

The Principle of Security Validation

A Cymulate Security Validation Best Practices eBook



Table of Contents

The Principle of Security Validation	. 3
Security Validation Essentials	. 3
	_
Cymulate Best Practices	. 5
Validate Controls	. 6
Validate Threats	23
Validate Response	30
Offensive Testing	35
About Cymulate	38



The Principle of Security Validation

Security Validation is a fundamental principle in cybersecurity aimed at ensuring that systems, applications, and processes are secure and operate as intended.

Validation of Security Controls Confirmation that the security controls put in place, such as email gateways, web gateways and firewalls, endpoint and cloud security, access controls, etc., are effectively implemented and function as expected.

Validation of Threats

Active testing for the latest persistent, emerging, and immediate threats discovered by the threat intelligence community and validated daily.

By adhering to the principle of security validation, organizations can **identify** weaknesses in their security controls, address threats to their IT assets, and improve overall resilience of their security operations.





03 Validation of Operational Response

Evaluation of security operations team to respond to alerts and recover from security incidents. This includes running purple teaming simulations and drills to assess the effectiveness of security operations and incident response plans.

04 Simulation

Simulation & Modeling of Attacks

Organizations can simulate and enact various breach and attack scenarios within a safe, controlled environment with an attacker's approach of the latest threat tactics and techniques that will better prepare their defenses to stop such attacks.

()5 Compliance Verification Ensuring that the security measures adhere to relevant industry standards, regulations, and best practices. Compliance validation often involves audits and assessments against standards such as ISO 27001, NIST, PCI DSS, GDPR, DORA, etc.

06 Continuous Improvement

Security validation is not a one-time event but an ongoing improvement process that begins by benchmarking an organization's risk level against peers in their industry. Security validation measures the performance of controls, threats, and responses over time with frequent assessments that help ensure security measures remain effective against evolving threats and changes in the IT environment and that these measures do not drift over time.



Cymulate Best Practices

As a recognized authority on security validation, Cymulate has published this eBook to outline the best practices for security validation across the IT environment.

These best practices have been established within the Cymulate Platform based on years of **red team**, blue team experience, testing and validating security operations and technologies, informed by the latest threat intelligence from the **Cymulate Threat Research Group**.

Cymulate best practices provide comprehensive assessments to validate security controls, immediate and persistent threats, and security operations response, to help security teams improve their defensive posture against the latest cyber attacks.

Validate Controls

- Email Gateway
- Web Gateway
- Web App Firewall
- Cloud Security
- Data Exfiltration
- SIEM Observability

- Endpoint Security

Validate

Threats

- Immediate Threats
- Lateral Movement
- Full Kill-Chain Attacks



Validate Response

- SOC Exercises
- Red Team Exercises





Validate Controls

- Email Gateway
- Web Gateway
- Web App Firewall
- Endpoint Security
- Cloud Security
- Data Exfiltration
- SIEM Observability

Threats

Cymulate Best Practices



• Immediate Threats Lateral Movement • Full Kill-Chain Attacks



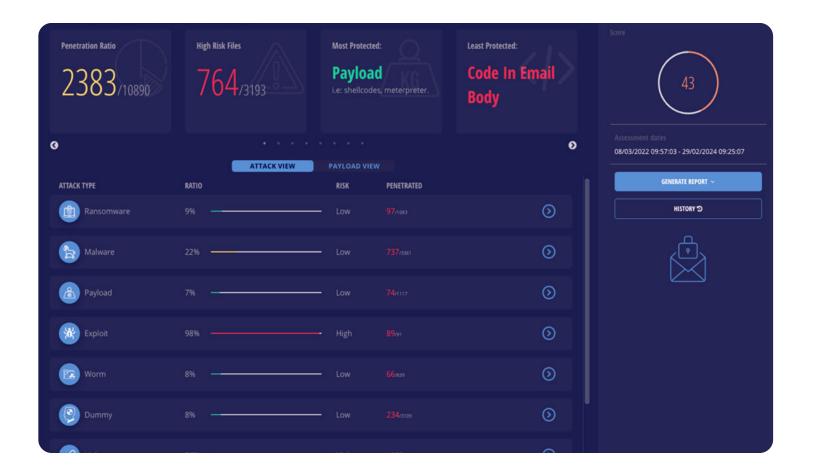
- SOC Exercises
- Red Team Exercises





SECURITY VALIDATION BEST PRACTICES **Email Gateway**

Email is the **most frequently used** delivery method of attack for exploiting security weaknesses and email gateways are critical components in defending against emailbased threats with executable payloads.



The Cymulate best practices for email gateway validation include a wide range of scenarios for:

- Malicious Links: Test for malicious links in the email body.
- Malicious Attachments: Test for emails containing malware embedded in attachments such as ransomware, worms, trojans, and exploits.
- Executable Payloads (Attachments): Test policy enforcement for handling emails with executable payloads like .exe, .com, .scr, file types.
- **Dummy Code Execution:** Simulate the possibility for real malicious code execution using dummy files.
- True File Type Detection: Test whether executable payloads with forged extensions are blocked.
- File Attachment Policies: Test policy enforcement for handling and blocking different file types.

Test the effectiveness of your organization's email gateway and policies by simulating different types of email-based threats, including ransomware, malware, worms, trojans, and exploits delivered through malicious links and attachments. These tests are production-safe and will not cause harm to your environment.

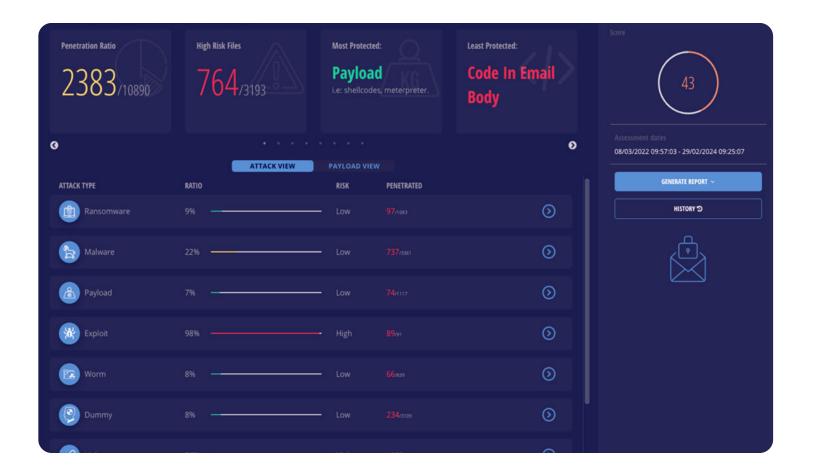






SECURITY VALIDATION BEST PRACTICES **Email Gateway**

Email is the **most frequently used** delivery method of attack for exploiting security weaknesses and email gateways are critical components in defending against emailbased threats with executable payloads.



Recommended Test Frequency	Weekly
	controls.
Test Scenarios	Over 10,000 test cases for the comprehensive validation of email gateway
	 File Type Policy
	 Code in Email Body
	True File Type
	• Links
	• Dummy
	 Payload
	• Exploit
	• Worm
Attack Types	Malware
Email Gateway	 Ransomware





SECURITY VALIDATION BEST PRACTICES Web Gateway

Securing web gateways is **crucial for** protecting organizations and blocking malicious websites and objectionable content from various web-based threats.

@ WEB GATEWAY R	EPOR	SUMMARY				REPORT SUMMARY
Inbound Penetration Ratio		Outbound Penetration Ratio	Most Protected:	Least Protected:		Score
810/1343		22679/121532	N/A	N/A		52
0					Ð	Assessment dates 31/03/2022 15:38:51 - 16/05/2024 02:52:59
АТТАСК ТҮРЕ	RATIO		RISK	ACCESSED		GENERATE REPORT ~
Phishing Outbound traffic					\odot	HISTORY D
C&C Outbound traffic			Medium		\odot	
Files Inbound Traffic			Medium		\odot	¢Ţ\$
Policy ⑦ Outbound traffic					\odot	
Files Policy ® Inbound Traffic					\odot	

The Cymulate best practices for web gateway security validation include broad spectrum assessments for:

Inbound Validation

- Payloads (Files): Test files that mimic malicious behavior of ransomware, worms, trojans, botnets, and other payloads downloaded over HTTPS.
- File Policies: Test for the detection of different file types like zip files, batch files, script files that the organization wishes to block users from downloading.

Outbound Validation

- Malicious Links: Test against a complete list of IP addresses and URLs associated with phishing and command and control activity.
- URL Category Policies: Test access to certain categories of objectionable websites and inappropriate content (gambling, pornography, terrorism, etc.) are blocked by the web gateway.

Malicious payload files used in the inbound validation tests should be detectable as malicious by the web gateway. These tests are production-safe and will not cause harm to your environment.





