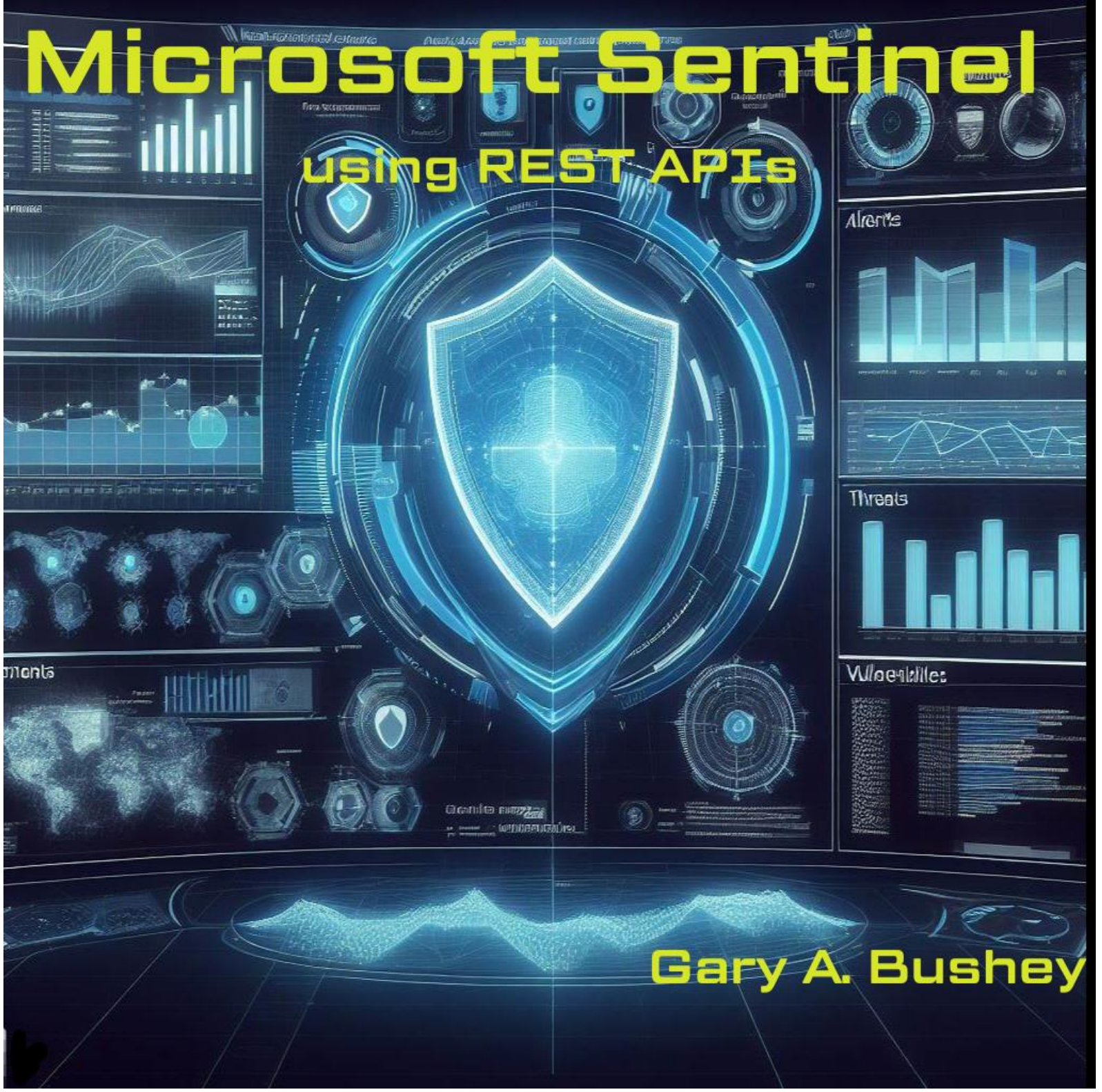
Programming Microsoft Sentinel

using REST APIs



Gary A. Bushey

Contents

Introduction

You may be asking why I would write a book on programming Microsoft Sentinel using the REST APIs when there is already documentation out there. Well, while I know the documentation team and that they do excellent work, the documentation for the REST API is lacking.

For example, the "Overview" for the "Alert Rules" section just lists the operations available. It doesn't really tell you what the "Alert Rules" APIs are for. Yes, you could figure it out by looking at the operations (and I really hope you can guess what they are for), but you really shouldn't have to, so I did it for you.

I also hope to give you a better idea of how to use the various REST APIs calls as well. Especially with the recent (at least it was recent when I started to write this book), announcement that there will not be any templates deployed as part of the Microsoft Sentinel installation (except for a few Analytic rule templates).

There are going to be some new REST API calls that are part of the preview (again, as of when I was writing this) that I will discuss in a different section. Those are going to be more important as time goes on.

Where possible, I will be making real calls into my own Microsoft Sentinel environment so you can see real examples of data. I will be using the "Microsoft Sentinel All In One V2" program to create the environment so you can easily duplicate my calls. There will be some places where I have to use my older installation, but that is mainly because of the data it already has.

Finally, I will present some use cases (probably ones I have already figured out) and show you how I went about solving them.

I hope you find some part of this book useful when creating programs for Microsoft Sentinel.

If you have ideas for additional use cases, errors, If you want more images showing how a REST API call maps to the Microsoft Sentinel portal like I did for the Analytic Rule Templates, or other comments feel free to contact me at garybushey@outlook.com. Thanks!

Version 1.0

Getting Started

There are many different programming languages available to use when developing Microsoft Sentinel programs. That is the best thing about using REST APIs, you can call them from any language.

Some of the more popular languages include PowerShell, JavaScript, C#, and Python. I will give you an introduction on using the REST APIs in PowerShell and JavaScript. I am not going to cover C#, mainly because it has been so long since I have programmed in it nor Python, since there is an amazing library called MSTICPy that you can handle most of the calls already.

For the most part, I am going to have all my code examples in PowerShell for many reasons including, easy to write, easy to use, easy to understand, and I already have a lot of examples written in PowerShell.

The main thing is to create the authentication token that you will use when making the call.

PowerShell

This article describes how to get started using PowerShell with Azure: https://learn.microsoft.com/en-us/powershell/azure/get-started-azureps. Once you have it setup, use the "Connect-AzAccount" command to connect to Azure.

After you connect to your tenant, the following PowerShell commands will get you ready to call the REST APIs. Basically, what you are doing is getting information from Azure to create the "$authHeader".

I am not going to go into details about how this all works, as you just need to know it works. BTW, I added blank lines between the different commands to give you a better idea of what each command is.

```
$context = Get-AzContext

$userProfile =
[Microsoft.Azure.Commands.Common.Authentication.Abstractions.AzureRmProfileProvid
er]::Instance.Profile

$profileClient = New-Object -TypeName
Microsoft.Azure.Commands.ResourceManager.Common.RMProfileClient -ArgumentList
($userProfile)

$token = $profileClient.AcquireAccessToken($context.Subscription.TenantId)

$authHeader = @{
    'Content-Type' = 'application/json'
    'Authorization' = 'Bearer ' + $token.AccessToken
  }
```

Once you have this information, you will use the "$authHeader" to make the call like shown below. Note that the "$url" variable uses other variables for things like the subscription Id, resource group name, and workspace name. See the next section, Common Parameters, for more information on those.

One thing I do is to define those variables at the top of my PowerShell script, or right after I run the commands above, so I can reuse them. I keep a file of all the different REST APIs call I make and by just changing the variables, it is easy for me to run the REST APIs in different environments.

```
$baseUrl = "https://management.azure.com/subscriptions/$SubscriptionId" +
"/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights" +
"/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/"
$apiVersion = "?api-version=2023-09-01-preview"
$url = $baseURL + "contentProductPackages" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader
).value
```

You may have noticed that the second provider being called is "Microsoft.SecurityInsights". This was the original name (or maybe the code name) for Microsoft Sentinel and, since it was used originally, it was kept for backward compatibility. If you try to find the Microsoft Sentinel REST APIs in Gitub, they are listed under "Microsoft:SecurityInsights".

Also, you may see "Azure Sentinel" listed in places which was the name of Microsoft Sentinel when it was initially released. Again this is for backward compatibility.

Once the URL has been defined, you can then use the "Invoke-RestMethod" in PowerShell to make the call. You will pass in the method type, "Get" in this case, the Uri, and the authentication header.

If you are doing a List REST API call you can add ".value" at the end to get the data, for the most part. If you are doing a Get REST API call, do not add it as the data is being returned at the top level. If you expect to get a skipToken returned, do not use add the ".value" otherwise you will not get the skipToken result. See the "Filtering" section below for more information.

If you were going to use the "Post" or "Put" methods, you would need to create and pass in the body as well.

This can be done like the following. Note that this is only one way to create the body. There are others.

```
 $body = @{
  "kind"       = "Scheduled"
  "properties" = @{
   "enabled"                = "true"
   "alertRuleTemplateName" = $name
   "displayName"           = $ruleTemplate.displayName
   "description"           = $ruleTemplate.description
   "severity"              = $ruleTemplate.severity
   "tactics"               = $ruleTemplate.tactics
   "techniques"            = $ruleTemplate.techniques
   "query"                 = $ruleTemplate.query
   }
}
```

BTW, this is a section of the code that shows the way I used to create an analytic rule from a rule template. I have since found a better way to do it. This will be shown later.

JavaScript

Calling Azure REST APIs from a JavaScript application is a bit more involved than it is with PowerShell. You will need to create an Azure AD application that has the proper permissions and can impersonate a user.

The main issue with using JavaScript is how to connect to Azure. Luckily there is a library called MSAL (Microsoft Authentication Library) that can be used to perform this function. I will not go into details here on how to use it as there is a great site that shows how to use this library with many different languages. Microsoft identity platform authentication libraries - Microsoft Entra | Microsoft Learn as well as Tutorial: Register a Single-page application with the Microsoft identity platform - Microsoft Entra | Microsoft Learn

When you have that configured, you can get the bearer token needed to make the call to the Azure REST API.

Once everything is setup, you can use the JavaScript "fetch" command to make the call and then, using the JavaScript promises, filter out the information you need. The PowerShell call to get the data needed show above would look like the following in JavaScript (assuming you have the "accessToken" value already and "rulesURL" is set to a REST API URL):

```
const headers = new Headers();
  headers.append("Authorization", `Bearer ${accessToken}`);
  const options = {
    method: "GET",
    headers: headers,
  };
let results = fetch(rulesURL, options) //Load the rules to see if a rule template
has been used
      .then((response) => response.json())
```

```
    .then((response) => response.value)
    .catch((error) => console.log(error))
```

Typically, you would either call the fetch command asynchronously or the entire function (which is what I do in my code). Note that I used Typescript and React when I wrote my sample code so the code may not look exactly right.

I have written a blog post on how to do this all here: [Call Microsoft Sentinel REST APIs from JavaScript – Yet Another Security Blog (garybushey.com)]

Common Parameters

Almost all the REST APIs will use the following parameters:

Name	Description
resourceGroupName	The name of the Resource Group where the MS Sentinel is located. Example: “devbookrg”
subscriptionId	The ID of the subscription where the MS Sentinel is located. This will be a GUID. Example: “15a9a6a9-0372-4dd9-be19-432f22c73e1a”
workspaceName	The name of the Log Analytics workspace where MS Sentinel is located. Example: “devbookwg”
apiVersion	The version of the API to use. For the stable REST APIs, this will “2023-02-01”. This version number will not change often. For any preview REST APIs, this will be “2023-09-01-preview”. This version will be updated almost monthly.
baseURL	Set to = “https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/"

Types of calls

While not a hard and fast rule, most of the different groups of REST API calls will include the following types of calls. There may be more than these or, in some cases, not all these REST API calls will be available.

Name	Description
Create/Update	This will allow you to create a new entry or update an existing one.
Delete	Delete an existing entry.
Get	Get a specific entry.
List	List all the entries. There may be limits as to how many you can return at one time and some will allow you to add filtering options (see below)

Filtering

Some List REST API calls will allow you to filter the results using the URL. In those cases, the different filtering options you can use will be shown with each entry.

Name	Description
$filter	Filters the results based on a Boolean expression
$orderby	Sorts the results
$skipToken	This can only be used if a skipToken was returned in a previous call. For example, if you have more than 50 incidents that would normally be returned in a query, there will be a "nextLink" value returned along with the 50 incidents. You then use this value to get more results, skipping the first 50
$top	Returns only the first X items

Using skipToken

This will return all the incidents that were created since 5 November 2023 at just about 5:44PM GMT.

Note the lack of ".value" at the end of the call to create the "$results" variable. Also, note how to specify the field you want to use in the filters.

Sample Request

```
$url = $baseUrl + "incidents" + $apiVersion + "$filter=properties\createdTimeUtc
ge 2023-11-05T17:43:59.824Z"
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Note that in the text below, I have deleted a lot of the characters being returned to save space.

If we look at "$results.nextlink", the value will look like what is shown below. If we need to get more incidents returned, we can just use this value as the URL for the next call. In this case we would need to use "$results.value" to get to the actual incidents being returned.

```
https://management.azure.com/subscriptions/34bdcce3-c06f-416b-aaa0-
24683117cc68/resourceGroups/devbookrg/providers/Microsoft.OperationalInsights/wor
kspaces/devbook/providers/Microsoft.SecurityInsights/incidents?api-version=2023-
```

```
09-01-preview&='properties.createdTimeUtc ge 2020-11-
01T17:43:59.824Z&$skipToken=H4sIAAAAAAAACk1WX..._AkAAA==
```

Keep in mind that we can use many different entries for the filter, as long as each entry returns either a true or false value. For example, here is a much more complex query which includes sorting and returning a specific number of items. Note that all the characters have been URL encoded. It is recommended that you do this for your queries.

The query below will return all those incidents that meet all the following criteria:

1) The incident's status equals "New" or "Active"
2) The incident's created time is greater than 5 November 2023 at 4:59.824 GMT and less than 23 November 2023 at 4:59.824 GMT

The incidents will be returned using the created time property in descending order and only the first 30 will be returned.

Sample Request

```
$url = $baseUrl + "incidents" + $apiVersion +
"&%24filter=(properties%2Fstatus%20eq%20'New'%20or%20properties%2Fstatus%20eq%20'
Active')%20and%20(properties%2FcreatedTimeUtc%20ge%202023-11-
05T17%3A43%3A59.824Z%20and%20properties%2FcreatedTimeUtc%20le%202020-11-
23T17%3A43%3A59.824Z)&%24orderby=properties%2FcreatedTimeUtc%20desc&%24top=30"
```

Stable APIs

I am not really sure what the difference is between Stable APIs and Preview APIs other than there is no guarantee that the Preview APIs will actually see the light of day (or are working correctly). I tend to use the preview APIs myself.

The stable API version number will not change as often as the preview APIs so you can be assured that you will not need to change your code often.

If you look at the main documentation page, Microsoft Sentinel REST API | Microsoft Learn, you will notice that there are more REST API calls in preview than in the stable version. This is great, as that means that Microsoft Sentinel functionality is constantly growing!

Note: As of right now, the preview REST APIs are not showing in this website anymore. Hopefully they will come back

---

Actions

This API is to set actions to an Analytics alert rule. The actions are automation that will be run when the analytic rule creates an incident.

THIS FEATURE HAS BEEN DEPRECATED IN MICROSOFT SENTINEL SO I WILL NOT GO INTO THIS REST API

Documentation URL: Actions - REST API (Azure Sentinel) | Microsoft Learn

Alert Rule Templates

This REST API will allow you to GET or LIST Alert Rule templates. Alert Rule templates are what you can use to create rules. They are either installed out of the box when a new Microsoft Sentinel is created (there are a few that are still created) or by installing solutions. Note that there is no REST API to CREATE a new rule template.

NOTE: As of writing this section, this will only return those Alert Rule Templates that came Out Of The Box (OOTB) with Microsoft Sentinel. It is still usable but will not return any Alert Rule Templates that have been deployed via Content Hub Solutions. Since Content Hubs Solutions are the new way to deploy almost all Alert Rule Templates in Microsoft Sentinel, either this REST API will be deprecated, or it will be rewritten to return the Alert Rule Templates that were created via the Content Hub Solution.

Documentation URL: Alert Rule Templates - REST API (Azure Sentinel) | Microsoft Learn

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/alertRuleTemplates/**{alertRuleTemplateId}**?**{apiVersion}**

You can use the LIST REST API call, shown below, to get a list of all the alert rule templates to get the "alertruleTemplateId" value.

Sample Request

```
$url = $baseURL + "alertRuleTemplates/968358d6-6af8-49bb-aaa4-187b3067fb95" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/AlertRuleTemplates/968358d6-6af8-49bb-aaa4-187b3067fb95",
  "name": "968358d6-6af8-49bb-aaa4-187b3067fb95",
  "type": "Microsoft.SecurityInsights/AlertRuleTemplates",
  "kind": "Scheduled",
  "properties": {
    "queryFrequency": "PT12H",
```

```
    "queryPeriod": "PT12H",
    "triggerOperator": "GreaterThan",
    "triggerThreshold": 0,
    "severity": "High",
    "query": "let successCodes = dynamic([200, 302, 401]);\nW3CIISLog\n| where
scStatus has_any (successCodes)\n| where ipv4_is_private(cIP) == False\n| where
csUriStem hasprefix \"/autodiscover/autodiscover.json\"\n| project TimeGenerated,
cIP, sIP, sSiteName, csUriStem, csUriQuery, Computer, csUserName, _ResourceId,
FileUri\n| where (csUriQuery !has \"Protocol\" and isnotempty(csUriQuery))\nor
(csUriQuery has_any(\"/mapi/\", \"powershell\"))\nor (csUriQuery contains \"@\"
and csUriQuery matches regex @\"\\.[a-zA-Z]{2,4}?(?:[a-zA-Z]{2,4}\\/)\")\nor
(csUriQuery contains \":\" and csUriQuery matches regex @\"\\:[0-9]{2,4}\\/\")\n|
extend timestamp = TimeGenerated, HostCustomEntity = Computer, IPCustomEntity =
cIP, AccountCustomEntity = csUserName, ResourceCustomEntity = _ResourceId,
FileCustomEntity = FileUri",
    "entityMappings": [
      {
        "entityType": "Account",
        "fieldMappings": [
          {
            "identifier": "FullName",
            "columnName": "AccountCustomEntity"
          }
        ]
      },
      {
        "entityType": "Host",
        "fieldMappings": [
          {
            "identifier": "FullName",
            "columnName": "HostCustomEntity"
          }
        ]
      },
      {
        "entityType": "IP",
        "fieldMappings": [
          {
            "identifier": "Address",
            "columnName": "IPCustomEntity"
          }
        ]
      },
      {
        "entityType": "AzureResource",
```

