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

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

NAME

Get-AzIotSecurityAnalyticsAggregatedRecommendation

SYNOPSIS

Get IoT security aggregated recommendation

SYNTAX

Get-AzIotSecurityAnalyticsAggregatedRecommendation [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Name <System.String> -ResourceGroupName <System.String> -SolutionName <System.String> [<CommonParameters>]

DESCRIPTION

The Get-AzIotSecurityAnalyticsAggregatedAlert cmdlet returns one or more aggregated recommendations on devices of iot hub. The name of an aggregated recommendation is its type

PARAMETERS

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

Resource name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

Resource group name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SolutionName <System.String>

Solution name

Required? true

Position? named

Default value None

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

None

OUTPUTS

Microsoft.Azure.Commands.Security.Models.IotSecuritySolutionAnalytics.PSIoTSecurityAggregatedRecommendation

NOTES

---------- Example 1 ----------

Get-AzIotSecurityAnalyticsAggregatedRecommendation -ResourceGroupName "MyResourceGroup" -SolutionName "MySolution" -Name IoT_OpenPorts

Id: "/subscriptions/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX/resourceGroups/MyResourceGroup/providers/Microsoft.Security/iotSecuritySolutions/MySolution/analyticsModels/default/aggregatedRecommendations/IoT_OpenPorts"

Name: "IoT_OpenPorts"

Type: "Microsoft.Security/IoTSecurityAggregatedRecommendation"

RecommendationName: "IoT_OpenPorts"

RecommendationDisplayName: "Device has open ports"

RecommendationTypeId: ""

DetectedBy: "IoTSecurity"

HealthyDevices: -1

UnhealthyDeviceCount: 5

RemediationSteps: "Review open ports on the device and make sure they belong to legitimate and necessary processes for the device to function correctly."

ReportedSeverity: "Medium"

Description: "Found a listening endpoint on the device."

LogAnalyticsQuery: "SecurityRecommendation | where tolower(AssessedResourceId) ==

tolower('/subscriptions/075423e9-7d33-4166-8bdf-3920b04e3735/resourcegroups/iot-hub-demo/providers/microsoft.devices/iothubs/ascforiot-demo') and

tolower(RecommendationName) == tolower('IoT_OpenPorts') and TimeGenerated < now()"

Get the aggregated recommendation "IoT_OpenPorts" in security solution "MySolution" and resource group "MyResourceGroup"

---------- Example 2 ----------

Get-AzIotSecurityAnalyticsAggregatedRecommendation -ResourceGroupName "MyResourceGroup" -SolutionName "MySolution"

Array of aggregated recommendation items as shown in example 1

Get a list of aggregated recommendations in security solution "MySolution" and resource group "MyResourceGroup"

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/az.security/Get-AzIotSecurityAnalyticsAggregatedRecommendation