SECURITY VALIDATION BEST PRACTICES Web Gateway

Securing web gateways is **crucial for** protecting organizations and blocking malicious websites and objectionable content from various web-based threats.

@ WEB GATEWAY R	EPOR	SUMMARY				REPORT SUMMARY
Inbound Penetration Ratio		Outbound Penetration Ratio	Most Protected:	Least Protected:		Score
810/1343		22679/121532	N/A	N/A		52
0					Ø	Assessment dates 31/03/2022 15:38:51 - 16/05/2024 02:52:59
АТТАСК ТҮРЕ	RATIO		RISK	ACCESSED		GENERATE REPORT ~
Phishing Outbound traffic					\odot	HISTORY D
C&C Outbound traffic			Medium		\odot	
Files Inbound Traffic			Medium		\odot	¢Ţ\$
Policy ⑦ Outbound traffic					\odot	
Files Policy ® Inbound Traffic					\odot	

Recommended Test Frequency	Weekly
Test Scenarios	Over 1,300 malicious payloads and nearly 120,000 known malicious and objectionable websites to validate web gateway controls.
	Outbound • Phishing • Command and Control • URL Category Policies
Web Gateway Attack Types:	Inbound • Files • File Policies





SECURITY VALIDATION BEST PRACTICES Web App Firewall

Web application attacks have become increasingly common and pose a significant threat to organizations. With the rise of these threats, it is imperative that organizations implement robust security measures to protect their web applications.

Penetration Ratio	Least Protected Site		Most Protected Attack Type: WAF Bypass		Least Protected Atta Comman Injection	nd S	Score
SITE	DATE	• • • •		SCORE	PENETRATED	ø	GENERATE REPORT ~ HISTORY ର
https://ftp.celestica.com/webclient/L	03/05/2024 16:52:26	10%		26 /100		\odot	
https://misoft.com.vn	03/04/2024 09:24:42	77% —		43 /100		\odot	
http://76.74.113.199	08/02/2024 09:29:18	22% —		18 /100		\odot	
	22/07/2023 10:07:36	91%				\odot	

The Cymulate best practices for web application firewall assessments include:

- **SQL Injection**: Test for SQL injection attacks using crafted payloads to inject malicious database commands (SQL code) into an application on the web.
- **NoSQL Injection**: Test for attacks involving injecting code into commands for databases that don't use SQL queries, such as MongoDB.
- Command Injection: Test when an application passes unsafe usersupplied data, such as forms, cookies, or HTTP headers, to a system shell.
- XML Injection: Test for attacks that manipulate or compromise the logic of an XML application or service.
- File Inclusion: Test for crafted payloads that have the potential to lead to remote code execution on the web server hosting the application.

- Cross-Site Scripting (XSS): Test for the injection of client-side scripts into web pages viewed by other users, potentially enabling attackers to steal sensitive information.
- Server-Side Request Forgery (SSRF): Test for the SSRF vulnerability that allows an attacker to induce a serverside application to make HTTP requests to an arbitrary domain of the attacker's choosing.
- Path (Directory) Traversal: Test for access to files and directories stored outside the web root folder.
- WAF Bypass: Test for obfuscation techniques being used to disguise malicious payloads and bypass the web app firewall.







SECURITY VALIDATION BEST PRACTICES Web App Firewall

Web application attacks have become increasingly common and pose a significant threat to organizations. With the rise of these threats, it is imperative that organizations implement robust security measures to protect their web applications.

Penetration Ratio	Least Protected Site		Most Protected Attack Type: WAF Bypass		Least Protected Atta Comman Injection	nd S	Score
SITE	DATE	• • • •		SCORE	PENETRATED	ø	GENERATE REPORT ~ HISTORY ର
https://ftp.celestica.com/webclient/L	03/05/2024 16:52:26	10%		26 /100		\odot	
https://misoft.com.vn	03/04/2024 09:24:42	77% —		43 /100		\odot	
http://76.74.113.199	08/02/2024 09:29:18	22% —		18 /100		\odot	
	22/07/2023 10:07:36	91%				\odot	

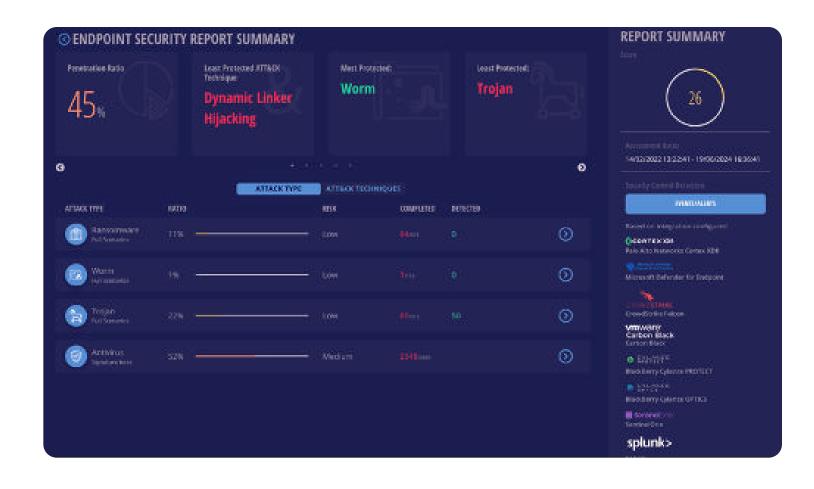
Web App Firewall Attack Types:	 File Inclusion Command Injection SQL / NoSQL Injection XML Injection Cross-Site Scripting (XSS) Server-Side Request Forgery (SSRF)
	 Path Traversal WAF Bypass
Test Scenarios	Over 7,000 malicious payloads used to validate web application firewall controls.
Recommended Test Frequency	Weekly





SECURITY VALIDATION BEST PRACTICES **Endpoint Security**

Endpoint security controls are **critical to** stopping breaches, especially malicious payloads that manage to evade detection by the email and web gateways and the web app firewalls.



Endpoint security solutions include both antivirus (Known Malicious File) and EDR: Endpoint Detection & Response (Malicious Behavior). The Cymulate best practices for endpoint security validation cover both antivirus and EDR solutions with:

- Known Malicious Files: Test for known malware samples written to disk without execution to validate the antivirus response.
- Malicious Behaviors: Test for attacks that simulate adversary behaviors using common malware types (ransomware, worms, trojans) and execution methods.

Plus:

- **Rootkits**: Test for unusual system behaviors that likely indicate the existence of a rootkit (collection of malicious payloads) to check the integrity of system files.
- DLL Side-Loading: Test for the misuse of trusted applications used by attackers to load malicious versions of application DLLs.
- **Code Injection**: Test for the injection of malicious code into input fields of trusted applications running on endpoints.

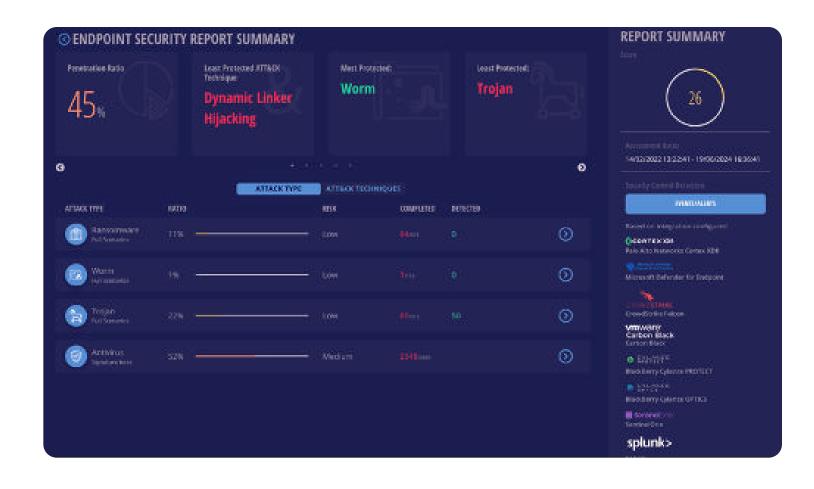






SECURITY VALIDATION BEST PRACTICES **Endpoint Security**

Endpoint security controls are **critical to** stopping breaches, especially malicious payloads that manage to evade detection by the email and web gateways and the web app firewalls.



