BEFORE SECURING ENVIRONMENT

Start Time	2023-12-26T20:28:30.2988492Z
Stop Time	2023-12-27T20:28:30.2988492Z
Security Events (Windows VMs)	65445
Syslog (Linux VMs)	5415
SecurityAlert (Microsoft Defender for Cloud)	53
SecurityIncident (Sentinel Incidents)	463
NSG Inbound Malicious Flows Allowed	4532

AFTER SECURING ENVIRONMENT

Start Time	2023-12-29T12:05:22.0643013Z
Stop Time	2023-12-30T12:05:22.0643013Z
Security Events (Windows VMs)	0
Syslog (Linux VMs)	5
SecurityAlert (Microsoft Defender for Cloud)	0
SecurityIncident (Sentinel Incidents)	0
NSG Inbound Malicious Flows Allowed	0

RESULTS (will auto update, do not edit formulas)

	Change after security environment
Security Events (Windows VMs)	-100.00%
Syslog (Linux VMs)	-99.91%
SecurityAlert (Microsoft Defender for Cloud)	-100.00%
Security Incident (Sentinel Incidents)	-100.00%
NSG Inbound Malicious Flows Allowed	-100.00%

HELPER QUERIES

Helper KQL Queries

	Start Time	range x from 1 to 1 step 1			
	Stop Time	| project StartTime = ago(24h), StopTime = no			
	Security Events (Windows VMs)	SecurityEvent | where TimeGenerated >= ago(24h) | count			
	Syslog (Linux VMs)	Syslog | where TimeGenerated >= ago(24h) | count			
	SecurityAlert (Microsoft Defender for Cloud)	SecurityAlert | where DisplayName !startswith "CUSTOM" and DisplayName !startswith "TEST" | where TimeGenerated >= ago(24h) | count			
	Security Incident (Sentinel Incidents)	SecurityIncident | where TimeGenerated >= ago(24h) | count			
	NSG Inbound Malicious Flows Allowed	AzureNetworkAnalytics_CL | where FlowType_s == "MaliciousFlow" and AllowedInFlows_d > 0 | where TimeGenerated >= ago(24h) | count			
	NSG Inbound Malicious Flows Blocked	AzureNetworkAnalytics_CL | where FlowType_s == "MaliciousFlow" and DeniedInFlows_d > 0 | where TimeGenerated >= ago(24h) | count			