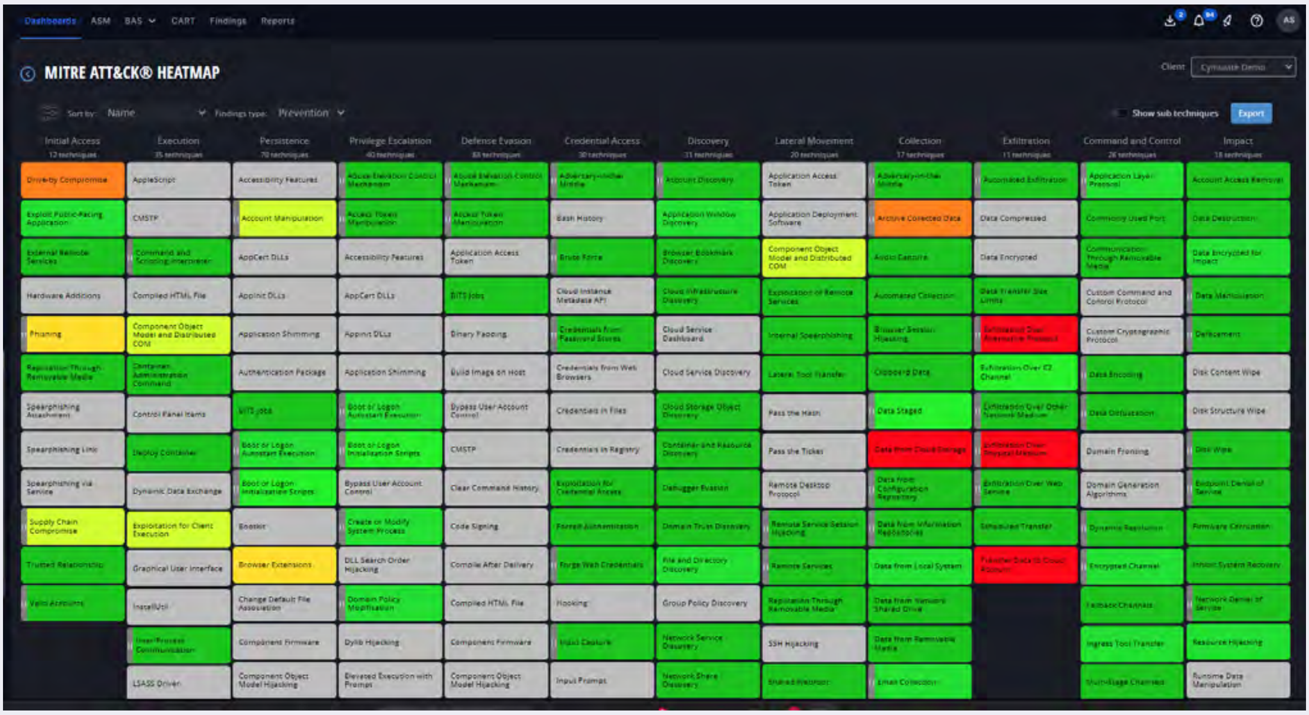
0.22% Not Detected

There is nothing to show

Try editing the dimension and filters for better results

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.



MITRE ATT&CK® HEATMAP

Client: Cymulate Demo

Sort by: Name

Findings type: Prevention

Show sub techniques

Initial Access 12 techniques	Execution 35 techniques	Persistence 70 techniques	Privilege Escalation 40 techniques	Defense Evasion 83 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	Adversary-in-the-Middle	Account Discovery	Application Access Token	Adversary-in-the-Middle	Automated Exfiltration	Application Layer Protocol	Account Access Removal
Exploit Public-Facing Application	CMSTP	Account Manipulation	Access Token Manipulation	Access Token Manipulation	Bash History	Application Window Discovery	Application Deployment Software	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	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	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	Data Staged	Exfiltration Over Other Network Medium	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	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	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	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