Endpoint Security Attack Types:	Known Malicious Files Antivirus
	Malicious Behaviors • Ransomware • Worm • Trojan
Test Scenarios	Over 4,000 known malicious files and 1,000 malicious behavior test scenarios across 60 MITRE ATT&CK techniques for the validation of endpoint security controls.
Recommended Test Frequency	Weekly





Cloud has become the latest frontier in the threat landscape as threat actors turn their attention to exploiting cloud platforms. Common cloud misconfigurations are the root cause of many cloud data breaches, requiring continuous validation given the very dynamic nature of a cloud environment.

inpat:		Conception (- PSANDON Z General VEREATTACK -				the with the	cholques the	e eeb ooduniquisi	laport
Annua Access Teoringser	biecalas Historiaco	Rectania Distributio	t ta lege Disalation	Certains e loss tans 26 rectar ques	Constant at Access Si costantars (Decivera Statement	Labrezh Movement Restrictare	Loberton Texenteer	lations Someo	Contraction point Contraction Of the Interpole	krigar) (24eminik.up
Drive-by Competence	Command and Scripturic Mangarites	Arement Mar publices	Abuss Creation Creation Creation	Abate Graction Londons Martinetter	1.122	Accessed University	The interview of Security Services	Adversarie re Die Vielale	Automateor Lafitration	Application Layer Protocol	Arm and Receipt Reviewed
Foginal Nation Noting Applications	Conseiner Administration Centralist	arn jaos	Access listen	Anne of the later Manual allocations	No. 1970	epolicition Vindew Deservey	invest Specified damp	due Mari Concerne Data	Sinta Franker Steellinds	orterreadely	Flass Flassing effect
Frontie Renies Services	Deploy Calculator	Rosseriegen Alsonart Resertes	Accessor Managedations	UTS(sta	Credentine Hom Perris and States	internet Information Desirvery	diamonal Tapis Triancales	лаво сарали	Portificantian Outer Alternantian Protocoli	Terra Makonaken	Dass Tempped for Equat
WAT INC	Exploitation for Client Execution	Andorsegun Indelestion Strate	Boon or Legan Autopolom	Lestinger Lynachere	sopication to: Craterial Action	doud mhannaan bhanaiy	Persola larges Santos Huadang	Automoted Collecter	Estimation (how)	Dynamic Resolution	eses Mantosiacon
Suppry Chain Composition	enal-Anorem Communication	Compromise Clamics of work Dimory	Book or Legan Intel Lation	Lapity Constants	Horge the b One downals	doud Swince Discovery	fornatio Services	Capitored (here	Extinuation Over Direct Notice a b	Encrypted channel	i Delacereri
teacted Referencesings	Halland N	Orbaic Artoviel	Crasses: Grasses: Goodby Spream	Line ware	tys: Space	Good Steenge Object Discovery	Saltura V Deposite ent Toole	Deles Scoped	Mediani Cofficiences Corp.	Engrade Tools Transfer	Desk Wige
Acid Accounts	Strecture Tencipie	Creater or Most ly by Chern Process	Process Description Folicy Machineseton	Estavia folicy Vacilication	Roberty Automotication Process	Container Just Behauste Déscriery	turni selavad Doetani	Colo Poel Cross merge	Reyson deraum	Hon Approach	Endpoint Decial of Service-
	sonpany	Trend Trigger ed Trend Zolger	Twent to they	forecition Curvelnais	Valistador Autorization Thereaster	Decide Tract Decivery	Use Alternation Automotione Harvitat	Ceta Iron Configuration Read-story	Over Ave Service	Non-Statement Part	teri biç System Birtineş
	Serverien Recollect	Notertal Rendertanteurs	Lechtgred	Baydo tatico for Dafar sa Guarion	New A Willing	File and Deleting		Carlos frame Index fronte ens. Representacións	TSJAPALI	Protocol Turnelleng	Notwark Con all of Service
8	shared stodules	Tet	Secure 1	Deard Read	CS Crastendal Dari pino	Decivery States 76 by	8 I	Geta from Local	Therefore Gales so Globald Accounts	1 Vices	Report for Hitselfing

The Cymulate best practices for cloud security validation use a wide variety of tactics and techniques across the Cloud MITRE ATT&CK framework, for example:

- Initial Access: Exploit public-facing applications, misuse of valid accounts, public / anonymous access granted.
- **Execution**: Cloud admin command execution, suspicious file downloads terminate processes, create containers.
- Persistence: Account manipulation, account takeover, exploit useradd.
- Privilege Escalation: Create highprivilege roles, create privileged containers, host path mount.

- Defense Evasion: Clear history files, delete events, disable logging, create cloud instance.
- Credential Access: Credential dumping, list secrets, access credentials in config files.
- Discovery: Discover cloud infrastructure, discover cloud groups, remote system discovery, host network access.
- Lateral Movement: Remote service abuse, deploy software tools.

Cloud workloads can also be validated using Cymulate, for example Windows virtual machines (VMs) running in cloud can be validated using the Endpoint Security module and a cloud web application firewall can be validated using the Web Application Firewall module in the Cymulate platform.





Cloud has become the **latest frontier in the** threat landscape as threat actors turn their attention to exploiting cloud platforms. Common cloud misconfigurations are the root cause of many cloud data breaches, requiring continuous validation given the very dynamic nature of a cloud environment.

inpat:		Conception (- PSANDON Z General VEREATTACK -				the with the	cholques the	e eeb ooduniquisi	laport
Annua Access Teoringser	biecalas Historiaco	Rectania Distributio	t ta lege Disalation	Certains e loss tans 26 rectar ques	Constant at Access Si costantars (Decivera Statement	Labrezh Mesonani Restrictari	Loberton Texenteer	lations Someo	Contraction point Contraction Of the Interpole	krigar) (24eministra
Drive-by Competence	Command and Scripturic Mangarites	Aremost Mar polatere	Abuss Creation Creation Creation	Abate Graction Londons Martinetter	1.122	Accessed University	The interview of Security Services	Adversarie re Die Vielale	Automateor Lafitration	Application Layer Protocol	Arm and Receipt Reviewed
Foginal Nation Noting Applications	Conseiner Administration Centralist	arn jaos	Access listen	Anne of the later Manual allocations	No. 1970	epolicition Vindew Deservey	invest Specified damp	due Mari Concerne Data	Sinta Franker Steellinds	orterreadely	Flass Flassing effect
Frontie Renies Services	Deploy Calculator	Rosseriegen Alsonart Resertes	Accessor Managedations	UTS(sta	Credentine Hom Perris and States	broader Informatie Deservery	diamonal Tapis Triancales	лаво сарали	Portificantian Outer Alternantian Protocoli	Terra Makonaken	Dass Tempped for Equat
WAT INC	Exploitation for Client Execution	Andorsegun Indelestion Strate	Boon or Legan Autopolom	Lestinger Lynachere	sopiositios to: Crodencial Acodo	doud mhannaan bhanaiy	Persola larges Santos Huadang	Automoted Collecter	Estimation (how)	Dynamic Resolution	tran Mantosiacon
Suppry Chain Composition	enal-Anorem Communication	Compromise Clamics of work Dimory	Book or Legan Intel Lation	Lapity Constants	Horge the b One downals	doud Swince Discovery	fornatio Services	Capitored (here	Extinuation Over Direct Notice a b	Encrypted channel	i Delacereri
teacted Referencesings	Halland N	Orbaic Arto, el	Crasses: Grasses: Goodby Spream	Line ware	tys: Space	Good Steenge Object Discovery	Saltura V Deposite ent Toole	Deles Scoped	Mediani Cofficiences Corp.	Engrade Tools Transfer	Desk Wøre
Acid Accounts	Strecture Tencipie	Creater or Most ly by Chern Process	Process Description Folicy Machineseton	Estavia folicy Vacilication	Roberty Automotication Process	Container Just Behauste Déscriery	turni selavad Doetani	Colo Poel Cross merge	Reyson deraum	Hon Approach	Endpoint Decial of Service-
	sonpany	Terral Tragger est Terral Tragger est	Twent to they	forecition Curvelnais	Valistador Autorization Thereaster	Decide Tract Decivery	Use Alternation Automotione Harvitat	Ceta Iron Configuration Read-story	Over Ave Service	Non-Statement Part	teri biç System Birtineş
	Serverien Recollect	Notertal Rendertanteurs	Lechtgred	Baydo tatico for Dafar sa Guardon	New A Willing	File and Deleting		Carlos frame Index fronte ens. Representacións	TSJAPALI	Protocol Turne Heng	Notwark Con all of Service
8	shared stodules	Tet	Secure 1	Deard Read	CS Crastendal Dari pino	Decivery States 76 by	8 I	Geta from Local	Therefore Gales so Globald Accounts	1 Vices	Report for Hitselfing

CONTROL TYPE	SECURITY CONTROL	TESTED LAYER						
Security Control	WAF	Business Application	Business Application	Business Application				
Container & Kubernetes	CWPP, CNAPP,	App Binaries & Libraries	App Binaries & Libraries	App Binaries & Libraries				
Security Controls	SIEM, FW/IPS	Container Engine / Kubernetes						
Cloud Workloads Security Controls	EDR, WG, SEG, SIEM, DLP, FW/IPS	Virtual Machines / Operating Systems / Container Host						
Cloud Infrastructure Security Controls	CSPM, CNAPP, SIEM	Infrastructure						

Cloud Applications

Validate using test scenarios for:

• Web App Firewall (WAF)

Containers & Kubernetes

Validate using test scenarios for:

- Cloud Workload Protection Platform (CWPP)
- Cloud-Native Application Protection Platform (CNAPP)
- Cloud-native container and Kubernetes security controls (Azure Cloud Defender, AWS GuardDuty, GCP Command Center)
- Security Information and Event Management (SIEM)





Cloud has become the latest frontier in the threat landscape as threat actors turn their attention to exploiting cloud platforms. Common cloud misconfigurations are the root cause of many cloud data breaches, requiring continuous validation given the very dynamic nature of a cloud environment.

inpat:		Conception (Constants	werk MEREAT	805	in take still t	the with the	cholques the	e eeb ooduniquisi	laport
Annua Access Teoringser	biecalas Historiaco	Rectania Distributio	t ta lege Disalation	Certains e loss tans 26 rectar ques	Constant at Access Si costantars (Decivera Statement	Labrezh Mesonani Restrictari	Loberton Texenteer	lations Someo	Contraction point Contraction Of the Interpole	krigar) (24eministra
Drive-by Competence	Command and Scripturic Mangarites	Aremost Mar polatere	Abuss Creation Creation Creation	Abate Graction Localization	1.122	Accessed University	The interview of Security Services	Adversarie re Die Vielale	Automateur Lafitindisen	Application Layer Protocol	Arm and Receipt Reviewed
Foginal Nation Noting Applications	Conseiner Administration Centralist	arn jaos	Access listen	Anne of the later Manual allocations	No. 1970	epolicition Vindew Deservey	invest Specified damp	due Mari Concerne Data	Sinta Franker Steellinds	orterreadely	Flass Flassing effect
Frontie Renies Services	Deploy Calculator	Rosseriegen Alsonart Resertes	Accessor Managedations	UTS(sta	Credentine Hom Perris and States	internet Information Desirvery	diamonal Tapis Triancales	лаво сарали	Portificantian Outer Alternantian Protocoli	Terra Makonaken	Dass Tempped for Equat
WAT INC	Exploitation for Client Execution	Andorsegun Indelestion Strate	Boon or Legan Autopolom	Lestinger Lynachere	sopiositios to: Crodencial Acodo	doud mhannaan bhanaiy	Persola larges Santos Huadang	Automoted Collecter	Estimation (how)	Dynamic Resolution	tran Mantosiacon
Suppry Chain Composition	enal-Anorem Communication	Compromise Clamics of work Dinory	Book or Legan Intel Lation	Lapity Constants	Horge the b One downals	doud Swince Discovery	fornatio Services	Capitored (here	Extinuation Over Direct Notice a b	Encrypted channel	i Delacereri
teacted Referencesings	Halland N	Orbaic Artoviel	Crasses: Grasses: Goodby Spream	Line ware	tys: Space	Good Steenge Object Discovery	Saltura V Deposite ent Toole	Deles Scoped	Mediani Cofficiences Corp.	Engrade Tools Transfer	Desk Wøre
Acid Accounts	Strecture Tencipie	Creater or Most ly by Chern Process	Process Description Folicy Machineseton	Estavia folicy Vacilication	Roberty Automotication Process	Container Just Behauste Déscriery	turni selavad Doetani	Colo Poel Cross merge	Reyson deraum	Hon Approach	Endpoint Decial of Service-
	sonpany	Terral Tragger est Terral Tragger est	Twent to they	forecition Curvelnais	Valistador Autorization Thereaster	Decide Tract Decivery	Use Alternation Automotione Harvitat	Ceta Iron Configuration Read-story	Over Ave Service	Non-Statement Part	teri biç System Birtineş
	Serverien Recollect	Notertal Rendertanteurs	Lechtgred	Baydo tatico for Dafar sa Guardon	New A Willing	File and Deleting		Carlos frame Index fronte ens. Representacións	TSJAPALI	Protocol Turnelleng	Notwark Con all of Service
8	shared stodules	Tet	Secure 1	De and	CS Crastendal Dari pino	Decivery States 76 by	8 I	Geta from Local	Therefore Gales so Globald Accounts	1 Vices	Report for Hitselfing

Cloud Workloads

Validate using test scenarios for:

- Endpoint Detection and Response (EDR)
- Web Gateway (WG)
- Secure Email Gateway (SEG)
- Security Information and Event Management (SIEM)
- Data Loss Prevention (DLP)
- Firewall (FW) / Intrusion Prevention System (IPS)

Cloud Infrastructure

Validate using test scenarios for:

- Cloud Logs
- Native Cloud Security Tools
- Cloud Security Posture Management (CSPM)
- Cloud Native Application Protection Platform (CNAPP)
- Security Information and Event Management (SIEM)







Cloud has become the latest frontier in the threat landscape as threat actors turn their attention to exploiting cloud platforms. Common cloud misconfigurations are the root cause of many cloud data breaches, requiring continuous validation given the very dynamic nature of a cloud environment.

impat:		T leak 3		2 Octorines	sout MIREAT	ACK .	a tak at r	the will be the	cholouse the	r rub-techniques	lopan
Andar Access Technolog	l'inclue Herreco	Reciterin Obtesio	Frankrys Ditabilion	Cedence iversion Xinche quot	Create attait Access Si contestada	Discover) Strategics	Laterat Movement Etatinitari	Trakston Normon	Saltanan Fisikasa	Freedomatic and Contract Ut to tempore	brigan) (2007/00.00
Delas-by Compension	Communic of 8 Scripting Interpreter	Accurry Margadates	Abate Cristian Castion Monte as	Abace Develop Losteral Manhantera	Ar manyaha Na tanàn	Accession Descently	Facilitation of Secult classifies	Adventancere Der Vol die	Automation Talibridian	Application Layer Protocol	Armani Arcent Fernand
Ngang Ngan Ngang Ngang Ngang	Conseiner Administration Carlintano	arm juos	Anness Kolton Mangadatara	Assess To her Manparistan	NAN KEW	epolicitan Vindew Deservey	leverad Specified decay	die Man Official Data	Cata Foundat Size Canalas	orteercadeg	Date Date and the
lares Servers	Deploy Carolide or	Rosterlagen Risoter Presetter	Acenter Deservations	LITS (sta	Credensian Inom Previsional Status	browser Informeter Desirety	daroral Tast Transfer	лаво сарале	Fontinarian Oyan Alternarian Fridadi	Terra Vibili conactina	Date Frenyther for Impact
PLATING.	Exploitation for Client Descubers	enstornagen indelesten Stres	Door on Legen Autopices	Lest'oran Incardiore	representation text Ore deviced Areas	doud nifettiscours bitoriory	Konsule tervise Sector Husting	Accessed Collector	Estimation Over CE Descriet	bynamic Resolution	esa menjalaran
Suppry Chain Comprise	enter-Artocata Commune colore	Compliantice ClanicSoftware Unory	Boot or Legan Intelligitor	Deploy Container	Horge theo Oredonials	doud Swince Discovery	Formation Surveying	Ciplicard Data	Extinue an Over Diver	Encrypted Channel	II Delacereri
lausteri Roletooimip	Nation 27	Orbele Artoviel	Cristians Grant Spream	Line wares	ligne Capacity	Chool Manage Chool Difference	nactura o Deployment Texas	Ovice Scopeni	Medium Defitiration Over	Legrens Tool Transfer	Dex Mpc
Acite Accounto	schwiszen Tenergob	Creater or Modify System Process	Process Decresie Roley MacHaster	Denvis Policy Vacilitation	Roberty Automotication Process	containes and Bergause Discovery	tion served Deep 19	Gala Iron Gloud merge	Rivstof defatan	Non Approximite Logier Protocole	Enclosed Decision of Second
-	Scripeing	See al Tragger est See Comp	Except to these	forecition Consideration	Makstean Autoriazia Therestean	Devictor Trust Descrivery	Use Alternate Activitation Harvitat	Geta from Configuration Reportiony	Over Alte Service School And	Nor-Scinibrit Port	teri biç Syrojav Referetiy
8	Serveriens Bassailles	Recentler Recollection Notes	Lens Traggered	Replaciation for Defense Constant	Alexandr Teolfrig	File (m) Deleting	1	Cura fran Internation Reportation	TNJKPET	Protocol Two long	Notwork Contail of Revisor
	shared stodules	1000	Execution	Figured	OS Optionda I	Destroyy State 76 by		Constron Inst	Transfer data so Glaud Account		Repol, to: Hij sching

Cloud Security Attack Types:	 Assume Breach Kubernetes for Azure, AWS, GCP
Test Scenarios	Over 40 assume breach with high privilege activity and 29 Kubernetes templates with 400+ executable scenarios to validate different components of a cloud environment.
Recommended Test Frequency	Weekly







SECURITY VALIDATION BEST PRACTICES **Data Exfiltration**

Data exfiltration controls are **one of the last** lines of defense in stopping a data breach. Organizations need to be able to protect sensitive files and data from leaving their organization and being held for ransom by threat actors.

