**KQL Queries Used for Log Analysis**

**1. Detecting Failed Login Attempts**

SecurityEvent

| where EventID == 4625

| summarize Count = count() by Account, bin(TimeGenerated, 10m)

| order by Count desc

**2. Identifying Malicious IPs**

FirewallLogs

| where Action == "Blocked"

| where IP in ("45.83.192.10", "185.220.101.45")

| summarize Count = count() by IP, ThreatCategory

**3. Tracking Unauthorized Access Attempts**

SigninLogs

| where ResultType != "0"

| project TimeGenerated, UserPrincipalName, AppDisplayName, Status

| order by TimeGenerated desc