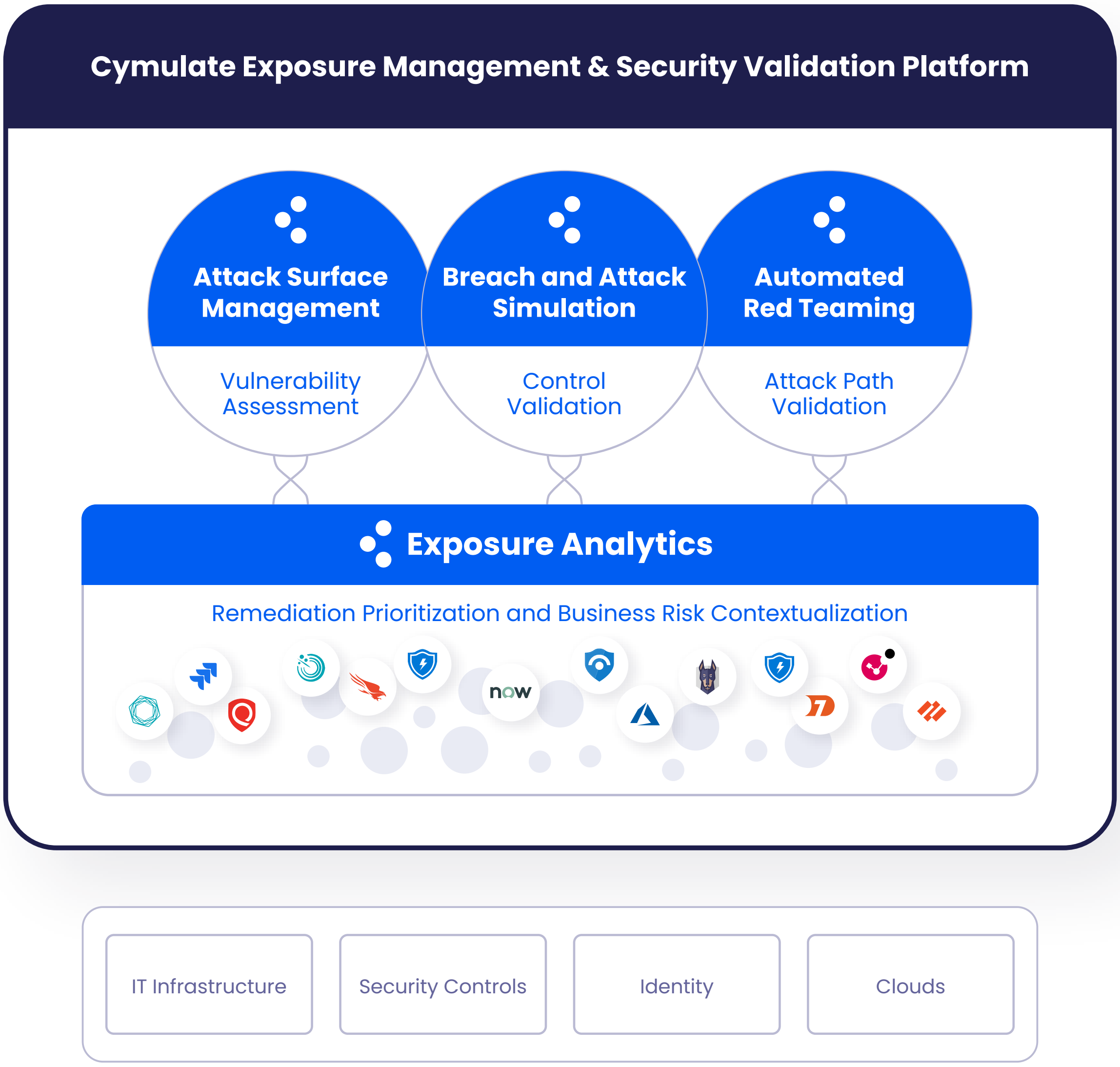
Validate and Improve Detection and Response with Security Control Integrations

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.