⊙ DATA EXFILTRATION R	EPORT SUMMARY				REPORT SUMMARY
Exfiltration Ratio	High Risk Attacks	Most Protected Phrase: Custom - Internal Doc	Least Protected Masterca Credit Ca	nrd	Assessment Score
0				٥	01/12/2022 12:06:41 - 07/05/2024 05:51:21
АТТАСК ТҮРЕ	PHRASES	RISK	EXFILTRATED		GENERATE REPORT 🛩
Gmail + Append	0%	Low		\odot	C HISTORY D
HTTP Exfiltration		High		⊘	<u> </u>
HTTPS Exfiltration				⊘	
DNS				\odot	
DNS Tunneling	2%	Low		\odot	
ICMP Tunneling	57%	Medium		⊘	
Email	0%	Low	O 7307	\odot	

The Cymulate best practices for data exfiltration assessments cover a range of data and file transfer methods including:

- **Email**: Test if sensitive information can be transmitted through the enterprise email system.
- Network Protocols: Test if sensitive data can be transmitted over network protocols like Telnet, SFTP, TCP (Open Ports).
- HTTP(S): Test if HTTP or HTTPS can be used to inject sensitive data into HTTP request headers (or HTTPS encrypted) and sent to a remote server.
- DNS: Test if controlled DNS servers or tunneling through public DNS servers can be used to inject sensitive data into a DNS request.

- Cloud Hosted Services: Test if sensitive files can be uploaded to external file hosting services like Gitlab, Github, Google Drive, Google Storage, AWS S3 Buckets, Azure Blobs, MS One Drive.
- Collaboration Applications: Test if sensitive files can be sent through applications used for collaboration like MS Teams, Slack.
- **Physical Devices**: Test if sensitive information can be copied to removable media devices like USB flash drives.

Test the effectiveness of your organization's data loss prevention capabilities and policies by simulating different types of transfer methods for data and files that are tagged as sensitive and confidential.





SECURITY VALIDATION BEST PRACTICES Data Exfibration

Data exfiltration controls are **one of the last lines of defense** in stopping a data breach. Organizations need to be able to protect sensitive files and data from leaving their organization and being held for ransom by threat actors.

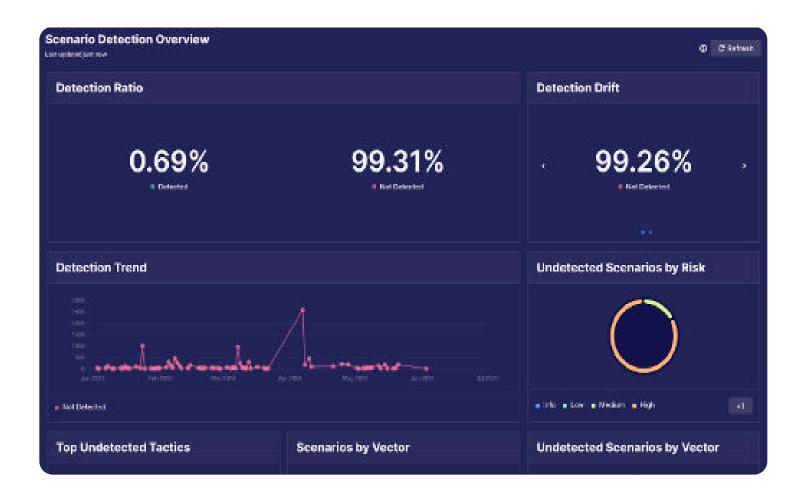
⊙ DATA EXFILTRATION R	EPORT SUMMARY				REPORT SUMMARY
Exfiltration Ratio	High Risk Attacks	Most Protected Phrase: Custom - Internal Doc	Least Protected Masterca Credit Ca	nrd	Assessment Score
0				٥	01/12/2022 12:06:41 - 07/05/2024 05:51:21
АТТАСК ТҮРЕ	PHRASES	RISK	EXFILTRATED		GENERATE REPORT 🛩
Gmail + Append	0%	Low		\odot	C HISTORY D
HTTP Exfiltration		High		⊘	<u> </u>
HTTPS Exfiltration				⊘	
DNS				\odot	
DNS Tunneling	2%	Low		\odot	
ICMP Tunneling	57%	Medium		⊘	
Email	0%	Low	O 7307	\odot	

Recommended Test Frequency	Weekly
	data from your environment.
Test Scenarios	Over 5,800 methods tested for exfiltrating
	 SFTP, Telnet
	 Gitlab, Github
	 Slack
	 MS Teams / OneDrive
	 Cloud AWS /Azure / Google
	Open Ports
	Removable Device
	ICMP Tunneling
	 DNS, DNS Tunneling
	 Browser HTTP / HTTPS
Attack Types:	 HTTP / HTTPS
Data Exfiltration	 Email, Gmail + Append



SECURITY VALIDATION BEST PRACTICES **SIEM Observability**

SIEM event logging and observability is a critical control for the correlation and alerting of malicious behaviors.



The Cymulate platform integrates with your SEIM to validate that events are captured in the SIEM and alerts are generated to notify security analysts, threat hunters, and incident responders of the threat activity taking place. The Cymulate best practices for validating SIEM observability include test cases from:

- Immediate Threats
 - Known malicious files written to disk
 - Email attachments with malicious code execution
 - Outbound traffic to a malicious link
 - Code execution file downloads from trusted sources
- Endpoint Security Detections
- Cloud Security Detections
- Other Advanced Scenarios

Sigma Rules

The Cymulate platform provides security analysts with Sigma Rules and enables the analyst to generate detection rules for their specific SIEM technology. These rules can be copied from the Cymulate platform into your SIEM configuration to enhance detection and alerting of malicious behaviors.

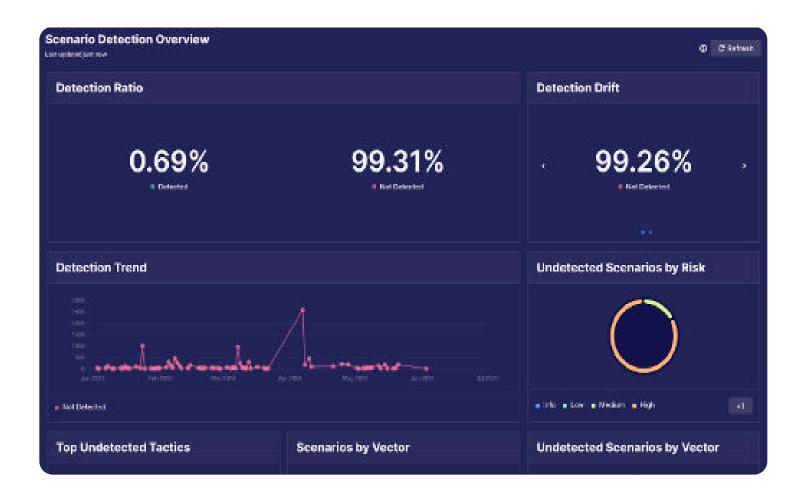






SECURITY VALIDATION BEST PRACTICES **SIEM Observability**

SIEM event logging and observability is a critical control for the correlation and alerting of malicious behaviors.



Advanced Scenarios for SIEM Observability:	 Immediate Threats Assessments Endpoint Security Assessments Advanced Scenarios Assume Breach: SIEM Validation (Cloud)
Test Scenarios	Over 500 templates used to evaluate SIEM effectiveness to detect threat activities.
Recommended Test Frequency	Weekly





Validate Controls

- Email Gateway
- Web Gateway
- Web App Firewall
- Endpoint Security
- Cloud Security
- Data Exfiltration
- SIEM Observability

Validate Threats

Cymulate Best Practices



• Immediate Threats • Lateral Movement • Full Kill-Chain Attacks



- SOC Exercises
- Red Team Exercises





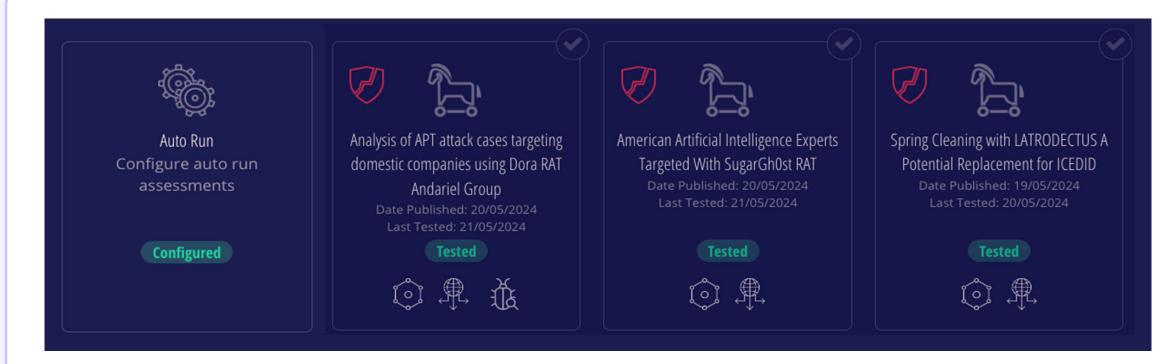
SECURITY VALIDATION BEST PRACTICES

Threat actors are constantly devising new tactics and techniques to exploit the latest vulnerabilities and gain unauthorized access to your network. **These new threats emerge daily** and represent an immediate threat to the security controls of your organization.