```
        "fieldMappings": [
          {
            "identifier": "ResourceId",
            "columnName": "ResourceCustomEntity"
          }
        ]
      }
    ],
    "version": "1.0.1",
    "tactics": [
      "InitialAccess"
    ],
    "techniques": [
      "T1190"
    ],
    "displayName": "Exchange SSRF Autodiscover ProxyShell - Detection",
    "description": "This query looks for suspicious request patterns to Exchange
servers that fit patterns recently\nblogged about by PeterJson. This exploitation
chain utilises an SSRF vulnerability in Exchange\nwhich eventually allows the
attacker to execute arbitrary Powershell on the server. In the
example\npowershell can be used to write an email to disk with an encoded
attachment containing a shell.\nReference:
https://peterjson.medium.com/reproducing-the-proxyshell-pwn2own-exploit-
49743a4ea9a1",
    "lastUpdatedDateUTC": "2022-10-31T00:00:00Z",
    "createdDateUTC": "2021-08-09T00:00:00Z",
    "status": "Available",
    "requiredDataConnectors": [
      {
        "connectorId": "AzureMonitor(IIS)",
        "dataTypes": [
          "W3CIISLog"
        ]
      }
    ],
    "alertRulesCreatedByTemplateCount": 0
  }
}
```

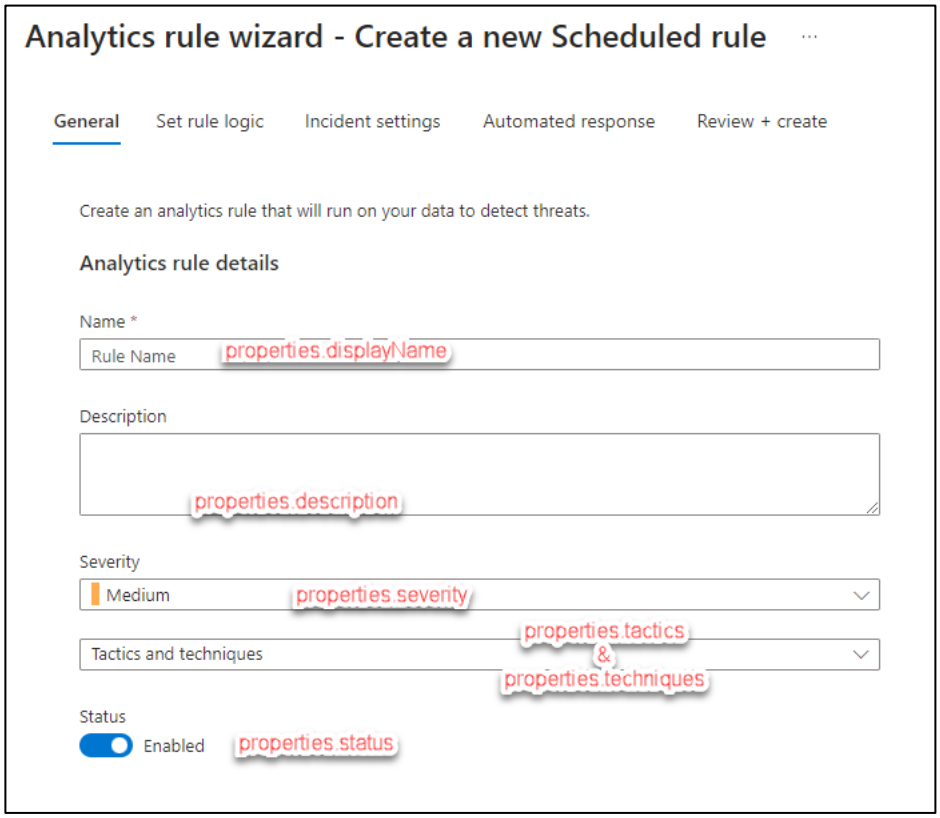

The “requiredDataConnectors” will show what data connectors should be activated before the rule template is used. I say should since you can still create the rule using the rule template even if you don’t have the required data connectors. Your rule will fail and the system will automatically deactivate it after a while, but you can still create it.

Notice that the last entry in the list called “alertRulesCreatedByTemplateCount”. This is how many rules were created using this template. If this is greater than zero, the “In Use” icon will show up before the rule template’s name in the GUI.

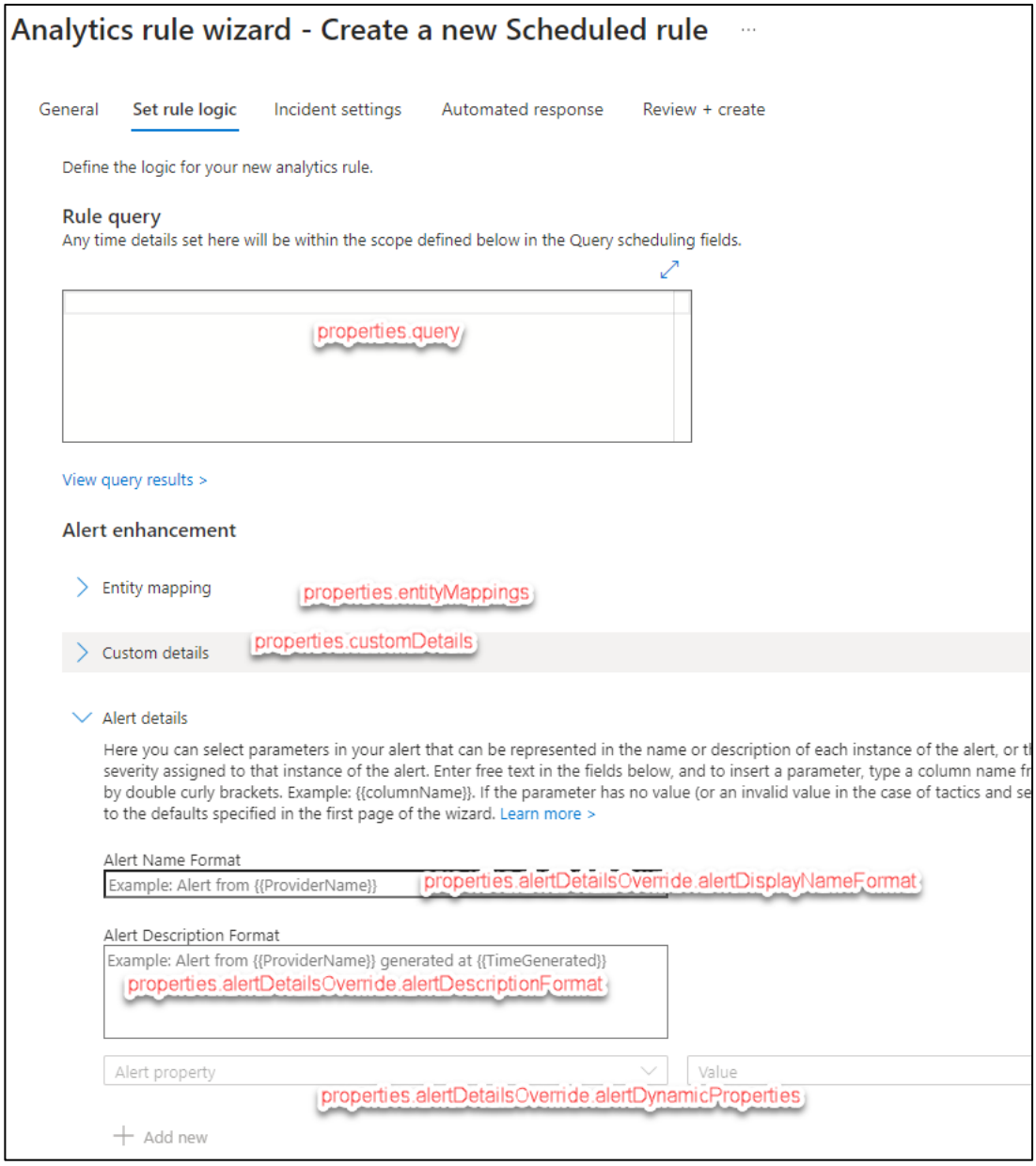
Scheduled Rule Mapping

This next section will show how the returned values in the JSON map to creating a new analytic rule using the GUI. Keep in mind that different rule types have different pages.

General tab

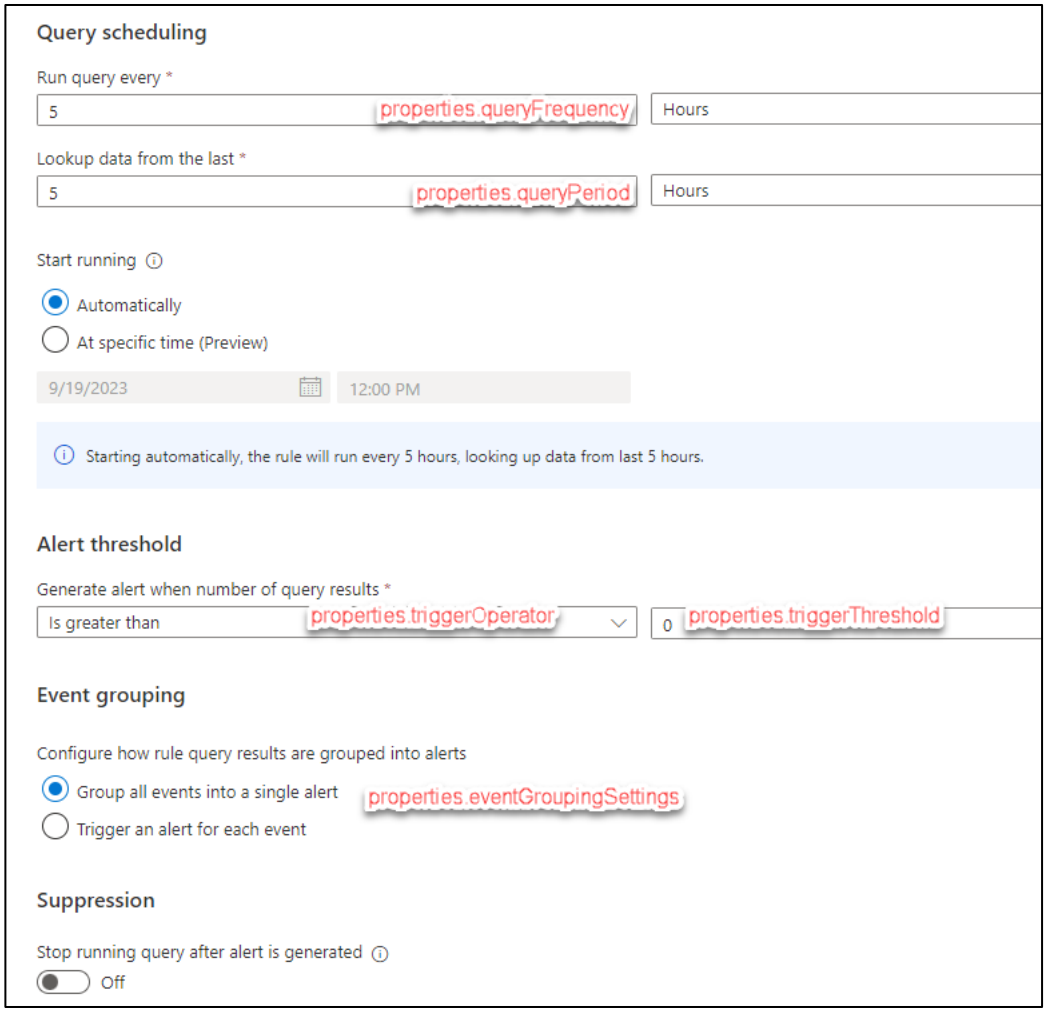


Set rule logic (top part of the page)



Note, that the Alert Details has that section for the dynamic properties but it also includes “properties.alertDetailsOverride.alertTacticsColumnName” and “properties.alertDetailsOverride.alertSeverityColumnName” if you want to override either the tactics or the techniques with the columns. The other entries (“AlertLink”,”ConfidenceLevel”,”ConfidenceScore”,”ExtendedLinks”,”ProductName”,”ProviderName”,”ProductComponentName”,”RemediationSteps”, and “Techniques” will use the “properties.alertDetailsOverride.alertDynamicProperties” field.

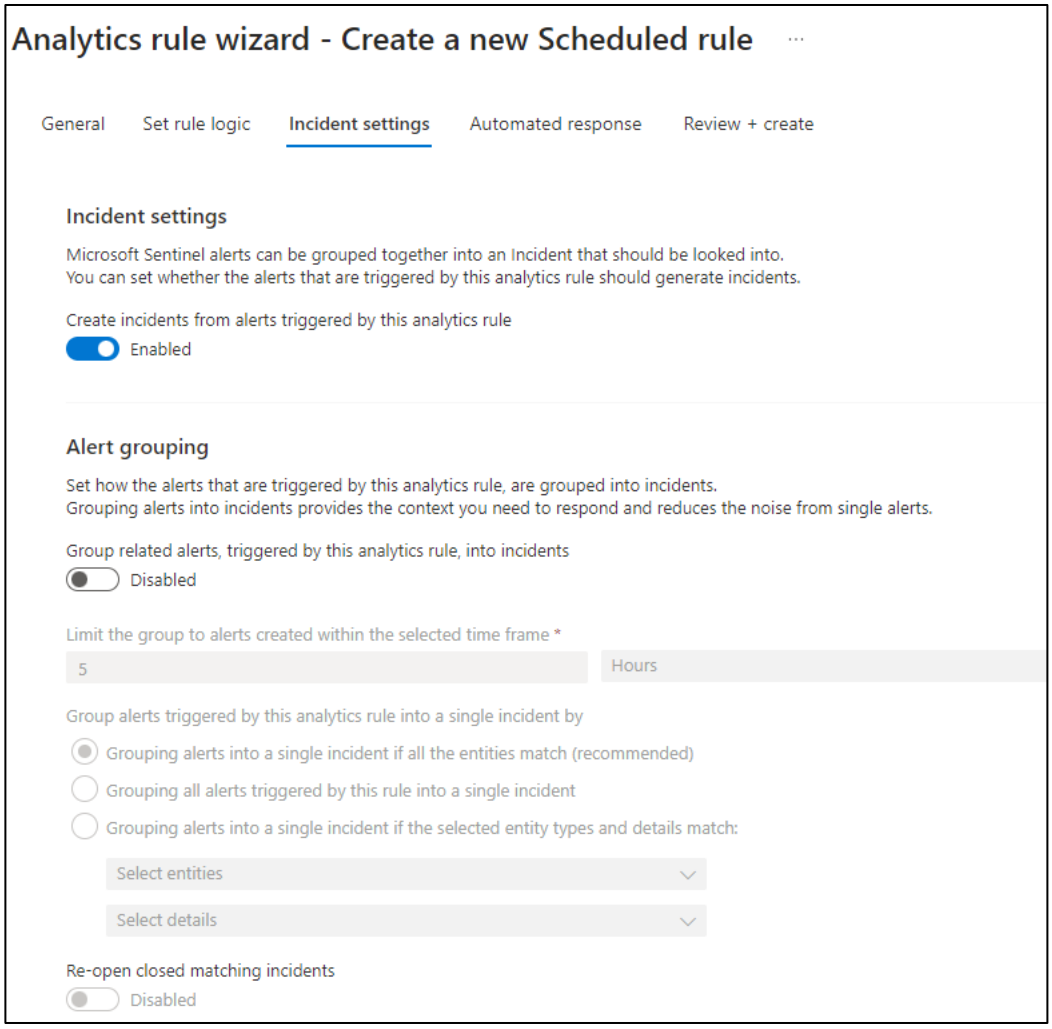
Set rule logic (bottom part of the page)



There is nothing in this REST API call for the ability to state when to start running the query as this is newer functionality than this version of the REST API supports.

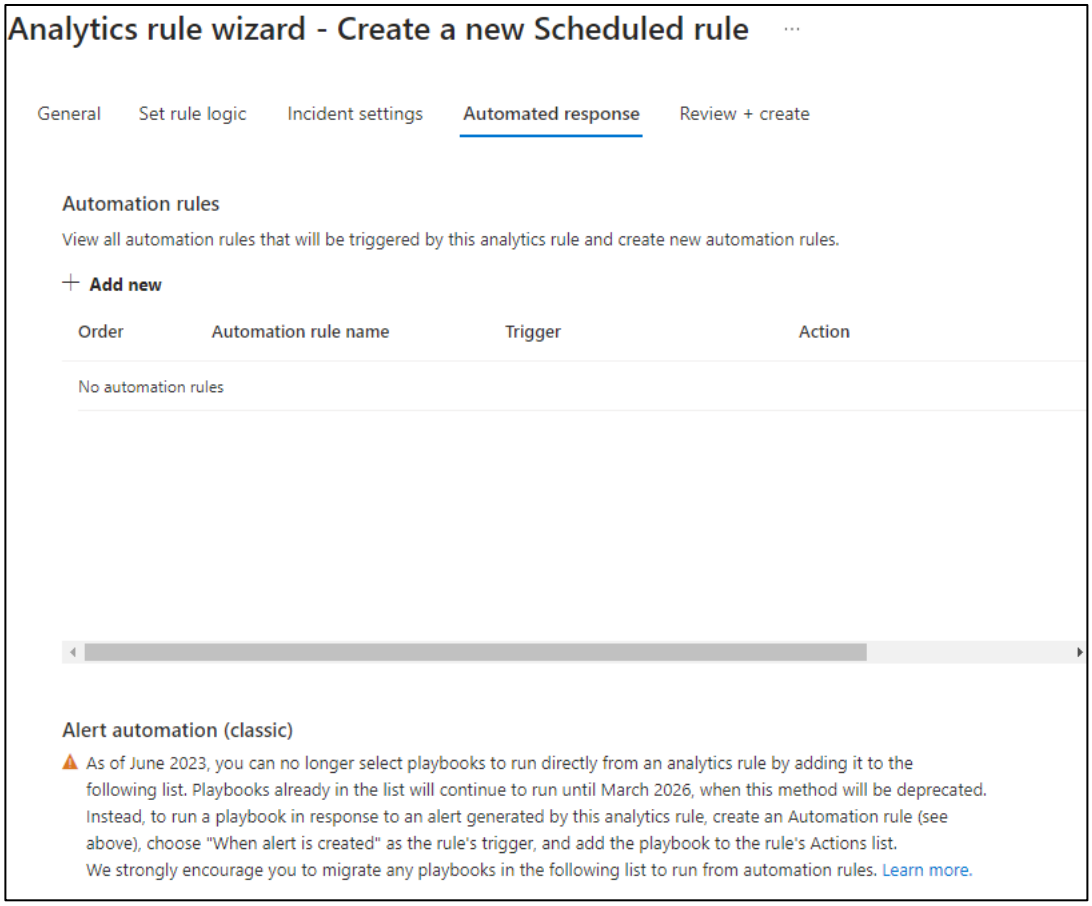
There is also no support in the template for alert suppression.

Incident Settings



There is nothing in the template REST API for any of these fields! You will be able to add this information when creating the rule itself.

Automated rule



There is nothing in the template for any of these fields. The “Automation rules” section will be handled by the “Automation Rules” REST API call and the “Alert automation” is deprecated (see the “Actions” section above)

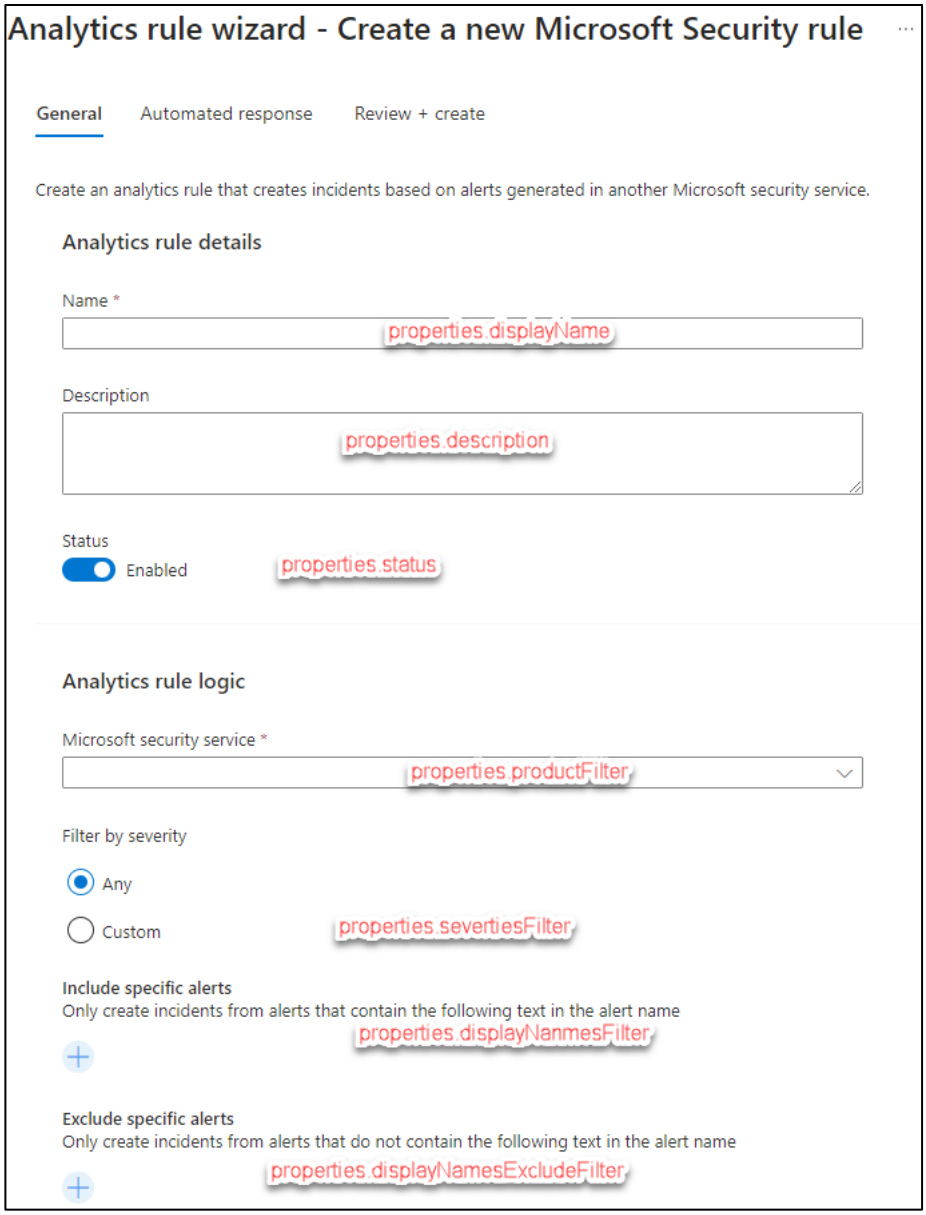
NRT

For a “NRT” rule, the screens are almost the same except there is no way to specify when the query will be run since it runs every minute.

The other screens are the same as for the Scheduled rules.

Microsoft incident

General



The “Automated Response” tab is the same as with “Scheduled” rules.

Additional fields of interest

Name	Definition
properties.requiredDataConnectors	These are the data connectors that the rule requires. If the table that the data connector creates does not exist, the rule will not be created.
properties.alertRulesCreatedByTemplateCount	How many rules have been created using this template. This will be discussed more in the “Alert Rules” section.

properties.version	The version number of the template. This is used to determine if there are changes that need to be updated.

List

Http Method: Get

REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/alertRuleTemplates?**{apiVersion}**

"List" works the same way a "Get" except that it returns a JSON array where each entry is an individual rule template.

Keep in mind that there is a chance that not all the fields you would get in the "Get" call would show in the "List" call. Therefore, if you are going to use the Rule Template to create a new Rule, it is better to make a "Get" call to load the individual Rule Template which will make sure all the fields are loaded. Hopefully this will change in the future.

Alert Rules

These REST APIs will allow you to CREATE/UPDATE, DELETE, GET or LIST Alert Rules. Alert rules are what get run to help determine if there are any events in your environment.

Note that while the REST API is called "Alert Rules", the rules will show up under "Analytic Rules" in the Microsoft Sentinel portal. For the rest of the section, I will refer to them as "Analytic Rules".

Documentation URL: Alert Rules - REST API (Azure Sentinel) | Microsoft Learn

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/alertRules/**{ruleId}**?**{apiVersion}**

This REST API call will allow you to either create a new Analytic Rule, if one with the "ruleId" does not exist or update one if it does.

For this call, you will need to pass in a body to the Http PUT call. The body will be different depending on what type of rule you are creating. The body will contain all the fields in the "properties" section that we have gone over in the "Rule Templates" section, so we will not go over them again. Also, look at the "Get" section below for information regarding the "Incident settings" page.

Here is a tip I have found after manually setting each field in the "properties" section. You can read the properties from the rule template and then set it directly to the properties of the body. If you want to make sure you can map the Analytic Rule back to the Rule Template, you will then need to add "alertRuleTemplateName" and "templateVersion" to the body. Then you just need to set the "kind" to the type of rule you are trying to create. For example, "MicrosoftSecurityIncidentCreation","NRT", or "Scheduled". This way, if there are new fields add to the rule template that can be added to a new rule, it will automatically be added. Some of my earlier code didn't do this and had to be constantly updated.

Based on the tip above, I could create the body in PowerShell using code like:

```
$body = ""
$properties = <properties from the rule template>
$properties.enabled = $true  #Added this to make sure each rule was enabled
#Add the field to link this rule with the rule template so that the rule template
will show up as used
#We had to use the "Add-Member" command since this field does not exist in the
rule template that we are copying from.
$properties | Add-Member -NotePropertyName "alertRuleTemplateName" -
NotePropertyValue $result.properties.mainTemplate.resources[0].name
```

```
$properties | Add-Member -NotePropertyName "templateVersion" -NotePropertyValue
$result.properties.mainTemplate.resources[1].properties.version

#Depending on the type of alert we are creating, the body has different
parameters
$body = @{
    "kind"       = "MicrosoftSecurityIncidentCreation"
    "properties" = $properties
}
```

Of course, you could modify any field in the "properties" section you want.

```
$guid = New-Guid
$url = $baseUrl + "alertRules/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $restURL -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

We do need to convert the body into JSON, hence the "ConvertTo-Json" call, and need to make sure we translate everything, hence the setting of "-Depth" to 50 (which is overkill).

If you are creating a new rule from scratch, you will need to fill out all the properties you need. Use the images of the GUI as the guideline as to what fields to fill in.

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/alertRules/**{ruleId}**?**{apiVersion}**

This REST API call will delete an existing Analytic rule where its Id matches the "ruleId" being passed in. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/alertRules/**{ruleId}**?**{apiVersion}**

This REST API call will retrieve a single Analytic rule as specified in the "ruleId" parameter. You can use the LIST REST API call, shown below, to get a list of all the automation rules to get the "ruleId" value.

Sample request

```
$url=$baseURL + "alertRules/99ce9db5-41b3-4cf9-b909-d408e21f277d" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

All the rules use a GUID for the "ruleId" except for the Fusion rule. That one uses "BuiltInFusion"

Sample Response

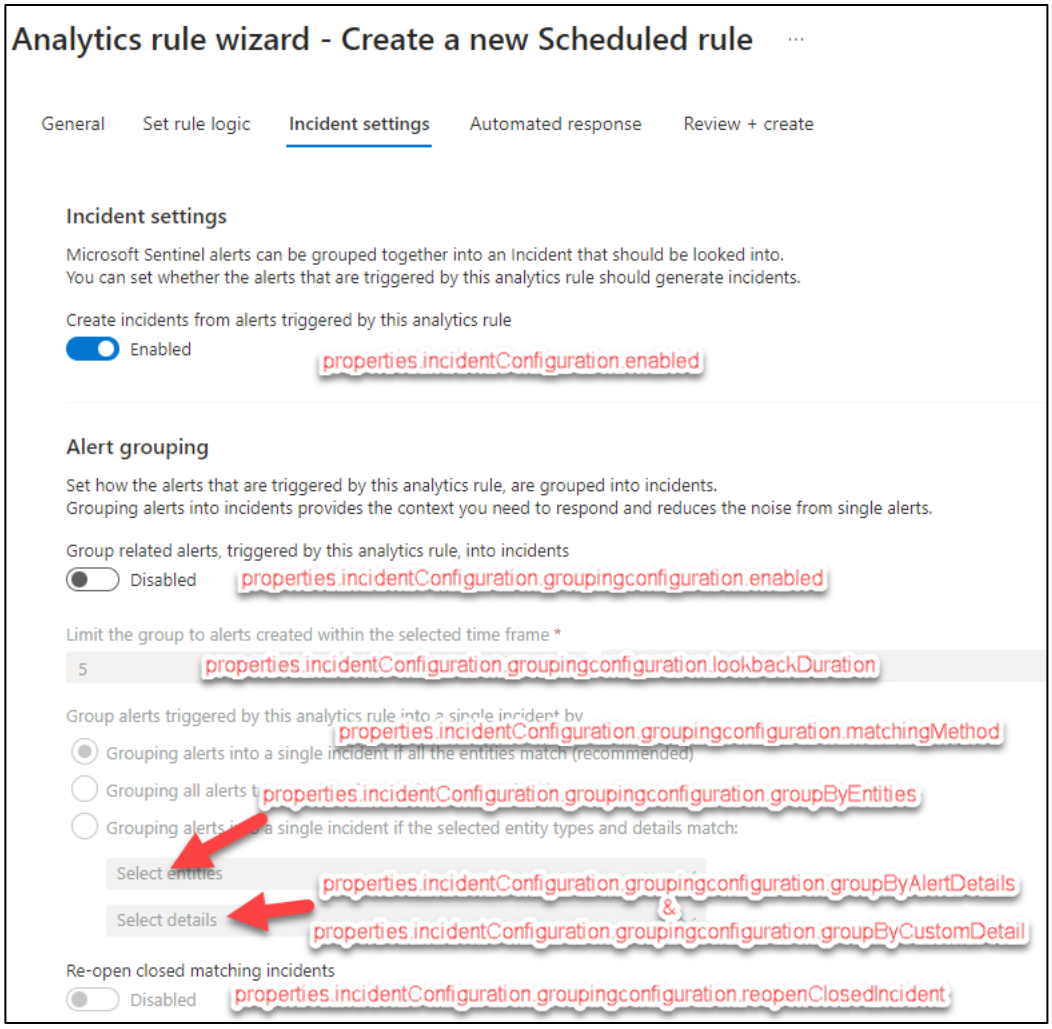

```
{
  "id": "/subscriptions/34bdcce3-c06f-416b-aaa0-
24683117cc68/resourceGroups/devbookrg/providers/Microsoft.OperationalInsights/wor
kspaces/devbookwg/providers/Microsoft.SecurityInsights/alertRules/99ce9db5-41b3-
4cf9-b909-d408e21f277d",
  "name": "99ce9db5-41b3-4cf9-b909-d408e21f277d",
  "etag": "\"01008fc3-0000-0100-0000-6502ffbf0000\"",
  "type": "Microsoft.SecurityInsights/alertRules",
  "kind": "Scheduled",
  "properties": {
    "queryFrequency": "PT1H",
    "queryPeriod": "PT1H",
    "triggerOperator": "GreaterThan",
    "triggerThreshold": 0,
    "incidentConfiguration": {
      "createIncident": true,
      "groupingConfiguration": {
        "enabled": false,
        "reopenClosedIncident": false,
        "lookbackDuration": "PT5M",
        "matchingMethod": "AllEntities",
        "groupByEntities": [],
        "groupByAlertDetails": null,
        "groupByCustomDetails": null
      }
    },
    "entityMappings": [
      {
        "entityType": "Account",
        "fieldMappings": [
          {
            "identifier": "Name",
            "columnName": "Name"
          },
          {
            "identifier": "UPNSuffix",
            "columnName": "UPNSuffix"
          }
        ]
```

```
      }
    ],
    "templateVersion": "1.0.1",
    "severity": "Medium",
    "query": "let locationThreshold = 1;\nlet aadFunc =
(tableName:string){\ntable(tableName)\n| where AppDisplayName =~
\"GitHub.com\"\n| where ResultType == 0\n| summarize CountOfLocations =
dcount(Location), Locations = make_set(Location,100), BurstStartTime =
min(TimeGenerated), BurstEndTime = max(TimeGenerated) by UserPrincipalName,
Type\n| where CountOfLocations > locationThreshold\n| extend timestamp =
BurstStartTime\n};\nlet aadSignin = aadFunc(\"SigninLogs\");\nlet aadNonInt =
aadFunc(\"AADNonInteractiveUserSignInLogs\");\nunion isfuzzy=true aadSignin,
aadNonInt\n| extend Name = tostring(split(UserPrincipalName,'@',0)[0]), UPNSuffix
= tostring(split(UserPrincipalName,'@',1)[0])\n",
    "suppressionDuration": "PT1H",
    "suppressionEnabled": false,
    "tactics": [
      "CredentialAccess"
    ],
    "techniques": [
      "T1110"
    ],
    "displayName": "GitHub Signin Burst from Multiple Locations",
    "enabled": true,
    "description": "This detection triggers when there is a Signin burst from
multiple locations in GitHub (AAD SSO).\n This detection is based on configurable
threshold which can be prone to false positives. To view the anomaly based
equivalent of thie detection, please see here https://github.com/Azure/Azure-
Sentinel/blob/master/Solutions/Azure%20Active%20Directory/Analytic%20Rules/Anomal
ousUserAppSigninLocationIncrease-detection.yaml. ",
    "alertRuleTemplateName": "d3980830-dd9d-40a5-911f-76b44dfdce16",
    "lastModifiedUtc": "2023-09-14T12:42:34.7977386Z"
  }
}
```


As you can see, this pretty much mimics the return from “Alert Rules Templates’ GET” call that we made above.

One exception is that the information for the “Incident settings” page is present now.

Incident settings



List

Http Method: Get

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/alertRules?**{apiVersion}**

"List" works the same way as "Get" except that it returns a JSON array where each entry is an individual analytic rule.

Automation Rules

These REST APIs will allow you to CREATE/UPDATE, DELETE, GET or LIST Automation Rules. Automation rules allow you to perform actions against your incidents when certain triggers, such as an Alert or Incident is created or an Incident is modified, and conditions, like the incident name matches, are met. It will then perform specific actions, like changing severity, or kicking off a playbook.

Documentation URL: [Automation Rules - REST API (Azure Sentinel) | Microsoft Learn]

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/automationRules/**{automationRuleId}**?**{apiVersion}**

This REST API will allow you to create a new Automation rule if one with the "automationRuleId" does not exist, or update an existing one if it does. Like all the other REST APIs that create something new or update, you will need to create a body that gets sent to the REST API call.

Sample request

```
$body = @{
    "properties" = @{
        "displayName"     = "BookTest"
        "order"           = 1
        "triggeringLogic" = @{
            "isEnabled"    = $true
            "triggersOn"   = "Incidents"
            "triggersWhen" = "Created"
            "conditions"   = @()
        }
        "actions"         = @(@{
                "order"               = 1
                "actionType"          = "ModifyProperties"
                "actionConfiguration" = @{
                    "severity" = "Low"

                }
            },
            @{
                "order"               = 2
                "actionType"          = "ModifyProperties"
                "actionConfiguration" = @{
                    "status" = "Active"

                }
            }
```

```
        )
    }
}
$guid = New-Guid
$url = $baseUrl + "automationRules/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

We will go over some of the less obvious entries:

Name	Meaning
properties.order	This is the order that the automation rule will run. Lower numbers run first
properties.triggeringLogic	This is what will trigger the automation rule
properties.triggeringLogic.triggersOn	What will cause this trigger to fire. Either “Incidents” or “Alerts”
properties.triggeringLogic.triggersWhen	What action is performed on the item listed in the “triggersOn”. Either “Created” for both “Incidents” and “Alerts” or “Updated” for “Incidents” only
properties.triggeringLogic.conditions	An array that lists the different conditions that need to happen before this automation rule triggers. This can be an empty array if you want the default trigger conditions.
properties.actions	This is an array of the actions that will be taken once this automation rule triggers
properties.actions.order	This is the order in which the action will happen. This must be unique in the array
properties.actions.actionType	What action will be performed
properties.actions.actionConfiguration	This is any of the configuration that needs to happen for the action. This will vary depending on the action being performed

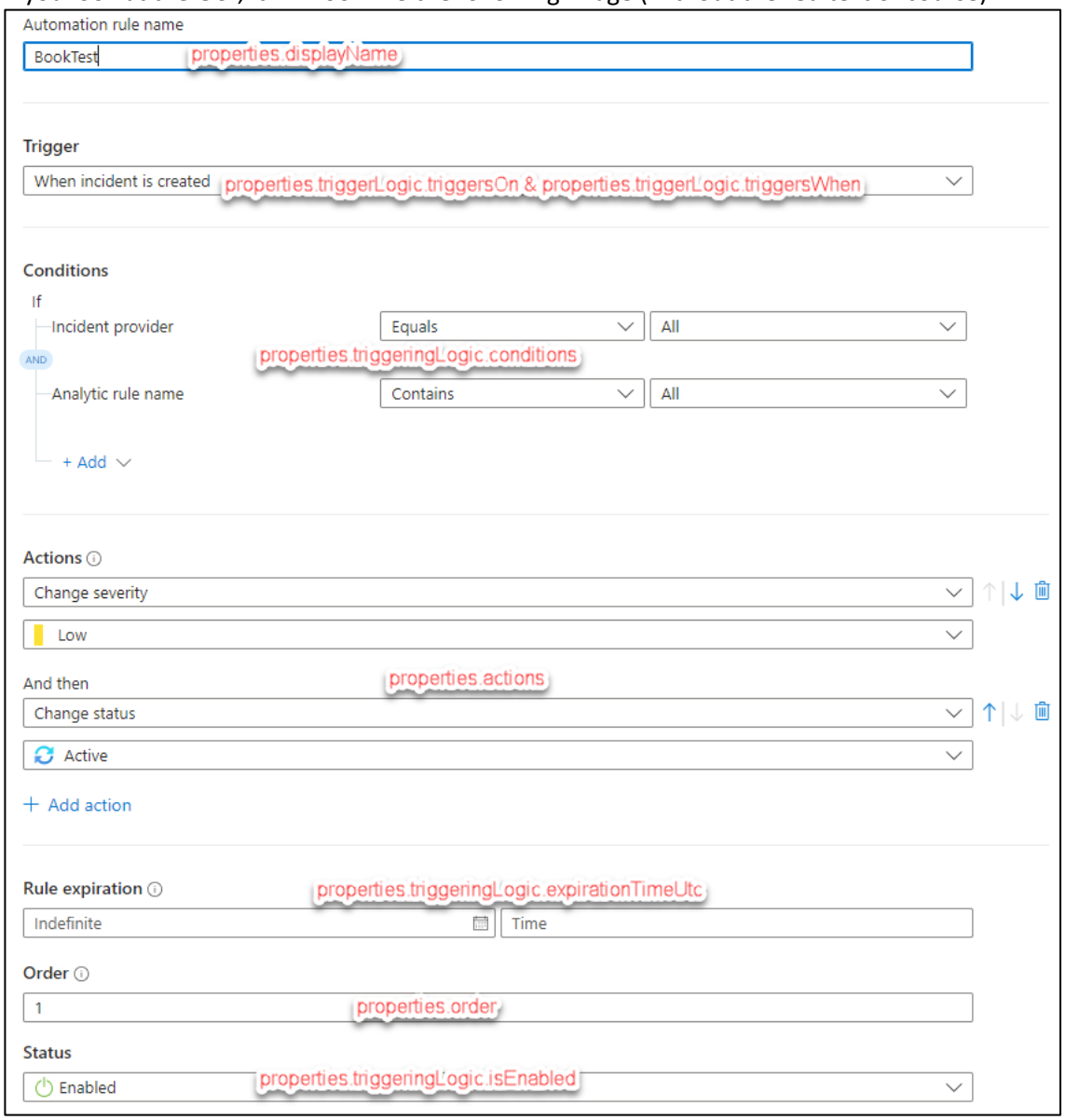
Sample response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/AutomationRules
/7d46439e-e8b4-41f9-b71f-7ad1399cad05",
    "name": "7d46439e-e8b4-41f9-b71f-7ad1399cad05",
    "etag": "\"4000fb75-0000-0100-0000-650f09710000\"",
    "type": "Microsoft.SecurityInsights/AutomationRules",
    "properties": {
      "displayName": "BookTest",
      "order": 1,
      "triggeringLogic": {
        "isEnabled": true,
```

```
        "triggersOn": "Incidents",
        "triggersWhen": "Created",
        "conditions": []
      },
      "actions": [
        {
          "order": 1,
          "actionType": "ModifyProperties",
          "actionConfiguration": {
            "severity": "Low",
            "status": null,
            "classification": null,
            "classificationReason": null,
            "classificationComment": null,
            "owner": null,
            "labels": null
          }
        },
        {
          "order": 2,
          "actionType": "ModifyProperties",
          "actionConfiguration": {
            "severity": null,
            "status": "Active",
            "classification": null,
            "classificationReason": null,
            "classificationComment": null,
            "owner": null,
            "labels": null
          }
        }
      ],
      "lastModifiedTimeUtc": "2023-09-23T15:51:13Z",
      "createdTimeUtc": "2023-09-23T15:49:24Z",
      "lastModifiedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey",
        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
      },
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey",
```

```
        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
      }
    }
  }
```

If you look at the GUI, it will look like the following image (without the red text of course)



Note that if you leave "properties.triggeringLogic.expirationTimeUtc" out of your body, it will set the automation rule to never expire.

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/automationRules/**{automationRuleId}**?**{restAPI}**

This REST API call will delete an existing Automation rule where its Id matches the "automationRuleId" being passed in. This is a simple call so I will not go into any detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/automationRules/**{automationRuleId}**?**{restAPI}**

This will get a single automation rule based on the "automationRuleId". You can use the LIST REST API call, shown below, to get a list of all the automation rules to get the "automationRuleId" value.

If your automation rule uses any of the preview features, like using the "OR" condition group, and you try to load it using this version, it will fail. You must use the preview version (see below)

Sample request

```
$url=$baseURL + "automationRules/7d46439e-e8b4-41f9-b71f-7ad1399cad05" +
$apiVersion"
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/AutomationRules
/7d46439e-e8b4-41f9-b71f-7ad1399cad05",
    "name": "7d46439e-e8b4-41f9-b71f-7ad1399cad05",
    "etag": "\"4000fb75-0000-0100-0000-650f09710000\"",
    "type": "Microsoft.SecurityInsights/AutomationRules",
    "properties": {
      "displayName": "BookTest",
      "order": 1,
      "triggeringLogic": {
        "isEnabled": true,
        "triggersOn": "Incidents",
        "triggersWhen": "Created",
        "conditions": []
```

```
    },
    "actions": [
      {
        "order": 1,
        "actionType": "ModifyProperties",
        "actionConfiguration": {
          "severity": "Low",
          "status": null,
          "classification": null,
          "classificationReason": null,
          "classificationComment": null,
          "owner": null,
          "labels": null
        }
      },
      {
        "order": 2,
        "actionType": "ModifyProperties",
        "actionConfiguration": {
          "severity": null,
          "status": "Active",
          "classification": null,
          "classificationReason": null,
          "classificationComment": null,
          "owner": null,
          "labels": null
        }
      }
    ],
    "lastModifiedTimeUtc": "2023-09-23T15:51:13Z",
    "createdTimeUtc": "2023-09-23T15:49:24Z",
    "lastModifiedBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey",
      "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
    },
    "createdBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey",
      "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
    }
```

```
    }
  }
```

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/automationRules?**{restAPI}**

This will return a JSON array containing all the individual automation rules. See the GET above.

This will only return those automation rule that do NOT use any of the preview features, like using the "OR" condition group.

Bookmarks

These REST APIs will allow you to CREATE/UPDATE, DELETE, GET or LIST Bookmarks. Bookmarks will store the results of queries that you run when you are doing your investigation. You can associate these with an incident and see them in the GUI.

Documentation URL: Bookmarks - REST API (Azure Sentinel) | Microsoft Learn

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/bookmarks/**{bookmarkId}**?**{apiVersion}**

This REST API will allow you to create a new Bookmark if one with the "bookmarkId" does not exist or update an existing one if it does. Like all the other REST APIs that create something new or update, you will need to create a body that gets sent to the REST API call.

One thing to note is that, in the GUI, if you select multiple results, a new Bookmark entry will be created for each result that has been selected. Also, you can associate entities and tactics/techniques in the GUI however you cannot add them here. You would need to use a preview version of this REST API call to add those items.

Sample request

```
$body = @{
    "properties" = @{
        "displayName"    = "AzureActivity - 6ad1d96bf2c1"
        "eventTime"      = "2023-09-23T11:51:13-04:00"
        "notes"          = "This is a note"
        "labels"         = @()
        "query"          = "AzureActivity\n\n"
        "queryResult"    = '{\"TenantId\":\"230c86ca-abf2-48f4-b95e-
8b977e67f4c6\",\"SourceSystem\":\"Azure\",\"CallerIpAddress\":\"75.165.135.234\",
\"CategoryValue\":\"Administrative\"}'
        "queryStartTime" = "2023-09-22T16:35:31.384-04:00"
        "queryEndTime"   = "2023-09-23T16:35:31.384-04:00"
        "incidentInfo"   = @{
            "incidentId" = "a60ef091-61ae-4e4c-aabf-7423c33318c3"
            "title" = "Manager Test"
            "relationName" = "3436356d-15c0-419f-846b-2779b38a1ace"
            "severity" = "Medium"
        }
    }
}
$guid = New-Guid
$url = $baseUrl + "bookmarks/" + $guid + $apiVersion
```

```
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Note that "queryResult" only shows a small subset of the fields in the result. I use it mainly to show that the value needs to be HTTP encoded. Also, PowerShell will require you use the single quote as the string designator since you have to escape the double quotes inside the string.

As near as I can tell "properties.incidentInfo.relationName" is just a random GUID and is not used. If you were to look at the Incident, you will see it uses the value of the "name" field to do the mapping.

Sample response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Bookmarks/479f1
d9a-6771-466f-918e-d78a71a0078f",
    "name": "479f1d9a-6771-466f-918e-d78a71a0078f",
    "etag": "\"0400ae60-0000-0100-0000-650f4c6b0000\"",
    "type": "Microsoft.SecurityInsights/Bookmarks",
    "properties": {
      "displayName": "AzureActivity - 6ad1d96bf2c1",
      "created": "2023-09-23T16:36:59.574239-04:00",
      "updated": "2023-09-23T16:36:59.574239-04:00",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey"
      },
      "updatedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey"
      },
      "eventTime": "2023-09-23T11:51:13-04:00",
      "notes": "This is a note",
      "labels": [],
      "query": "AzureActivity\n\n",
      "queryResult": "{\"TenantId\":\"230c86ca-abf2-48f4-b95e-
8b977e67f4c6\",\"SourceSystem\":\"Azure\",\"CallerIpAddress\":\"75.165.135.234\",
\"CategoryValue\":\"Administrative\"}",
      "queryStartTime": "2023-09-22T16:35:31.384-04:00",
      "queryEndTime": "2023-09-23T16:35:31.384-04:00",
      "incidentInfo": {
        "incidentId": "a60ef091-61ae-4e4c-aabf-7423c33318c3",
        "title": "Manager Test",
```

```
        "relationName": "3436356d-15c0-419f-846b-2779b38a1ace",
        "severity": "Medium"
      }
    }
  }
```


Again, the "queryResults" was trimmed to only show a small subset to save space.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/bookmarks/**{bookmarkId}**?**{apiVersion}**

This REST API will allow you to retrieve a single bookmark based on the "bookmarkId". You can use the LIST REST API call, shown below, to get a list of all bookmarks to get the "bookmarkId" value.

Sample request

```
$url= $baseUrl + "bookmarks/479f1d9a-6771-466f-918e-d78a71a0078f" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Bookmarks/479f1
d9a-6771-466f-918e-d78a71a0078f",
    "name": "479f1d9a-6771-466f-918e-d78a71a0078f",
    "etag": "\"0400ae60-0000-0100-0000-650f4c6b0000\"",
    "type": "Microsoft.SecurityInsights/Bookmarks",
    "properties": {
      "displayName": "AzureActivity - 6ad1d96bf2c1",
      "created": "2023-09-23T16:36:59.574239-04:00",
      "updated": "2023-09-23T16:36:59.574239-04:00",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey"
      },
      "updatedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey"
```

```
      },
      "eventTime": "2023-09-23T11:51:13-04:00",
      "notes": "This is a note",
      "labels": [],
      "query": "AzureActivity\n\n",
      "queryResult": "{\"TenantId\":\"230c86ca-abf2-48f4-b95e-
8b977e67f4c6\",\"SourceSystem\":\"Azure\",\"CallerIpAddress\":\"75.165.135.234\",
\"CategoryValue\":\"Administrative\"}",
      "queryStartTime": "2023-09-22T16:35:31.384-04:00",
      "queryEndTime": "2023-09-23T16:35:31.384-04:00",
      "incidentInfo": {
        "incidentId": "a60ef091-61ae-4e4c-aabf-7423c33318c3",
        "title": "Manager Test",
        "relationName": "3436356d-15c0-419f-846b-2779b38a1ace",
        "severity": "Medium"
      }
    }
  }
```


Again, the “queryResults” was trimmed to only show a small subset to save space.

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/bookmarks?**{restAPI}**

This will return a JSON array containing all the individual bookmarks. See the GET above.

Data Connectors

These REST APIs will allow you to CREATE/UPDATE, DELETE, GET or LIST Data Connectors. Note that there are only 8 different data connectors available, all from Microsoft (and using older names): Azure Active Directory, Azure Advanced Threat Protection, Azure Security Center, Amazon Web Services CloudTrail, Microsoft Cloud App Security, Microsoft Defender Advanced Threat Protection, Office Data connector, Threat Intelligence Data Connector.

Because of the limited usefulness of these REST APIs, I will not be covering here. Data Connectors will be covered more in the Preview section around solutions.

Documentation URL: Data Connectors - REST API (Azure Sentinel) | Microsoft Learn

Incidents

Do I really need to tell you what incident are? These REST APIs will allow you to CREATE/UPDATE, DELETE, GET or LIST incidents as well as list Alerts, Bookmarks, and Entities related to a single incident.

Documentation URL: Incidents - REST API (Azure Sentinel) | Microsoft Learn

Create/Update

Http Method: PUT

REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**?**{apiVersion}**

This REST API will allow you to create a new incident if one with the "incidentId" does not exist or update an existing one if it does exist.

If you use the REST API to create an incident, you will not be able to associate any alerts with it.

This REST API will also make use of some of the REST API filters including "$filter", "$orderby", "$skipToken", and "$top". This will be discussed later.

Sample Request

```
$body = @{
    "properties" = @{
        "lastActivityTimeUtc"   = "2023-09-24T13:05:30Z"
        "firstActivityTimeUtc"  = "2019-09-24T13:00:30Z"
        "description"           = "This is an incident created for the book"
        "title"                 = "Book incident"
        "owner"                 = @{
            "objectId" = "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e"
        }
        "severity"              = "High"
        "classification"        = "FalsePositive"
        "classificationComment" = "Not a malicious activity"
        "classificationReason"  = "IncorrectAlertLogic"
        "status"                = "Closed"
        "labels"                = @( @{
                "labelName" = "Gary Test"
                "labelType" = "User"
            }
        )
        "providerName"          = "Microsoft Sentinel"

    }
}
$guid = New-Guid
$url = $baseUrl + "incidents/" + $guid + $apiVersion
```

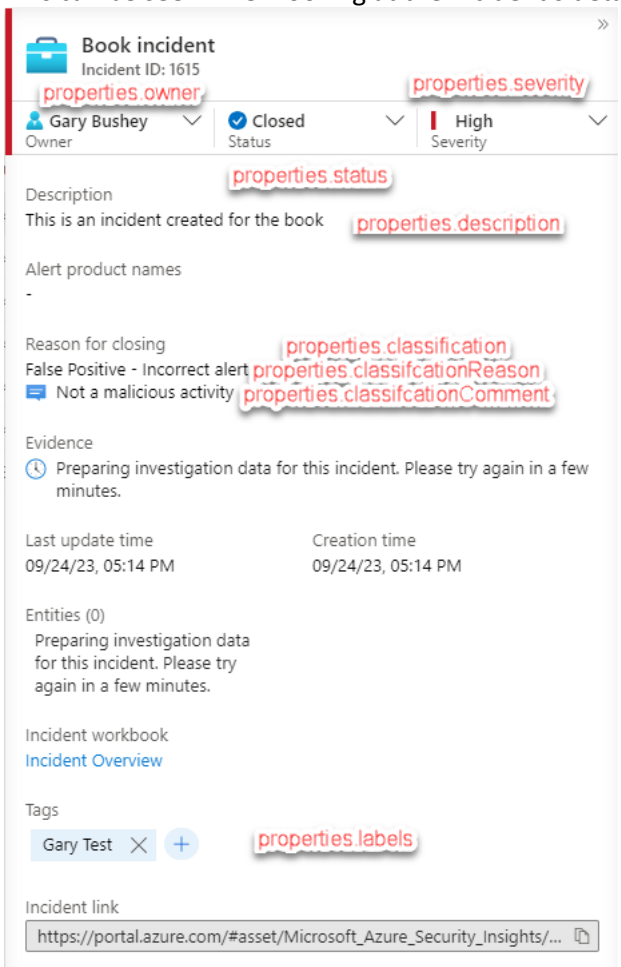
```
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/7e78c
6c7-e608-496f-94e6-bdba172f0332",
    "name": "7e78c6c7-e608-496f-94e6-bdba172f0332",
    "etag": "\"1c00d734-0000-0100-0000-6510a6b70000\"",
    "type": "Microsoft.SecurityInsights/Incidents",
    "properties": {
      "title": "Book incident",
      "description": "This is an incident created for the book",
      "severity": "High",
      "status": "Closed",
      "classification": "FalsePositive",
      "classificationReason": "IncorrectAlertLogic",
      "classificationComment": "Not a malicious activity",
      "owner": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "assignedTo": "Gary Bushey",
        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
      },
      "labels": [
        {
          "labelName": "Gary Test",
          "labelType": "User"
        }
      ],
      "firstActivityTimeUtc": "2019-09-24T13:00:30Z",
      "lastActivityTimeUtc": "2023-09-24T13:05:30Z",
      "lastModifiedTimeUtc": "2023-09-24T21:14:31.0217094Z",
      "createdTimeUtc": "2023-09-24T21:14:31.0217094Z",
      "incidentNumber": 1615,
      "additionalData": {
        "alertsCount": 0,
        "bookmarksCount": 0,
        "commentsCount": 0,
        "alertProductNames": [],
        "tactics": []
      },
```

```
      "relatedAnalyticRuleIds": [],
      "incidentUrl":
"https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/Incident/subsc
riptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/7e78c
6c7-e608-496f-94e6-bdba172f0332",
      "providerName": "Azure Sentinel",
      "providerIncidentId": "1615"
    }
  }
```


This can be seen when looking at the Incident's detail pane



You may notice that the "Alert product names", not to mention "Tactics", are not showing. This is because they would be defined in the "properties.additionalData"

field which I was not able to get working. Seems to be an error in the API and I will update the document if I get it to work.

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**?**{apiVersion}**

This REST API call will delete an existing incident where its Id matches the "incidentId" being passed in. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**?**{apiVersion}**

This REST API call will retrieve a single incident as specified in the "incidentId" parameter.

Sample Request

```
$url= $baseURL + "incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/7752c
995-4e1c-d0a1-3d07-f3c90ca48bf4",
    "name": "7752c995-4e1c-d0a1-3d07-f3c90ca48bf4",
    "etag": "\"22006ae8-0000-0100-0000-65134d1e0000\"",
    "type": "Microsoft.SecurityInsights/Incidents",
    "properties": {
      "title": "Test Rule",
      "description": "",
      "severity": "Medium",
      "status": "New",
      "owner": {
        "objectId": null,
        "email": null,
        "assignedTo": null,
```

```
        "userPrincipalName": null
      },
      "labels": [],
      "firstActivityTimeUtc": "2023-09-26T16:12:09.25Z",
      "lastActivityTimeUtc": "2023-09-26T21:12:09.25Z",
      "lastModifiedTimeUtc": "2023-09-26T21:29:02.0775198Z",
      "createdTimeUtc": "2023-09-26T21:17:10.5784245Z",
      "incidentNumber": 1618,
      "additionalData": {
        "alertsCount": 1,
        "bookmarksCount": 2,
        "commentsCount": 0,
        "alertProductNames": [
          "Azure Sentinel"
        ],
        "tactics": [
          "Collection",
          "CommandAndControl"
        ]
      },
      "relatedAnalyticRuleIds": [
        "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/alertRules/586c
e94f-26d6-4fef-9335-7cd54b04b211"
      ],
      "incidentUrl":
"https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/Incident/subsc
riptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/7752c
995-4e1c-d0a1-3d07-f3c90ca48bf4",
      "providerName": "Azure Sentinel",
      "providerIncidentId": "1618"
    }
  }
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the individual incidents for the given “incidentId”. See the GET above.

List Alerts

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/alerts?**{apiVersion}**

This will return a JSON array containing all the individual alerts for the given “incidentId”.

Note that this is a POST rather than a GET call.

Sample Request

```
$url=$baseUrl + "incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/alerts" + $apiVersion
$results = (Invoke-RestMethod -Method "POST" -Uri $url -Headers $authHeader ).value
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Entities/3fa8c363-f32b-6a79-f192-39919d8827cb",
    "name": "3fa8c363-f32b-6a79-f192-39919d8827cb",
    "type": "Microsoft.SecurityInsights/Entities",
    "kind": "SecurityAlert",
    "properties": {
      "systemAlertId": "3fa8c363-f32b-6a79-f192-39919d8827cb",
      "tactics": [
        "Collection",
        "CommandAndControl"
      ],
      "alertDisplayName": "Test Rule",
      "description": "",
      "confidenceLevel": "Unknown",
      "severity": "Medium",
      "vendorName": "Microsoft",
```

```
      "productName": "Azure Sentinel",
      "productComponentName": "Scheduled Alerts",
      "alertType": "230c86ca-abf2-48f4-b95e-8b977e67f4c6_586ce94f-26d6-4fef-9335-
7cd54b04b211",
      "processingEndTime": "2023-09-26T21:17:10.3473176Z",
      "status": "New",
      "endTimeUtc": "2023-09-26T21:12:09.25Z",
      "startTimeUtc": "2023-09-26T16:12:09.25Z",
      "timeGenerated": "2023-09-26T21:17:10.3863528Z",
      "providerAlertId": "eb209357-14e9-4db1-9f15-24c3164dab0e",
      "resourceIdentifiers": [
        {
          "type": "LogAnalytics",
          "workspaceId": "230c86ca-abf2-48f4-b95e-8b977e67f4c6",
          "subscriptionId": "9790d913-b5da-460d-b167-ac985d5f3b83",
          "resourceGroup": "azuresentinel"
        }
      ],
      "additionalData": {
        "AlertMessageEnqueueTime": "2023-09-26T21:17:10.384Z",
        "Search Query Results Overall Count": "2",
        "OriginalProductName": "Azure Sentinel",
        "OriginalProductComponentName": "Scheduled Alerts"
      },
      "friendlyName": "Test Rule"
    }
  }
```


Note that because there is only a single entry, the data is not stored as a JSON array.

List Bookmarks

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/bookmarks?**{apiVersion}**

This will return a JSON array containing all the individual alerts for the given “incidentId”.

Note that this is a POST rather than a GET call.

Sample Request

```
$url=$baseUrl + "incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/bookmarks" +
$apiVersion
$results = (Invoke-RestMethod -Method "POST" -Uri $url -Headers $authHeader
).value
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Entities/d92209
f6-fb44-4adb-8658-eee9e7159b91",
    "name": "d92209f6-fb44-4adb-8658-eee9e7159b91",
    "type": "Microsoft.SecurityInsights/Entities",
    "kind": "Bookmark",
    "properties": {
      "displayName": "AzureActivity - ec3eb66a390a",
      "created": "2023-09-26T17:16:09.8922022-04:00",
      "updated": "2023-09-26T17:16:09.8922022-04:00",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey"
      },
      "updatedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey"
      },
      "eventTime": "2023-09-26T15:27:39-04:00",
      "notes": "This is the bookmark note",
      "labels": [],
      "query": "AzureActivity\n\n",
      "queryResult": "{\"TenantId\":\"230c86ca-abf2-48f4-b95e-
8b977e67f4c6\",\"SourceSystem\":\"Azure\"}",
      "additionalData": {
        "EntityMappings": "[]",
        "Tactics": "[\"Collection\"]",
        "Techniques": "[]",
        "ETag": "\"05001b57-0000-0100-0000-65134d1e0000\"",
        "EntityId": "d92209f6-fb44-4adb-8658-eee9e7159b91"
      },
      "friendlyName": "AzureActivity - ec3eb66a390a"
    }
  }
```

Note that because there is only a single entry, the data is not stored as a JSON array. I also truncated the "queryResults" to save space.

List Entities

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/entities?**{apiVersion}**

This will return a JSON array containing all the individual entities for the given "incidentId".

Note that this is a POST rather than a GET call.

Sample Request

```
$url=$baseUrl + "incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/entities" +
$apiVersion
$results = (Invoke-RestMethod -Method "POST" -Uri $url -Headers $authHeader
).entities
```

Sample Response


```
[
    {
      "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Entities/41c57c
d2-a539-cc4e-89d0-38824a117a50",
      "name": "41c57cd2-a539-cc4e-89d0-38824a117a50",
      "type": "Microsoft.SecurityInsights/Entities",
      "kind": "Account",
      "properties": {
        "accountName": "Gary Bushey",
        "friendlyName": "Gary Bushey"
      }
    },
    {
      "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
```

```
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Entities/7e11e7
6f-53a9-a5e4-bb49-6480c6f9812a",
      "name": "7e11e76f-53a9-a5e4-bb49-6480c6f9812a",
      "type": "Microsoft.SecurityInsights/Entities",
      "kind": "Ip",
      "properties": {
        "address": "192.168.1.1",
        "friendlyName": "192.168.1.1"
      }
    }
  ]
```

Incident Comments

These REST APIs will allow you to CREATE/UPDATE, DELETE, GET or LIST comments assigned to incidents.

Documentation URL: [Incident Comments - REST API (Azure Sentinel) | Microsoft Learn]

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/comments/**{incidentCommentId}**?**{apiVersion}**

This REST API will allow you to create a new comment if one with the "bookmarkId" does not exist or update an existing one if it does exist. Note that you need to know the Incident ID that you want to attach this comment to as well as the "incidentCommentId"

Like all the other REST APIs that create something new or update, you will need to create a body that gets sent to the REST API call. In this case, it is very basic.

