BEFORE SECURING ENVIRONMENT

Start Time	2024-09-26T00:38:49.3401183Z
Stop Time	2024-09-27T00:38:49.3401183Z
Security Events (Windows VMs)	278844
Syslog (Linux VMs)	4271
SecurityAlert (Microsoft Defender for Cloud)	0
SecurityIncident (Sentinel Incidents)	180
NSG Inbound Malicious Flows Allowed	3655

AFTER SECURING ENVIRONMENT

Start Time	9/27/2024, 9:42:19 PM
Stop Time	9/28/2024, 9:42:19 PM
Security Events (Windows VMs)	923
Syslog (Linux VMs)	0
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)	-99.67%
Syslog (Linux VMs)	-100.00%
SecurityAlert (Microsoft Defender for Cloud)	#DIV/0!
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 | project StartTime = ago(24h), StopTime = nc
Stop Time	

	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			