American Artificial Intelligence Ex 21/05	05/2024 02:52:06 75		 RATIO 314	vectors ©ः ऱ्रिः	CVE	Ð	GENERATE REPORT ~
Analysis of APT attack cases targe 21/05				<u>ي</u> ة. ©			À
Analysis of APT attack cases targe 21/05	05/2024 14:42:15 33	396					
American Artificial Intelligence Ex 21/05				© .¶.			
	05/2024 14:42:00 33	3%		<u>ي</u> ة. (ج			
	05/2024 14:31:33 20)%		© .¶.			
Spring Cleaning with LATRODECT 20/05	05/2024 14:42:00 50	<u> </u>		© 🤋			
ViperSoftX Uses Deep Learning-b 19/05	35/2024 14:42:00 67	7%		@ . R .			
Cullin Ransomware as a service 16/05	05/2024 14:42:00 50	9%		<u>ې چ</u>			
CRUST Shellcode Loader Uses GoTo 15/05	05/2024 14:42:00 56	5%		ê î 🤻			

The Cymulate best practices for security validation of immediate threats includes **Auto Run** for validation tests for all new threats and notifications through email when you have exposure to a threat.

- Emerging Threats: Test for exposure to the latest immediate threats identified by trusted cybersecurity community threat intelligence sources.
- Attack Vectors: Tests should include validation of your email gateway, web gateway, and endpoint security to determine if compensating controls can detect and block the attack.







SECURITY VALIDATION BEST PRACTICES

Threat actors are constantly devising new tactics and techniques to exploit the latest vulnerabilities and gain unauthorized access to your network. **These new threats emerge daily** and represent an immediate threat to the security controls of your organization.

American Artificial Intelligence Ex 21/05	05/2024 02:52:06 75		 RATIO 314	vectors ं ऱ्रि	CVE	Ð	GENERATE REPORT ~
Analysis of APT attack cases targe 21/05				<u>ي</u> ة. ©			À
Analysis of APT attack cases targe 21/05	05/2024 14:42:15 33	396					
American Artificial Intelligence Ex 21/05				© .¶.			
	05/2024 14:42:00 33	3%		<u>ي</u> ة. (ج			
	05/2024 14:31:33 20)%		© .¶.			
Spring Cleaning with LATRODECT 20/05	05/2024 14:42:00 50	<u> </u>		© 🤋			
ViperSoftX Uses Deep Learning-b 19/05	35/2024 14:42:00 67	7%		@ . R .			
Cullin Ransomware as a service 16/05	05/2024 14:42:00 50	9%		<u>ې چ</u>			
CRUST Shellcode Loader Uses GoTo 15/05	05/2024 14:42:00 56	5%		ê î 🤻			

Recommended Test Frequency	Daily (Auto Run)
Test Scenarios	New emerging threats are added to the Cymulate platform daily.
Immediate Threats Intelligence	 Ransomware Group Threats APT Advanced Attacks Other Threat Group Scenarios



SECURITY VALIDATION BEST PRACTICES Lateral Movement

The goal of many threat actors is to gain access and move laterally across your network until they find systems and data of value (aka your crown jewels).

O HOPPER REPORT SU	JMMARY						Score
Most Protected Target: CRWDSTRK-W2016	Least Prote	cted Target:	Most Common Spre	ead Method:	P	ost Common Attack Method: Pass The Token	27 GENEBATE REPORT ~
9						Ø	HISTORY D
TARGET (17)	DATE	WORKSTATIONS	RISK	HOPPED	SCORE		
TESTPC (NT AUTHORITY\S	28/03/2024 23:09:07	0%	Low			୍ଦ 🕁 📀	670
JUMPSERVER (NT AUTHORI	25/03/2024 23:22:05	0%	Low			다 🍲 📀	
WIN11-DAVIDK (AzureAD\	21/02/2024 11:04:35	0%	Low			수 쌉 📀	
EC2AMAZ-3BHK6IA (NT AU	20/02/2024 12:21:13	0%	Low			රු සු 📀	
ACC-WINDOWS (NT AUTH	05/12/2023 08:57:30	0%	Low			රු 🕁 📀	
WIN-DAVIDK (NT AUTHORI	04/12/2023 10:38:17	0%	Low			4 🗳 📀	
SITE-WIN2016-2 (SITE-WIN	31/10/2023 13:11:37	0%	Low			ශ ස ()	

The Cymulate best practices for lateral movement test your network segmentation and privilege management using:

Attack Methods simulate techniques used to obtain credentials and compromise systems including:

- Pass the Hash
- Brute Force
- Password Spraying
- Keberoasting
- Credentials Harvesting
- Verify SSH/SFTP Access
- Steal Local Admin Passwords
- LLMNR/NBT-NS Poisoning and Relay

Spreading Methods simulate methods used to traverse the network and gain access to systems and data including:

- SMB
- DCOM
- SSH
- WinRM
- RPC
- WMI
- RDP
- RDP Port
- MSSQL

The focus of these test scenarios is to test your internal network configuration and segmentation policies against the various techniques and methods that attackers use to spread within a network and gain control over additional systems. Lateral movement is often achieved using evasion techniques and privilege escalation to disguise as legitimate users with the objective of reaching your critical IT assets.





SECURITY VALIDATION BEST PRACTICES Lateral Movement

The goal of many threat actors is to gain access and move laterally across your network until they find systems and data of value (aka your crown jewels).

O HOPPER REPORT SUM	/ MARY						Score
Most Protected Target: CRWDSTRK-W2016	Least Protec		Most Common Spre	ad Method:	P	ost Common Attack Method: ass The oken	27 GENERATE REPORT ~
0						Ð	HISTORY ©
TARGET (17) DAT	TE	WORKSTATIONS	RISK	HOPPED	SCORE		
TESTPC (NT AUTHORITY'S 28/	/03/2024 23:09:07		Low			다 쌀 📀	6 70
JUMPSERVER (NT AUTHORI 25/	/03/2024 23:22:05	0%	Low			4 de 🕑	
WIN11-DAVIDK (AzureAD\ 21/	/02/2024 11:04:35		Low			다 쌀 📀	
EC2AMAZ-3BHK6IA (NT AU 20/	/02/2024 12:21:13	0%	_ Low			다 쌉 ()	
ACC-WINDOWS (NT AUTH 05/	/12/2023 08:57:30	0%	_ Low			ශ සු 📀	
WIN-DAVIDK (NT AUTHORI 04/	/12/2023 10:38:17	0%	Low			୍ଦ 🗳 📀	
SITE-WIN2016-2 (SITE-WIN 31/	/10/2023 13:11:37	0%	Low	0,0	0 /100	다 쌉 📀	

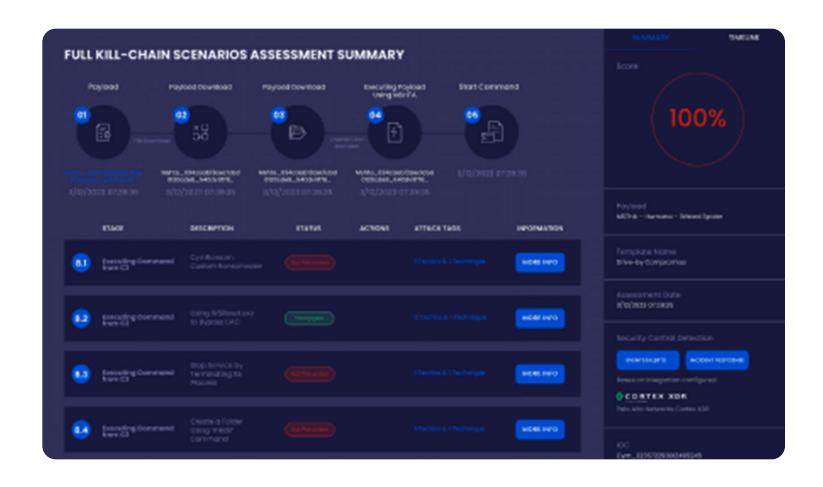
Hopper Attack Types	 Pass the Hash (Domain/Local)
	Offline Brute Force
	 Password Spraying
	 Kerberoasting
	 3rd Party Credentials Harvester
	 Verifiy SSH/SFTP Access
	 Steal LAPS Passwords
	 LLMNR/NBT-NS Poisoning and Relay
Test Scenarios	Choose from 8 attack methods and 9
	spreading methods to validate network
	segmentation and privilege management.
Recommended	Weekly
Test Frequency	





SECURITY VALIDATION BEST PRACTICES **Full Kill-Chain Attacks**

Full kill-chain attacks simulate Advanced Persistent Threat (APT) groups and the sophisticated techniques they use to gain access to a network and remain **undiscovered** for extended periods of time.



