Windows PowerShell Get-Help on Cmdlet 'Get-AzSentinelThreatIntelligenceIndicator'

PS:\>Get-HELP Get-AzSentinelThreatIntelligenceIndicator -Full

NAME

Get-AzSentinelThreatIntelligenceIndicator

SYNOPSIS

View a threat intelligence indicator by name.

SYNTAX

Get-AzSentinelThreatIntelligenceIndicator -ResourceGroupName <String> [-SubscriptionId <String[]>] -WorkspaceName <String> [-Filter <String>] [-Orderby <String>]

[-SkipToken <String>] [-Top <Int32>] [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy

<Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [<CommonParameters>]

Get-AzSentinelThreatIntelligenceIndicator -Name <String> -ResourceGroupName <String> [-SubscriptionId <String[]>] -WorkspaceName <String> [-DefaultProfile <PSObject>]

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

[-ProxyUseDefaultCredentials] [<CommonParameters>]

Get-AzSentinelThreatIntelligenceIndicator -InputObject <ISecurityInsightsIdentity> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>]

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

DESCRIPTION

View a threat intelligence indicator by name.

PARAMETERS

-Name <String>

Threat intelligence indicator name field.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-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

-SubscriptionId <String[]>

The ID of the target subscription.

Required? false

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

-InputObject <ISecurityInsightsIdentity>

Identity Parameter

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

Required? true

Position? named

Default value

Accept pipeline input? true (ByValue)

Accept wildcard characters? false

-Filter <String>

Filters the results, based on a Boolean condition.

Optional.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Orderby <String>

Sorts the results.

Optional.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SkipToken <String>

Skiptoken is only used if a previous operation returned a partial result.

If a previous response contains a nextLink element, the value of the nextLink element will include a skiptoken parameter that specifies a starting point to use

for subsequent calls.

Optional.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Top <Int32>

Returns only the first n results.

Optional.

Required? false

Position? named

Default value 0

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

<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

Microsoft.Azure.PowerShell.Cmdlets.SecurityInsights.Models.ISecurityInsightsIdentity

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.

INPUTOBJECT <ISecurityInsightsIdentity>: Identity Parameter

[ActionId <String>]: Action ID

[AlertRuleTemplateId <String>]: Alert rule template ID

[AutomationRuleId <String>]: Automation rule ID

[BookmarkId <String>]: Bookmark ID

[ConsentId <String>]: consent ID

[DataConnectorId <String>]: Connector ID

[EntityId <String>]: entity ID

[EntityQueryId <String>]: entity query ID

[EntityQueryTemplateId <String>]: entity query template ID

[Id <String>]: Resource identity path

[IncidentCommentId <String>]: Incident comment ID

[IncidentId <String>]: Incident ID

[MetadataName <String>]: The Metadata name.

[Name <String>]: Threat intelligence indicator name field.

[RelationName <String>]: Relation Name

[ResourceGroupName <String>]: The name of the resource group. The name is case insensitive.

[RuleId <String>]: Alert rule ID

[SentinelOnboardingStateName <String>]: The Sentinel onboarding state name. Supports - default

[SettingsName <String>]: The setting name. Supports - Anomalies, EyesOn, EntityAnalytics, Ueba

[SourceControlId <String>]: Source control Id

[SubscriptionId <String>]: The ID of the target subscription.

[WorkspaceName <String>]: The name of the workspace.

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

PS C:\>Get-AzSentinelThreatIntelligenceIndicator -ResourceGroupName "myResourceGroupName" -workspaceName "myWorkspaceName"

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

PS C:\>Get-AzSentinelThreatIntelligenceIndicator -ResourceGroupName "myResourceGroupName" -workspaceName "myWorkspaceName" -Name "514840ce-5582-f7a4-8562-7996e29dc07a"

---------- EXAMPLE 3 ----------

PS C:\>$tiIndicators = Get-AzSentinelThreatIntelligenceIndicator -ResourceGroupName "myResourceGroupName" -workspaceName "myWorkspaceName" -Top 3

RELATED LINKS

https://learn.microsoft.com/powershell/module/az.securityinsights/get-azsentinelthreatintelligenceindicator