CORTEX XSOAR BY PALO ALTO NETWORKS
CROWDSTRIKE
cybereason
IBM QRadar
LogRhythm
SentinelOne
splunk>
sumo logic
Trellix

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.



Cymulate Exposure Management & Security Validation Platform
Attack Surface Management
Vulnerability Assessment
Breach and Attack Simulation
Control Validation
Automated Red Teaming
Attack Path Validation
Exposure Analytics
Remediation Prioritization and Business Risk Contextualization
now
IT Infrastructure
Security Controls
Identity
Clouds

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

Start Your Live Demo

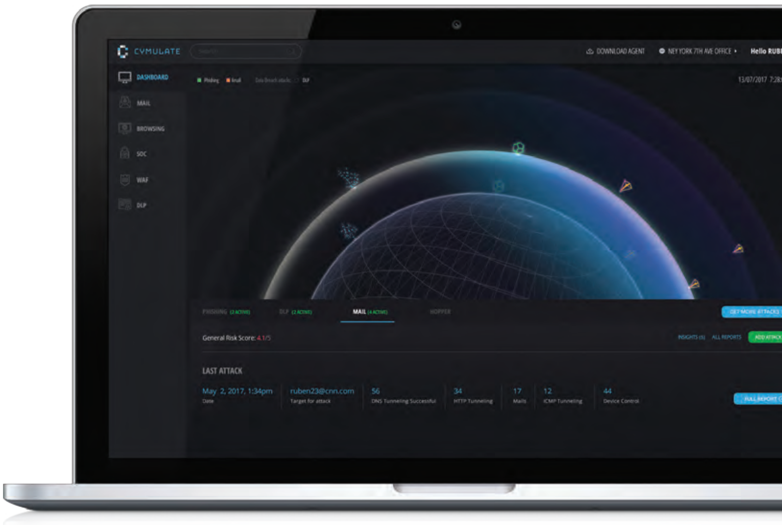
info@cymulate.com | www.cymulate.com

BREACH & ATTACK SIMULATION

THE EFFECTIVE APPROACH TO CYBER SECURITY VALIDATION

Cymulate's cyber simulation platform allows you to test your security assumptions, identify possible security gaps and receive actionable insights to improve your security posture.

It works by simulating a multi-vector, internal or external attack – which includes the very latest vulnerabilities derived from Cymulate's research unit. The result is a comprehensive validation of your organization's current security posture status – delivered on-demand and with a zero false positive.



General Risk Score: 4.1/5

LAST ATTACK

May 2, 2017, 1:34pm Date | ruben23@cnn.com Target for attack | 56 DNS Tunneling Successful | 34 HTTP Tunneling | 17 Mails | 12 ICMP Tunneling | 44 Device Control

