Windows PowerShell Get-Help on Cmdlet 'New-AzSentinelEntityQuery'

PS:\>Get-HELP New-AzSentinelEntityQuery -Full

NAME

New-AzSentinelEntityQuery

SYNOPSIS

Creates or updates the entity query.

SYNTAX

New-AzSentinelEntityQuery -ResourceGroupName <String> -WorkspaceName <String> [-SubscriptionId <String>] [-Id <String>] -Kind <EntityQueryKind> -Title <String>

-Content <String> -Description <String> -QueryDefinitionQuery <String> -InputEntityType <EntityType> [-RequiredInputFieldsSet <String[]>] [-EntitiesFilter

<ActivityEntityQueriesPropertiesEntitiesFilter>] [-TemplateName <String>] [-DefaultProfile <PSObject>] [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>]

[-HttpPipelinePrepend <SendAsyncStep[]>] [-NoWait] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm]

[<CommonParameters>]

DESCRIPTION

Creates or updates the entity query.

PARAMETERS

-ResourceGroupName <String>

The Resource Group Name.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-WorkspaceName <String>

[Alias('DataConnectionName')]

The name of the workspace.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SubscriptionId <String>

Gets subscription credentials which uniquely identify Microsoft Azure subscription.

The subscription ID forms part of the URI for every service call.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Id <String>

The Id of the Entity Query.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Kind <EntityQueryKind>

Kind of the the Entity Query

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Title <String>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Content <String>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Description <String>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-QueryDefinitionQuery <String>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-InputEntityType <EntityType>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-RequiredInputFieldsSet <String[]>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-EntitiesFilter <ActivityEntityQueriesPropertiesEntitiesFilter>

To construct, see NOTES section for ENTITIESFILTER properties and create a hash table.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-TemplateName <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DefaultProfile <PSObject>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-AsJob [<SwitchParameter>]

Run the command as a job

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-Break [<SwitchParameter>]

Wait for .NET debugger to attach

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelineAppend <SendAsyncStep[]>

SendAsync Pipeline Steps to be appended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelinePrepend <SendAsyncStep[]>

SendAsync Pipeline Steps to be prepended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-NoWait [<SwitchParameter>]

Run the command asynchronously

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-Proxy <Uri>

The URI for the proxy server to use

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyCredential <PSCredential>

Credentials for a proxy server to use for the remote call

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyUseDefaultCredentials [<SwitchParameter>]

Use the default credentials for the proxy

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

OUTPUTS

Microsoft.Azure.PowerShell.Cmdlets.SecurityInsights.Models.Api20210901Preview.CustomEntityQuery

NOTES

COMPLEX PARAMETER PROPERTIES

To create the parameters described below, construct a hash table containing the appropriate properties. For

information on hash tables, run Get-Help

about_Hash_Tables.

ENTITIESFILTER <ActivityEntityQueriesPropertiesEntitiesFilter>:

[(Any) <String[]>]: This indicates any property can be added to this object.

---------- EXAMPLE 1 ----------

PS C:\>$template = Get-AzSentinelEntityQueryTemplate -ResourceGroupName "myResourceGroupName" -workspaceName "myWorkspaceName" -Id "myEntityQueryTemplateId"

New-AzSentinelEntityQuery -ResourceGroupName "myResourceGroupName" -workspaceName "myWorkspaceName" -Kind Activity -Title ($template.title) -InputEntityType

($template.inputEntityType) -TemplateName ($template.Name)

---------- EXAMPLE 2 ----------

PS C:\>New-AzSentinelEntityQuery -ResourceGroupName "myResourceGroupName" -workspaceName "myWorkspaceName" -Id ((New-Guid).Guid) -Kind Activity -Title 'An account was

deleted on this host' -InputEntityType 'Host' -Content "On 'SomeCompute' the account 'SomeAccount' was deleted by 'SomeUser'" -Description "Account deleted on host"

-QueryDefinitionQuery 'let GetAccountActions = (v_Host_Name:string, v_Host_NTDomain:string, v_Host_DnsDomain:string, v_Host_AzureID:string,

v_Host_OMSAgentID:string){\nSecurityEvent\n| where EventID in (4725, 4726, 4767, 4720, 4722, 4723, 4724)\n// parsing for Host to handle variety of conventions coming

from data\n| extend Host_HostName = case(\nComputer has "@", tostring(split(Computer, "@")[0]),\nComputer has "\\", tostring(split(Computer,

"\\")[1]),\nComputer has ".", tostring(split(Computer, ".")[0]),\nComputer\n)\n| extend Host_NTDomain = case(\nComputer has "\\", tostring(split(Computer,

"\\")[0]), \nComputer has ".", tostring(split(Computer, ".")[-2]), \nComputer\n)\n| extend Host_DnsDomain =

case(\nComputer has "\\", tostring(split(Computer,

"\\")[0]), \nComputer has ".", strcat_array(array_slice(split(Computer,"."),-2,-1),"."), \nComputer\n)\n| where (Host_HostName =~ v_Host_Name and

Host_NTDomain =~ v_Host_NTDomain) \nor (Host_HostName =~ v_Host_Name and Host_DnsDomain =~ v_Host_DnsDomain) \nor v_Host_AzureID =~ _ResourceId \nor v_Host_OMSAgentID

== SourceComputerId\n| project TimeGenerated, EventID, Activity, Computer, TargetAccount, TargetUserName, TargetDomainName, TargetSid, SubjectUserName,

SubjectUserSid, _ResourceId, SourceComputerId\n| extend AddedBy = SubjectUserName\n// Future support for Activities\n| extend timestamp = TimeGenerated,

HostCustomEntity = Computer, AccountCustomEntity = TargetAccount\n};\nGetAccountActions("someHost", "SomeNTDomain", "SomeDNSDomain", "SomeID",

"SomeOMSAgentID")\n \n| where EventID == 4726' -RequiredInputFieldsSet

@(@("Host_HostName","Host_NTDomain"),@("Host_HostName","Host_DnsDomain"),@("Host_AzureID"),@("Host_OMSAgentID")) -EntitiesFilter @{"Host_OsFamily" = @("Windows")}

RELATED LINKS

https://learn.microsoft.com/powershell/module/az.securityinsights/new-azsentinelentityquery