KQL Language

resources

https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-language?view=o365-worldwide

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/

https://learn.microsoft.com/en-us/training/modules/explore-fundamentals-kql/

https://aka.ms/lademo

https://www.youtube.com/@TenMinuteKQL

Syntax

- // > comment
- ctrl + k + c > comment
- ctrl + k + u > uncomment
- where >> clause is used to filter records based on specified conditions
- take >> operator is used to limit the number of records (rows)
- cluster('help').database('SecurityLogs').Email >> KQL made from cluster contain DB contain table
- == >> exact match
- != >> does not include
- =~ >> matching for regex pattern
- contains >> operator for string matching
- has >> looks for full string but can use delimiters and is not case sensitive
- endswith >> to get the end of a string
- startswith >> to get the starting of the string
- to make it case sensitive add _cs >> startswith_cs or endswith_cs
- sort by >> sorts the result by time or hostname or what ever u want
- order by >> similar to sort by
- distinct >> used to retrieve unique values from a specified column in a table

- project >> display the rows we want only
- project-reorder >> To achieve reordering of columns
- instead of using two where user one where and (and)
- where * has "389" >> to search in all the records for 389
- limit >> same as take
- top >> same as take but it give u the top of the results // top 10 by TimeGenerated desc
- TimeGenerated >= ago(7d) >> to display a timestamp greater than 7 days
- TimeGenerated <= ago(4h) >> less than four hours // less than mean older
- between >> to display a the frame between two dates // where StartTime between (datetime(2007-07-27) .. datetime(2007-07-30))
- now >> display the time between date and NOW // where StartTime between (datetime(2007-07-27) .. now())
- now - date >> same as above but to display four hours earlier //// where StartTime between (datetime(2007-07-27) .. now() -4h))