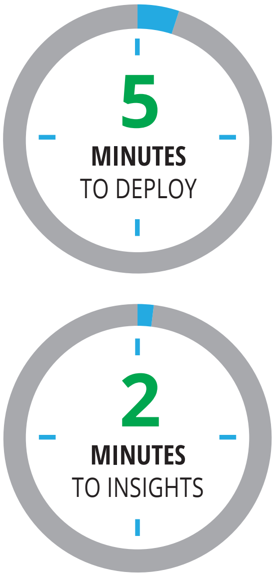
CYMULATE

KNOW YOUR REAL SECURITY POSTURE

24/7 365

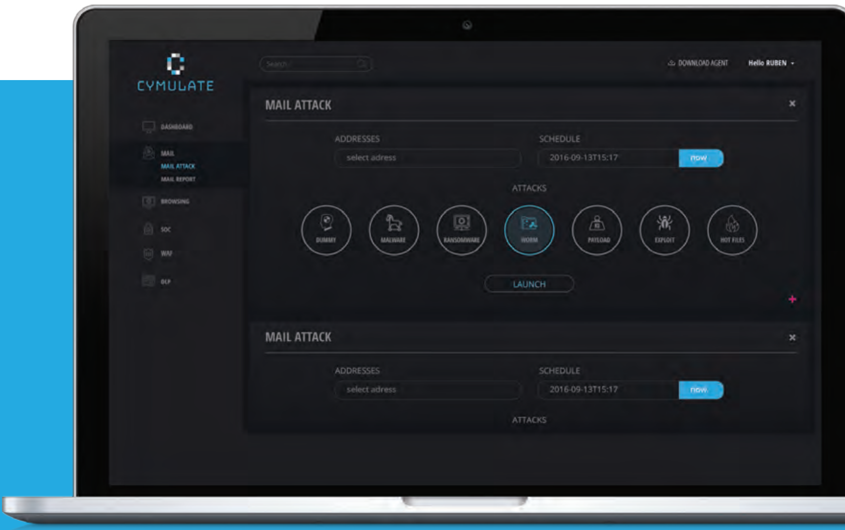
Organizations now have the power to verify their security posture, on-demand through a unique breach and attack simulation platform. Cymulate's advanced technology provides organizations with the capability to launch simulations of cyber-attacks against themselves, immediately exposing vulnerabilities and providing procedures to mitigate them.Fully-automated and diversified attacks allow for complete security testing anytime, providing organizations with a better understanding of their security posture and allowing them to improve it, continuously. By eliminating false positive, Cymulate delivers only accurate and actionable results.

YOU ARE 7 MINUTES AWAY FROM KNOWING IF YOU ARE SECURE!



STAY ONE STEP AHEAD OF HACKERS

Cyber-attacks today are more sophisticated and dynamic than ever before, as hackers work around the clock to breach networks, steal intellectual property, and disrupt operations. Organizations worldwide invested more than $80 billion last year to protect their data, block malware, and safeguard critical business processes. Yet despite all the time, money, and effort invested in cybersecurity solutions, many CISOs still can't answer an essential question: **Is my organization safe right now?** Cymulate provides the answer to this question and empowers organizations to validate their cyber defenses more frequently and comprehensively.