Sample Request

```
$body = @{
    "properties" = @{
        "message"= "<p ><strong>This</strong> <em>comment</em> <u>uses</u> a
<s>lot</s> of the HTML encoding features </p>"
    }
}
$guid = New-Guid
$url = $baseUrl + "incidents/a60ef091-61ae-4e4c-aabf-7423c33318c3/comments/" +
$guid + $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Note that if you use the HTML formatting features in the GUI, each HTML tag also has the "elementTiming" attribute added to it. As it does not seem to be needed, I did not add it here.

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/a60ef
091-61ae-4e4c-aabf-7423c33318c3/Comments/4e280bb6-91bd-46e9-b2a6-f983f8287821",
    "name": "4e280bb6-91bd-46e9-b2a6-f983f8287821",
    "etag": "\"1a004d10-0000-0100-0000-650f5e550000\"",
    "type": "Microsoft.SecurityInsights/Incidents/Comments",
```

```
    "properties": {
      "message": "<p ><strong>This</strong> <em>comment</em> <u>uses</u> a
<s>lot</s> of the HTML encoding features </p>",
      "createdTimeUtc": "2023-09-23T21:53:25.0243509Z",
      "lastModifiedTimeUtc": "2023-09-23T21:53:25.0243509Z",
      "author": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey",
        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
      }
    }
  }
```

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/comments/**{incidentCommentId}**?**{apiVersion}**

This REST API call will delete an existing Automation rule where its Id matches the "automationRuleId" being passed in. This is a simple call so I will not go into any detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/comments/**{incidentCommentId}**?**{apiVersion}**

This will get a single incident comment. You can use the LIST REST API call, shown below, to get a list of all the automation rules to get the "incidentCommentId" value.

Sample Request

```
$url= $baseUrl + "incidents/a60ef091-61ae-4e4c-aabf-
7423c33318c3/comments/4e280bb6-91bd-46e9-b2a6-f983f8287821" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response

```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
```

```
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/a60ef
091-61ae-4e4c-aabf-7423c33318c3/Comments/4e280bb6-91bd-46e9-b2a6-f983f8287821",
    "name": "4e280bb6-91bd-46e9-b2a6-f983f8287821",
    "etag": "\"1a004d10-0000-0100-0000-650f5e550000\"",
    "type": "Microsoft.SecurityInsights/Incidents/Comments",
    "properties": {
      "message": "<p ><strong>This</strong> <em>comment</em> <u>uses</u> a
<s>lot</s> of the HTML encoding features </p>",
      "createdTimeUtc": "2023-09-23T21:53:25.0243509Z",
      "lastModifiedTimeUtc": "2023-09-23T21:53:25.0243509Z",
      "author": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey",
        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
      }
    }
  }
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/comments?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the individual incident comments. See the GET above.

Incident Relations

Incident Relations allow you to link bookmarks to an incident if you did not do so when you create the bookmark. I am not sure if you can use this to relate anything else but if I find out, I will update the document.

Documentation URL: Incident Relations - REST API (Azure Sentinel) | Microsoft Learn

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/relations/**{relationName}**?**{apiVersion}**

Sample Request

```
$body = @{
    "properties" = @{
        "relatedResourceId" = "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Bookmarks/d9220
9f6-fb44-4adb-8658-eee9e7159b91"
    }
}
$guid = New-Guid
$url = $baseUrl + "incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/relations/" +
$guid + $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

When creating the URL, the “relationName” value will be a new GUID that will create the link.

Sample Response

```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/7752c
995-4e1c-d0a1-3d07-f3c90ca48bf4/relations/63b2d125-5012-464d-857a-f81314ed2bbd",
    "name": "63b2d125-5012-464d-857a-f81314ed2bbd",
    "etag": "\"22006ae8-0000-0100-0000-65134d1e0000\"",
    "type": "Microsoft.SecurityInsights/Incidents/relations",
    "properties": {
      "relatedResourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
```

```
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Bookmarks/d9220
9f6-fb44-4adb-8658-eee9e7159b91",
      "relatedResourceName": "d92209f6-fb44-4adb-8658-eee9e7159b91",
      "relatedResourceType": "Microsoft.SecurityInsights/Bookmarks"
    }
  }
```


Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/relations/**{relationName}**?**{apiVersion}**

This REST API call will delete an existing incident relation where its Id matches the "relationName" and the "incidentId" matches the incident that the relation belongs to. This is a simple call so I will not go into any detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/relations/**{relationName}**?**{apiVersion}**

This gets a single instance of an Incident Relation where its Id matches the "relationName" and the "incidentId" matches the incident that the relation belongs to.

Sample Request

```
$url= $baseUrl + "incidents/7752c995-4e1c-d0a1-3d07-
f3c90ca48bf4/relations/63b2d125-5012-464d-857a-f81314ed2bbd " + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/7752c
995-4e1c-d0a1-3d07-f3c90ca48bf4/relations/63b2d125-5012-464d-857a-f81314ed2bbd",
    "name": "63b2d125-5012-464d-857a-f81314ed2bbd",
    "etag": "\"22006ae8-0000-0100-0000-65134d1e0000\"",
```

```
    "type": "Microsoft.SecurityInsights/Incidents/relations",
    "properties": {
      "relatedResourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Bookmarks/d9220
9f6-fb44-4adb-8658-eee9e7159b91",
      "relatedResourceName": "d92209f6-fb44-4adb-8658-eee9e7159b91",
      "relatedResourceType": "Microsoft.SecurityInsights/Bookmarks"
    }
  }
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/relations?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the individual incident relations for the given “incidentId”. See the GET above.

Metadata

This one is a bit odd. I have tried to figure out the rhyme or reason behind some of these entries but so far, I have only figured out Analytic Rules. I have found entries for Analytic Rules, Solutions, Data Connectors, Playbooks, Parsers, and Workbooks. There could be more entries if other items were added to my Sentinel installation.

Documentation URL: Metadata - REST API (Azure Sentinel) | Microsoft Learn

Create

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/metadata/**{metadataName}**?**{apiVersion}**

This REST API will allow you to create a metadata (is that the correct way of saying that). Note that this is one of the few REST APIs where the CREATE and the UPDATE are different URLs.

I am not going to go into much detail here, since each call is very different. You can check out the Preview section's Alert Rule entry for an example of how to do this.

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/metadata/**{metadataName}**?**{restAPI}**

This REST API call will delete an existing metadata where its Id matches the "metadataName" being passed in. This is a simple call so I will not go into any detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/metadata/**{metadataName}**?**{restAPI}**

This REST API call will get a single metadata based on the "metadataName" that gets passed in.

Sample Request

```
$url= $baseUrl + "metadata/analyticsrule-f32ad97a-b6a7-4be9-84ea-cd7ca448fb6c" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader ).value
```

Sample Response


```
{
    "id": "/subscriptions/34bdcce3-c06f-416b-aaa0-
24683117cc68/resourceGroups/devbookrg/providers/Microsoft.OperationalInsights/wor
kspaces/devbookwg/providers/Microsoft.SecurityInsights/metadata/analyticsrule-
20d10588-7a7a-48e3-85a1-8292047a4146",
    "name": "analyticsrule-20d10588-7a7a-48e3-85a1-8292047a4146",
    "type": "Microsoft.SecurityInsights/metadata",
    "systemData": {
      "createdAt": "2023-09-14T12:43:53.197731Z",
      "createdBy": "431918a1-4886-4bb5-932c-37a99afc7347",
      "createdByType": "Application",
      "lastModifiedAt": "2023-09-14T12:43:53.197731Z",
      "lastModifiedBy": "431918a1-4886-4bb5-932c-37a99afc7347",
      "lastModifiedByType": "Application"
    },
    "properties": {
      "contentId": "20d10588-7a7a-48e3-85a1-8292047a4146",
      "parentId": "/subscriptions/34bdcce3-c06f-416b-aaa0-
24683117cc68/resourceGroups/devbookrg/providers/Microsoft.OperationalInsights/wor
kspaces/devbookwg/providers/Microsoft.SecurityInsights/alertRules/20d10588-7a7a-
48e3-85a1-8292047a4146",
      "kind": "AnalyticsRule",
      "version": "1.1.4",
      "source": {
        "kind": "Solution",
        "name": "Azure Active Directory",
        "sourceId": "azuresentinel.azure-sentinel-solution-azureactivedirectory"
      },
      "author": {
        "name": "Microsoft",
        "email": "support@microsoft.com"
      },
      "support": {
        "tier": "Microsoft",
        "name": "Microsoft Corporation",
        "email": "support@microsoft.com",
        "link": "https://support.microsoft.com/"
      }
    }
  }
```

List Entities

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/metadata/**{metadataName}**?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the individual metadata. See the GET above for details.

Update

Http Method: PATCH

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/metadata/**{metadataName}**?**{apiVersion}**

This will work just like the CREATE listed above except that 1) It uses the PATCH Http Method and 2) you need to use an existing “metadataName”

Operations

This is kind of an oddball REST API. Its only purpose is to show you the other calls you can make. Note that is also does not follow the typical format for a Microsoft Sentinel REST API

Documentation URL: Operations - REST API (Azure Sentinel) | Microsoft Learn

List

Http Method: GET
REST API URL:
https://management.azure.com/providers/Microsoft.SecurityInsights/operations?**{apiVersion}**

Due to the size of the return value, I am not going to show a sample call. I really doubt you would ever use this REST API in any case.

Security ML Analytics Settings

This name is a bit misleading. Yes, it does deal with ML Analytics but it would be easier to understand if this was called "Anomalies" since that is exactly what is being returned.

Documentation URL: Security ML Analytics Settings - REST API (Azure Sentinel) | Microsoft Learn

Create

Http Method: PUT

REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/securityMLAnalyticsSettings/**{settingsResourceName}**?**{apiVersion}**

While you really will not be creating new Anomalies, you can duplicate an existing one. You can edit it but there is only a limited number of fields you can edit including:

Field	Description
properties.enabled	Is the rule enabled? Keep in mind that only one copy of any Anomaly rule can be activate at one time. So if you copy an existing rule the copy will be disabled by default if the original rule is enabled.
properties.settingsStatus	"Production" or "Flighting". "Flighting" basically means you are testing and "Production" means you are in production. You should set this to "Flighting" when first creating an entry unless you have fully tested your settings.
Properties.customizableObservations.thresholdObservations.value	The current threshold value. This only appears to be editable when working on a copied entry.

Sample request

```
$body = @{
    "kind"       = "Anomaly"
    "properties" = @{
        "displayName"              = "Anomalous volume of privileged process
calls of commonly seen windows attack vectors on a daily basis - Customized"
```

```
        "description"              = "This anomaly algorithm detects unusual
volume of privileged (Full or Elevated security token) process creation calls
made by a user account from a selected process list in the last 21 days. These
selected processes are commonly used attack vectors in windows systems. This
activity may indicate that the user account is compromised."
        "enabled"                  = $false
        "tactics"                  = @(
            "InitialAccess"
        )
        "anomalyVersion"           = "1.0.12"
        "techniques"               = @(
            "T1078"
        )
        "frequency"                = "P1D"
        "ruleStatus"               = "Flighting"
        "isDefaultSettings"        = $false
        "anomalyRuleVersion"       = 0
        "customizableObservations" = @{
            "multiSelectObservations"       = $null
            "singleSelectObservations"      = $null
            "prioritizeExcludeObservations" = $null
            "thresholdObservations"         = @( @{
                    "minimum" = "0"
                    "maximum" = "1"
                    "value" = "1"
                    "name" = "Score"
                    "description" = "Generate an anomaly when score is greater
than the chosen value"
                    "sequenceNumber" = 1
                    "rerun" = "NotRequired"
                }
            )
            "singleValueObservations"       = $null
        }
        "settingsDefinitionId" = "c9053c76-c6cd-409a-a10f-e20b05cc91f5"
        "requiredDataConnectors"    = @(
            @{
                "ConnectorId" = "SecurityEvents"
                "DataTypes" = @(
                    "SecurityEvents"
                )
            }
        )
        "settingsStatus" = "Flighting"
        "anomalySettingsVersion"    = 0
```

```
    }
}
$guid = New-Guid
$url = $baseUrl + " securityMLAnalyticsSettings/" + $guid + $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/securityMLAnaly
ticsSettings/2fd3b6aa-0aec-40c6-8f3c-a647cc97e934",
    "name": "2fd3b6aa-0aec-40c6-8f3c-a647cc97e934",
    "etag": "\"0b00e2b6-0000-0100-0000-6515fb640000\"",
    "type": "Microsoft.SecurityInsights/securityMLAnalyticsSettings",
    "kind": "Anomaly",
    "properties": {
      "displayName": "Anomalous volume of privileged process calls of commonly
seen windows attack vectors on a daily basis - Customized",
      "anomalyVersion": "1.0.12",
      "techniques": [
        "T1078"
      ],
      "customizableObservations": {
        "multiSelectObservations": null,
        "singleSelectObservations": null,
        "prioritizeExcludeObservations": null,
        "thresholdObservations": [
          {
            "minimum": "0",
            "maximum": "1",
            "value": "1",
            "name": "Score",
            "description": "Generate an anomaly when score is greater than the
chosen value",
            "sequenceNumber": 1,
            "rerun": "NotRequired"
          }
        ],
        "singleValueObservations": null
      },
      "frequency": "P1D",
```

```
      "settingsStatus": "Flighting",
      "isDefaultSettings": false,
      "anomalySettingsVersion": 0,
      "settingsDefinitionId": "c9053c76-c6cd-409a-a10f-e20b05cc91f5",
      "tactics": [
        "InitialAccess"
      ],
      "enabled": false,
      "description": "This anomaly algorithm detects unusual volume of privileged
(Full or Elevated security token) process creation calls made by a user account
from a selected process list in the last 21 days. These selected processes are
commonly used attack vectors in windows systems. This activity may indicate that
the user account is compromised.",
      "lastModifiedUtc": "2023-09-28T22:17:07.93221Z",
      "requiredDataConnectors": [
        {
          "ConnectorId": "SecurityEvents",
          "DataTypes": [
            "SecurityEvents"
          ]
        }
      ]
    }
  }
```


You can only create one copy of an out of the box Anomaly rule otherwise you will get an error message.

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/securityMLAnalyticsSettings/**{settingsResourceName}**?**{apiVersion}**

This REST API call will delete an existing Analytic rule where its Id matches the “ruleId” being passed in. This is a simple call so I will not go into much detail.

You are unable to delete any of the out of the box Anomaly rules.

Get

Http Method: GET

REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/securityMLAnalyticsSettings/**{settingsResourceName}**?**{apiVersion}**

This will get a single Anomaly rule.

Sample Request

```
$url = $baseUrl + "securityMLAnalyticsSettings/2fd3b6aa-0aec-40c6-8f3c-a647cc97e934" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/securityMLAnalyticsSettings/2fd3b6aa-0aec-40c6-8f3c-a647cc97e934",
    "name": "2fd3b6aa-0aec-40c6-8f3c-a647cc97e934",
    "etag": "\"0b00e2b6-0000-0100-0000-6515fb640000\"",
    "type": "Microsoft.SecurityInsights/securityMLAnalyticsSettings",
    "kind": "Anomaly",
    "properties": {
      "displayName": "Anomalous volume of privileged process calls of commonly seen windows attack vectors on a daily basis - Customized",
      "anomalyVersion": "1.0.12",
      "techniques": [
        "T1078"
      ],
      "customizableObservations": {
        "multiSelectObservations": null,
        "singleSelectObservations": null,
        "prioritizeExcludeObservations": null,
        "thresholdObservations": [
          {
            "minimum": "0",
            "maximum": "1",
            "value": "1",
            "name": "Score",
            "description": "Generate an anomaly when score is greater than the chosen value",
            "sequenceNumber": 1,
```

```
            "rerun": "NotRequired"
          }
        ],
        "singleValueObservations": null
      },
      "frequency": "P1D",
      "settingsStatus": "Flighting",
      "isDefaultSettings": false,
      "anomalySettingsVersion": 0,
      "settingsDefinitionId": "c9053c76-c6cd-409a-a10f-e20b05cc91f5",
      "tactics": [
        "InitialAccess"
      ],
      "enabled": false,
      "description": "This anomaly algorithm detects unusual volume of privileged
(Full or Elevated security token) process creation calls made by a user account
from a selected process list in the last 21 days. These selected processes are
commonly used attack vectors in windows systems. This activity may indicate that
the user account is compromised.",
      "lastModifiedUtc": "2023-09-28T22:17:07.93221Z",
      "requiredDataConnectors": [
        {
          "ConnectorId": "SecurityEvents",
          "DataTypes": [
            "SecurityEvents"
          ]
        }
      ]
    }
  }
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/securityMLAnalyticsSettings?**{apiVersion}**

This will return a JSON array containing all the individual anomaly rules. See the GET above.

Sentinel Onboarding States

Right now, this will only let your set or tell you if you have customer managed keys or not.

Documentation URL: [Sentinel Onboarding States - REST API (Azure Sentinel) | Microsoft Learn]

Create

Http Method: PUT
REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/onboardingStates/**{sentinelOnboardingStateName}**?**{apiVersion}**

This will allow you to set the flag that indicates if the customer is using a customer Managed Key. Note that currently, the only "sentinelOnboardingStateName" to use is "default". There is no Edit so it appears you just do another create with the "customerManagedKey" to either $true or $false (in PowerShell at least).

Sample request

```
$body = @{
    "properties" = @{
        "customerManagedKey" = $false
    }
}
$url = $baseUrl + " onboardingStates/default" + $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample response

```
{
    "id": "/subscriptions/d0cfe6b2-9ac0-4464-9919-
dccaee2e48c0/resourceGroups/myRg/providers/Microsoft.OperationalInsights/workspac
es/myWorkspace/providers/Microsoft.SecurityInsights/onboardingStates/default",
    "name": "default",
    "type": "Microsoft.SecurityInsights/onboardingStates",
    "properties": {
      "customerManagedKey": false
    }
  }
```

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/securityMLAnalyticsSettings/**{settingsResourceName}**?**{apiVersion}**

This REST API call will delete an existing onboarding state where its Id matches the "settingsResourceName" being passed in. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/onboardingStates/**{sentinelOnboardingStateName}**?**{apiVersion}**

Note that currently, the only "sentinelOnboardingStateName" to use is "default". This call will get the only entry.

Sample Request

```
$url=$baseUrl + "onboardingStates/default" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response

```
{
    "properties": {},
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/onboardingState
s/default",
    "name": "default",
    "type": "Microsoft.SecurityInsights/onboardingStates",
    "systemData": {}
  }
```

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/onboardingStates?**{apiVersion}**

This call is identical to using the GET above. Since there is only the single entry, it doesn't return an array like other LIST calls do.

Threat Intelligence Indicator

Threat Intelligence Indicators are the indicators of compromise that you can use to help detect issues with your environment. Most of the time this will be coming from a 3rd part source, like Recorded Future, or Microsoft's Defender Threat Intelligence. However, if you want to add your own, use these REST APIs.

These are just some examples of Threat Intelligence Feeds. I have no preference for one over the other (although, for full disclosure, I do work for Microsoft)

This is where some of the naming of the REST APIs groups gets a little weird. This section is "Threat Intelligence Indicator" (singular). Note that there is no way to get a listing of all the indicators. To do that you use the "LIST" REST API that is listed under "Threat Intelligence Indicators" (plural). I also see this with some of the new groups under the preview section.

Documentation URL: [Threat Intelligence Indicator - REST API (Azure Sentinel) | Microsoft Learn]

Append Tags

Http Method: POST

REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/**{name}**/appendTags?**{apiVersion}**

This will allow you to add one or more tags to an existing Threat Intelligence Indicator.

Sample Request

```
$body = @{
    "threatIntelligenceTags" = @(
        "Gary", "Bushey"
    )
}
$guid = New-Guid
$url = $baseUrl + " threatIntelligence/main/indicators/b4b222b3-cca0-7f13-8dd7-e61b720fe0ee" + $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body ($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.OperationalInsights
```

```
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/b4b222b3-cca0-7f13-8dd7-e61b720fe0ee",
    "name": "b4b222b3-cca0-7f13-8dd7-e61b720fe0ee",
    "etag": "\"08006ea3-0000-0100-0000-6518a1a90000\"",
    "type": "Microsoft.SecurityInsights/threatIntelligence/main/indicators",
    "kind": "indicator",
    "properties": {
      "confidence": 100,
      "created": "2023-09-06T14:23:56.4952117Z",
      "createdByRef": "identity--d7adaba4-c743-4ac3-ac90-798880696e84",
      "extensions": {
        "sentinel-ext": {
          "severity": null
        },
        "IndicatorProvider": "Microsoft"
      },
      "externalId": "indicator--2e652ca7-3916-24f5-27e0-899a0434fab1",
      "externalLastUpdatedTimeUtc": "2023-09-30T22:31:05.0355328Z",
      "externalReferences": [
        {
          "description": "This STIX Object was created from a Microsoft OneIndicator Object.",
          "externalId": "2e652ca7391624f527e0899a0434fab1a5a26d65634a1461a61f4ec806e0a5d0",
          "sourceName": "Interflow"
        }
      ],
      "labels": [
        "Gary",
        "Bushey",
        "honeypot"
      ],
      "lastUpdatedTimeUtc": "2023-09-30T22:31:05.0355328Z",
      "objectMarkingRefs": [
        "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"
      ],
      "source": "Microsoft Defender Threat Intelligence",
      "threatIntelligenceTags": [
        "Gary",
        "Bushey",
        "honeypot"
      ],
      "displayName": "Microsoft Identified IOC",
      "description": "MSTIC HoneyPot: An attacker used a brute force attack to gain access to a service or device",
```

```
      "threatTypes": [
        "Botnet"
      ],
      "parsedPattern": [
        {
          "patternTypeKey": "network-traffic",
          "patternTypeValues": [
            {
              "valueType": "src_ref.value",
              "value": "124.6.150.118"
            }
          ]
        }
      ],
      "pattern": "[network-traffic:src_ref.value = '124.6.150.118']",
      "patternType": "stix",
      "validFrom": "2023-09-30T22:08:34.3229698Z",
      "validUntil": "2023-10-01T03:06:27.4598815Z"
    }
  }
```

As you can see, the entire Threat Intelligence Indicator will get returned and you will see the additional tags added.

Create

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/**{name}**?**{apiVersion}**

This REST API name is very misleading. You do not actually use this to **create** a new Threat Intelligence Indicator. Instead, this is only used for **updating** an existing Threat Intelligence Indicator. If you want to create a new Threat Intelligence Indicator, see "Create Indicator" below.

Sample Request

```
$body = @{
    "name"       = "2d86220d-2772-885c-733f-5cc62798fb72"
    "kind"       = "indicator"
    "properties" = @{
        "confidence"             = 78
        "created"                = "2023-09-30T22:46:45.7612605Z"
        "createdByRef"           = "contoso@contoso.com"
        "extensions"             = @{
            "sentinel-ext" = @{
                "severity" = $null
```

```
            }
        }
        "externalId"             = "indicator--e10a9f5f-bed3-a62c-441f-
333f15655613"
        "externalReferences"     = @()
        "granularMarkings"       = @()
        "labels"                 = @(
            "new schema"
        )
        "lastUpdatedTimeUtc"     = "2023-09-30T22:46:45.8080387Z"
        "revoked"                = $false
        "source"                 = "Microsoft Sentinel"
        "threatIntelligenceTags" = @(
            "new schema"
        )
        "displayName"            = "new schema"
        "description"            = "debugging indicators"
        "threatTypes"            = @(
            "compromised"
        )
        "killChainPhases"        = @()
        "parsedPattern"          = @( @{
                "patternTypeKey"    = "url"
                "patternTypeValues" = @( @{
                        "valueType" = "url"
                        "value"     = "https://www.contoso.com"
                    }
                )
            }
        )
        "pattern"                = "[url:value = 'https://www.contoso.com']"
        "patternType"            = "url"
        "validFrom"              = "2023-04-15T17:44:00.114052Z"
    }
}
$guid = New-Guid
$url = $baseUrl + " threatIntelligence/main/indicators/" + $guid + $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.OperationalInsights
```

```
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/2d86220d-2772-885c-733f-5cc62798fb72",
    "name": "2d86220d-2772-885c-733f-5cc62798fb72",
    "etag": "\"08000eb1-0000-0100-0000-6518a7720000\"",
    "type": "Microsoft.SecurityInsights/threatIntelligence/main/indicators",
    "kind": "indicator",
    "properties": {
      "confidence": 78,
      "created": "2023-09-30T22:46:45.7612605Z",
      "createdByRef": "contoso@contoso.com",
      "extensions": {
        "sentinel-ext": {
          "severity": null
        }
      },
      "externalId": "indicator--e10a9f5f-bed3-a62c-441f-333f15655613",
      "externalReferences": [],
      "granularMarkings": [],
      "labels": [
        "new schema"
      ],
      "lastUpdatedTimeUtc": "2023-09-30T22:46:45.8080387Z",
      "revoked": false,
      "source": "Microsoft Sentinel",
      "threatIntelligenceTags": [
        "new schema"
      ],
      "displayName": "new schema",
      "description": "debugging indicators",
      "threatTypes": [
        "compromised"
      ],
      "killChainPhases": [],
      "parsedPattern": [
        {
          "patternTypeKey": "url",
          "patternTypeValues": [
            {
              "valueType": "url",
              "value": "https://www.contoso.com"
            }
          ]
        }
      ],
      "pattern": "[url:value = 'https://www.contoso.com']",
```

```
      "patternType": "url",
      "validFrom": "2020-04-15T17:44:00.114052Z"
    }
  }
```

Create Indicator

Http Method: POST

REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/createIndicator?**{apiVersion}**

This is the REST API call you make to create a new Threat Intelligence Indicator. Unlike other REST API calls that create a new entry, this one does not require a new GUID, it will create one behind the scenes.

Sample Request

