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

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

NAME

Update-AzSentinelBookmark

SYNOPSIS

Creates or updates the bookmark.

SYNTAX

Update-AzSentinelBookmark -Id <String> -ResourceGroupName <String> [-SubscriptionId <String>] -WorkspaceName <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>]

Update-AzSentinelBookmark -InputObject <ISecurityInsightsIdentity> [-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>]

DESCRIPTION

Creates or updates the bookmark.

PARAMETERS

-Id <String>

Bookmark ID

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

-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.ISecurityInsightsIdentity

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.

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:\>$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"

Update-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/update-azsentinelbookmark