Windows PowerShell Get-Help on Cmdlet 'Invoke-AzSentinelThreatIntelligenceIndicatorQuery'

PS:\>Get-HELP Invoke-AzSentinelThreatIntelligenceIndicatorQuery -Full

NAME

Invoke-AzSentinelThreatIntelligenceIndicatorQuery

SYNOPSIS

Query threat intelligence indicators as per filtering criteria.

SYNTAX

Invoke-AzSentinelThreatIntelligenceIndicatorQuery -ResourceGroupName <String> -WorkspaceName <String> [-SubscriptionId <String>] [-Id <String[]>] [-IncludeDisabled]

[-Keyword <String[]>] [-MaxConfidence <Int32>] [-MaxValidUntil <String>] [-MinConfidence <Int32>] [-MinValidUntil <String>] [-PageSize <Int32>] [-PatternType

<String[]>] [-SkipToken <String>] [-SortBy <IThreatIntelligenceSortingCriteria[]>] [-Source <String[]>] [-ThreatType <String[]>] [-DefaultProfile <PSObject>] [-Break]

[-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials]

[-WhatIf] [-Confirm] [<CommonParameters>]

DESCRIPTION

Query threat intelligence indicators as per filtering criteria.

PARAMETERS

-ResourceGroupName <String>

The name of the resource group.

The name is case insensitive.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-WorkspaceName <String>

The name of the workspace.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SubscriptionId <String>

The ID of the target subscription.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Id <String[]>

Ids of threat intelligence indicators

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-IncludeDisabled [<SwitchParameter>]

Parameter to include/exclude disabled indicators.

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-Keyword <String[]>

Keywords for searching threat intelligence indicators

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-MaxConfidence <Int32>

Maximum confidence.

Required? false

Position? named

Default value 0

Accept pipeline input? false

Accept wildcard characters? false

-MaxValidUntil <String>

End time for ValidUntil filter.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-MinConfidence <Int32>

Minimum confidence.

Required? false

Position? named

Default value 0

Accept pipeline input? false

Accept wildcard characters? false

-MinValidUntil <String>

Start time for ValidUntil filter.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-PageSize <Int32>

Page size

Required? false

Position? named

Default value 0

Accept pipeline input? false

Accept wildcard characters? false

-PatternType <String[]>

Pattern types

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SkipToken <String>

Skip token.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SortBy <IThreatIntelligenceSortingCriteria[]>

Columns to sort by and sorting order

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

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Source <String[]>

Sources of threat intelligence indicators

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ThreatType <String[]>

Threat types of threat intelligence indicators

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DefaultProfile <PSObject>

The DefaultProfile parameter is not functional.

Use the SubscriptionId parameter when available if executing the cmdlet against a different subscription.

Required? false

Position? named

Default value

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

-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.IThreatIntelligenceInformation

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.

SORTBY <IThreatIntelligenceSortingCriteria[]>: Columns to sort by and sorting order
[ItemKey <String>]: Column name
[SortOrder <ThreatIntelligenceSortingCriteriaEnum?>]: Sorting order (ascending/descending/unsorted).

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

PS C:\>Invoke-AzSentinelThreatIntelligenceIndicatorQuery -ResourceGroupName "myResourceGroupName" -WorkspaceName "myWorkspaceName"

RELATED LINKS

https://learn.microsoft.com/powershell/module/az.securityinsights/invoke-azsentinelthreatintelligenceindicatorquery