|  |  |  |
| --- | --- | --- |
|  | **BEFORE SECURING ENVIRONMENT** | |
|  |  |  |
|  | Start Time | 1/29/2024, 6:36:56.839 PM |
|  | Stop Time | 1/30/2024, 6:36:56.839 PM |
|  | Security Events (Windows VMs) | 42004 |
|  | Syslog (Linux VMs) | 18363 |
|  | SecurityAlert (Microsoft Defender for Cloud) | 401 |
|  | SecurityIncident (Sentinel Incidents) | 654 |
|  | NSG Inbound Malicious Flows Allowed | 59433 |
|  | NSG Inbound Malicious Flows Blocked | 0 |
|  |  |  |
|  | **AFTER SECURING ENVIRONMENT** | |
|  |  |  |
|  | Start Time | 1/30/2024, 5:17:15.359 PM |
|  | Stop Time | 1/31/2024, 5:17:15.359 PM |
|  | Security Events (Windows VMs) | 9611 |
|  | Syslog (Linux VMs) | 1 |
|  | SecurityAlert (Microsoft Defender for Cloud) | 6 |
|  | SecurityIncident (Sentinel Incidents) | 6 |
|  | NSG Inbound Malicious Flows Allowed | 0 |
|  | NSG Inbound Malicious Flows Blocked | 197 |
|  |  |  |
|  | **RESULTS** | |
|  |  | **Change after security environment** |
|  | Security Events (Windows VMs) | -77.12% |
|  | Syslog (Linux VMs) | -99.99% |
|  | SecurityAlert (Microsoft Defender for Cloud) | -98.50% |
|  | Security Incident (Sentinel Incidents) | -99.08% |
|  | 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 = now() |
|  | 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 |