```
$body = @{
    "kind"       = "indicator"
    "properties" = @{
        "source"             = "Azure Sentinel"
        "threatIntelligenceTags" = @(
            "new schema"
        )
        "displayName"        = "new schema"
        "confidence"         = 78
        "createdByRef"       = "contoso@contoso.com"
        "description"        = "debugging indicators"
        "externalReferences" = @()
        "granularMarkings"   = @()
        "threatTypes"        = @(
            "compromised"
        )
        "killChainPhases"    = @()
        "labels"             = @()
        "modified"           = ""
        "pattern"            = "[url:value = 'https://www.contoso.com']"
        "patternType"        = "url"
        "revoked"            = $false
        "validFrom"          = "2020-04-15T17:44:00.114052Z"
        "validUntil"         = ""
    }
}
```

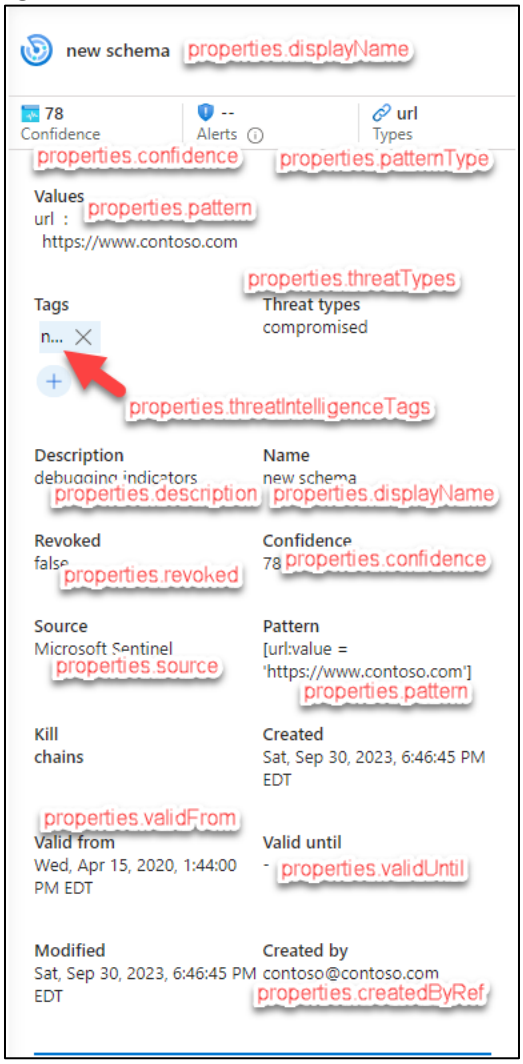
```
$url = $baseUrl + " threatIntelligence/main/indicators/createIndicator" + $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Post -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/threatIntellige
nce/main/indicators/2d86220d-2772-885c-733f-5cc62798fb72",
    "name": "2d86220d-2772-885c-733f-5cc62798fb72",
    "etag": "\"0800feab-0000-0100-0000-6518a5550000\"",
    "type": "Microsoft.SecurityInsights/threatIntelligence/main/indicators",
    "kind": "indicator",
    "properties": {
      "confidence": 78,
      "created": "2023-09-30T22:46:45.7612605Z",
      "createdByRef": "contoso@contoso.com",
      "extensions": {
        "sentinel-ext": {
          "severity": null
        }
      },
      "externalId": "indicator--e10a9f5f-bed3-a62c-441f-333f15655613",
      "externalReferences": [],
      "granularMarkings": [],
      "labels": [
        "new schema"
      ],
      "lastUpdatedTimeUtc": "2023-09-30T22:46:45.8080387Z",
      "revoked": false,
      "source": "Microsoft Sentinel",
      "threatIntelligenceTags": [
        "new schema"
      ],
      "displayName": "new schema",
      "description": "debugging indicators",
      "threatTypes": [
        "compromised"
      ],
      "killChainPhases": [],
      "parsedPattern": [
        {
```

```
        "patternTypeKey": "url",
        "patternTypeValues": [
          {
            "valueType": "url",
            "value": "https://www.contoso.com"
          }
        ]
      }
    ],
    "pattern": "[url:value = 'https://www.contoso.com']",
    "patternType": "url",
    "validFrom": "2020-04-15T17:44:00.114052Z"
  }
}
```

If you examine the Threat Intelligence Indicator in the GUI, it would look like



Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/**{name}**?**{apiVersion}**

This REST API call will delete an existing Threat Intelligence Indicator where its name matches the "name" being passed in. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/**{name}**?**{apiVersion}**

Gets a single Threat Intelligence Indicator where its name matches the "name" parameter.

Sample Request

```
$url=$baseUrl + "threatIntelligence/main/indicators/2d86220d-2772-885c-733f-5cc62798fb72" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/2d86220d-2772-885c-733f-5cc62798fb72",
    "name": "2d86220d-2772-885c-733f-5cc62798fb72",
    "etag": "\"080012b1-0000-0100-0000-6518a7740000\"",
    "type": "Microsoft.SecurityInsights/threatIntelligence/main/indicators",
    "kind": "indicator",
    "properties": {
      "confidence": 78,
      "created": "2023-09-30T22:46:45.7612605Z",
      "createdByRef": "contoso@contoso.com",
      "extensions": {
        "sentinel-ext": {
          "severity": null
        }
      },
      "externalId": "indicator--e10a9f5f-bed3-a62c-441f-333f15655613",
      "externalReferences": [],
      "granularMarkings": [],
```

```
      "labels": [
        "new schema"
      ],
      "lastUpdatedTimeUtc": "2023-09-30T22:46:45.8080387Z",
      "revoked": false,
      "source": "Microsoft Sentinel",
      "threatIntelligenceTags": [
        "new schema"
      ],
      "displayName": "new schema",
      "description": "debugging indicators",
      "threatTypes": [
        "compromised"
      ],
      "killChainPhases": [],
      "parsedPattern": [
        {
          "patternTypeKey": "url",
          "patternTypeValues": [
            {
              "valueType": "url",
              "value": "https://www.contoso.com"
            }
          ]
        }
      ],
      "pattern": "[url:value = 'https://www.contoso.com']",
      "patternType": "url",
      "validFrom": "2020-04-15T17:44:00.114052Z"
    }
  }
```


Query Indicators

Http Method: GET
REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/**{name}**?**{apiVersion}**

This will allow you to perform a query to get the list of Threat Intelligence Indicators you want. While you can use the REST API filters on the LIST REST API call, this provides a much finer control of your query. You also need to define your query in a BODY and pass it in, rather than as part of the REST API URL.

Sample Request

```
$body = @{
    "pageSize"      = 100
    "minConfidence" = 25
    "maxConfidence" = 80
    "minValidUntil" = "2023-09-05T17:44:00.114052Z"
    "maxValidUntil" = "2023-09-30T17:44:00.114052Z"
    "sources"       = @(
        "Microsoft Defender Threat Intelligence"
    )
    "sortBy"        = @(
        @{
            "itemKey"   = "lastUpdatedTimeUtc"
            "sortOrder" = "descending"
        }
    )
}
$guid = New-Guid
$url = $baseUrl + " threatIntelligence/main/indicators/" + $guid + $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Post -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

This will return a JSON array of all the Threat Intelligence Indicators that match the filter passed in.

In this case we want the first 100 Threat Intelligence Indicators that have at least a confidence of 25 and not more than 80, is valid between September 5, 2023 5:44PM Zulu and September 30, 2023 5:44PM Zulu, and was created by "Microsoft Defender Threat Intelligence". The return values will be sorted by the "lastUpdatedTimeUtc" field in descending order.

Replace Tags

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/**{name}**/replaceTags?**{apiVersion}**

This call works just like the "Append Tags", but instead of adding the passed in tag as an additional tag, it will delete all the existing tags and only add the ones that were passed in.

Sample Request

```
$body = @{
    "properties" = @{
        "threatIntelligenceTags" = @(
            "Gary", "Bushey"
        )
```

```
    }
}
$url = $baseUrl + " threatIntelligence/main/indicators/2d86220d-2772-885c-733f-5cc62798fb72"
+ $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/threatIntellige
nce/main/indicators/2d86220d-2772-885c-733f-5cc62798fb72",
    "name": "2d86220d-2772-885c-733f-5cc62798fb72",
    "etag": "\"080060d2-0000-0100-0000-6518b4880000\"",
    "type": "Microsoft.SecurityInsights/threatIntelligence/main/indicators",
    "kind": "indicator",
    "properties": {
      "confidence": 78,
      "created": "2023-09-30T22:46:45.7612605Z",
      "createdByRef": "contoso@contoso.com",
      "extensions": {
        "sentinel-ext": {
          "severity": null
        }
      },
      "externalId": "indicator--e10a9f5f-bed3-a62c-441f-333f15655613",
      "externalLastUpdatedTimeUtc": "2023-09-30T23:51:36.0135157Z",
      "externalReferences": [],
      "granularMarkings": [],
      "labels": [
        "Gary",
        "Bushey"
      ],
      "lastUpdatedTimeUtc": "2023-09-30T23:51:36.0135157Z",
      "revoked": false,
      "source": "Microsoft Sentinel",
      "threatIntelligenceTags": [
        "Gary",
        "Bushey"
      ],
      "displayName": "new schema",
      "description": "debugging indicators",
```

```
    "threatTypes": [
      "compromised"
    ],
    "killChainPhases": [],
    "parsedPattern": [
      {
        "patternTypeKey": "url",
        "patternTypeValues": [
          {
            "valueType": "url",
            "value": "https://www.contoso.com"
          }
        ]
      }
    ],
    "pattern": "[url:value = 'https://www.contoso.com']",
    "patternType": "url",
    "validFrom": "2020-04-15T17:44:00.114052Z"
  }
}
```

Threat Intelligence Indicator Metrics

From what I can gather, this should give you the counts of the various types of Threat Intelligence Indicators in your environment. However, when I ran this, all I got back were zeros for each "metricValue" except for one. I would think I would have a value for "Microsoft Defender Threat Intelligence" since that is where most of the Threat Intelligence Indicators came from.

Documentation URL: [Threat Intelligence Indicator Metrics - REST API (Azure Sentinel) | Microsoft Learn]

List

Http Method: Get

REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/threatIntelligence/main/metrics?**{apiVersion}**

Sample Request

```
$url=$baseUrl + "threatIntelligence/main/metrics" + $apiVersion
$results = (Invoke-RestMethod -Method "POST" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
    "lastUpdatedTimeUtc": "2023-09-30T22:13:04.9997821Z",
    "threatTypeMetrics": [
      {
        "metricName": "botnet",
        "metricValue": 0
      },
      {
        "metricName": "maliciousurl",
        "metricValue": 0
      },
      {
        "metricName": "phishing",
        "metricValue": 0
      },
      {
        "metricName": "malware",
        "metricValue": 0
      },
      {
        "metricName": "variant",
        "metricValue": 0
      },
      {
```

```
      "metricName": "watchlist",
      "metricValue": 0
    }
  ],
  "patternTypeMetrics": [
    {
      "metricName": "network-traffic",
      "metricValue": 0
    },
    {
      "metricName": "url",
      "metricValue": 0
    },
    {
      "metricName": "file",
      "metricValue": 0
    },
    {
      "metricName": "ipv4-addr",
      "metricValue": 0
    },
    {
      "metricName": "domain-name",
      "metricValue": 0
    },
    {
      "metricName": "x509-certificate",
      "metricValue": 0
    },
    {
      "metricName": "email-addr",
      "metricValue": 0
    },
    {
      "metricName": "mutex",
      "metricValue": 0
    }
  ],
  "sourceMetrics": [
    {
      "metricName": "Bing Safety Phishing URL",
      "metricValue": 2675645
    },
    {
      "metricName": "Microsoft Defender Threat Intelligence",
```

```
      "metricValue": 0
    },
    {
      "metricName": "Microsoft Emerging Threat Feed",
      "metricValue": 0
    }
  ]
}
```

Threat Intelligence Indicators

This will provide a list of the various Threat Intelligence Indicators in your environment.

As I mentioned above, it seems strange that this is in its own group (although this does seem to be the pattern that the new APIs follow).

Documentation URL: Threat Intelligence Indicators - REST API (Azure Sentinel) | Microsoft Learn

List

Http Method: Get

REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array of the latest 100 Threat Intelligence Indicators in your environment. There are some REST API filters that you can apply to fine tune which items are returned.

Watchlists

These REST API calls will allow you to work with watchlists. A watchlist is like a pseudo table that gets created from a CSV file that you can either reference directly or upload into a storage account and access via a SAS URL.

Documentation URL: [Watchlists - REST API (Azure Sentinel) | Microsoft Learn]

Create/Update

Http Method: PUT

REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/watchlists/**{watchlistAlias}**?**{apiVersion}**

This REST API will allow you to create a new watchlist if one with the "watchlistAlias" does not exist or update an existing one if it does exist. Note that unlike most REST API calls to create or update, this one requires the alias for the watchlist, rather than an internal GUID.

Sample Request (local file)

```
$body = @{
    "properties" = @{
        "watchlistAlias"      = "networkdata"
        "displayName"         = "NetworkData"
        "sourceType"          = "Local"
        "contentType"         = "Text/Csv"
        "source"              = "Network Addresses.csv"
        "description"         = "This is the network data created from a CSV
file"
        "numberOfLinesToSkip" = 0
        "itemsSearchKey"      = "IP Subnet"
        "provider"            = "Microsoft"
        "defaultDuration"     = "P1DT3H"
        "rawContent"          = "IP Subnet,Range
Name,Tags\r\n192.168.1.1,first,\r\n192.168.1.2,second,\r\n"
    }
}
$url = $baseUrl + "watchlists/networkdata" + $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
```

```
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Watchlists/netw
orkdata",
  "name": "networkdata",
  "etag": "\"ab00f7e1-0000-0100-0000-654677370000\"",
  "type": "Microsoft.SecurityInsights/Watchlists",
  "systemData": {
    "createdAt": "2023-11-04T16:54:14.4449703Z",
    "createdBy": "garybushey@outlook.com",
    "createdByType": "User",
    "lastModifiedAt": "2023-11-04T16:54:14.4449703Z",
    "lastModifiedBy": "garybushey@outlook.com",
    "lastModifiedByType": "User"
  },
  "properties": {
    "watchlistId": "a8629aeb-9f71-408f-af0f-2e995e7b2e55",
    "displayName": "NetworkData",
    "provider": "Microsoft",
    "source": "Network Addresses.csv",
    "sourceType": "Local",
    "itemsSearchKey": "IP Subnet",
    "created": "2023-11-04T16:54:14.4449703+00:00",
    "updated": "2023-11-04T16:54:14.4449703+00:00",
    "createdBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "a0965655-eecb-4c9f-8e21-2488aadf59fe"
    },
    "updatedBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "a0965655-eecb-4c9f-8e21-2488aadf59fe"
    },
    "description": "This is the network data created from a CSV file",
    "watchlistType": "watchlist",
    "watchlistAlias": "networkdata",
    "isDeleted": false,
    "labels": [],
    "defaultDuration": "P1DT3H",
    "tenantId": "ae0818a0-ede8-4da6-9786-2d9d5fd5295f",
    "numberOfLinesToSkip": 0,
    "provisioningState": "Uploading",
    "sasUri": "",
    "watchlistCategory": "General"
```

```
  }
}
```

Sample Request (file stored in Azure storage)

```
$body = @{
    "properties" = @{
      "watchlistAlias"      = "NetworkData3"
      "displayName"         = "High Value Assets Watchlist"
      "sourceType"          = "AzureStorage"
      "contentType"         = "Text/Csv"
      "source"              = "Remote file"
      "description"         = "Watchlist from CSV content"
      "numberOfLinesToSkip" = 0
      "itemsSearchKey"      = "IP Subnet"
      "provider"            = "Microsoft"
      "defaultDuration"     = "P1DT3H"
      "sasUri"              = <SAS URL>
    }
  }
$url = $baseUrl + " watchlists/networksdata3" + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Watchlists/netw
orkdata3",
    "name": "networkdata3",
    "etag": "\"b9019ffe-0000-0100-0000-65381b270000\"",
    "type": "Microsoft.SecurityInsights/Watchlists",
    "systemData": {
      "createdAt": "2023-10-24T19:29:43.0621864Z",
      "createdBy": "garybushey@outlook.com",
      "createdByType": "User",
      "lastModifiedAt": "2023-10-24T19:29:43.0621864Z",
      "lastModifiedBy": "garybushey@outlook.com",
      "lastModifiedByType": "User"
    },
    "properties": {
      "watchlistId": "faeafbfa-3699-4abd-9109-c66a3ae6062c",
      "displayName": "High Value Assets Watchlist",
      "provider": "Microsoft",
      "source": "Remote file",
```

```
      "sourceType": "AzureStorage",
      "itemsSearchKey": "IP Subnet",
      "created": "2023-10-24T15:29:43.0621864-04:00",
      "updated": "2023-10-24T15:29:43.0621864-04:00",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "a0965655-eecb-4c9f-8e21-2488aadf59fe"
      },
      "updatedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "a0965655-eecb-4c9f-8e21-2488aadf59fe"
      },
      "description": "Watchlist from CSV content",
      "watchlistType": "watchlist",
      "watchlistAlias": "networkdata3",
      "isDeleted": false,
      "labels": [],
      "defaultDuration": "P1DT3H",
      "tenantId": "ae0818a0-ede8-4da6-9786-2d9d5fd5295f",
      "numberOfLinesToSkip": 0,
      "provisioningState": "Uploading",
      "sasUri": "",
      "watchlistCategory": "General"
    }
  }
```


Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/watchlists/**{watchlistAlias}**?**{apiVersion}**

This REST API call will delete an existing Watchlist item where its Id matches the “watchlistItemId” being passed in. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/watchlists/**{watchlistAlias}**?**{apiVersion}**

This will retrieve a single watchlist item based on the “watchlistItemId” passed in.

Sample Request

```
$url=$baseUrl + "watchlists/SolutionData/watchlistitems/fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13" +$apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader ).value
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Watchlists/SolutionData/WatchlistItems/fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13",
    "name": "fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13",
    "etag": "\"fe001968-0000-0100-0000-65244bd10000\"",
    "type": "Microsoft.SecurityInsights/Watchlists/WatchlistItems",
    "systemData": {
      "createdAt": "2023-10-09T18:51:42.1272644Z",
      "createdBy": "garybushey@outlook.com",
      "createdByType": "User",
      "lastModifiedAt": "2023-10-09T18:51:42.1272644Z",
      "lastModifiedBy": "garybushey@outlook.com",
      "lastModifiedByType": "User"
    },
    "properties": {
      "watchlistItemType": "watchlist-item",
      "watchlistItemId": "fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13",
      "tenantId": "ae0818a0-ede8-4da6-9786-2d9d5fd5295f",
      "isDeleted": false,
      "created": "2023-10-09T14:51:42.1272644-04:00",
      "updated": "2023-10-09T14:51:42.1272644-04:00",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "a0965655-eecb-4c9f-8e21-2488aadf59fe"
      },
      "updatedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "a0965655-eecb-4c9f-8e21-2488aadf59fe"
      },
      "itemsKeyValue": {
        "Index": "1",
        "SolutionName": "42Crunch Microsoft Sentinel Connector",
        "SolutionType": "Solution",
```

```
        "SolutionDescription": "APIs are increasingly the number one attack
vector for adversaries due to their growing abundance and ease of attack via
automated scripts and tools. Most public APIs are under constant attack by
skilled human adversaries and growing legions of bots.<br><br>Well-designed,
secure APIs are critical to mitigating the risk of attack, but it is essential to
also actively monitor and defend your APIs - the frontline of your perimeter -
via direct integration into SIEM and SOCs. <br><br>Using the 42Crunch Sentinel
connector, you can quickly set up Sentinel to start ingesting logs from the
42Crunch micro-API Firewall directly into Log Analytics workspaces. With this
integration you can:<div><br><div><ul><li>Create alerts on common API error
conditions</li><li>Enrich API logs with threat intelligence data (i.e. known bad
IPs)</li><li>Detect attack patterns for common adversarial tools (i.e.
Kiterunner)</li><li>Understand common bot behaviors and evasion
techniques</li><li>Identify key trends and patterns across all exposed
APIs</li></ul></div></div>",
        "ResourceType": "Workbook",
        "ResourceName": "42Crunch API Protection Workbook",
        "RequiredDataConnectors": "",
        "RequiredDataTypes": ""
      },
      "entityMapping": {},
      "labels": []
    }
  }
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/watchlists?**{apiVersion}**

Filters Available: $skipToken

This will return a JSON array containing all the individual anomaly rules. See the GET above.

Watchlist Items

These REST API calls will allow you to work with individual items in a watchlist. Watchlists are much like a pseudo table that you can update. Once a watchlist has been created (see below), you can use these REST APIs to work against the items in it. They will all require that you have a watchlist alias that you will use as part of the URL.

Documentation URL: [Watchlist Items - REST API (Azure Sentinel) | Microsoft Learn]

Create/Update

Http Method: PUT

REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/watchlists/**{watchlistAlias}**/watchlistItems/**{watchlistItemId}**?**{apiVersion}**

This REST API will allow you to create a new watchlist item if one with the "watchlistItemId" does not exist or update an existing one if it does exist.

The thing to remember is that since each watchlist can (and probably will) have different columns, you need to pass in the columns as JSON in the properties field. You can get this using the LIST REST API call by looking at the "itemsKeyValue" column.

Sample Request

```
$body = @{
    "properties" = @{
        "itemsKeyValue" = @{
            "Index"                 = "1"
            "SolutionName"          = "42Crunch Microsoft Sentinel Connector"
            "SolutionType"          = "Solution"
            "SolutionDescription"   = "Description"
            "ResourceType"          = "Workbook"
            "ResourceName"          = "42Crunch API Protection Workbook"
            "RequiredDataConnectors" = ""
            "RequiredDataTypes"     = ""
        }
    }
}
$url = $baseUrl + " watchlists/main/SolutionData/watchlistsItems/fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13" + $apiVersion

$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body ($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
```

```
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Watchlists/Solu
tionData/WatchlistItems/fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13",
    "name": "fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13",
    "etag": "\"8601a32e-0000-0100-0000-6536e2fb0000\"",
    "type": "Microsoft.SecurityInsights/Watchlists/WatchlistItems",
    "systemData": {
      "createdAt": "2023-10-09T18:51:42.1272644Z",
      "createdBy": "garybushey@outlook.com",
      "createdByType": "User",
      "lastModifiedAt": "2023-10-23T21:17:47.1748211Z",
      "lastModifiedBy": "garybushey@outlook.com",
      "lastModifiedByType": "User"
    },
    "properties": {
      "watchlistItemType": "watchlist-item",
      "watchlistItemId": "fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13",
      "tenantId": "ae0818a0-ede8-4da6-9786-2d9d5fd5295f",
      "isDeleted": false,
      "created": "2023-10-09T14:51:42.1272644-04:00",
      "updated": "2023-10-23T17:17:47.1748211-04:00",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "a0965655-eecb-4c9f-8e21-2488aadf59fe"
      },
      "updatedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "a0965655-eecb-4c9f-8e21-2488aadf59fe"
      },
      "itemsKeyValue": {
        "SolutionName": "42Crunch Microsoft Sentinel Connector",
        "ResourceName": "42Crunch API Protection Workbook",
        "ResourceType": "Workbook",
        "RequiredDataTypes": "",
        "Index": "1",
        "RequiredDataConnectors": "",
        "SolutionDescription": "Description",
        "SolutionType": "Solution"
      },
      "entityMapping": {}
    }
  }
```

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/watchlists/**{watchlistAlias}**/watchlistItems/**{watchlistItemId}**?**{apiVersion}**

This REST API call will delete an existing Watchlist item where its Id matches the "watchlistItemId" being passed in. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/watchlists/**{watchlistAlias}**/watchlistItems/**{watchlistItemId}**?**{apiVersion}**

This will retrieve a single watchlist item based on the "watchlistItemId" passed in.

Sample Request

```
$url=$baseUrl + "watchlists/SolutionData/watchlistitems/fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader ).value
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Watchlists/SolutionData/WatchlistItems/fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13",
    "name": "fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13",
    "etag": "\"fe001968-0000-0100-0000-65244bd10000\"",
    "type": "Microsoft.SecurityInsights/Watchlists/WatchlistItems",
    "systemData": {
      "createdAt": "2023-10-09T18:51:42.1272644Z",
      "createdBy": "garybushey@outlook.com",
      "createdByType": "User",
      "lastModifiedAt": "2023-10-09T18:51:42.1272644Z",
      "lastModifiedBy": "garybushey@outlook.com",
      "lastModifiedByType": "User"
    },
    "properties": {
      "watchlistItemType": "watchlist-item",
      "watchlistItemId": "fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13",
      "tenantId": "ae0818a0-ede8-4da6-9786-2d9d5fd5295f",
```

```
      "isDeleted": false,
      "created": "2023-10-09T14:51:42.1272644-04:00",
      "updated": "2023-10-09T14:51:42.1272644-04:00",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "a0965655-eecb-4c9f-8e21-2488aadf59fe"
      },
      "updatedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "a0965655-eecb-4c9f-8e21-2488aadf59fe"
      },
      "itemsKeyValue": {
        "Index": "1",
        "SolutionName": "42Crunch Microsoft Sentinel Connector",
        "SolutionType": "Solution",
        "SolutionDescription": "APIs are increasingly the number one attack
vector for adversaries due to their growing abundance and ease of attack via
automated scripts and tools. Most public APIs are under constant attack by
skilled human adversaries and growing legions of bots.<br><br>Well-designed,
secure APIs are critical to mitigating the risk of attack, but it is essential to
also actively monitor and defend your APIs - the frontline of your perimeter -
via direct integration into SIEM and SOCs. <br><br>Using the 42Crunch Sentinel
connector, you can quickly set up Sentinel to start ingesting logs from the
42Crunch micro-API Firewall directly into Log Analytics workspaces. With this
integration you can:<div><br><div><ul><li>Create alerts on common API error
conditions</li><li>Enrich API logs with threat intelligence data (i.e. known bad
IPs)</li><li>Detect attack patterns for common adversarial tools (i.e.
Kiterunner)</li><li>Understand common bot behaviors and evasion
techniques</li><li>Identify key trends and patterns across all exposed
APIs</li></ul></div></div>",
        "ResourceType": "Workbook",
        "ResourceName": "42Crunch API Protection Workbook",
        "RequiredDataConnectors": "",
        "RequiredDataTypes": ""
      },
      "entityMapping": {},
      "labels": []
    }
  }
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/watchlists/**{watchlistAlias}**/watchlistItems?**{apiVersion}**

Filters Available: $skipToken

This will return a JSON array containing all the individual anomaly rules. See the GET above.

Preview APIs

Just because a REST API is marked as preview, does not mean it will not work. It has been tested and, in some cases, is being used in Microsoft Sentinel.

For instance, if you look at the calls made when modifying an Analytic Rule, you will find that there is a call made to the "alertRules" REST API using the "2023-04-01-preview" API version. So don't be afraid to use these REST APIs, just keep in mind that there is still a chance that things may not work quite right. There are some that do not seem to work yet, and those are called out in their definitions.

Personally, I use the latest preview version of the REST APIs whenever I can to make sure I get the most information possible. For example, by using the REST API preview when getting or creating/editing analytic rules, I get all the latest functionality of the analytic rule being returned including the ability to specify when the analytic rule should run. Since this functionality is in preview, I would need to use a preview call to get it.

If a feature of Microsoft Sentinel is listed as being in preview, you will need to call a preview REST API to get that data. So rather than having "?api-version=2023-02-01" at the end of the REST API's URL it would be like "?api-version=2023-09-01-preview".

For the preview APIs, if there is an existing REST API in the stable section of this book, I am only going to cover the new parts.

Alert Rule Templates

There is nothing new in the “alertRuleTemplates” REST API, other than some new fields may be returned, however I do not see any new fields that are being returned.

The new field for stating when an alert rule starts to run is not being returned in a rule template, which makes sense. The rule template would have no idea when you would want to start running the rule, that is something you would set when creating the rule.

See the Alert Rule Templates stable REST API

Alert Rules

There aren't a lot of changes here. The only one is being able to say when to start the rule running. The strange part is I was not able to find the field to set in the JSON definition file for the alertRules (called "AlertRules.json). I did see it when I created a new rule and watched the network traffic so I was able to determine it is "properties.startTimeUtc"

See the Alert Rules stable REST API.

One additional thing you will need to do is make a call to the metadata REST API. You will need to get the information from a solution, so you would need to get the template data from "contentProductPackages" REST API call described below.

