Query Logs in Microsoft Sentinel

# Understand Common Tables

|  |  |
| --- | --- |
| **Table** | **Description** |
| AzureActivity | Entries from Azure Activity log that provides insight into any subscription-level or management group level events that have occurred in Azure. |
| AzureDiagnostics | Stores resource logs for Azure Services that use Azure Diagnostics mode. Resource logs describe the internal operation of Azure resources. |
| AuditLogs | Audit log for Azure AD. Includes system activity information about user and group management, managed applications and directory activities. |
| CommonSecurityLog | Syslog messages using the Common Event Format (CEF) |
| McasShadowItReporting | Microsoft Cloud App Security logs |
| OfficeActivity | Audit logs for Office 365 tenants collected by sentinel. Including Exchange, SharePoint and Teams logs. |
| SecurityEvent | Security events collected from windows machines by Azure Security Centre or Sentinel. |
| SigninLogs | Azure Active Directory Sign-in logs |
| Syslog | Syslog events on linux computers using the log analytics agent |
| Event | Sysmon Events collected from a Windows host |
| WindowsFirewall | Windows Firewall events |

# Microsoft 365 Defender Tables

|  |  |
| --- | --- |
| **Table** | **Description** |
| DeviceEvents | The miscellaneous device events table contains information about various event types, including events triggered by security controls, such as Microsoft Defender Antivirus and exploit protection. |
| DeviceFileEvents | This table contains information about file creation modification and other file system events. |
| DeviceImageLoadEvents | This table contains information about DLL loading events. |
| DeviceInfo | This table contains information about devices in the organisation including their OS version, active users and computer name. |
| DeviceLogonEvents | This table contains information about user logons and other authentication events. |
| DeviceNetworkEvents | This table contains information about network connections and related events. |
| DeviceNetworkInfo | This table contains information about networking configuration of devices, including network adapters, IP and MAC addresses, and connected networks or domains. |
| DeviceProcessEvents | This table contains information about process creation and related events. |
| DeviceRegistryEvents | This table contains information about the creation and modification of registry entries |