Microsoft Azure Sentinel – ServiceNow app Classes and Functions

Table of Contents

[Introduction 4](#_Toc75190297)

[Prerequisites 5](#_Toc75190298)

[Azure: Create the Service Principal 5](#_Toc75190299)

[Delegate permissions to the Service Principal 8](#_Toc75190300)

[ServiceNow: create a user for Azure Sentinel 10](#_Toc75190301)

[Installation 11](#_Toc75190302)

[Import the application in ServiceNow 11](#_Toc75190303)

[Configure the OAuth credentials 13](#_Toc75190304)

[Configure the application 15](#_Toc75190305)

[Verify the “Closure classification” table entries 16](#_Toc75190306)

[Verify the “Sentinel Severity to ServiceNow” table mapping 17](#_Toc75190307)

[Verify the “Sentinel State to ServiceNow” table mapping 18](#_Toc75190308)

[Verify the “ServiceNow Severity to Sentinel” table mapping 18](#_Toc75190309)

[Verify the “ServiceNow State to Sentinel” table mapping 19](#_Toc75190310)

[Configure the Azure Sentinel workspace(s) details 19](#_Toc75190311)

[Review and validate the system properties 21](#_Toc75190312)

[Additional configuration 23](#_Toc75190313)

[Classes 25](#_Toc75190314)

[Alerts 25](#_Toc75190315)

[getIncidentAlerts 25](#_Toc75190316)

[alertsToHtmlTable 25](#_Toc75190317)

[AppUtils 25](#_Toc75190318)

[CustomMapping 25](#_Toc75190319)

[Entities 25](#_Toc75190320)

[getIncidentEntities 25](#_Toc75190321)

[entitiesToHtmlTable 25](#_Toc75190322)

[getEntitiesByType 26](#_Toc75190323)

[SentinelIncidents 26](#_Toc75190324)

[getSentinelIncidents 26](#_Toc75190325)

[createIncidents 26](#_Toc75190326)

[updateSentinelIncident 26](#_Toc75190327)

[updateChangedIncidents 26](#_Toc75190328)

[createUrlForObject 27](#_Toc75190329)

[getIncidentComments 27](#_Toc75190330)

[addIncidentComments 27](#_Toc75190331)

# Classes

## Alerts

This class contains functions to manipulate incidents alerts.

### getIncidentAlerts

Function used to retrieve an incident’s alerts.

Parameters:

* Environment: Sentinel environment for which we want to retrieve the alerts
* IncidentId: incident for which we want to retrieve the alerts
* Format: used to specify the format to return (json or html)
* LastSync: used to filter the incident alerts, based on the last time we queried the Sentinel API

### alertsToHtmlTable

Function formatting a list of alerts to an html table.

Parameters:

* Alerts: list of alerts objects

## AppUtils

## CustomMapping

## Entities

This class contains functions to manipulate an incident entities, like users, Ips, hosts and more.

### getIncidentEntities

Function used to retrieve an incident’s entities.

Parameters:

* Environment: Sentinel environment for which we want to retrieve the alerts
* IncidentId: incident for which we want to retrieve the alerts
* Format: used to specify the format to return (json or html)

### entitiesToHtmlTable

Function formatting a list of entities to an html table.

Parameters:

* Alerts: list of alerts objects

### getEntitiesByType

Function returning a list of entities of a specific type (ex: users, Ips, …).

Parameters:

* Entities: list of entities to filter
* Type: type of entities to return

## SentinelIncidents

This class contains the functions to retrieve Sentinel incidents, create or update incidents in ServiceNow and Sentinel, plus supporting functions for those operations.

### getSentinelIncidents

Function retrieving Azure Sentinel incidents, based on a time and custom filter (by default, a specific tag), stored in the environment configuration table.

Parameters:

* Environment: Azure Sentinel environment from which we want to retrieve the incidents
* Id: Azure Sentinel incident ID. Used when you want to get a specific incident details
* Operation: used to specify if we want to retrieve the new (created) or updated incidents, when calling the API

### createIncidents

Function creating ServiceNow incidents, based on the Sentinel incidents.

Parameters:

* Environment: Azure Sentinel environment from which the incidents has been retrieved
* Incidents: Azure Sentinel incidents to create in ServiceNow

### updateSentinelIncident

Function updating an Azure Sentinel incident, based on the ServiceNow incident changes to sync.

Parameters:

* Environment: Azure Sentinel environment where the incident to update is located
* incidentId: Id of the Azure Sentinel incident to update
* properties: changes from the ServiceNow incident to sync to Azure Sentinel

### updateChangedIncidents

Function updating a ServiceNow incident, based on the Azure Sentinel changes, like the status, severity or comments.

Parameters:

* Environment: Azure Sentinel environment where the incident is located
* modifiedIncidents: list of incidents to update in ServiceNow
* modifiedLastSync: timestamp from the updated incidents last sync. Used when retrieving latest comments or alerts

### createUrlForObject

Function used to generate the direct link to the ServiceNow incident, before being added to Azure Sentinel comments.

Parameters:

### getIncidentComments

Function used to retrieve comments from an Azure Sentinel incident, based on the last sync.

Parameters:

### addIncidentComments

Function used to add new comments to an Azure Sentinel incident, once a new work note is added to a ServiceNow incident.

Parameters:

## 