As you can see, you get the name of the rule from the return call's output variable when you create it. Then you need to create another body for this call, with some of the information coming from that same variable. For the example below, "$solution" is the solution where the rule's template information was obtained. Also note that the version of the API we are using is different than we have used in the other REST API calls as this is not a Microsoft Sentinel REST API.

```
$metabody = @{
  "apiVersion" = "2022-01-01-preview"
  "name"       = "analyticsrule-" + $verdict.name
  "type"       = "Microsoft.OperationalInsights/workspaces/providers/metadata"
  "id"         = $null
  "properties" = @{
      "contentId" = $verdict.name
      "parentId"  = $verdict.id
      "kind"      = "AnalyticsRule"
      "version"   = $templateVersion
      "source"    = $solution.source
      "author"    = $solution.author
      "support"   = $solution.support
  }
}
```

Then it is a simple call:

```
$metaVerdict = Invoke-RestMethod -Uri $metaURI -Method Put -Headers $authHeader -
Body ($metabody | ConvertTo-Json -EnumsAsStrings -Depth 5)
```

Now, when the rule template gets updated, your rule will be notified of the update and give you the option to update the rule as well.

Automation Rules

There are some new features in Automation Rules, including being able to add "OR" groupings for Conditions. There also appears to be a much larger list of the conditions you can check against. Likewise, the only new action is the ability to add a task to an incident (still waiting for that "Send Email" action!)

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/automationRules/**{automationRuleId}**?**{apiVersion}**

Sample Request

```
$body = @{
  "properties" = @{
    "displayName"     = "Book Test"
    "order"           = 1
    "triggeringLogic" = @{
      "isEnabled"         = $false
      "expirationTimeUtc" = $null
      "triggersOn"        = "Incidents"
      "triggersWhen"      = "Created"
      "conditions"        = @(
        @{
          "conditionType"       = "Property"
          "conditionProperties" = @{
            "propertyName"   = "HostName"
            "operator"       = "Contains"
            "propertyValues" = @(
              "Gary"
            )
          }
        }
      )
    }
    "actions"         = @(
      @{
        "order"               = 1
        "actionType"          = "AddIncidentTask"
        "actionConfiguration" = @{
          "title"       = "This is a test task"
```

```
          "description" = "<div><strong>Look </strong><em>at </em><u>this
</u><s>description</s>. Isn't it amazing?</div>"
        }
      }
      @{
        "order"               = 2
        "actionType"          = "AddIncidentTask"
        "actionConfiguration" = @{
          "title"       = "Second task"
          "description" = "<div>The first amazing task</div>"
        }
      }
    )

  }
}
$guid = New-Guid
$url = $baseUrl + "bookmarks/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/AutomationRules
/a72295b0-41a5-45a3-b436-cef14769ec71",
  "name": "a72295b0-41a5-45a3-b436-cef14769ec71",
  "etag": "\"83013fdb-0000-0100-0000-6546b6cc0000\"",
  "type": "Microsoft.SecurityInsights/AutomationRules",
  "properties": {
    "displayName": "Book Test",
    "order": 1,
    "triggeringLogic": {
      "isEnabled": false,
      "triggersOn": "Incidents",
      "triggersWhen": "Created",
      "conditions": [
        {
          "conditionType": "Property",
          "conditionProperties": {
            "propertyName": "HostName",
            "operator": "Contains",
            "propertyValues": [
              "Gary"
```

```
            ]
          }
        }
      ]
    },
    "actions": [
      {
        "order": 1,
        "actionType": "AddIncidentTask",
        "actionConfiguration": {
          "title": "This is a test task",
          "description": "<div><strong>Look </strong><em>at </em><u>this
</u><s>description</s>. Isn't it amazing?</div>"
        }
      },
      {
        "order": 2,
        "actionType": "AddIncidentTask",
        "actionConfiguration": {
          "title": "Second task",
          "description": "<div>The first amazing task</div>"
        }
      }
    ],
    "lastModifiedTimeUtc": "2023-11-04T21:25:32Z",
    "createdTimeUtc": "2023-11-04T21:25:32Z",
    "lastModifiedBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey",
      "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
    },
    "createdBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey",
      "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
    }
  }
}
```


Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/automationRules/**{automationRuleId}**?**{restAPI}**

This REST API call will delete an existing Automation rule where its Id matches the "automationRuleId" being passed in. This is a simple call so I will not go into any detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/automationRules/**{automationRuleId}**?**{restAPI}**

This will get a single automation rule based on the "automationRuleId". You can use the LIST REST API call, shown below, to get a list of all the automation rules to get the "automationRuleId" value.

Sample request

```
$url=$baseURL + "automationRules/eb2ad42f-930d-40cb-8563-d6d629569cbb
" + $apiVersion"
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/AutomationRules
/eb2ad42f-930d-40cb-8563-d6d629569cbb",
  "name": "eb2ad42f-930d-40cb-8563-d6d629569cbb",
  "etag": "\"84015c36-0000-0100-0000-6546bada0000\"",
  "type": "Microsoft.SecurityInsights/AutomationRules",
  "properties": {
    "displayName": "Use Case Automation Rule",
    "order": 2,
    "triggeringLogic": {
      "isEnabled": true,
      "expirationTimeUtc": "2023-11-30T13:00:00Z",
      "triggersOn": "Incidents",
      "triggersWhen": "Updated",
      "conditions": [
        {
          "conditionType": "Property",
          "conditionProperties": {
            "propertyName": "IncidentProviderName",
```

```
            "operator": "Equals",
            "propertyValues": [
              "Azure Sentinel"
            ]
          }
        },
        {
          "conditionType": "Property",
          "conditionProperties": {
            "propertyName": "IncidentRelatedAnalyticRuleIds",
            "operator": "Contains",
            "propertyValues": [
              "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/alertRules/d3c1
e682-14f3-40a2-80b6-34072cd9c272"
            ]
          }
        },
        {
          "conditionType": "Boolean",
          "conditionProperties": {
            "operator": "Or",
            "innerConditions": [
              {
                "conditionType": "PropertyChanged",
                "conditionProperties": {
                  "propertyName": "IncidentStatus",
                  "changeType": "ChangedTo",
                  "operator": "Equals",
                  "propertyValues": [
                    "Closed"
                  ]
                }
              },
              {
                "conditionType": "PropertyChanged",
                "conditionProperties": {
                  "propertyName": "IncidentSeverity",
                  "changeType": "ChangedFrom",
                  "operator": "Equals",
                  "propertyValues": [
                    "Low"
                  ]
                }
```

```
              }
            ]
          }
        }
      ]
    },
    "actions": [
      {
        "order": 1,
        "actionType": "ModifyProperties",
        "actionConfiguration": {
          "severity": null,
          "status": null,
          "classification": null,
          "classificationReason": null,
          "classificationComment": null,
          "owner": {
            "objectId": "2fc92ec6-0d4c-4d31-a5ea-08364b7fca2e",
            "email": null,
            "assignedTo": "Gary Test",
            "userPrincipalName": "garytest@artutillc.com"
          },
          "labels": null
        }
      },
      {
        "order": 2,
        "actionType": "RunPlaybook",
        "actionConfiguration": {
          "logicAppResourceId": "/subscriptions/34bdcce3-c06f-416b-aaa0-
24683117cc68/resourceGroups/MSSentinel/providers/Microsoft.Logic/workflows/Create
JiraIssue",
          "tenantId": "ae0818a0-ede8-4da6-9786-2d9d5fd5295f"
        }
      }
    ],
    "lastModifiedTimeUtc": "2023-11-04T21:42:50Z",
    "createdTimeUtc": "2023-11-04T21:42:50Z",
    "lastModifiedBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey",
      "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
    },
```

```
    "createdBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey",
      "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
    }
  }
}
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/automationRules?**{restAPI}**

This will return a JSON array containing all the individual automation rules. See the GET call above.

Billing Statistics

I never got this REST API to work, it kept throwing a 404 error. Not quite sure why since I tried this one various Microsoft Sentinel instances. In any case, this would only return information regarding SAP right now (and one of the instances I tried it on did have the SAP solution enabled)

My guess is that this isn't quite ready for general use, so it is set to throw the 404. Hopefully this will change soon.

Bookmarks

These are the same bookmarks that you can create using the stable REST API although there are some new fields you can add. You now can add entities, tactics, and techniques to your bookmark.

The other REST APIs are the same and you will get the same information back with the addition of the forementioned fields.

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/bookmarks?**{apiVersion}**

Note that in the request and response below, the "queryResult" has been truncated to save space.

Sample request

```
$body = @{
  "properties" = @{
    "bookmarkId"     = "1f422fde-ad0a-468f-ae62-7dcc4f454373"
    "displayName"    = "AzureActivity - 5d396ad41829"
    "queryResult"    = "{`"TenantId`":`"230c86ca-abf2-48f4-b95e-
8b977e67f4c6`",`"SourceSystem`":`"Azure`",`"CallerIpAddress`":`"52.224.188.169`"}
"
    "query"          = "AzureActivity\n"
    "queryStartTime" = "2023-11-04T14:54:41.376Z"
    "queryEndTime"   = "2023-11-05T14:54:41.376Z"
    "labels"         = @(
      "Book Tag"
    )
    "notes"          = "This is a note describing why I created this bookmark"
    "tactics"        = @(
      "Reconnaissance"
      "Execution"
    )
    "techniques"     = @(
      "T1589.001"
      "T1059"
    )
    "eventTime"      = "2023-11-05T11:36:29.000Z"
    "entityMappings" = @(
```

```
      @{
        "entityType"    = "Host"
        "fieldMappings" = @(
          @{
            "identifier" = "HostName"
            "value"      = "Azure"
          }
        )
      }
    )
  }
}
$guid = New-Guid
$url = $baseUrl + "bookmarks/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Bookmarks/1f422
fde-ad0a-468f-ae62-7dcc4f454373",
  "name": "1f422fde-ad0a-468f-ae62-7dcc4f454373",
  "etag": "\"0601e6cb-0000-0100-0000-6547ad210000\"",
  "type": "Microsoft.SecurityInsights/Bookmarks",
  "properties": {
    "displayName": "AzureActivity - 5d396ad41829",
    "created": "2023-11-05T14:56:33.7066463+00:00",
    "updated": "2023-11-05T14:56:33+00:00",
    "createdBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey"
    },
    "updatedBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey"
    },
    "eventTime": "2023-11-05T11:36:29+00:00",
    "notes": "This is a note describing why I created this bookmark",
    "labels": [
      "Book Tag"
```

```
    ],
    "query": "AzureActivity\n",
    "queryResult": "{\"TenantId\":\"230c86ca-abf2-48f4-b95e-
8b977e67f4c6\",\"SourceSystem\":\"Azure\",\"CallerIpAddress\":\"52.224.188.169\"
}",
    "queryStartTime": "2023-11-04T14:54:41.376+00:00",
    "queryEndTime": "2023-11-05T14:54:41.376+00:00",
    "incidentInfo": {
      "incidentId": null,
      "title": null,
      "relationName": null,
      "severity": null
    },
    "entityMappings": [
      {
        "entityType": "Host",
        "fieldMappings": [
          {
            "identifier": "HostName",
            "value": "Azure"
          }
        ]
      }
    ],
    "tactics": [
      "Reconnaissance",
      "Execution"
    ],
    "techniques": [
      "T1589.001",
      "T1059"
    ]
  }
}
```


List

This is the same as the stable version except for the following filters:

Filters Available: $filter, $orderby, $skipToken, $top

All the other calls are the same as the stable REST API calls.

Content Packages

This is a new REST API that allows you to get a list of the content that you have deployed in your environment. As a reminder, content is the items deployed in the Content Hub in the Microsoft Sentinel portal. Notice that there is no Create/Update call as you cannot create a new content package, you can only Install it.

Delete

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/contentPackages/**{packageId}**?**{apiVersion}**

This REST API call will delete an existing Content Package where its name matches the "packageId" being passed in. This is a simple call so I will not go into much detail.

Keep in mind that this will not delete any active content created by the solution. So if you have a Workbook Template that has been saved to "My workbooks", it will not be deleted.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/contentPackages/**{packageId}**?**{apiVersion}**

This will get a single Content package based on the "packageId" passed in.

Sample Request

```
$url= $baseUrl + "contentPackages/azuresentinel.azure-sentinel-solution-amazonwebservices" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Note that in the Sample Response below, a number of the "criteria" was deleted to save space.

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
```

```
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/contentpackages
/azuresentinel.azure-sentinel-solution-amazonwebservices",
  "name": "azuresentinel.azure-sentinel-solution-amazonwebservices",
  "type": "Microsoft.SecurityInsights/contentpackages",
  "systemData": {
    "createdAt": "2023-06-16T12:32:24.2302819Z",
    "createdBy": "garybushey@outlook.com",
    "createdByType": "User",
    "lastModifiedAt": "2023-06-16T12:32:24.2302819Z",
    "lastModifiedBy": "garybushey@outlook.com",
    "lastModifiedByType": "User"
  },
  "properties": {
    "contentId": "azuresentinel.azure-sentinel-solution-amazonwebservices",
    "contentKind": "Solution",
    "contentSchemaVersion": "3.0.0",
    "contentProductId": "azuresentinel.azure-sentinel-solution-amazonwebser-sl-
kmjeftlz6ckqi",
    "version": "2.0.5",
    "displayName": "Amazon Web Services",
    "source": {
      "kind": "Solution",
      "name": "Amazon Web Services",
      "sourceId": "azuresentinel.azure-sentinel-solution-amazonwebservices"
    },
    "author": {
      "name": "Microsoft"
    },
    "support": {
      "tier": "Microsoft",
      "name": "Microsoft Corporation",
      "email": "support@microsoft.com",
      "link": "https://support.microsoft.com"
    },
    "dependencies": {
      "operator": "AND",
      "criteria": [
        {
          "contentId": "AWS",
          "kind": "DataConnector",
          "version": "1.0.0"
        },
        {
          "contentId": "AwsS3",
          "kind": "DataConnector",
```

```
        "version": "1.0.0"
      },
      {
        "contentId": "AmazonWebServicesNetworkActivitiesWorkbook",
        "kind": "Workbook",
        "version": "1.0.0"
      },
      {
        "contentId": "AmazonWebServicesUserActivitiesWorkbook",
        "kind": "Workbook",
        "version": "1.0.0"
      },
      {
        "contentId": "8c2ef238-67a0-497d-b1dd-5c8a0f533e25",
        "kind": "AnalyticsRule",
        "version": "1.0.1"
      },
      {
        "contentId": "65360bb0-8986-4ade-a89d-af3cf44d28aa",
        "kind": "AnalyticsRule",
        "version": "1.0.2"
      },
      {
        "contentId": "e0a67cd7-b4e5-4468-aae0-26cb16a1bbd2",
        "kind": "HuntingQuery",
        "version": "1.0.0"
      },
      {
        "contentId": "e1a91db8-f2b3-4531-bff6-da133d4f4f1a",
        "kind": "HuntingQuery",
        "version": "1.0.0"
      }
    ]
  },
  "providers": [
    "Amazon Web Services"
  ],
  "firstPublishDate": "2022-05-26",
  "categories": {
    "domains": [
      "Security - Cloud Security"
    ]
  },
```

```
    "icon": "https://store-images.s-microsoft.com/image/apps.64685.2be652b5-01b5-4297-91de-fb1bdca4520e.3b2d6c32-9299-492f-9684-b4890e8acdd9.dff4bda0-283e-49e6-9007-b35209b0a2fd"
  }
}
```

Notice that there are no details about the content being deployed. See the "Content Packages Templates" REST API call below for more information.

Install

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/contentPackages?**{apiVersion}**

This REST API is supposed to install the solution. I say supposed to since even after calling this REST API correctly, the Content Package is not completely installed. Normally, after installing a content, if you go into Microsoft Sentinel's Content Hub and select the content, you would see the "Manage" button at the bottom of the detail pane. Not so if you use this REST API.

While the content will show up in the list as installed, if you select it, you will not see the "Manage button"

Because of this I cannot recommend using this REST API right now. Hopefully it will work in the future and because of that, I will show you how to use it.

Note, in order to get the needed values, you will need to use the "Content Product Packages" REST API call discussed below.

Sample Request

```
$body = @{
  "properties" = @{
    "contentId"      = "azuresentinel.azure-sentinel-solution-akamai"
    "contentProductId"    = "azuresentinel.azure-sentinel-solution-akamai-sl-mf763jf3ctm5i"
    "contentKind"    = "Solution"
    "version"          = "3.0.0"
    "displayName" = "Akamai Security"
  }
}

$url = $baseUrl + "contentPackages/azuresentinel.azure-sentinel-solution-akamai" + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body ($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
```

```
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/contentpackages
/azuresentinel.azure-sentinel-solution-akamai",
  "name": "azuresentinel.azure-sentinel-solution-akamai",
  "type": "Microsoft.SecurityInsights/contentpackages",
  "systemData": {
    "createdAt": "2023-11-05T15:28:21.0392552Z",
    "createdBy": "garybushey@outlook.com",
    "createdByType": "User",
    "lastModifiedAt": "2023-11-05T15:28:21.0392552Z",
    "lastModifiedBy": "garybushey@outlook.com",
    "lastModifiedByType": "User"
  },
  "properties": {
    "contentId": "azuresentinel.azure-sentinel-solution-akamai",
    "contentKind": "Solution",
    "contentProductId": "azuresentinel.azure-sentinel-solution-akamai-sl-
mf763jf3ctm5i",
    "version": "3.0.0",
    "displayName": "Akamai Security"
  }
}
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/contentPackages?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the individual anomaly rules. See the GET above.

One thing I have noticed is that if you are using an older Microsoft Sentinel installation, one that was created before Microsoft switched to using only content from the Content Hub, this will only return those Content Packages there installed using the Content Hub. Any that were installed automatically due to the change will not show up.

Content Product Packages

This is a new REST API that allows you to get a list of the content in your environment, not just the deployed ones like with the "Content Packages". As a reminder, content is the items deployed in the Content Hub in the Microsoft Sentinel portal. Notice that there are no Create/Update or Delete calls as you have no control over what content packages are available in your environment.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/contentProductPackages/**{packageId}**?**{apiVersion}**

This will return a single content package.

Sample Request

```
$url = $baseUrl + "contentPackages/azuresentinel.azure-sentinel-solution-akamai" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Note that in the Sample Response below, I have deleted several entries under "resources" to save space. Normally, each item that gets deployed will have its entire definition listed there.

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/contentproductpackages/azuresentinel.azure-sentinel-solution-akamai-sl-mf763jf3ctm5i",
  "name": "azuresentinel.azure-sentinel-solution-akamai-sl-mf763jf3ctm5i",
  "type": "Microsoft.SecurityInsights/contentproductpackages",
  "systemData": {},
  "properties": {
    "contentId": "azuresentinel.azure-sentinel-solution-akamai",
    "contentKind": "Solution",
    "contentProductId": "azuresentinel.azure-sentinel-solution-akamai-sl-mf763jf3ctm5i",
    "installedVersion": null,
```

```
"isNew": false,
"isPreview": false,
"isFeatured": false,
"version": "3.0.0",
"displayName": "Akamai Security",
"description": null,
"source": {
  "kind": "Solution",
  "name": "Akamai Security Events",
  "sourceId": "azuresentinel.azure-sentinel-solution-akamai"
},
"author": {
  "name": "Microsoft",
  "email": "support@microsoft.com"
},
"support": {
  "tier": "Microsoft",
  "name": "Microsoft Corporation",
  "email": "support@microsoft.com",
  "link": "https://support.microsoft.com"
},
"dependencies": {
  "operator": "AND",
  "criteria": [
    {
      "contentId": "AkamaiSecurityEvents",
      "kind": "DataConnector",
      "version": "1.0.0"
    },
    {
      "contentId": "AkamaiSecurityEventsAma",
      "kind": "DataConnector",
      "version": "1.0.0"
    },
    {
      "contentId": "AkamaiSIEMEvent-Parser",
      "kind": "Parser",
      "version": "1.0.0"
    }
  ]
},
"providers": [
  "Akamai"
],
"firstPublishDate": "2022-03-23",
```

```
    "lastPublishDate": "0001-01-01",
    "categories": {
      "domains": [
        "Security - Cloud Security"
      ]
    },
    "threatAnalysisTactics": null,
    "threatAnalyticsTechniques": null,
    "metadataResourceId": null,
    "icon": "https://store-images.s-microsoft.com/image/apps.33880.cd71756a-a6d5-
48b2-8e5b-6c4c24e77e0d.ac33d759-f432-41ab-bf85-a4a26df1dc7d.5e0074f9-c075-4fd6-
be7c-bc92d9b1f788",
    "packagedContent": {
      "$schema": "https://schema.management.azure.com/schemas/2019-04-
01/deploymentTemplate.json#",
      "contentVersion": "1.0.0.0",
      "metadata": {},
      "parameters": {
        "location": {
          "type": "string",
          "minLength": 1,
          "defaultValue": "[resourceGroup().location]",
          "metadata": {
            "description": "Not used, but needed to pass arm-ttk test `Location-
Should-Not-Be-Hardcoded`.  We instead use the `workspace-location` which is
derived from the LA workspace"
          }
        },
        "workspace-location": {
          "type": "string",
          "defaultValue": "",
          "metadata": {
            "description": "[concat('Region to deploy solution resources --
separate from location selection',parameters('location'))]"
          }
        },
        "workspace": {
          "defaultValue": "",
          "type": "string",
          "metadata": {
            "description": "Workspace name for Log Analytics where Microsoft
Sentinel is setup"
          }
        }
      },
```

```
      "resources": [
        {
          "name": "pid-cd71756a-a6d5-48b2-8e5b-6c4c24e77e0d-partnercenter",
          "type": "Microsoft.Resources/deployments",
          "apiVersion": "2020-10-01",
          "properties": {
            "mode": "Incremental",
            "template": {
              "$schema": "https://schema.management.azure.com/schemas/2019-04-
01/deploymentTemplate.json#",
              "contentVersion": "1.0.0.0",
              "resources": []
            }
          }
        },
        {
          "type":
"Microsoft.OperationalInsights/workspaces/providers/contentTemplates",
          "apiVersion": "2023-04-01-preview",
          "name":
"[concat(parameters('workspace'),'/Microsoft.SecurityInsights/',concat(parameters
('workspace'),'-dc-',uniquestring('AkamaiSecurityEvents')))]",
          "location": "[parameters('workspace-location')]",
          "dependsOn": [
            "[extensionResourceId(resourceId('Microsoft.OperationalInsights/works
paces', parameters('workspace')), 'Microsoft.SecurityInsights/contentPackages',
'azuresentinel.azure-sentinel-solution-akamai')]"
          ],
          "properties": {
            "description": "Akamai Security Events data connector with template
version 3.0.0",
            "mainTemplate": {
              "$schema": "https://schema.management.azure.com/schemas/2019-04-
01/deploymentTemplate.json#",
              "contentVersion": "1.0.0",
              "parameters": {},
              "variables": {},
              "resources": [
                {
                  "name":
"[concat(parameters('workspace'),'/Microsoft.SecurityInsights/','AkamaiSecurityEv
ents')]",
                  "apiVersion": "2021-03-01-preview",
                  "type":
"Microsoft.OperationalInsights/workspaces/providers/dataConnectors",
```

```
                    "location": "[parameters('workspace-location')]",
                    "kind": "GenericUI",
                    "properties": {
                      "connectorUiConfig": {
                        "id": "AkamaiSecurityEvents",
                        "title": "[Deprecated] Akamai Security Events via Legacy
Agent",
                        "publisher": "Akamai",
                        "descriptionMarkdown": "Akamai Solution for Microsoft
Sentinel",
                        "additionalRequirementBanner": "These queries are dependent
on a parser based on a Kusto Function deployed as part of the solution.",
                        "graphQueries": "",
                        "sampleQueries": "",
                        "dataTypes": "",
                        "connectivityCriterias": "",
                        "availability": "@{status=1; isPreview=False}",
                        "permissions": "@{resourceProvider=System.Object[]}",
                        "instructionSteps": "    "
                      }
                    }
                  },
                  {
                    "type":
"Microsoft.OperationalInsights/workspaces/providers/metadata",
                    "apiVersion": "2023-04-01-preview",
                    "name":
"[concat(parameters('workspace'),'/Microsoft.SecurityInsights/',concat('DataConne
ctor-',
last(split(extensionResourceId(resourceId('Microsoft.OperationalInsights/workspac
es', parameters('workspace')), 'Microsoft.SecurityInsights/dataConnectors',
'AkamaiSecurityEvents'),'/'))))]",
                    "properties": {
                      "parentId":
"[extensionResourceId(resourceId('Microsoft.OperationalInsights/workspaces',
parameters('workspace')), 'Microsoft.SecurityInsights/dataConnectors',
'AkamaiSecurityEvents')]",
                      "contentId": "AkamaiSecurityEvents",
                      "kind": "DataConnector",
                      "version": "1.0.0",
                      "source": {
                        "kind": "Solution",
                        "name": "Akamai Security Events",
                        "sourceId": "azuresentinel.azure-sentinel-solution-akamai"
                      },
```

```
                    "author": {
                      "name": "Microsoft",
                      "email": "support@microsoft.com"
                    },
                    "support": {
                      "name": "Microsoft Corporation",
                      "email": "support@microsoft.com",
                      "tier": "Microsoft",
                      "link": "https://support.microsoft.com"
                    }
                  }
                }
              ]
            },
            "packageKind": "Solution",
            "packageVersion": "3.0.0",
            "packageName": "Akamai Security Events",
            "packageId": "azuresentinel.azure-sentinel-solution-akamai",
            "contentSchemaVersion": "3.0.0",
            "contentId": "AkamaiSecurityEvents",
            "contentKind": "DataConnector",
            "displayName": "[Deprecated] Akamai Security Events via Legacy
Agent",
            "contentProductId": "azuresentinel.azure-sentinel-solution-akamai-dc-
ybfbxbvnj6ojg",
            "id": "azuresentinel.azure-sentinel-solution-akamai-dc-
ybfbxbvnj6ojg",
            "version": "1.0.0",
            "isDeprecated": false
          }
        },
        {
          "type": "Microsoft.OperationalInsights/workspaces/providers/metadata",
          "apiVersion": "2023-04-01-preview",
          "name":
"[concat(parameters('workspace'),'/Microsoft.SecurityInsights/',concat('DataConne
ctor-',
last(split(extensionResourceId(resourceId('Microsoft.OperationalInsights/workspac
es', parameters('workspace')), 'Microsoft.SecurityInsights/dataConnectors',
'AkamaiSecurityEvents'),'/'))))]",
          "dependsOn": [
            "[extensionResourceId(resourceId('Microsoft.OperationalInsights/works
paces', parameters('workspace')), 'Microsoft.SecurityInsights/dataConnectors',
'AkamaiSecurityEvents')]"
          ],
```

```
          "location": "[parameters('workspace-location')]",
          "properties": {
            "parentId":
"[extensionResourceId(resourceId('Microsoft.OperationalInsights/workspaces',
parameters('workspace')), 'Microsoft.SecurityInsights/dataConnectors',
'AkamaiSecurityEvents')]",
            "contentId": "AkamaiSecurityEvents",
            "kind": "DataConnector",
            "version": "1.0.0",
            "source": {
              "kind": "Solution",
              "name": "Akamai Security Events",
              "sourceId": "azuresentinel.azure-sentinel-solution-akamai"
            },
            "author": {
              "name": "Microsoft",
              "email": "support@microsoft.com"
            },
            "support": {
              "name": "Microsoft Corporation",
              "email": "support@microsoft.com",
              "tier": "Microsoft",
              "link": "https://support.microsoft.com"
            }
          }
        }
      ]
    },
    "contentSchemaVersion": "3.0.0",
    "publisherDisplayName": "Microsoft Sentinel, Microsoft Corporation",
    "descriptionHtml": "<p><strong>Note:</strong> Please refer to the following
before installing the..",
    "isDeprecated": false
  }
}
```

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/contentProductPackages?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the individual anomaly rules. See the GET above.