Cymulate best practices for full kill-chain attack validation include example scenarios for specific threat groups like:

Full Kill-Chain Scenarios (Examples)

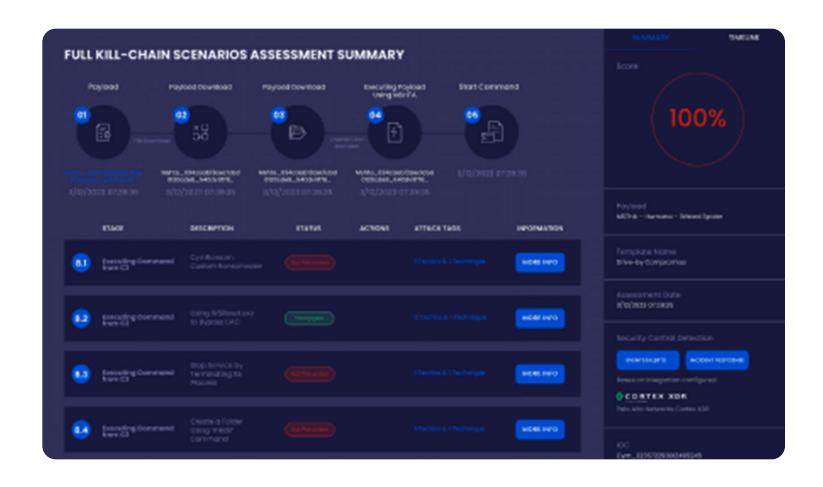
- Cobalt Group (APT29): Simulation of an APT attack technique that sends email to deliver Cobalt Strike payloads to download and create a scheduled task that runs a remote key ransomware to encrypt files.
- OceanLotus (APT32): Simulation of an APT attack technique that sends email with a malicious link that downloads a MSHTA application that executes a trojan to exfiltrate data.
- Refined Kitten (APT33): Simulation of an APT attack technique using excel with an embedded macro to establish persistence and use LaZagne tool to extract credentials.
- Lazarus Group (APT38): Simulation of an APT attack technique that downloads a malicious DLL file that executes a trojan to exfiltrate data.





SECURITY VALIDATION BEST PRACTICES **Full Kill-Chain Attacks**

Full kill-chain attacks simulate Advanced Persistent Threat (APT) groups and the sophisticated techniques they use to gain access to a network and remain **undiscovered** for extended periods of time.



Full Kill-Chain Scenarios:	 APT Templates
Test Scenarios	Choose from over 25 full kill-chain templates for real-world APT threat actors or create custom scenarios using hundreds of prebuilt delivery methods, payload structures, execution methods, and compiled scenarios.
Recommended Test Frequency	Monthly





Validate Controls

- Email Gateway
- Web Gateway
- Web App Firewall
- Endpoint Security
- Cloud Security
- Data Exfiltration
- SIEM Observability

Validate Threats

Cymulate Best Practices

• Immediate Threats Lateral Movement • Full Kill-Chain Attacks

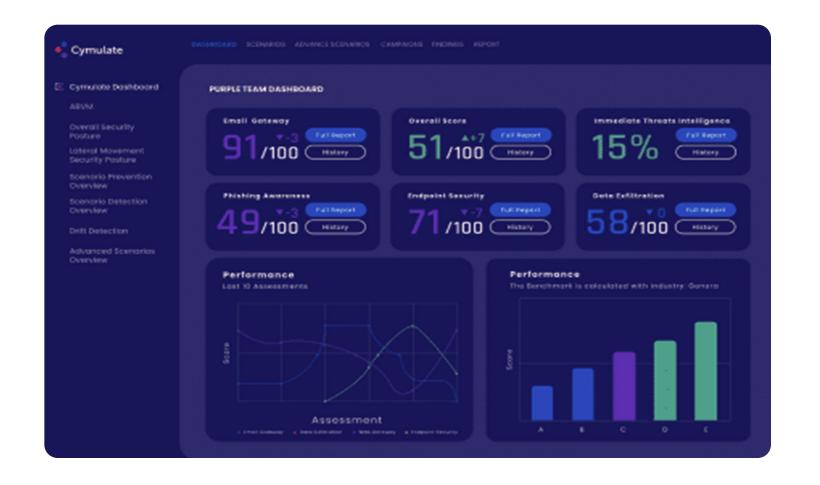
Validate Response

- SOC Exercises
- Red Team Exercises



SECURITY VALIDATION BEST PRACTICES **SOC Exercises**

SOC exercises are used to validate security processes, policies, and incident response playbooks using full kill-chain scenarios for common threat group attacks.



These red team / blue team exercises go beyond traditional tabletop exercises with production-safe simulations of real-life attack scenarios in a purple teaming exercise that validates advanced APT scenarios. Cymulate best practices for SOC validation exercises include examples of highly prevalent threat groups using specific attacks like:

Full Kill-Chain Scenarios (Examples)

- Lockbit 2.0: An advanced and highly effective ransomware variant that exfiltrates sensitive data and encrypts files, making them inaccessible without a decryption key.
- **Qakbot**: A highly sophisticated banking trojan designed to steal banking credentials and financial data.
- **Ryuk**: A sophisticated ransomware simulation that has been involved in numerous high-profile cyberattacks targeting critical sectors like healthcare, government, and education.
- Lokibot: A type of malware that targets the Windows OS and is known for stealing credentials and other sensitive data.

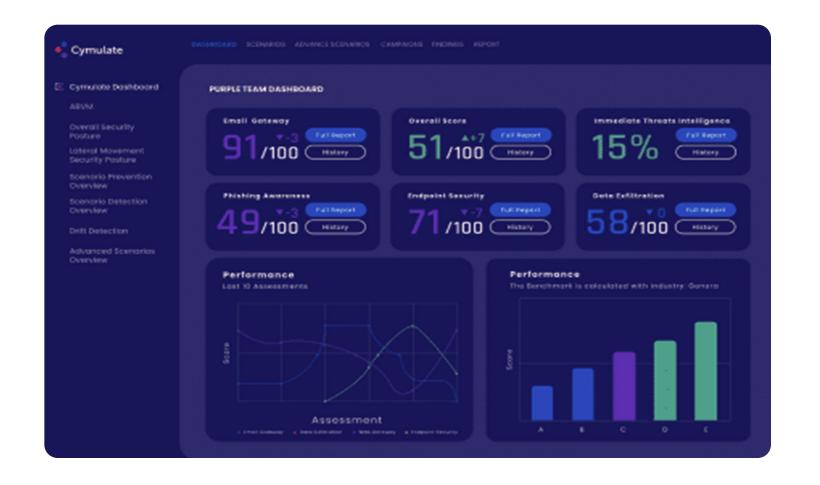






SECURITY VALIDATION BEST PRACTICES **SOC Exercises**

SOC exercises are used to validate security processes, policies, and incident response playbooks using full kill-chain scenarios for common threat group attacks.



Full Kill-Chain Scenarios	 APT Templates 		
Test Scenarios	Choose from over 25 full kill-chain templates for real-world APT threat actors or create custom scenarios using hundreds of prebuilt delivery methods, payload structures, execution methods, and compiled scenarios.		
Recommended Test Frequency	Quarterly		







SECURITY VALIDATION BEST PRACTICES **Red Team Exercises**

Red team exercises are **offensive testing exercises** to determine how deep into a full kill-chain an advanced threat actor could penetrate your environment.

©FULL KILL-CHAIN CAMPAIGN ASSESSMENT SUMMARY				REPORT SUMMARY		
- Em		Nor Connes Smilled Crossie belade Trojan	Powe	ren Gaulaad Arthui rshell 1ject	Not Connect Strated Settinget N/A	
0					0	2000/10/201 -
69	Guttom-LucarP	AURT DENT	DATE	9006	⊗	CHARTER
390	Teste (2)		1245/303 95555		O	
8		(840-(640)	0946/2020 (1512-17	····	O	
	er.	040 040	08/04/2024 09:10:25	DN	0	
	Earnin		evve-2004 07:5020	10	Ø	
	Public Charry Task APT		15/08/3024 21:00:40	L99	O	
0	BUINGAM	(993) (598)	66/13/2022 19:19:49	14%		

The real-life attack scenarios begin with a phishing campaign directly to your end users and then run a full APT campaign from a notorious threat actor.