MAIL ATTACK

ADDRESSES: select adress

SCHEDULE: 2016-09-13T15:17

ATTACKS

MAIL ATTACK

ADDRESSES: select adress

SCHEDULE: 2016-09-13T15:17

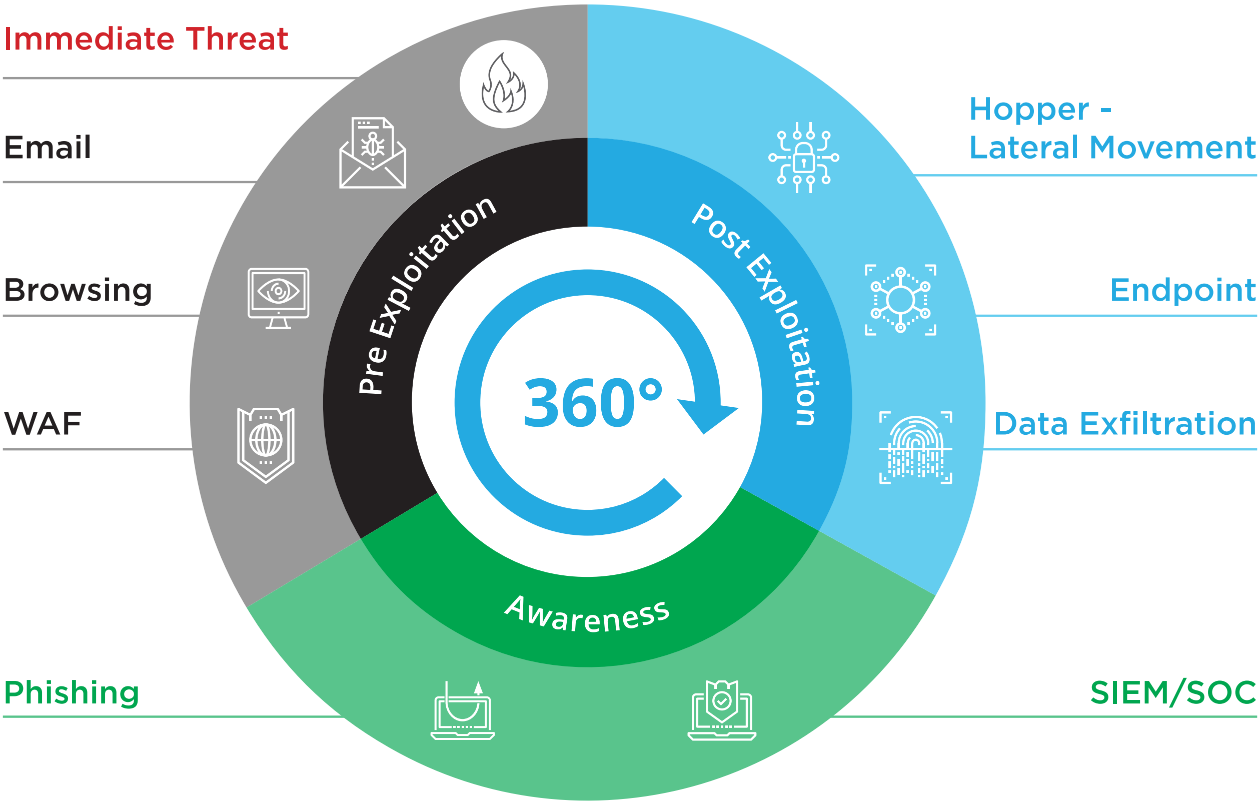
ATTACKS

Mail Attack

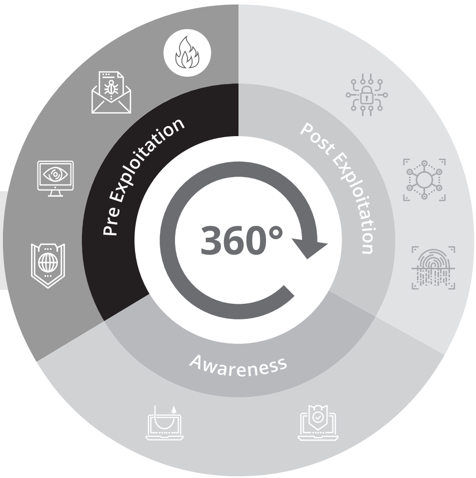
OUR SOLUTIONS

Cymulate's platform comprehensively exercises your defenses with the industry's widest range of attack vectors, providing an Advanced Persistent Threat (APT) simulation of your security posture at all times. Test your network's ability to cope with pre-exploitation-stage threats in Email, Browsing, and WAF. Analyze your ability to respond to real incidents with our post-exploitation solutions as the Hopper, Endpoint and Data Exfiltration And improve awareness among employees against phishing, ransomware and other attacks.

Gain a clear picture of your vulnerabilities from every point of exposure and learn what will really happen when you are attacked.



PRE EXPLOITATION



IMMEDIATE THREAT ALERT

Test your organization's security posture against clear and present cyber danger

To help organizations protect themselves against new threats that hackers have just launched, Cymulate provides its Immediate Threat solution that simulates the latest attack. This simulation is created by the Cymulate Research team that catches and analyzes threats immediately after they were launched by cybercriminals. By running this simulation, a customer can validate within an hour if its organization would be vulnerable to this threat and take measures before the attack will take place.