Content Product Templates

This is a new REST API that allows you to get a list of the templates for all your content in your environment (as opposed to "Content Templates" which returns templates for the content you have installed). As a reminder, content is the items deployed in the Content Hub in the Microsoft Sentinel portal. Notice that there are no Create/Update or Delete calls as you have no control over what content product templates are available in your environment.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/contentProductTemplates/**{templateId}**?**{apiVersion}**

This will return a template from any content.

Sample Request

```
$url= $baseUrl + "contentProductTemplates/azuresentinel.azure-sentinel-solution-azureactivit-ar-mrf6upirdpfw6" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Note that in the following Sample Response, I got rid of some of the dependencies, shortened some descriptions, and removed the query to save space.

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/contentproducttemplates/azuresentinel.azure-sentinel-solution-azureactivit-ar-mrf6upirdpfw6",
  "name": "azuresentinel.azure-sentinel-solution-azureactivit-ar-mrf6upirdpfw6",
  "type": "Microsoft.SecurityInsights/contentproducttemplates",
  "systemData": {},
  "properties": {
    "packagedContent": {
      "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
      "contentVersion": "2.0.1",
      "parameters": {
        "location": {
          "type": "string",
```

```
          "minLength": 1,
          "defaultValue": "[resourceGroup().location]",
          "metadata": {
            "description": "Not used, but needed to pass arm-ttk test `Location-
Should-Not-Be-Hardcoded`.  We instead use the `workspace-location` which is
derived from the LA workspace"
          }
        },
        "workspace": {
          "defaultValue": "",
          "type": "string",
          "metadata": {
            "description": "Workspace name for Log Analytics where Microsoft
Sentinel is setup"
          }
        },
        "workspace-location": {
          "type": "string",
          "defaultValue": "",
          "metadata": {
            "description": "[concat('Region to deploy solution resources --
separate from location selection',parameters('location'))]"
          }
        }
      },
      "resources": [
        {
          "type":
"Microsoft.OperationalInsights/workspaces/providers/contentTemplates",
          "name":
"[concat(parameters('workspace'),'/Microsoft.SecurityInsights/',concat(concat(par
ameters('workspace'),'-ar-',uniquestring('9736e5f1-7b6e-4bfb-a708-
e53ff1d182c3')),'2.0.1'))]",
          "location": "[parameters('workspace-location')]",
          "apiVersion": "2023-04-01-preview",
          "dependsOn": [
            "[extensionResourceId(resourceId('Microsoft.OperationalInsights/works
paces', parameters('workspace')), 'Microsoft.SecurityInsights/contentPackages',
'azuresentinel.azure-sentinel-solution-azureactivity')]"
          ],
          "properties": {
            "contentId": "9736e5f1-7b6e-4bfb-a708-e53ff1d182c3",
            "displayName": "Creation of expensive computes in Azure",
            "contentKind": "AnalyticsRule",
            "mainTemplate": {
```

```
            "$schema": "https://schema.management.azure.com/schemas/2019-04-
01/deploymentTemplate.json#",
            "contentVersion": "2.0.1",
            "parameters": {},
            "variables": {},
            "resources": [
              {
                "type": "Microsoft.SecurityInsights/AlertRuleTemplates",
                "name": "9736e5f1-7b6e-4bfb-a708-e53ff1d182c3",
                "apiVersion": "2022-04-01-preview",
                "kind": "Scheduled",
                "location": "[parameters('workspace-location')]",
                "properties": {
                  "description": "Identifies the creation of large size or
expensive VMs (with GPUs or with a large number of virtual CPUs) in Azure.",
                  "displayName": "Creation of expensive computes in Azure",
                  "enabled": false,
                  "query": "<query>",
                  "queryFrequency": "P1D",
                  "queryPeriod": "P1D",
                  "severity": "Low",
                  "suppressionDuration": "PT1H",
                  "suppressionEnabled": false,
                  "triggerOperator": "GreaterThan",
                  "triggerThreshold": 1,
                  "status": "Available",
                  "requiredDataConnectors": [
                    {
                      "dataTypes": [
                        "AzureActivity"
                      ],
                      "connectorId": "AzureActivity"
                    }
                  ],
                  "tactics": [
                    "DefenseEvasion"
                  ],
                  "techniques": [
                    "T1578"
                  ],
                  "entityMappings": [
                    {
                      "entityType": "Account",
                      "fieldMappings": [
                        {
```

```
                        "columnName": "Name",
                        "identifier": "Name"
                      },
                      {
                        "columnName": "UPNSuffix",
                        "identifier": "UPNSuffix"
                      }
                    ]
                  },
                  {
                    "entityType": "IP",
                    "fieldMappings": [
                      {
                        "columnName": "CallerIpAddress",
                        "identifier": "Address"
                      }
                    ]
                  }
                ]
              }
            },
            {
              "type":
"Microsoft.OperationalInsights/workspaces/providers/metadata",
              "apiVersion": "2022-01-01-preview",
              "name":
"[concat(parameters('workspace'),'/Microsoft.SecurityInsights/',concat('Analytics
Rule-', last(split(resourceId('Microsoft.SecurityInsights/AlertRuleTemplates',
'9736e5f1-7b6e-4bfb-a708-e53ff1d182c3'),'/'))))]",
              "properties": {
                "description": "Azure Activity Analytics Rule 5",
                "parentId":
"[resourceId('Microsoft.SecurityInsights/AlertRuleTemplates', '9736e5f1-7b6e-
4bfb-a708-e53ff1d182c3')]",
                "contentId": "9736e5f1-7b6e-4bfb-a708-e53ff1d182c3",
                "kind": "AnalyticsRule",
                "version": "2.0.1",
                "source": {
                  "kind": "Solution",
                  "name": "Azure Activity",
                  "sourceId": "azuresentinel.azure-sentinel-solution-
azureactivity"
                },
                "author": {
                  "name": "Microsoft",
```

```
                    "email": "support@microsoft.com"
                  },
                  "support": {
                    "tier": "Microsoft",
                    "name": "Microsoft Corporation",
                    "email": "support@microsoft.com",
                    "link": "https://support.microsoft.com/"
                  }
                }
              }
            ]
          },
          "packageKind": "Solution",
          "packageVersion": "2.0.6",
          "packageName": "Azure Activity",
          "packageId": "azuresentinel.azure-sentinel-solution-azureactivity",
          "contentProductId": "azuresentinel.azure-sentinel-solution-
azureactivit-ar-mrf6upirdpfw6",
          "id": "azuresentinel.azure-sentinel-solution-azureactivit-ar-
mrf6upirdpfw6",
          "contentSchemaVersion": "3.0.0",
          "version": "2.0.1",
          "isDeprecated": false
        }
      },
      {
        "type":
"Microsoft.OperationalInsights/workspaces/providers/contentPackages",
        "name":
"[concat(parameters('workspace'),'/Microsoft.SecurityInsights/',
'azuresentinel.azure-sentinel-solution-azureactivity')]",
        "location": "[parameters('workspace-location')]",
        "apiVersion": "2023-04-01-preview",
        "properties": {
          "version": "2.0.6",
          "kind": "Solution",
          "contentSchemaVersion": "3.0.0",
          "contentId": "azuresentinel.azure-sentinel-solution-azureactivity",
          "source": {
            "kind": "Solution",
            "name": "Azure Activity",
            "sourceId": "azuresentinel.azure-sentinel-solution-azureactivity"
          },
          "author": {
            "name": "Microsoft",
```

```
            "email": "support@microsoft.com"
          },
          "support": {
            "name": "Microsoft Corporation",
            "email": "support@microsoft.com",
            "tier": "Microsoft",
            "link": "https://support.microsoft.com/"
          },
          "dependencies": {
            "operator": "AND",
            "criteria": [
              {
                "kind": "DataConnector",
                "contentId": "AzureActivity",
                "version": "2.0.0"
              },
              {
                "kind": "HuntingQuery",
                "contentId": "ef7ef44e-6129-4d8e-94fe-b5530415d8e5",
                "version": "2.0.1"
              },
            {
                "kind": "AnalyticsRule",
                "contentId": "86a036b2-3686-42eb-b417-909fc0867771",
                "version": "2.0.1"
              },
              {
                "kind": "Workbook",
                "contentId": "AzureActivityWorkbook",
                "version": "2.0.0"
              }
            ]
          },
          "firstPublishDate": "2022-04-18",
          "providers": [
            "Microsoft"
          ],
          "categories": {
            "domains": [
              "IT Operations"
            ]
          },
          "contentKind": "Solution",
          "contentProductId": "azuresentinel.azure-sentinel-solution-
azureactivit-sl-cewdk2emk4lrc",
```

```
            "id": "azuresentinel.azure-sentinel-solution-azureactivit-sl-
cewdk2emk4lrc",
            "displayName": "Azure Activity",
            "publisherDisplayName": "Microsoft Sentinel, Microsoft Corporation",
            "descriptionHtml": "<p><strong>Note:</strong> <em>There may be <a
target=\"_blank\" ",
            "icon": "https://store-images.s-
microsoft.com/image/apps.64828.1f6369a4-223e-4c86-808c-1d26a17c4def.5cdcf0e0-
1405-4829-b75c-eebf340fe7f6.8700ba50-ca62-485b-8a98-caeb96314bd0",
            "isPreview": false,
            "isDeprecated": false
          }
        }
      ]
    },
    "isDeprecated": false,
    "packageKind": "Solution",
    "packageId": "azuresentinel.azure-sentinel-solution-azureactivity",
    "packageVersion": "2.0.6",
    "contentSchemaVersion": "3.0.0",
    "contentProductId": "azuresentinel.azure-sentinel-solution-azureactivit-ar-
mrf6upirdpfw6",
    "contentId": "9736e5f1-7b6e-4bfb-a708-e53ff1d182c3",
    "displayName": "Creation of expensive computes in Azure",
    "contentKind": "AnalyticsRule",
    "version": "2.0.1",
    "source": {
      "kind": "Solution",
      "name": "Azure Activity",
      "sourceId": "azuresentinel.azure-sentinel-solution-azureactivity"
    },
    "author": {
      "name": "Microsoft",
      "email": "support@microsoft.com"
    },
    "support": {
      "tier": "Microsoft",
      "name": "Microsoft Corporation",
      "email": "support@microsoft.com",
      "link": "https://support.microsoft.com/"
    },
    "firstPublishDate": "0001-01-01",
    "lastPublishDate": "0001-01-01"
  }
}
```

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/contentProductTemplates?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the individual content templates. See the GET above. Note that the individual GET calls will return more information than you get using the LIST REST API.

Content Templates

This is a new REST API that allows you to get a list of the templates for all your content in your environment (as opposed to "Content Templates" which returns templates for the content you have installed). As a reminder, content is the items deployed in the Content Hub in the Microsoft Sentinel portal. Notice that there are no Create/Update or Delete calls as you have no control over what content product templates are available in your environment.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/contentTemplates/**{templateId}**?**{apiVersion}**

This will return a template from any installed content.

Note that I am getting the same template that I got in the "Content Product Templates" above just to show the differences in the calls.

Sample Request

```
$url= $baseUrl + "contentTemplates/gabazuresentinel-ar-dhepd4eos4ilo2.0.1" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Note that in the "Sample Response" below, the query was removed to save space.

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/contenttemplates/gabazuresentinel-ar-dhepd4eos4ilo2.0.1",
  "name": "gabazuresentinel-ar-dhepd4eos4ilo2.0.1",
  "type": "Microsoft.SecurityInsights/contenttemplates",
  "systemData": {
    "createdAt": "2023-06-27T12:20:26.0011023Z",
    "createdBy": "garybushey@outlook.com",
    "createdByType": "User",
    "lastModifiedAt": "2023-06-27T12:26:23.9862563Z",
    "lastModifiedBy": "garybushey@outlook.com",
    "lastModifiedByType": "User"
```

```
  },
  "properties": {
    "packageKind": "Solution",
    "packageId": "azuresentinel.azure-sentinel-solution-azureactivity",
    "packageVersion": "2.0.1",
    "contentSchemaVersion": "3.0.0",
    "contentProductId": "azuresentinel.azure-sentinel-solution-azureactivit-ar-
mrf6upirdpfw6",
    "contentId": "9736e5f1-7b6e-4bfb-a708-e53ff1d182c3",
    "displayName": "Creation of expensive computes in Azure",
    "contentKind": "AnalyticsRule",
    "version": "2.0.1",
    "mainTemplate": {
      "$schema": "https://schema.management.azure.com/schemas/2019-04-
01/deploymentTemplate.json#",
      "contentVersion": "2.0.1",
      "parameters": {},
      "variables": {},
      "resources": [
        {
          "type": "Microsoft.SecurityInsights/AlertRuleTemplates",
          "name": "9736e5f1-7b6e-4bfb-a708-e53ff1d182c3",
          "apiVersion": "2022-04-01-preview",
          "kind": "Scheduled",
          "location": "eastus",
          "properties": {
            "description": "Identifies the creation of large size or expensive
VMs (with GPUs or with a large number of virtual CPUs) ",
            "displayName": "Creation of expensive computes in Azure",
            "enabled": false,
            "query": "<query>",
            "queryFrequency": "P1D",
            "queryPeriod": "P1D",
            "severity": "Low",
            "suppressionDuration": "PT1H",
            "suppressionEnabled": false,
            "triggerOperator": "GreaterThan",
            "triggerThreshold": 1,
            "status": "Available",
            "requiredDataConnectors": [
              {
                "dataTypes": [
                  "AzureActivity"
                ],
                "connectorId": "AzureActivity"
```

```
            }
          ],
          "tactics": [
            "DefenseEvasion"
          ],
          "techniques": [
            "T1578"
          ],
          "entityMappings": [
            {
              "entityType": "Account",
              "fieldMappings": [
                {
                  "columnName": "Name",
                  "identifier": "Name"
                },
                {
                  "columnName": "UPNSuffix",
                  "identifier": "UPNSuffix"
                }
              ]
            },
            {
              "entityType": "IP",
              "fieldMappings": [
                {
                  "columnName": "CallerIpAddress",
                  "identifier": "Address"
                }
              ]
            }
          ]
        }
      },
      {
        "type": "Microsoft.OperationalInsights/workspaces/providers/metadata",
        "apiVersion": "2022-01-01-preview",
        "name": "gabazuresentinel/Microsoft.SecurityInsights/AnalyticsRule-
9736e5f1-7b6e-4bfb-a708-e53ff1d182c3",
        "properties": {
          "description": "Azure Activity Analytics Rule 5",
          "parentId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.SecurityInsights/Al
ertRuleTemplates/9736e5f1-7b6e-4bfb-a708-e53ff1d182c3",
          "contentId": "9736e5f1-7b6e-4bfb-a708-e53ff1d182c3",
```

```
            "kind": "AnalyticsRule",
            "version": "2.0.1",
            "source": {
              "kind": "Solution",
              "name": "Azure Activity",
              "sourceId": "azuresentinel.azure-sentinel-solution-azureactivity"
            },
            "author": {
              "name": "Microsoft",
              "email": "support@microsoft.com"
            },
            "support": {
              "tier": "Microsoft",
              "name": "Microsoft Corporation",
              "email": "support@microsoft.com",
              "link": "https://support.microsoft.com/"
            }
          }
        }
      ]
    }
  }
}
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/contentTemplates?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the individual content templates. See the GET above. Note that the individual GET calls will return more information than you get using the LIST REST API.

Enrichment

Enrichment allows you to enrich an incident, or anything else, with additional data. Currently, there are only two calls; one to get geographical data and one to get information about a domain

Get Geographical Information for an IP Address

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers /Microsoft.SecurityInsights/enrichmanet/ip/geodata ?ipAddress=**{ipAddress}**&**{apiVersion}**

This will return information about the IP Address passed in including City, Country, Carrier, and other data.

Note that this doesn't follow the normal URL for Microsoft Sentinel REST API calls.

Sample Request

```
url="https://management.azure.com/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.SecurityInsights/enrichment/ip/geodata?ipaddress=162.216.150.233&api-version=2023-09-01-preview"
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
  "asn": "396982",
  "carrier": "google",
  "city": "north charleston",
  "cityCf": 95,
  "continent": "north america",
  "country": "united states",
  "countryCf": 99,
  "ipAddr": "162.216.150.233",
  "ipRoutingType": "fixed",
  "latitude": "32.89008",
  "longitude": "-80.05894",
  "organization": "google",
  "organizationType": "Internet Service Provider",
  "region": "southeast",
  "state": "south carolina",
  "stateCf": 97,
  "stateCode": "sc"
```

```
}
```

Get Domain Information

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers /Microsoft.SecurityInsights/enrichmanet/domain/whois ?domain=**{domain}**&**{apiVersion}**

This will return information about the IP Address passed in including City, Country, Carrier, and other data.

Note that this doesn't follow the normal URL for Microsoft Sentinel REST API calls.

Sample Request

```
$url="https://management.azure.com/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.SecurityInsights/enrichment/domain/whois?domain=microsoft.com&api-version=2023-09-01-preview"
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
  "domain": "microsoft.com",
  "server": "whois.markmonitor.com",
  "created": "1991-05-02T00:00:00Z",
  "updated": "2023-08-18T00:00:00Z",
  "expires": "2025-05-03T00:00:00Z",
  "parsedWhois": {
    "registrar": {
      "name": "MarkMonitor, Inc.",
      "abuseContactPhone": "12086851750",
      "abuseContactEmail": "abusecomplaints@markmonitor.com",
      "ianaId": "292",
      "url": "http://www.markmonitor.com",
      "whoisServer": "whois.markmonitor.com"
    },
    "contacts": {
      "admin": {
        "name": "Domain Administrator",
        "org": "Microsoft Corporation",
        "street": [
          "One Microsoft Way,"
        ],
```

```
    "city": "Redmond",
    "state": "WA",
    "postal": "98052",
    "country": "us",
    "phone": "14258828080",
    "fax": "14259367329",
    "email": "admin@domains.microsoft"
  },
  "registrant": {
    "name": "Domain Administrator",
    "org": "Microsoft Corporation",
    "street": [
      "One Microsoft Way,"
    ],
    "city": "Redmond",
    "state": "WA",
    "postal": "98052",
    "country": "us",
    "phone": "14258828080",
    "fax": "14259367329",
    "email": "admin@domains.microsoft"
  },
  "billing": {
    "name": "",
    "org": "",
    "street": [],
    "city": "",
    "state": "",
    "postal": "",
    "country": "",
    "phone": "",
    "fax": "",
    "email": ""
  },
  "tech": {
    "name": "MSN Hostmaster",
    "org": "Microsoft Corporation",
    "street": [
      "One Microsoft Way,"
    ],
    "city": "Redmond",
    "state": "WA",
    "postal": "98052",
    "country": "us",
    "phone": "14258828080",
```

```
        "fax": "14259367329",
        "email": "msnhst@microsoft.com"
      }
    },
    "nameServers": [
      "ns1-39.azure-dns.com",
      "ns2-39.azure-dns.net",
      "ns3-39.azure-dns.org",
      "ns4-39.azure-dns.info"
    ],
    "statuses": [
      "clientUpdateProhibited",
      "clientTransferProhibited",
      "clientDeleteProhibited",
      "serverUpdateProhibited",
      "serverTransferProhibited",
      "serverDeleteProhibited"
    ]
  }
}
```

Entities

These REST APIs are used when you to into the Entity Behavior page in the Microsoft Sentinel portal as opposed to showing the entities when looking at an incident. If you then go from the Incident Details page into the Entity Behavior page, these REST APIs will kick in.

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entities/**{entityId}**?**{apiVersion}**

Expand

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entities/**{entityId}**?**{apiVersion}**

I am not certain what this REST API call is supposed to do. I see the call being made when selecting an entity but I am not getting any data back. I am unable to determine what it is supposed to do from the example JSON files as well.

In the Sample Request below, I have no idea where the value for the "expansionId" came from. I see the value being used in the portal but cannot determine if this is the same for all IP addresses (which is the only values I see this for). From what I can tell, this is the same value no matter which Microsoft Sentinel instance you are using but the value is not listed anywhere.

Sample Request

```
$body = @{
    "expansionId"                = "fa16a940-53cc-4e45-9e6f-d8409cb42390"
    "startTime"                  = "2023-10-13T15:34:59.351Z"
    "endTime"                    = "2023-11-12T16:34:59.351Z"
    "limitMaxResults"            = 100
    "addDefaultExtendedTimeRange" = $false
}
$url = $baseUrl + "entities/7e11e76f-53a9-a5e4-bb49-6480c6f9812a/expand" + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method POST -Headers $authHeader -Body ($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
    "value": {
        "entities": [],
        "edges": []
```

```
    },
    "metaData": {
        "aggregations": []
    }
}
```

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entities/**{entityId}**?**{apiVersion}**

Get a single entity.

Sample Request

```
$url = $baseUrl + "entities/d9c3136f-d10e-75f5-7346-97332578ab95" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/entities/d9c313
6f-d10e-75f5-7346-97332578ab95",
    "name": "d9c3136f-d10e-75f5-7346-97332578ab95",
    "type": "Microsoft.SecurityInsights/entities",
    "kind": "Account",
    "properties": {
      "accountName": "matthew.lowe",
      "upnSuffix": "live.com",
      "aadTenantId": "ae0818a0-ede8-4da6-9786-2d9d5fd5295f",
      "aadUserId": "3a89ff88-db1e-4433-8adf-fc6ebab28812",
      "isDomainJoined": true,
      "displayName": "Matt Guest Account",
      "additionalData": {
        "Sources": "[\"AzureActiveDirectory\"]",
        "IsDeleted": "True",
        "IsEnabled": "True",
        "MailAddress": "matthew.lowe@live.com",
        "UserType": "Guest",
        "UpnName": "matthew.lowe@live.com",
        "SyncFromAad": "True",
        "HardDeletedDateTime": "2023-09-11T04:52:09.884238Z"
      },
```

```
      "friendlyName": "Matt Guest Account"
    }
  }
```

Get TimeLine

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entities/**{entityId}**/getTimeline?**{apiVersion}**

This will retrieve the results of all the Entity Queries that get run in the middle of the User Entity Behavior Analytics page in the Entity timeline section.

Sample Request

```
$body = @{
    "kinds"          = @(
        "SecurityAlert"
        "Bookmark"
        "Activity"
        "Anomaly"
    )
    "startTime"      = "2023-11-11T19:28:55.721Z"
    "endTime"        = "2023-11-12T19:28:55.721Z"
    "numberOfBucket" = 6
}
$url = $baseUrl + "entities/7e11e76f-53a9-a5e4-bb49-6480c6f9812a/timeline" + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method POST -Headers $authHeader -Body ($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

In the Sample Response below, I have removed a large number of entries under “value” hence the reason the numbers in the “metadata” do not match.