Cymulate best practices for red team exercises begin with phishing campaigns to your end users and relies on users being manipulated to open the malicious files or links in the email.

- Phishing Campaigns: Simulation of a trusted entity used to deceive users into clicking on a malicious links or downloading malicious payloads.
- APT Campaigns: Start with a phishing campaign and continue through an end-to-end cyber attack from an APT group.

Red Team

- Reconnaissance: Gather information about the target.
- Exploitation: Identify and exploit vulnerabilities.
- Lateral Movement: Move within the network to reach highervalue targets.
- **Persistence**: Establish a foothold to maintain access.
- **Exfiltration**: Extract data from the network.





SECURITY VALIDATION BEST PRACTICES **Red Team Exercises**

Red team exercises are **offensive testing** exercises to determine how deep into a full kill-chain an advanced threat actor could penetrate your environment.

©FULL KILL-CHAIN CAMPAIGN ASSESSMENT SUMMARY				REPORT SUMMARY		
- Em		Nor Connes Smilled Crossie belade Trojan	Powe	ren Gaulaad Arthui rshell 1ject	Not Connect Strated Settinget N/A	
0					0	2000/10/201 -
69	Guttom-LucarP	AURT DENT	DATE	9006	⊗	CHARTER
390	Teste (2)		1245/303 95555		O	
8		(840-(640)	0946/2020 (1512-17	····	O	
	er.	040 040	08/04/2024 09:10:25	DN	0	
	Earnin		evve-2004 07:5020	10	Ø	
	Public Charry Task APT		15/08/3024 21:00:40	L99	O	
0	BUINGAM	(993) (598)	66/13/2022 19:19:49	14%		

Continuous Automated Red Teaming:	 Phishing Awareness Full Kill-Chain Campaigns
Test Scenarios	Over 30 pre-built phishing resources and full kill-chain campaigns to test user awareness and security operations detection and response to APT attacks.
Recommended Test Frequency	Quarterly





Offensive Testing

Moving from Defense to Offense

Offensive testing simulates real-world attack scenarios, providing insights into how an actual attacker might exploit your systems.

This perspective allows you to understand the potential impact of an attack and take appropriate measures to strengthen your defenses.

Offensive security testing isn't so much about finding the flaws; it's about finding the courage to fix them before they're exploited.



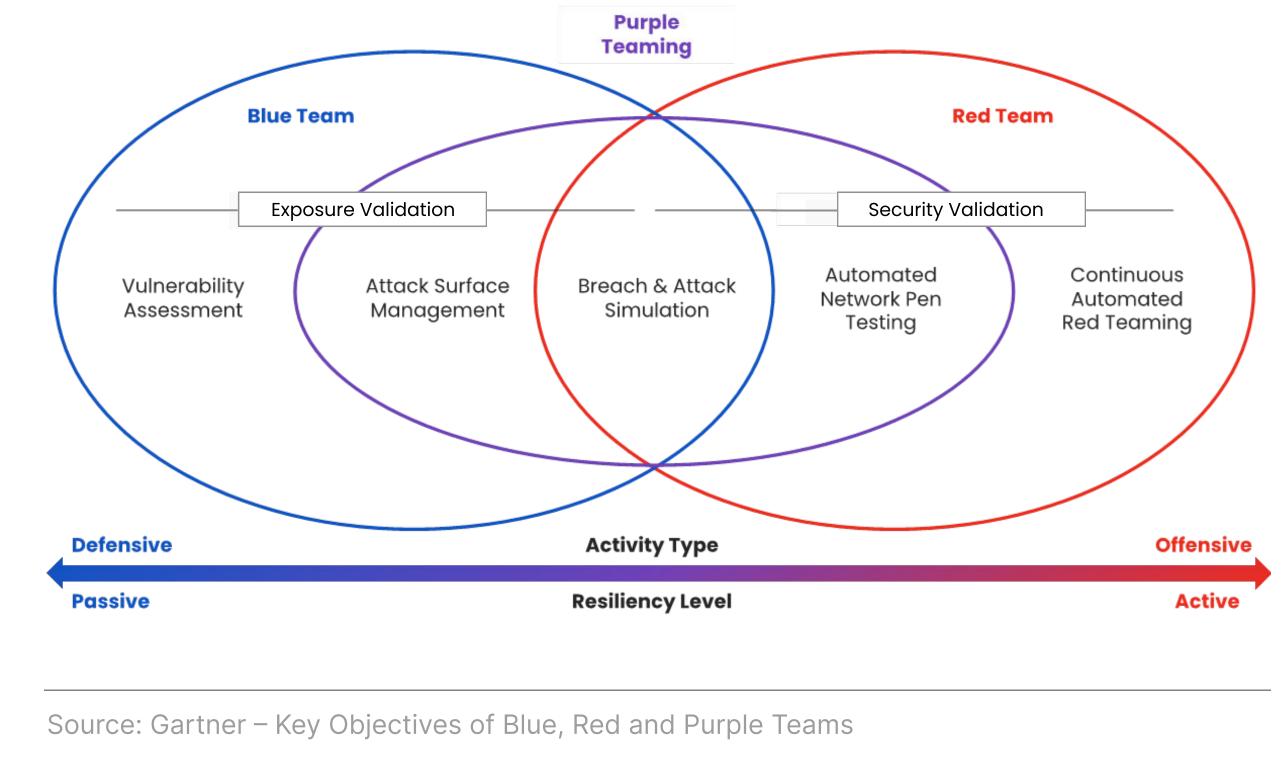




Purple Teaming

The Rise of Purple Teaming in Offensive Strategies

The Cymulate platform is a catalyst for **Purple** Teaming and the integration of offensive (Red Team) and **defensive** (Blue Team) strategies, creating a more holistic approach to validate controls, threats, and response.





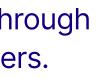


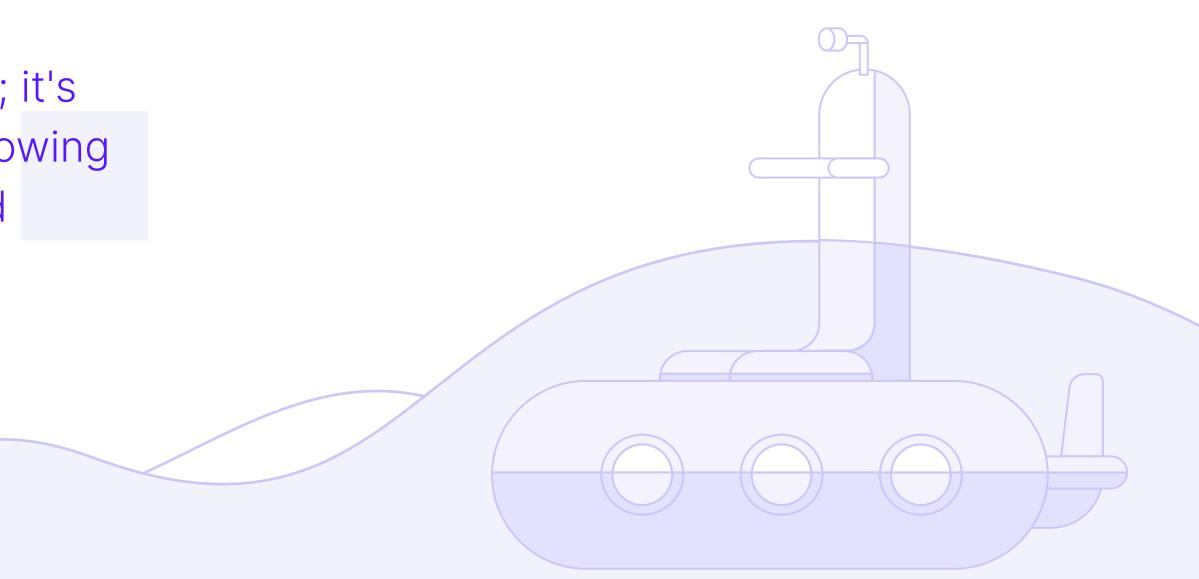
Building Trust & Confidence

Demonstrating a commitment to continuous improvement of cybersecurity through offensive testing can enhance trust with customers, partners, and stakeholders.

It shows that you take security seriously and are proactive in safeguarding sensitive information.

Cyber resiliency isn't just about preventing attacks; it's about confidently navigating through adversity, knowing that every challenge strengthens our defenses and prepares us for what's next.









About Cymulate

Leading Security & Exposure Validation **Platform**, founded in June 2016

A team of top cybersecurity experts with strong technology background and enterprise security domain knowledge

Committed to continuous improvement of cyber defenses.

Over 500 customers in 50 countries





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 of all sizes 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

The leader in exposure management and security validation, provides a modular platform for continuously assessing, testing, and improving cybersecurity resilience — before an attack occurs.





