



Cheat Sheet

Intro

Kusto Query Language (KQL) is a powerful language to query structured & unstructured data.

Example queries below will abbreviate the table name with **T**

Common Input

To put **comments** in your queries, use double forward slash.

```
// Comment
```

The **pipe delimiter** (|) is crucial for KQL queries, it is used to separate data transformation operators.

```
T |
```

Applying **timeframes** with **ago**

```
T | where TimeGenerated > ago(1d)
```

To **filter rows** of a table by column, use **where**

```
T | where TimeGenerated > ago(1d) | where Type == "AzureActivity"
```

Key Operators

Equal to & Case Sensitive	==
Equal to & Case insensitive	==~
Not equal to & Case Sensitive	!=
Not equal to & Case insensitive	!~

[Full list of operators](#)

Common Output

Show selected columns in the output with **project**

```
T | project TimeGenerated, Level, CallerIpAddress
```

Hide selected columns in the output with **project-away**

```
T | project-away SubscriptionId, Caller
```

Key Tables for Microsoft Sentinel

AuditLogs	Audit Logs for Entra ID	DeviceInfo	MDE table for machine information
SigninLogs	Sign-in Logs for Entra ID	DeviceEvents	MDE table for device security events
AzureActivity	Azure Subscription level events	DeviceFileEvents	MDE device level file operations (creation/modification)
OfficeActivity	M365 Audit logs for Exchange, Teams & SharePoint	DeviceImageLoadEvents	MDE table containing DLL events
SecurityEvent	Event logs collected from Windows machines	DeviceLogonEvents	MDE table for device level authentication events
SecurityIncidents	Microsoft Sentinel incident table	DeviceNetworkInfo	MDE device network info (IP, MAC, connected networks)
IdentityInfo	Sentinel UEBA table containing user identity information	DeviceNetworkEvents	MDE device table for network level events
Watchlist	Imported data used for join queries or for filters in queries	DeviceProcessEvents	MDE device table for process creation
Usage	Sentinel hourly usage for each table	DeviceRegistryEvents	MDE device table for registry creation and modification