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.	Check this link.
Kubernetes Assessments	Check this link.	Check this link.

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.
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.

Cloud & Kubernetes Assessments - AWS

* Mandatory

Specific Requirements for Cloud Testing:

1. aws_access_key *
2. aws_account_id *
3. aws_account_ key_id
4. aws_ec2_instance_public_ip
5. aws_ec2_instance_ssh_key_file_path
6. aws_ec2_instance_username
7. aws_ec2_snapshot_id
8. aws_iam_group_name
9. aws_instance_id
10. aws_instance_profile_name
11. aws_instance_profile_role
12. aws_instance_profile_role_arn
13. aws_lambda_function_arn
14. aws_policy_arn
15. aws_region *
16. aws_role_arn
17. aws_s3_bucket_name
18. aws_s3_file_name_to_download
19. aws_secret_access_key
20. aws_secret_name
21. aws_security_group_id
22. aws_target_account_name
23. aws_target_account_password
24. database_instance_identifier
25. database_password
26. database_username
27. domain_user_name
28. domain_user_password
29. eks_cluster_name
30. lightsail_instance_name
31. log_group
32. organization_name
33. prefix
34. role_name
35. s3_bucket_name
36. source_instance_id
37. table_name
38. target_database_address
39. target_database_name
40. target_external_aws_account_id
41. target_instance_id
42. target_user_name
43. vpc_id
44. aws_ami_id
45. aws_cli_installer_path
46. aws_cli_url
47. aws_cloudtrail_logs_prefix
48. aws_credentials_file_path
49. aws_instance_type
50. aws_lambda_function_name
51. aws_target_environment
52. cloudtrail_name
53. fq_domain_name
54. iam_user_action
55. lambda_handler
56. lambda_runtime_language
57. policy_name

Specific Requirements for Containers:

1. aws_region *
2. eks_cluster_name *
3. kubernetes_api_server_url *
4. kubernetes_namespace *
5. kubernetes_namespaces_list *

cymulate

Cloud & Kubernetes Assessments - Azure

* Mandatory

Specific Requirements for Cloud Testing:

az_cli_installer_path
az_cli_url
Az-Password *
Az-Username *
azure_account_subscription_id
azure_application_name
azure_auth_domain_name
azure_client_id
azure_client_secret
azure_container_policy_name
azure_key_name
azure_key_vault_access_token
azure_key_vault_resource_name
azure_keyvault_name
azure_keyvault_secret_value
azure_lifecycle_policy
azure_managed_identity_location
azure_managed_identity_name
azure_pod_name
azure_region *
azure_resource_group_name
azure_rule_name
azure_secret_name
azure_service_principal_name
azure_storage_account_name
azure_storage_container_name
azure_subscription_id
azure_tenant_id *
azure_user_name *
azure_user_password *
azure_users_file_path
azure_users_list
azure_vault_name
azure_virtual_machine_name
azure_vm_disk_name
database_password
database_type
database_username
default_resource_group
default_server_name
destination_address_prefix
destination_port_range
device_name_to_register
domain_name *
vm_admin_username
vm_image_name
Vmadminuser
subscription_id *
role_name

Azure

Specific Requirements for Containers:

azure_region *
kubernetes_api_server_url *
kubernetes_namespace *
kubernetes_namespaces_list *
azure_kubernetes_access_token
azure_kubernetes_service_name

cymulate

Cloud & Kubernetes Assessments - GCP

* Mandatory

Specific Requirements for Cloud Testing:

gcloud_installer_file_path
gcp_account_name *
gcp_auth_json_file_name
gcp_auth_json_key_path
gcp_bucket_file_name
gcp_bucket_item_url
gcp_bucket_name
gcp_cli_url
gcp_cloud_function_code_zip_src
gcp_cloud_function_entry_point
gcp_cloud_function_name
gcp_cloud_function_region
gcp_custom_role_name
gcp_delegated_service_account_email
gcp_image
gcp_instance_name *
gcp_instance_user_password *
gcp_instance_username *
gcp_instance_zone
gcp_org_id
gcp_private_key_file_path
gcp_project_id
gcp_region *
gcp_region_name *
gcp_repo_name
gcp_scheduler_job_name
gcp_scheduler_job_region
gcp_secret_name
gcp_secret_value
gcp_service_account
gcp_service_account_client_email
gcp_service_account_email
gcp_service_account_name
gcp_service_account_private_key
gcp_snapshot_name
gcp_target_service_account_email
gcp_token
gcp_zone_name *
database_password
target_database_name
role_name *
role_name_list
service_account_email_address
service_account_role
metadata_key
metadata_key_to_update
metadata_value
metadata_value_to_update
sql_instance_name
ssh_key_path
system_user_command_execution
table_name
token_audience
user_names_list
user_type

Specific Requirements for Containers:

1.gcp_region *
3.kubernetes_api_server_url *
4.kubernetes_namespace *
5.kubernetes_namespaces_list *
6.kube_binary_url
7.kube_config_path
gcp_cluster_name
gcp_cluster_zone