E-MAIL ASSESSMENT

Test Your Entire E-Mail Security with Our Vast & Diverse Email Assessment

Despite the widespread use of mail filters, email getway security and sandboxes, the majority of attacks still originate via email. Poor configuration or implementation of security products might lead to the false assumption that you are safe. Cymulate's Email Assessment module enables organizations to challenge this significant attack vector and test your assumptions.

BROWSING ASSESSMENT

Test Your HTTP/HTTPS Outbound Exposure to Malicious Websites

The vast majority of web malware encounters occur via legitimate browsing of mainstream websites. A significant amount of malware is delivered through browser add-ons – malicious scripts that use Flash, Java and Microsoft Silverlight plug-ins on webpages make up a quarter of malware attacks. Cymulate's Browsing Assessment solution enables you to assess your outbound exposure to malicious websites using common HTTP/HTTPS protocols.

WEB APPLICATION FIREWALL ASSESSMENT (WAF)

Test Your WAF security resilience to web payloads for better protection of your web apps

Web applications have become a central business component; huge amounts of money and effort are spent protecting them. Whereas in the past, IT security teams were tasked with defending just a few enterprise web apps, now they must protect a multitude of web backends of mobile apps, SaaS apps and other cloud- delivered solutions. Cymulate WAF tests your WAF configuration, implementation and features, ensuring that it can block payloads.

POST EXPLOITATION

Pre Exploitation
Post Exploitation
360°
Awareness

HOPPER - LATERAL MOVEMENT

Test Your Windows Domain Network Configuration Using Our Sophisticated Algorithm

Lateral movement inside a Windows Domain Network is a common penetration scenario. As threat actors move deeper into the network, their movements and methods become difficult to detect, especially when they utilize Windows features and tools typically used by IT administrators. Cymulate Hopper's sophisticated and efficient algorithm gathers all the common and clever techniques used by the most sophisticated hackers to move laterally inside the network to reveal the breach spots of your Windows Domain Network.

ENDPOINT ASSESSMENT

Test if your Endpoint solutions are tuned properly and if they are protecting you against the latest attack vectors

Endpoints have become the target of choice by hackers. Organizations reinforce their endpoints with layers of protection such as anti-virus, anti-spyware and behavioral detection. They often deploy highly sophisticated deception systems to lead attackers away from the real endpoints and information to honeypots and traps. Cymulate's Endpoint Assessment simulation shows you which of your products are really protecting your endpoints and which are not working properly, exposing your organization to breach. This Assessment allows you to understand the actual security state of your endpoints by comprehensively testing: Automated behavioral detection (EDR), Signature-based detection (Anti-Virus), Known vulnerabilities including Windows patches and your 3rd-party software, Hardening of your endpoints according to Proven methodologies. The results will provide you a unified report of all endpoint security aspects in an easy-to-understand format that lets you take specific actions to upgrade the security state of each of your endpoints.

DATA EXFILTRATION ASSESSMENT

Test Your Outbound Critical Data Safely Before Real Data is Exposed

Laws and regulations are increasingly putting the onus on companies to fully safeguard their data. Breaches create huge financial impact and damage a victim company's reputation. Data Loss Prevention products are designed to protect against data exfiltration. Precious digital assets depend almost entirely on DLP implementation, methodology and configuration. Cymulate's Data Exfiltration Assessment allows you to test your outbound flows to validate that information assets stay indoors.

AWARENESS

Pre Exploitation
Post Exploitation
360°
Awareness

PHISHING & AWARENESS

Test Your Employees' Awareness of Phishing Campaigns

Designed to reduce the risk of spear-phishing, ransomware or CEO fraud, Cymulate Phishing solution minimizes malware-related downtime and saves money on incident response. Focused on raising organization's employees' security awareness by creating and executing simulated phishing campaigns, it finds weak links in your organization, helping you build tailored training programs that improve and reinforce proper employee cyber-security behavior.

