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

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

NAME

New-AzSentinelBookmark

SYNOPSIS

Creates or updates the bookmark.

SYNTAX

New-AzSentinelBookmark -ResourceGroupName <String> -WorkspaceName <String> [-Id <String>] [-SubscriptionId <String>] [-DisplayName <String>] [-EventTime <DateTime>]

[-IncidentInfoIncidentId <String>] [-IncidentInfoRelationName <String>] [-IncidentInfoSeverity <IncidentSeverity>] [-IncidentInfoTitle <String>] [-Label <String[]>]

[-Note <String>] [-Query <String>] [-QueryEndTime <DateTime>] [-QueryResult <String>] [-QueryStartTime <DateTime>] [-DefaultProfile <PSObject>] [-Break]

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

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

New-AzSentinelBookmark -ResourceGroupName <String> -WorkspaceName <String> [-Id <String>] [-SubscriptionId <String>] -Bookmark <IBookmark> [-DefaultProfile

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

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

DESCRIPTION

Creates or updates the bookmark.

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

-Id <String>

Bookmark ID

Required? false

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

-Bookmark <IBookmark>

Represents a bookmark in Azure Security Insights.

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

Required? true

Position? named

Default value

Accept pipeline input? true (ByValue)

Accept wildcard characters? false

-DisplayName <String>

The display name of the bookmark

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-EventTime <DateTime>

The bookmark event time

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-IncidentInfoIncidentId <String>

Incident Id

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-IncidentInfoRelationName <String>

Relation Name

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-IncidentInfoSeverity <IncidentSeverity>

The severity of the incident

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-IncidentInfoTitle <String>

The title of the incident

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Label <String[]>

List of labels relevant to this bookmark

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Note <String>

The notes of the bookmark

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Query <String>

The query of the bookmark.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-QueryEndTime <DateTime>

The end time for the query

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-QueryResult <String>

The query result of the bookmark.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-QueryStartTime <DateTime>

The start time for the query

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

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

OUTPUTS

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

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.

BOOKMARK <IBookmark>: Represents a bookmark in Azure Security Insights.

[Etag <String>]: Etag of the azure resource

[SystemDataCreatedAt <DateTime?>]: The timestamp of resource creation (UTC).

[SystemDataCreatedBy <String>]: The identity that created the resource.

[SystemDataCreatedByType <CreatedByType?>]: The type of identity that created the resource.

[SystemDataLastModifiedAt <DateTime?>]: The timestamp of resource last modification (UTC)

[SystemDataLastModifiedBy <String>]: The identity that last modified the resource.

[SystemDataLastModifiedByType <CreatedByType?>]: The type of identity that last modified the resource.

[Created <DateTime?>]: The time the bookmark was created

[CreatedByObjectId <String>]: The object id of the user.

[DisplayName <String>]: The display name of the bookmark

[EventTime <DateTime?>]: The bookmark event time

[IncidentInfoIncidentId <String>]: Incident Id

[IncidentInfoRelationName <String>]: Relation Name

[IncidentInfoSeverity <IncidentSeverity?>]: The severity of the incident

[IncidentInfoTitle <String>]: The title of the incident

[Label <String[]>]: List of labels relevant to this bookmark

[Note <String>]: The notes of the bookmark

[Query <String>]: The query of the bookmark.

[QueryEndTime <DateTime?>]: The end time for the query

[QueryResult <String>]: The query result of the bookmark.

[QueryStartTime <DateTime?>]: The start time for the query

[Updated <DateTime?>]: The last time the bookmark was updated

[UpdatedByObjectId <String>]: The object id of the user.

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

PS C:\>$queryStartTime = (Get-Date).AddDays(-1).ToUniversalTime() | Get-Date -Format "yyyy-MM-ddThh:00:00.000Z"

```
$queryEndTime = (Get-Date).ToUniversalTime() | Get-Date -Format "yyyy-MM-ddThh:00:00.000Z"

New-AzSentinelBookmark -ResourceGroupName "myResourceGroup" -WorkspaceName "myWorkspaceName" -Id ((New-Guid).Guid) -DisplayName "Incident Evidence" -Query "SecurityEvent | take 1" -QueryStartTime $queryStartTime -QueryEndTime $queryEndTime -EventTime $queryEndTime
```

RELATED LINKS

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