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

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

NAME

New-AzSentinelAlertRule

SYNOPSIS

Creates the alert rule.

SYNTAX

New-AzSentinelAlertRule -ResourceGroupName <String> -WorkspaceName <String> [-SubscriptionId <String>] [-RuleId <String>] -Kind <AlertRuleKind> -AlertRuleTemplate

<String> [-Enabled] [-DefaultProfile <PSObject>] [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-NoWait] [-Proxy

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

New-AzSentinelAlertRule -ResourceGroupName <String> -WorkspaceName <String> [-SubscriptionId <String>] [-RuleId <String>] -Kind <AlertRuleKind> [-Enabled] -Query

<String> -DisplayName <String> -Severity <AlertSeverity> [-AlertRuleTemplateName <String>] [-Description <String>] [-SuppressionDuration <TimeSpan>]

[-SuppressionEnabled] [-Tactic <String[]>] [-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] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzSentinelAlertRule -ResourceGroupName <String> -WorkspaceName <String> [-SubscriptionId <String>] [-RuleId <String>] -Kind <AlertRuleKind> [-Enabled] -Query
<String> -DisplayName <String> -Severity <AlertSeverity> -QueryFrequency <TimeSpan> -QueryPeriod <TimeSpan> -TriggerOperator <TriggerOperator> -TriggerThreshold
<Int32> [-AlertRuleTemplateName <String>] [-Description <String>] [-SuppressionDuration <TimeSpan>] [-SuppressionEnabled] [-Tactic <String[]>] [-CreateIncident]
[-GroupingConfigurationEnabled] [-ReOpenClosedIncident] [-LookbackDuration <TimeSpan>] [-MatchingMethod <String>] [-GroupByAlertDetail <AlertDetail[]>]
[-GroupByCustomDetail <String[]>] [-GroupByEntity <EntityMappingType[]>] [-EntityMapping <EntityMapping[]>] [-AlertDescriptionFormat <String>]
[-AlertDisplayNameFormat <String>] [-AlertSeverityColumnName <String>] [-AlertTacticsColumnName <String>] [-EventGroupingSettingAggregationKind
<EventGroupingAggregationKind>] [-DefaultProfile <PSObject>] [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>]
[-NoWait] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

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

DESCRIPTION

Creates 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

-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

-RuleId <String>

[Alias('RuleId')]

The Id of the Rule.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Kind <AlertRuleKind>

Kind of the the data connection

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-AlertRuleTemplate <String>

Required? true

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

-Query <String>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DisplayName <String>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Severity <AlertSeverity>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-QueryFrequency <TimeSpan>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-QueryPeriod <TimeSpan>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-TriggerOperator <TriggerOperator>

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-TriggerThreshold <Int32>

Required? true

Position? named

Default value 0

Accept pipeline input? false

Accept wildcard characters? false

-AlertRuleTemplateName <String>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Description <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

-Tactic <String[]>

[Microsoft.Azure.PowerShell.Cmdlets.SecurityInsights.Support.AttackTactic]

InitialAccess, Execution, Persistence, PrivilegeEscalation, DefenseEvasion, CredentialAccess, Discovery, LateralMovement, Collection, Exfiltration,

CommandAndControl, Impact, PreAttack

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

-EventGroupingSettingAggregationKind <EventGroupingAggregationKind>

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProductFilter <MicrosoftSecurityProductName>

Required? true

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

-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

-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

-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.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

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

PS C:\>$AlertRuleTemplateName = "f71aba3d-28fb-450b-b192-4e76a83015c8"

New-AzSentinelAlertRule -ResourceGroupName "myResourceGroupName" -WorkspaceName "myWorkspaceName" -Kind Fusion -Enabled -AlertRuleTemplateName $AlertRuleTemplateName

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

PS C:\>$AlertRuleTemplateName = "fa118b98-de46-4e94-87f9-8e6d5060b60b"

New-AzSentinelAlertRule -ResourceGroupName "myResourceGroupName" -WorkspaceName "myWorkspaceName" -Kind MLBehaviorAnalytics -Enabled -AlertRuleTemplateName
$AlertRuleTemplateName

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

PS C:\>$AlertRuleTemplateName = "0dd422ee-e6af-4204-b219-f59ac172e4c6"

New-AzSentinelAlertRule -ResourceGroupName "myResourceGroupName" -WorkspaceName "myWorkspaceName" -Kind ThreatIntelligence -Enabled -AlertRuleTemplateName
$AlertRuleTemplateName

---------- EXAMPLE 4 ----------

PS C:\>$AlertRuleTemplateName = "a2e0eb51-1f11-461a-999b-cd0ebe5c7a72"

New-AzSentinelAlertRule -ResourceGroupName "myResourceGroupName" -WorkspaceName "myWorkspaceName" -Kind MicrosoftSecurityIncidentCreation -Enabled
-AlertRuleTemplateName $AlertRuleTemplateName -ProductFilter "Azure Security Center for IoT"

---------- EXAMPLE 5 ----------

PS C:\>New-AzSentinelAlertRule -ResourceGroupName "myResourceGroup" -WorkspaceName "myWorkspaceName" -Kind Scheduled -Enabled -DisplayName "Powershell Exection Alert
(Several Times per Hour)" -Severity Low -Query "SecurityEvent | where EventId == 4688" -QueryFrequency (New-TimeSpan -Hours 1) -QueryPeriod (New-TimeSpan -Hours 1)
-TriggerThreshold 10

---------- EXAMPLE 6 ----------

PS C:\>New-AzSentinelAlertRule -ResourceGroupName "myResourceGroup" -WorkspaceName "myWorkspaceName" -Kind NRT -Enabled -DisplayName "Break glass account accessed"
-Severity High -Query "let Break_Glass_Account = _GetWatchlist('break_glass_account')\n|project UPN;\nSigninLogs\n| where UserPrincipalName in (Break_Glass_Account)"

RELATED LINKS

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