SIEM/SOC SIMULATION ASSESSMENT

Test Your SIEM/SOC Alert Configuration and Team Competence

SOC teams are built to react, and can sometimes get a little rusty. To adapt cyber defenses to the current threat landscape, a proactive security approach is needed. Rather than reacting to the last attack, organizations need to continuously monitor their networks, hunt attackers and create strategic intelligence. SIEN/SOC Simulation Assessment allows organizations to test the SIEM events correlation and to validate the SIEM alerts. Furthermore, it enables the CISO to test the SOC Team Incident Response procedures.

KEY BENEFITS

KEY BENEFITS

Mitigate attacks before they happen

Plug & Play solution
Easy to deploy and use

Eliminate false positives

SaaS solution
No hardware required

Remote test your entire Security

Immediate results:
24/7/365

Audit your security products - Maximize your ROI

Fully Automated -
Continuous testing
& improvement

Compare solutions before purchase

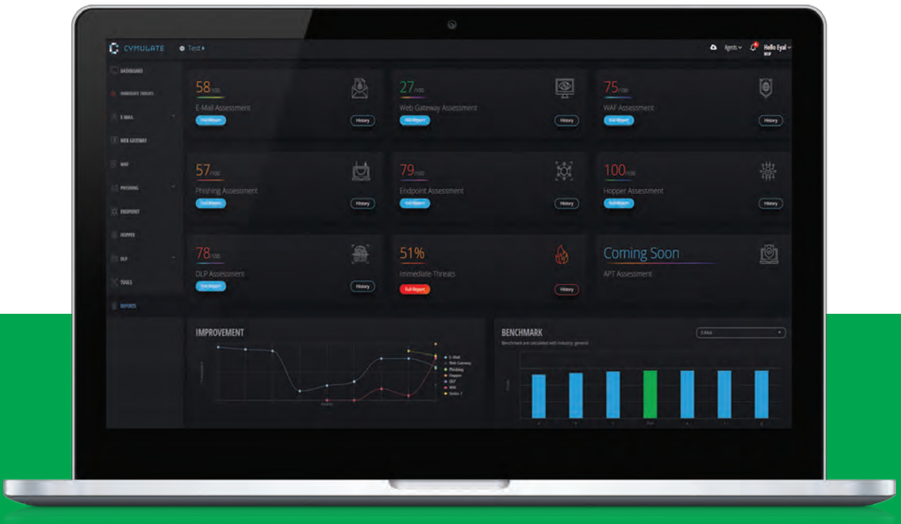
CYMULATE RESEARCH UNIT

Comprising top Reverse Engineers, Penetration Testers & Programmers, Cymulate’s distinguished Cyber Support Unit is what sets us apart. Our primary role is to uncover flaws across a variety of vectors, and continuously search for new vulnerabilities and exploits.

With diverse backgrounds encompassing private security, military and intelligence experience, and combined with the understanding of how your business works, our highly experienced security experts can deliver the visibility into threats and the actors behind them that you need to protect your organization.

We monitor the cyber threat landscape to provide a globalized view of emerging threats, zero-day vulnerabilities, and the tactics, techniques, and procedures (TTP) of advanced threat actors. Our researchers proactively identify new and one-of-a-kind breach methods through emulation of hacker's tactics and strategies.

Results Dashboard



ABOUT CYMULATE

Cymulate was founded by an elite team of former Israel Defense Forces intelligence officers and leading cyber researchers with world-class experience in offensive cyber solutions. Combining vast expertise in cyber simulation technology with extensive field experience to mimic the latest and most sophisticated cyber-attacks. Cymulate employs software-as-a-service applications to simulate the myriad tactics and strategies employed by hackers to attack network and endpoint security infrastructures.

Cymulate helps companies stay one step ahead of cyber attackers with a unique breach and attack simulation platform that empower organizations with complex security solutions made easy to safeguard their digital assets and maintain business continuity. With Cymulate, organizations can assess their true readiness to handle cyber security threats effectively.

For more information, visit **www.cymulate.com**