KQL Threat Hunting Workbook

This workbook contains sample KQL queries for SOC threat hunting.

1. Password Spray Detection:

```
SigninLogs
| where ResultType != 0
| summarize Users = dcount(UserPrincipalName) by IPAddress
| where Users > 5
| order by Users desc
```

2. MFA Fatigue Detection:

```
SigninLogs
| where ResultDescription contains "denied"
| summarize Denials = count() by UserPrincipalName
| where Denials > 3
```

3. Suspicious PowerShell:

```
DeviceProcessEvents
| where FileName == "powershell.exe"
| where ProcessCommandLine has_any ("IEX","DownloadString","-enc","http")
```

4. LSASS Dump Attempt:

```
DeviceProcessEvents
| where ProcessCommandLine has_any ("lsass","procdump","MiniDump","lsass.dmp")
```

5. Kerberoasting:

```
SecurityEvent
| where EventID == 4769
| where TicketEncryptionType == "0x17"

| summarize Count=count() by Account, ServiceName
```