cymulate

Cymulate PoC Pre-Requirements

PoC Requisites - Checklist

Module	Test Type	Requirement
Endpoint, Web Gateway, Network Propagation, DLP	Ransomwares, Worms, Trojans, Malicious Link, General TTPs, IOC, IOA	• Test Point (Host) with CymulateAgent Installed.
Web Application Firewall Assessments	SQL Injection, XSS, SSRF, Command Injection etc..	One valid URL behind the WAF for testing purpose.
Email Gateway	Ransomwares, Worms, Trojans, Malicious Link.	• Dedicated MailBox • Test Point (Host) with Cymulate Agent Installed.
Cloud Assessments	Check this link.	AWS | GCP | AZURE
Kubernetes Assessments	Check this link.	Kubernetes

System Requirements for a Test Point

Important Note:

If your main use case is **Security Control Validation**, it's essential to have a baseline computer from your company.

You can, for example, use the same image that is deployed to every new employee. This image must include all standard applications used by end users (such as Microsoft Office and Adobe), as well as your official antivirus solution installed.

It is also recommended to have a dedicated domain user account with a password (to be inserted into the platform) and a dedicated user mailbox for the PoC. *(As this mailbox will receive a large number of malware samples, using a production mailbox is not recommended).*

If your company uses a proxy, please ensure that this computer accesses the internet through the proxy as well.

Based on the explanation above, please refer to the following checklist for your PoC computer:

Item	Minimum	Recommmended
CPU	2 Cores	4 Cores
Memory (RAM)	8 GB	16 GB
Free disk Space (SSD)	30 GB	60 GB
Network	One Network Interface	One Network Interface

Criteria	Description
Company Anti-Virus (EPP, ERD) Installed	If one of the use cases is check your Endpoint Security posture please have it.
Proxy Access (If Applicable)	If the company have a proxy, please be sure this computer access the internet though proxy also
Acrobat Reader (If Applicable)	If users usually have Acrobat Reader installed on their computer, install it.
Microsoft Office (If Applicable)	If the company use Microsoft Office, install it
Dedicated Mailbox	If one of the use cases is check your Mail Security posture please have it.
Dedicated Network Username	Malwares behaviors will be simulated with the account logged on the computer. To be sure not to impact any production account, we recommend you to have a dedicated account

Required Exception – All Modules

Item	Requirement		Detail	Description
Cymulate agent machine	*.app.cymulate.com *.us-app.cymulate.com *.cymulate.com (Recommended)		443 HTTPS	Essential Agent Communication Exclude those from any blocking.
General Assessments	*Windows:* • *C:\Program Files\Cymulate\Agent** • *C:\ProgramData\Cymulate\Agent**	Linux: • */usr/local/lib/Cymulate/Agent/** • */usr/local/share/Cymulate/Agent/**	Aplied only in the hosts that will have the agent installed.	All Assessments that depends on agent need this exception on EPP, EDR. *Never put the entire cymulate path in exception Ex. *C:\Program Files\Cymulate** exception to all controls.
Hopper	File name: • CymulateLM.exe • CymulateLM64.exe	File name: • HopperMaster.dll • HopperReport.zip	Aplied to **all hosts** on the network	Hopper Assessments only. Exclude those to all computers in the network. * Please check also the hashes at: Settings > Agent Management > Download agent > Agent hashes.
Employee Awareness	Domain: • EU - support-eu.lionnets.com • US - support-us.lionnets.com • IP address: 54.170.181.225			Make sure to exclude/whitelist these IPs and domains from all controls and filters. They must be fully whitelisted with no blocking applied
Web Application Firewall	EU: - 54.217.50.18 - 52.208.202.111 - 52.49.144.209	US: - 54.237.172.129 - 35.169.219.115 - 52.4.48.52		Exclusion in anti-bot/anti-DDoS controls. Check also Geolocation settings and reputation settings. *Never apply exception to all WAF controls.
Email Gateway	• IP: 18.202.69.111 • Domain: cymulatemailgateway.com			Exclude the following from anti-spam filtering and Rate Liming and Throling policies, but keep AV, Sanbox and any L7 controls in place. *Never apply exception to all Email controls.
Web Gateway	• https://cym-files-download.s3.eu-west-1.amazonaws.com • https://s3-eu-west-1-r-w.amazonaws.com/			Exclude those from URL Filtering only, but keep AV, Sanbox and any other antimalware scan enabled.