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

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

NAME

Update-AzSentinelAlertRule

SYNOPSIS

Updates the alert rule.

SYNTAX

Update-AzSentinelAlertRule -ResourceGroupName <String> -WorkspaceName <String> -RuleId <String> [-SubscriptionId <String>] [-AlertRuleTemplateName <String>]

[-Enabled] [-Disabled] [-Description <String>] [-Query <String>] [-DisplayName <String>] [-SuppressionDuration <TimeSpan>] [-SuppressionEnabled] [-Severity

<AlertSeverity>] [-Tactic <AttackTactic>] [-CreateIncident] [-GroupingConfigurationEnabled] [-ReOpenClosedIncident] [-LookbackDuration <TimeSpan>] [-MatchingMethod

<String>] [-GroupByAlertDetail <AlertDetail[]>] [-GroupByCustomDetail <String[]>] [-GroupByEntity <EntityMappingType[]>] [-EntityMapping <EntityMapping[]>]

[-AlertDescriptionFormat <String>] [-AlertDisplayNameFormat <String>] [-AlertSeverityColumnName <String>] [-AlertTacticsColumnName <String>] [-QueryFrequency

<TimeSpan>] [-QueryPeriod <TimeSpan>] [-TriggerOperator <TriggerOperator>] [-TriggerThreshold <Int32>] [-EventGroupingSettingAggregationKind

<EventGroupingAggregationKind>] [-DefaultProfile <PSObject>] -Scheduled [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend
<SendAsyncStep[]>] [-NoWait] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

Update-AzSentinelAlertRule -ResourceGroupName <String> -WorkspaceName <String> -RuleId <String> [-SubscriptionId <String>] [-AlertRuleTemplateName <String>]
[-Enabled] [-Disabled] [-DefaultProfile <PSObject>] [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-NoWait]
[-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] -FusionMLorTI [-WhatIf] [-Confirm] [<CommonParameters>]

Update-AzSentinelAlertRule -ResourceGroupName <String> -WorkspaceName <String> -RuleId <String> [-SubscriptionId <String>] [-AlertRuleTemplateName <String>]
[-Enabled] [-Disabled] [-Description <String>] [-DisplayNamesFilter <String[]>] [-DisplayNamesExcludeFilter <String[]>] [-ProductFilter
<MicrosoftSecurityProductName>] [-SeveritiesFilter <AlertSeverity[]>] [-DefaultProfile <PSObject>] [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>]
[-HttpPipelinePrepend <SendAsyncStep[]>] [-NoWait] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] -MicrosoftSecurityIncidentCreation
[-WhatIf] [-Confirm] [<CommonParameters>]

Update-AzSentinelAlertRule -ResourceGroupName <String> -WorkspaceName <String> -RuleId <String> [-SubscriptionId <String>] [-AlertRuleTemplateName <String>]
[-Enabled] [-Disabled] [-Description <String>] [-Query <String>] [-DisplayName <String>] [-SuppressionDuration <TimeSpan>] [-SuppressionEnabled] [-Severity
<AlertSeverity>] [-Tactic <AttackTactic>] [-CreateIncident] [-GroupingConfigurationEnabled] [-ReOpenClosedIncident] [-LookbackDuration <TimeSpan>] [-MatchingMethod
<String>] [-GroupByAlertDetail <AlertDetail[]>] [-GroupByCustomDetail <String[]>] [-GroupByEntity <EntityMappingType[]>] [-EntityMapping <EntityMapping[]>]
[-AlertDescriptionFormat <String>] [-AlertDisplayNameFormat <String>] [-AlertSeverityColumnName <String>] [-AlertTacticsColumnName <String>] [-DefaultProfile
<PSObject>] [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>]

[-NoWait] [-Proxy <Uri>] [-ProxyCredential
<PSCredential>] [-ProxyUseDefaultCredentials] -NRT [-WhatIf] [-Confirm] [<CommonParameters>]

Update-AzSentinelAlertRule -InputObject <ISecurityInsightsIdentity> [-AlertRuleTemplateName <String>] [-Enabled] [-Disabled] [-DefaultProfile <PSObject>] [-AsJob]
[-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-NoWait] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]
[-ProxyUseDefaultCredentials] -FusionMLorTI [-WhatIf] [-Confirm] [<CommonParameters>]

Update-AzSentinelAlertRule -InputObject <ISecurityInsightsIdentity> [-AlertRuleTemplateName <String>] [-Enabled] [-Disabled] [-Description <String>]
[-DisplayNamesFilter <String[]>] [-DisplayNamesExcludeFilter <String[]>] [-ProductFilter <MicrosoftSecurityProductName>] [-SeveritiesFilter <AlertSeverity[]>]
[-DefaultProfile <PSObject>] [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-NoWait] [-Proxy <Uri>]
[-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] -MicrosoftSecurityIncidentCreation [-WhatIf] [-Confirm] [<CommonParameters>]

