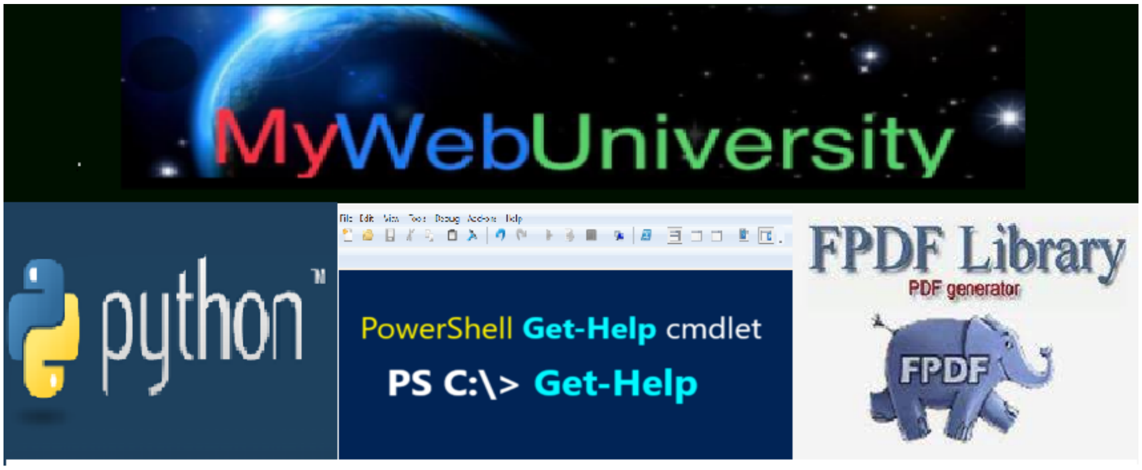

Full credit is given to all the above companies including the Operating System that this PDF file was generated!

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

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

NAME

New-AzSentinelIncident

SYNOPSIS

Creates or updates the incident.

SYNTAX

```
    New-AzSentinelIncident -ResourceGroupName <String> -WorkspaceName <String> [-Id <String>] [-SubscriptionId
<String>] [-Classification <IncidentClassification>]
     [-ClassificationComment <String>] [-ClassificationReason <IncidentClassificationReason>] [-Description <String>]
[-FirstActivityTimeUtc <DateTime>] [-Label
      <IIncidentLabel[]>] [-LastActivityTimeUtc <DateTime>] [-OwnerAssignedTo <String>] [-OwnerEmail <String>]
[-OwnerObjectId <String>] [-OwnerUserPrincipalName <String>]
   [-ProviderIncidentId <String>] [-ProviderName <String>] [-Severity <IncidentSeverity>] [-Status <IncidentStatus>] [-Title
<String>] [-DefaultProfile <PSObject>]
      [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>]
[-ProxyCredential <PSCredential>]
  [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]
```

New-AzSentinelIncident -ResourceGroupName <String> -WorkspaceName <String> [-Id <String>] [-SubscriptionId <String>] -Incident <IIncident> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

DESCRIPTION

Creates or updates the incident.

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>

Incident 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

-Incident <IIncident>

Represents an incident in Azure Security Insights.

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

Required? true

Position? named

Default value

Accept pipeline input? true (ByValue)

Accept wildcard characters? false

-Classification <IncidentClassification>

The reason the incident was closed

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ClassificationComment <String>

Describes the reason the incident was closed

Required?   false

Position?   named

Default value

Accept pipeline input?   false

Accept wildcard characters? false

-ClassificationReason <IncidentClassificationReason>

The classification reason the incident was closed with

Required?   false

Position?   named

Default value

Accept pipeline input?   false

Accept wildcard characters? false

-Description <String>

The description of the incident

Required?   false

Position?   named

Default value

Accept pipeline input?   false

Accept wildcard characters? false

-FirstActivityTimeUtc <DateTime>

The time of the first activity in the incident

Required?   false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Label <IIncidentLabel[]>

List of labels relevant to this incident

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

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-LastActivityTimeUtc <DateTime>

The time of the last activity in the incident

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-OwnerAssignedTo <String>

The name of the user the incident is assigned to.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-OwnerEmail <String>

The email of the user the incident is assigned to.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-OwnerObjectId <String>

The object id of the user the incident is assigned to.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-OwnerUserPrincipalName <String>

The user principal name of the user the incident is assigned to.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProviderIncidentId <String>

The incident ID assigned by the incident provider

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProviderName <String>

The name of the source provider that generated the incident

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Severity <IncidentSeverity>

The severity of the incident

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Status <IncidentStatus>

The status of the incident

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Title <String>

The title of the incident

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.IIncident

OUTPUTS

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

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.

INCIDENT <IIncident>: Represents an incident 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.

[Classification <IncidentClassification?>]: The reason the incident was closed

[ClassificationComment <String>]: Describes the reason the incident was closed

[ClassificationReason <IncidentClassificationReason?>]: The classification reason the incident was closed with

[Description <String>]: The description of the incident

[FirstActivityTimeUtc <DateTime?>]: The time of the first activity in the incident

[Label <IIncidentLabel[]>]: List of labels relevant to this incident

LabelName <String>: The name of the label

[LastActivityTimeUtc <DateTime?>]: The time of the last activity in the incident

[OwnerAssignedTo <String>]: The name of the user the incident is assigned to.

[OwnerEmail <String>]: The email of the user the incident is assigned to.

[OwnerObjectId <String>]: The object id of the user the incident is assigned to.

[OwnerUserPrincipalName <String>]: The user principal name of the user the incident is assigned to.

[ProviderIncidentId <String>]: The incident ID assigned by the incident provider

[ProviderName <String>]: The name of the source provider that generated the incident

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

[Status <IncidentStatus?>]: The status of the incident

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

LABEL <IIncidentLabel[]>: List of labels relevant to this incident

LabelName <String>: The name of the label

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

```
 PS C:\>New-AzSentinelIncident -ResourceGroupName "myResourceGroup" -WorkspaceName "myWorkspaceName" -Id
((New-Guid).Guid) -Title "NewIncident" -Description "My
    Description" -Severity Low -Status New
```

RELATED LINKS

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