Update-AzSentinelAlertRule -InputObject <ISecurityInsightsIdentity> [-AlertRuleTemplateName <String>] [-Enabled] [-Disabled] [-Description <String>] [-Query <String>]
[-DisplayName <String>] [-SuppressionDuration <TimeSpan>] [-SuppressionEnabled] [-Severity <AlertSeverity>] [-Tactic <AttackTactic>] [-CreateIncident]
[-GroupingConfigurationEnabled] [-ReOpenClosedIncident] [-LookbackDuration <TimeSpan>] [-MatchingMethod <String>] [-GroupByAlertDetail <AlertDetail[]>]
[-GroupByCustomDetail <String[]>] [-GroupByEntity <EntityMappingType[]>] [-EntityMapping <EntityMapping[]>] [-AlertDescriptionFormat <String>]
[-AlertDisplayNameFormat <String>] [-AlertSeverityColumnName <String>] [-AlertTacticsColumnName <String>] [-DefaultProfile <PSObject>] [-AsJob] [-Break]
[-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-NoWait] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]
[-ProxyUseDefaultCredentials] -NRT [-WhatIf] [-Confirm] [<CommonParameters>]

Update-AzSentinelAlertRule -InputObject <ISecurityInsightsIdentity> [-AlertRuleTemplateName <String>] [-Enabled]

[-Disabled] [-Description <String>] [-Query <String>]

[-DisplayName <String>] [-SuppressionDuration <TimeSpan>] [-SuppressionEnabled] [-Severity <AlertSeverity>] [-Tactic <AttackTactic>] [-CreateIncident]

[-GroupingConfigurationEnabled] [-ReOpenClosedIncident] [-LookbackDuration <TimeSpan>] [-MatchingMethod <String>] [-GroupByAlertDetail <AlertDetail[]>]

[-GroupByCustomDetail <String[]>] [-GroupByEntity <EntityMappingType[]>] [-EntityMapping <EntityMapping[]>] [-AlertDescriptionFormat <String>]

[-AlertDisplayNameFormat <String>] [-AlertSeverityColumnName <String>] [-AlertTacticsColumnName <String>] [-QueryFrequency <TimeSpan>] [-QueryPeriod <TimeSpan>]

[-TriggerOperator <TriggerOperator>] [-TriggerThreshold <Int32>] [-EventGroupingSettingAggregationKind <EventGroupingAggregationKind>] [-DefaultProfile <PSObject>]

-Scheduled [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-NoWait] [-Proxy <Uri>] [-ProxyCredential

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

DESCRIPTION

Updates the alert rule.

PARAMETERS

-ResourceGroupName <String>

The Resource Group Name.

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

-RuleId <String>

[Alias('RuleId')]

The name of Operational Insights Resource Provider.

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

-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

-AlertRuleTemplateName <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Enabled [<SwitchParameter>]

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-Disabled [<SwitchParameter>]

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-Description <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Query <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DisplayName <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SuppressionDuration <TimeSpan>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SuppressionEnabled [<SwitchParameter>]

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-Severity <AlertSeverity>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Tactic <AttackTactic>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-CreateIncident [<SwitchParameter>]

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-GroupingConfigurationEnabled [<SwitchParameter>]

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-ReOpenClosedIncident [<SwitchParameter>]

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-LookbackDuration <TimeSpan>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-MatchingMethod <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-GroupByAlertDetail <AlertDetail[]>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-GroupByCustomDetail <String[]>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-GroupByEntity <EntityMappingType[]>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-EntityMapping <EntityMapping[]>

'Account', 'Host', 'IP', 'Malware', 'File', 'Process', 'CloudApplication', 'DNS', 'AzureResource', 'FileHash', 'RegistryKey', 'RegistryValue', 'SecurityGroup',

'URL', 'Mailbox', 'MailCluster', 'MailMessage', 'SubmissionMail'

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

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-AlertDescriptionFormat <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-AlertDisplayNameFormat <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-AlertSeverityColumnName <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-AlertTacticsColumnName <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-QueryFrequency <TimeSpan>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-QueryPeriod <TimeSpan>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-TriggerOperator <TriggerOperator>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-TriggerThreshold <Int32>

Required? false

Position? named

Default value 0

Accept pipeline input? false

Accept wildcard characters? false

-EventGroupingSettingAggregationKind <EventGroupingAggregationKind>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DisplayNamesFilter <String[]>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DisplayNamesExcludeFilter <String[]>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProductFilter <MicrosoftSecurityProductName>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SeveritiesFilter <AlertSeverity[]>

High, Medium, Low, Informational

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

-Scheduled [<SwitchParameter>]

Required? true

Position? named

Default value False

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

-NRT [<SwitchParameter>]

Required? true

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-MicrosoftSecurityIncidentCreation [<SwitchParameter>]

Required? true

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-FusionMLorTI [<SwitchParameter>]

Required? true

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.AlertRule

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.

ENTITYMAPPING <EntityMapping[]>: 'Account', 'Host', 'IP', 'Malware', 'File', 'Process', 'CloudApplication', 'DNS', 'AzureResource', 'FileHash', 'RegistryKey',
'RegistryValue', 'SecurityGroup', 'URL', 'Mailbox', 'MailCluster', 'MailMessage', 'SubmissionMail'
[EntityType <EntityMappingType?>]: The V3 type of the mapped entity
[FieldMapping <IFieldMapping[]>]: array of field mappings for the given entity mapping
[ColumnName <String>]: the column name to be mapped to the identifier
[Identifier <String>]: the V3 identifier of the entity

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:\>Update-AzSentinelAlertRule -ResourceGroupName "myResourceGroupName" -WorkspaceName "myWorkspaceName" -ruleId "4a21e485-75ae-48b3-a7b9-e6a92bcfe434" -Query

"SecurityAlert | take 2"

RELATED LINKS

https://learn.microsoft.com/powershell/module/az.securityinsights/Update-azsentinelalertrule