Sample Response

```
{
    "value": [
        {
            "intent": "InitialAccess",
            "azureResourceId": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/entities/ed0b30a1-6629-807e-08bd-4703d16855ae",
```

```
            "description": "This query over Azure AD sign-in activity highlights
Azure AD apps with \nan unusually high ratio of distinct geolocations versus
total number of authentications",
            "productName": "Azure Sentinel",
            "displayName": "Anomalous Azure Active Directory apps based on
authentication location",
            "severity": "Medium",
            "endTimeUtc": "2023-11-12T18:53:09.4969426Z",
            "startTimeUtc": "2023-11-12T14:50:51.5786329Z",
            "timeGenerated": "2023-11-12T19:26:00.2476674Z",
            "alertType": "8ecf8077-cf51-4820-aadd-14040956f35d_ba57f0c2-2937-
4c35-9b26-7c6a9c6e1726",
            "kind": "SecurityAlert"
        },
        {
            "intent": "InitialAccess",
            "azureResourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/entities/3455c7
06-223f-4bc2-b0f9-4e4fc9851fd3",
            "description": "User PDemo@seccxpninja.onmicrosoft.com Attempted to
Logon a High Number of Time from Outside the UK",
            "productName": "Azure Sentinel",
            "displayName": "High Number of Logon Attempts from Outside UK",
            "severity": "Medium",
            "endTimeUtc": "2023-11-12T15:51:42.6696234Z",
            "startTimeUtc": "2023-11-12T11:51:42.6696234Z",
            "timeGenerated": "2023-11-12T15:56:45.458707Z",
            "alertType": "8ecf8077-cf51-4820-aadd-14040956f35d_dfd2db7d-3f5b-
48af-b408-1a8c94530f29",
            "kind": "SecurityAlert"
        },
        {
            "queryId": "6b68d147-efdb-4c1e-ab5b-950fdac39066",
            "bucketStartTimeUTC": "2023-11-11T19:28:55+00:00",
            "bucketEndTimeUTC": "2023-11-12T19:28:55+00:00",
            "firstActivityTimeUTC": "2023-11-11T22:20:38.074+00:00",
            "lastActivityTimeUTC": "2023-11-11T22:56:15.4076094+00:00",
            "content": "The account: 'PDemo', with sid = 'Maayan' has done '10'
activity times",
            "title": "Ori and Yaniv",
            "kind": "Activity"
        }
    ],
    "metaData": {
```

```
        "aggregations": [
            {
                "kind": "SecurityAlert",
                "count": 341
            },
            {
                "kind": "Bookmark",
                "count": 0
            },
            {
                "kind": "Activity",
                "count": 1
            },
            {
                "kind": "Anomaly",
                "count": 0
            }
        ],
        "totalCount": 201
    }
}
```


Get Queries

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entities/**{entityId}/**queries?**{apiVersion}&kind=Insight**

This will return a listing of the queries that will be used to populate the Insights column that is on the right hand side of the User Entity Behavior Analytics page in the Microsoft Sentinel Portal

Sample Request

```
$url = $baseUrl + "entities/c385943a-6320-0534-778f-ae9e84396d78/queries" + $apiVersion + "&kind=Insight"
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Note that in the Sample Response below, I have removed a number of entries to save space. That is why the values in “metaData” do not match.

Sample Response


```
[
    {
```

```
        "id": "/subscriptions/d1d8779d-38d7-4f06-91db-
9cbc8de0176f/resourceGroups/soc/providers/Microsoft.OperationalInsights/workspace
s/cybersecuritysoc/providers/Microsoft.SecurityInsights/entities/c385943a-6320-
0534-778f-ae9e84396d78/queries/ce14b423-4f00-47cc-a23f-c0fdf7e3af76",
        "name": "ce14b423-4f00-47cc-a23f-c0fdf7e3af76",
        "type": "Microsoft.SecurityInsights/entities/queries",
        "kind": "Insight",
        "properties": {
            "displayName": "Actions by account",
            "description": "Summary of actions taken by the specified account
(InitiatedByAccount), grouped by action: password resets and changes, account
lockouts (policy or admin), account creation and deletion, account enabled and
disabled\n",
            "baseQuery": "let GetAccountActions = (Account_Name:string,
Account_NTDomain:string, Account_UPNSuffix:string, Account_AadUserId:string,
Account_Sid:string){\nlet Account_UPN = strcat(Account_Name, '@',
Account_UPNSuffix);\nlet Account_Win = strcat(Account_NTDomain,'\\\\',
Account_Name);\nunion isfuzzy=true\n(AuditLogs\n  |
where  tostring(bag_keys(InitiatedBy)[0]) == \"user\"\n  | where OperationName
in~ ('Add user', 'Update user', 'Delete user', 'Change user password', 'Reset
user password',  'Reset password (by admin)', 'Change password (self-service)',
'Reset password (self-service)')\n  | where Account_UPN =~
tostring(parse_json(tostring(InitiatedBy.user)).userPrincipalName) or
Account_AadUserId =~ tostring(parse_json(tostring(InitiatedBy.user)).id)\n  |
extend InitiatedByAccount =
tostring(parse_json(tostring(InitiatedBy.user)).userPrincipalName)\n  | parse
InitiatedByAccount with userName:string '@' userUpnSuffix:string\n  | extend
InitiatedByAADUserId = tostring(parse_json(tostring(InitiatedBy.user)).id)\n  |
extend TargetAccount = tostring(TargetResources[0].userPrincipalName)\n  | parse
TargetAccount with TargetAccountName:string '@'
TargetAccountUPNSuffix:string\n  | extend TargetAADUserId =
tostring(TargetResources[0].id)\n  | extend Action =
tostring(parse_json(tostring(parse_json(tostring(TargetResources[0].modifiedPrope
rties))[0])))\n  | extend ModifiedProperty =
tostring(parse_json(Action).displayName), ModifiedValue =
tostring(parse_json(Action).newValue)\n  | extend DisableUser =
iif(ModifiedProperty =~ 'AccountEnabled' and ModifiedValue =~ '[false]', 'True',
'False')\n),\n(SecurityEvent\n  | where AccountType =~ \"user\" or
isempty(AccountType)\n  | where EventID in (4720, 4722, 4723, 4724, 4725, 4726,
4740)\n  | where Account_Win =~ SubjectAccount or Account_Sid =~
SubjectUserSid\n  | parse TargetAccount with TargetAccountNTDomain '\\\\'
TargetAccountName\n  | extend InitiatedByAccount = SubjectAccount,
InitiatedByUserSid = SubjectUserSid, OperationName = tostring(EventID),
ModifiedProperty = Activity\n)\n};\nGetAccountActions('PDemo', '',
'seccxpninja.onmicrosoft.com', '', '')",
```

```
            "tableQuery": {
                "columnsDefinitions": [
                    {
                        "header": "Action",
                        "outputType": "String",
                        "supportDeepLink": false
                    },
                    {
                        "header": "Change",
                        "outputType": "String",
                        "supportDeepLink": false
                    },
                    {
                        "header": "Most Recent",
                        "outputType": "Date",
                        "supportDeepLink": false
                    },
                    {
                        "header": "Count",
                        "outputType": "Number",
                        "supportDeepLink": true
                    }
                ],
                "queriesDefinitions": [
                    {
                        "filter": "where OperationName in~ ('Change user
password', 'Reset user password', 'Change password (self-service)',  'Reset
password (by admin)', 'Reset password (self-service)', '4724', '4723')",
                        "summarize": "summarize MostRecent = max(TimeGenerated),
Count = count() by OperationName, ModifiedProperty",
                        "project": "project Title = OperationName,
ModifiedProperty, MostRecent, Count",
                        "linkColumnsDefinitions": [
                            {
                                "projectedName": "Count",
                                "Query": "{{BaseQuery}} | "
                            }
                        ]
                    },
                    {
                        "filter": "where OperationName in~ ('Blocked from self-
service password reset', '4740')",
                        "summarize": "summarize MostRecent = max(TimeGenerated),
Count = count() by OperationName, ModifiedProperty",
```

```
                        "project": "project Title = OperationName,
ModifiedProperty, MostRecent, Count",
                        "linkColumnsDefinitions": [
                            {
                                "projectedName": "Count",
                                "Query": "{{BaseQuery}} | "
                            }
                        ]
                    },
                    {
                        "filter": "where OperationName =~ '4725'",
                        "summarize": "summarize MostRecent = max(TimeGenerated),
Count = count() by OperationName, ModifiedProperty",
                        "project": "project Title = OperationName,
ModifiedProperty, MostRecent, Count",
                        "linkColumnsDefinitions": [
                            {
                                "projectedName": "Count",
                                "Query": "{{BaseQuery}} | "
                            }
                        ]
                    },
                    {
                        "filter": "where OperationName in~ ('Add user', '4720')",
                        "summarize": "summarize MostRecent = max(TimeGenerated),
Count = count() by OperationName, ModifiedProperty",
                        "project": "project Title = OperationName,
ModifiedProperty, MostRecent, Count",
                        "linkColumnsDefinitions": [
                            {
                                "projectedName": "Count",
                                "Query": "{{BaseQuery}} | "
                            }
                        ]
                    },
                    {
                        "filter": "where OperationName in~ ('Delete user',
'4726')",
                        "summarize": "summarize MostRecent = max(TimeGenerated),
Count = count() by OperationName, ModifiedProperty",
                        "project": "project Title = OperationName,
ModifiedProperty, MostRecent, Count",
                        "linkColumnsDefinitions": [
                            {
                                "projectedName": "Count",
```

```
                            "Query": "{{BaseQuery}} | "
                        }
                    ]
                },
                {
                    "filter": "where OperationName in~ ('4725', 'Blocked from
self-service password reset', '4740') or (OperationName  =~ 'Update user' and
DisableUser =~ 'True')",
                    "summarize": "summarize MostRecent = max(TimeGenerated),
Count = count() by OperationName, ModifiedProperty",
                    "project": "project Title = OperationName,
ModifiedProperty, MostRecent, Count",
                    "linkColumnsDefinitions": [
                        {
                            "projectedName": "Count",
                            "Query": "{{BaseQuery}} | "
                        }
                    ]
                },
                {
                    "filter": "where OperationName in~ ('4722', '4767') or
(OperationName  =~ 'Update user' and DisableUser =~ 'False')",
                    "summarize": "summarize MostRecent = max(TimeGenerated),
Count = count() by OperationName, ModifiedProperty",
                    "project": "project Title = OperationName,
ModifiedProperty, MostRecent, Count",
                    "linkColumnsDefinitions": [
                        {
                            "projectedName": "Count",
                            "Query": "{{BaseQuery}} | "
                        }
                    ]
                },
                {
                    "filter": "where OperationName =~ '4738'",
                    "summarize": "summarize MostRecent = max(TimeGenerated),
Count = count() by OperationName, ModifiedProperty",
                    "project": "project Title = OperationName,
ModifiedProperty, MostRecent, Count",
                    "linkColumnsDefinitions": [
                        {
                            "projectedName": "Count",
                            "Query": "{{BaseQuery}} | "
                        }
                    ]
```

```
                    }
                ]
            },
            "chartQuery": {
                "title": "Actions by type",
                "dataSets": [
                    {
                        "query": "summarize Count = count() by bin(TimeGenerated,
1h), OperationName",
                        "xColumnName": "TimeGenerated",
                        "yColumnName": "Count",
                        "legendColumnName": "OperationName"
                    }
                ],
                "type": "BarChart"
            },
            "additionalQuery": {
                "text": "See all account activity",
                "query": "project TimeGenerated, InitiatedByAccount,
SubjectAccount, InitiatedByUserSid, SubjectUserSid, InitiatedByAADUserId,
TargetAccount, TargetSid, TargetAADUserId, OperationName, ModifiedProperty,
Activity, DisableUser, AADTenantId, AccountType, Computer, EventData"
            },
            "defaultTimeRange": {
                "beforeRange": "12h",
                "afterRange": "12h"
            },
            "referenceTimeRange": null,
            "dataTypes": [
                {
                    "dataType": "AuditLogs"
                },
                {
                    "dataType": "SecurityEvent"
                }
            ],
            "inputEntityType": "Account",
            "requiredInputFieldsSets": [
                [
                    "Account_Name",
                    "Account_NTDomain"
                ],
                [
                    "Account_Name",
                    "Account_UPNSuffix"
```

```
                ],
                [
                    "Account_AadUserId"
                ],
                [
                    "Account_Sid"
                ]
            ],
            "entitiesFilter": {}
        }
    },
    "metaData": {
        "totalCount": 9,
        "errors": []
    }
}
```

Get Insights

Get Relations

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entities/**{entityId}/**relations?**{apiVersion}**

This will show the other alerts that this entity belongs to.

Sample Request

```
$url = $baseUrl + "Incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/relations" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader ).value
```

Sample Response

```
[
    {
      "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/relations/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4_3fa8c363-f32b-6a79-f192-39919d8827cb",
      "name": "7752c995-4e1c-d0a1-3d07-f3c90ca48bf4_3fa8c363-f32b-6a79-f192-39919d8827cb",
      "type": "Microsoft.SecurityInsights/Incidents/relations",
```

```
      "properties": {
        "relatedResourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/entities/3fa8c3
63-f32b-6a79-f192-39919d8827cb",
        "relatedResourceName": "3fa8c363-f32b-6a79-f192-39919d8827cb",
        "relatedResourceType": "Microsoft.SecurityInsights/entities",
        "relatedResourceKind": "SecurityAlert"
      }
    },
    {
      "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/7752c
995-4e1c-d0a1-3d07-f3c90ca48bf4/relations/7752c995-4e1c-d0a1-3d07-
f3c90ca48bf4_1f9ee3e3-0f18-5549-d53d-25ca49d3986e",
      "name": "7752c995-4e1c-d0a1-3d07-f3c90ca48bf4_1f9ee3e3-0f18-5549-d53d-
25ca49d3986e",
      "type": "Microsoft.SecurityInsights/Incidents/relations",
      "properties": {
        "relatedResourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/entities/1f9ee3
e3-0f18-5549-d53d-25ca49d3986e",
        "relatedResourceName": "1f9ee3e3-0f18-5549-d53d-25ca49d3986e",
        "relatedResourceType": "Microsoft.SecurityInsights/entities",
        "relatedResourceKind": "SecurityAlert"
      }
    },
    {
      "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/7752c
995-4e1c-d0a1-3d07-f3c90ca48bf4/relations/7752c995-4e1c-d0a1-3d07-
f3c90ca48bf4_41e93e74-3116-bef1-60a7-57037a44cb7f",
      "name": "7752c995-4e1c-d0a1-3d07-f3c90ca48bf4_41e93e74-3116-bef1-60a7-
57037a44cb7f",
      "type": "Microsoft.SecurityInsights/Incidents/relations",
      "properties": {
        "relatedResourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/entities/41e93e
74-3116-bef1-60a7-57037a44cb7f",
        "relatedResourceName": "41e93e74-3116-bef1-60a7-57037a44cb7f",
        "relatedResourceType": "Microsoft.SecurityInsights/entities",
```

```
        "relatedResourceKind": "SecurityAlert"
      }
    }
  ]
```

Get a Relation

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entities/**{entityId}/**relations/**{relationName}**?**{apiVersion}**

Retrieve a single relation.

Note that the "relationName" is not a GUID or text name

Sample Request

```
$url = $baseUrl + "Incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/relations/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4_3fa8c363-f32b-6a79-f192-39919d8827cb" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response

```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/relations/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4_3fa8c363-f32b-6a79-f192-39919d8827cb",
    "name": "7752c995-4e1c-d0a1-3d07-f3c90ca48bf4_3fa8c363-f32b-6a79-f192-39919d8827cb",
    "type": "Microsoft.SecurityInsights/Incidents/relations",
    "properties": {
      "relatedResourceId": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/entities/3fa8c363-f32b-6a79-f192-39919d8827cb",
      "relatedResourceName": "3fa8c363-f32b-6a79-f192-39919d8827cb",
      "relatedResourceType": "Microsoft.SecurityInsights/entities",
      "relatedResourceKind": "SecurityAlert"
    }
  }
```

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entities?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

Returns a JSON array of all the entities. See the Get command above.

Entity Queries

When you are investigating an incident and you go into the graphical incident investigation graph, you will see all the entities for the incident you are investigating. If you mouse-over one of them, there is a list of different queries that are being run in the background. Those are the Entity Queries.

These are broken down into different categories as only certain queries make sense to run against certain types of entities. Right now, the categories are:

- Account
- AzureResource
- CloudApplication
- DNS
- File
- FileHash
- Host
- HuntingBookmark
- IotDevice
- IP
- Mailbox
- MailCluster
- MailMessage
- Malware
- Nic
- Process
- RegistryKey
- SecurityAlert
- SecurityGroup
- SubmissionMail
- URL

Sadly, while there is a Create/Update for these entity queries, it is not for these types of queries. Instead, they are for the Entity Query Templates discussed below. Confused? Me too! The ability to add new Entity Queries has been requested. Maybe in the future.

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entityQueries/**{entityQueryId}**?**{apiVersion}**

As mentioned above, this will **NOT** create a new Entity Query, rather it creates a new Entity Query Template discussed below.

Note that in the Sample Request and Sample Response below, the query was removed to save space.

Sample Request

```
$body = @{
  "properties" = @{
    "description"              = "Account added to the Domain Admins group"
    "templateName"             = "aaad22c3-be50-465f-b258-8570d629c3db"
    "entitiesFilter"           = @{
      "Host_OsFamily" = @(
        "Windows"
      )
    }
    "inputEntityType"          = "Host"
    "requiredInputFieldsSets" = @(
      @(
        "Host_HostName"
        "Host_NTDomain"
      )
      @(
        "Host_HostName"
        "Host_DnsDomain"
      )
      @(
        "Host_AzureID"
      )
      @(
        "Host_OMSAgentID"
      )
    )
    "queryDefinitions"         = @{
      "query" = "<query>"
    }
    "enabled"                  = $true
    "title"                    = "An account was added to the Domain Admins group"
    "content"                  = "On '{{Computer}}' the user '{{MemberAdded}}' was
added by '{{AddedBy}}' to group='{{GroupName}}'"
    "createdTimeUtc"           = $null
    "lastModifiedTimeUtc"      = $null
  }
}
$guid = New-Guid
```

```
$url = $baseUrl + "entityQueries/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/entityQueries/8
a85f63a-c734-4601-9e94-89b04d4720ee",
  "name": "8a85f63a-c734-4601-9e94-89b04d4720ee",
  "etag": "\"e0046a16-0000-0100-0000-6547f32a0000\"",
  "type": "Microsoft.SecurityInsights/entityQueries",
  "kind": "Activity",
  "properties": {
      "title": "An account was added to the Domain Admins group",
      "content": "On '{{Computer}}' the user '{{MemberAdded}}' was added by
'{{AddedBy}}' to group: '{{GroupName}}'",
      "description": "Account added to the Domain Admins group",
      "queryDefinitions": {
          "query": "<query>"
      },
      "requiredInputFieldsSets": [
          [
              "Host_HostName",
              "Host_NTDomain"
          ],
          [
              "Host_HostName",
              "Host_DnsDomain"
          ],
          [
              "Host_AzureID"
          ],
          [
              "Host_OMSAgentID"
          ]
      ],
      "entitiesFilter": {
          "Host_OsFamily": [
              "Windows"
          ]
      },
      "templateName": "aaad22c3-be50-465f-b258-8570d629c3db",
      "enabled": true,
```

```
      "createdTimeUtc": "2023-11-05T19:55:22.4214588Z",
      "lastModifiedTimeUtc": "2023-11-05T19:55:22.4214588Z",
      "inputEntityType": "Host"
  }
}
```

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entityQueries/**{entityQueryId}**?**{apiVersion}**

This will return a template from any installed content.

Sample Request

```
$url= $baseUrl + "entityQueries/98b974fd-cc64-48b8-9bd0-3a209f5b944b" +
$apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/entityQueries/9
8b974fd-cc64-48b8-9bd0-3a209f5b944b",
  "name": "98b974fd-cc64-48b8-9bd0-3a209f5b944b",
  "type": "Microsoft.SecurityInsights/entityQueries",
  "kind": "Expansion",
  "properties": {
    "displayName": "Related entities",
    "queryTemplate": "let GetAlertRelatedEntities =
(v_SecurityAlert_SystemAlertId:string){\r\nSecurityAlert\r\n | where
SystemAlertId == v_SecurityAlert_SystemAlertId\r\n | project entities =
todynamic(Entities)\r\n | mv-expand entities\r\n | project-rename
entity=entities};\r\n GetAlertRelatedEntities('<systemAlertId>')",
    "inputFields": [
      "systemAlertId"
    ],
    "outputEntityTypes": [],
    "dataSources": [
      "SecurityAlert"
    ],
    "inputEntityType": "SecurityAlert"
```

```
    }
}
```

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entityQueries?**{apiVersion}**

This will return a JSON array containing all the entity queries. See the GET above.

Entity Query Templates

You would think that "Entity Query Templates" would be the templates for "Entity Queries". I know I did. I also know that I was wrong. Instead, these are the queries that get run to show the information in the center of the Entity Behavior screen.

If you were not aware, you can add your own queries by going to the main Entity behavior screen and selecting "Customize entity page" in the header bar at the top of the page.

While you can create custom entries in the Microsoft Sentinel Portal, you cannot do this using these REST APIs. Instead you have to make a call to the Entity Query REST APIs as discussed above.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entityQueryTemplates/**{entityQueryTemplateId}**?**{apiVersion}**

This will return an Entity Query Template.

Sample Request

```
$url = $baseUrl + "entityQueryTemplates/d6d08c94-455f-4ea5-8f76-fc6c0c442cfa" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Note that in the Sample Response below, I have deleted the query to save space.

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/entityQueryTemplates/d6d08c94-455f-4ea5-8f76-fc6c0c442cfa",
  "name": "d6d08c94-455f-4ea5-8f76-fc6c0c442cfa",
  "type": "Microsoft.SecurityInsights/entityQueryTemplates",
  "kind": "Activity",
  "properties": {
    "title": "The user has created an account",
    "content": "The user {{InitiatedByAccount}} has created the account {{TargetAccount}} {{Count}} time(s)",
    "description": "This activity displays account creation events performed by the user",
```

```
    "queryDefinitions": {
      "query": "<query>"
    },
    "dataTypes": [
      {
        "dataType": "AuditLogs"
      },
      {
        "dataType": "SecurityEvent"
      }
    ],
    "inputEntityType": "Account",
    "requiredInputFieldsSets": [
      [
        "Account_Name",
        "Account_NTDomain"
      ],
      [
        "Account_Name",
        "Account_UPNSuffix"
      ],
      [
        "Account_AadUserId"
      ],
      [
        "Account_Sid"
      ]
    ],
    "entitiesFilter": {}
  }
}
```

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/entityQueryTemplates?**{apiVersion}**

This will return a JSON array containing all the entity query templates. See the GET above.

File Imports

This will allow you to import a file full of Threat Intelligence indicators. You can download a file template from the Microsoft Sentinel portal when you start the file import process.

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/fileImports/**{fileImportId}**?**{apiVersion}**

This will allow you to import a file that contains Threat Intelligence Indicators.

Sample Request

```
$body = @{
  "properties" = @{
    "source"         = "Book Demo"
    "importFile"     = @{
      "fileName"    = "ThreatIntelFile.csv"
      "fileSize"    = 307
      "fileFormat" = "CSV"
    }
    "contentType"    = "BasicIndicator"
    "ingestionMode" = "IngestOnlyIfAllAreValid"
  }
}
$guid = New-Guid
$url = $baseUrl + "fileImports/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/FileImports/b9e
b6b7a-542c-4554-96a3-fa5c7fff7ef3",
  "name": "b9eb6b7a-542c-4554-96a3-fa5c7fff7ef3",
  "type": "Microsoft.SecurityInsights/FileImports",
  "properties": {
      "importFile": {
          "fileName": "ThreatIntelFile.csv",
          "fileSize": 307,
          "fileFormat": "CSV",
```

```
          "fileContentUri":
"https://sentinelimportsprodeus2.blob.core.windows.net/230c86ca-abf2-48f4-b95e-
8b977e67f4c6/b9eb6b7a-542c-4554-96a3-fa5c7fff7ef3/d2197fe1-9a31-4303-ac2d-
7851180424ec?skoid=f016f5fa-b85b-4174-bbd3-f75ae8761eb1&sktid=33e01921-4d64-4f8c-
a055-5bdaffd5e33d&skt=2023-11-05T20%3A33%3A47Z&ske=2023-11-
05T21%3A33%3A47Z&sks=b&skv=2023-01-03&sv=2023-01-03&st=2023-11-
05T20%3A33%3A47Z&se=2023-11-
05T21%3A33%3A47Z&sr=b&sp=cw&sig=E4aJQI8J5vBLrP%2FIpvuoFPGGYsxo8hUiPUPlNuUILqw%3D"
,
          "deleteStatus": "NotDeleted"
      },
      "contentType": "BasicIndicator",
      "ingestionMode": "IngestOnlyIfAllAreValid",
      "source": "Book Demo",
      "state": "WaitingForUpload",
      "totalRecordCount": null,
      "validRecordCount": null,
      "ingestedRecordCount": null,
      "createdTimeUTC": "2023-11-05T20:33:47.6163441Z",
      "filesValidUntilTimeUTC": "2023-11-06T20:33:47.6163442Z",
      "importValidUntilTimeUTC": "2023-12-05T20:33:47.6163442Z"
  }
}
```


Notice that the “state” is set to “WaitingForUpload”. The actual uploading of the file is done in the background.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/fileImports/**{entityQueryTemplateId}**?**{apiVersion}**

This will return a single File Import process.

Sample Request

```
$url = $baseUrl + "fileImports/b9eb6b7a-542c-4554-96a3-fa5c7fff7ef3" +
$apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
```

```
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/FileImport/b9eb
6b7a-542c-4554-96a3-fa5c7fff7ef3",
  "name": "b9eb6b7a-542c-4554-96a3-fa5c7fff7ef3",
  "type": "Microsoft.SecurityInsights/FileImport",
  "properties": {
    "importFile": {
      "fileName": "ThreatIntelFile.csv",
      "fileSize": 307,
      "fileFormat": "CSV",
      "fileContentUri": null,
      "deleteStatus": "NotDeleted"
    },
    "contentType": "BasicIndicator",
    "ingestionMode": "IngestOnlyIfAllAreValid",
    "source": "Book Demo",
    "state": "Ingested",
    "totalRecordCount": 1,
    "validRecordCount": 1,
    "ingestedRecordCount": 1,
    "createdTimeUTC": "2023-11-05T20:33:47.6163441Z",
    "filesValidUntilTimeUTC": "2023-11-06T20:33:47.6163442Z",
    "importValidUntilTimeUTC": "2023-12-05T20:33:47.6163442Z"
  }
}
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/fileImports?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the file import definitions. See the GET above.

Hunts

Hunts are a new feature of Microsoft Sentinel that allows you to group different Microsoft Sentinel Hunting queries together to validate a hypothesis.

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**?**{apiVersion}**

This will allow you to create a new hunt. You cannot add any of the hunting queries when you do this creation.

Sample Request

```
$body = @{
    "properties" = @{
        "displayName"      = "Book Demo"
        "description"      = "<p elementtiming=`"219`">This is a <u
elementtiming=`"222`">demo</u> for the <strong
elementtiming=`"223`">book</strong></p>"
        "owner"            = @{
            "objectId" = "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e"
        }
        "status"           = "Active"
        "hypothesisStatus" = "Unknown"
    }
}
$guid = New-Guid
$url = $baseUrl + "hunts/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
                "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/hunts/2f82ef7e-
fa90-4079-9fed-bd839e49a5cf",
                "name": "2f82ef7e-fa90-4079-9fed-bd839e49a5cf",
                "etag": "\"36008207-0000-0100-0000-654952c20000\"",
                "type": "Microsoft.SecurityInsights/hunts",
                "systemData": {
                    "createdAt": "2023-11-06T20:55:30.2421876Z",
```

```
                    "createdBy": "garybushey@outlook.com",
                    "createdByType": "User",
                    "lastModifiedAt": "2023-11-06T20:55:30.2421876Z",
                    "lastModifiedBy": "garybushey@outlook.com",
                    "lastModifiedByType": "User"
                },
                "properties": {
                    "displayName": "Book Demo",
                    "description": "<p elementtiming=\"219\">This is a <u
elementtiming=\"222\">demo</u> for the <strong
elementtiming=\"223\">book</strong></p>",
                    "owner": {
                        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
                        "email": "garybushey@outlook.com",
                        "assignedTo": "Gary Bushey",
                        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com",
                        "ownerType": "User"
                    },
                    "status": "Active",
                    "hypothesisStatus": "Unknown"
                }
            }
```


Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**?**{apiVersion}**

This will delete a hunt. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**?**{apiVersion}**

This will get a single hunt.

Sample Request

```
$url = $baseUrl + "hunts/2f82ef7e-fa90-4079-9fed-bd839e49a5cf" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/hunts/2f82ef7e-
fa90-4079-9fed-bd839e49a5cf",
    "name": "2f82ef7e-fa90-4079-9fed-bd839e49a5cf",
    "etag": "\"36008207-0000-0100-0000-654952c20000\"",
    "type": "Microsoft.SecurityInsights/hunts",
    "systemData": {
      "createdAt": "2023-11-06T20:55:30.2421876Z",
      "createdBy": "garybushey@outlook.com",
      "createdByType": "User",
      "lastModifiedAt": "2023-11-06T20:55:30.2421876Z",
      "lastModifiedBy": "garybushey@outlook.com",
      "lastModifiedByType": "User"
    },
    "properties": {
      "displayName": "Book Demo",
      "description": "<p elementtiming=\"219\">This is a <u
elementtiming=\"222\">demo</u> for the <strong
elementtiming=\"223\">book</strong></p>",
      "owner": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "assignedTo": "Gary Bushey",
        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com",
        "ownerType": "User"
      },
      "status": "Active",
      "hypothesisStatus": "Unknown"
    }
  }
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the hunts' definitions. See the GET above.

Create/Update Hunt Comment

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**/comment/**{commentId}**?**{apiVersion}**

This will allow you to add a comment to an existing hunt.

Sample Request

```
$body = @{
    "properties" = @{
        "message" = "<p elementtiming=`"323`">Adding a comment for the <strong
elementtiming=`"358`">book</strong></p>"
    }
}
$guid = New-Guid
$url = $baseUrl + "hunts/2f82ef7e-fa90-4079-9fed-bd839e49a5cf/comments" + $guid +
$apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/hunts/2f82ef7e-
fa90-4079-9fed-bd839e49a5cf/comments/44cf6d91-0635-4b5b-9e4c-b6cfc303b1a0",
    "name": "44cf6d91-0635-4b5b-9e4c-b6cfc303b1a0",
    "etag": "\"3600001a-0000-0100-0000-654959790000\"",
    "type": "Microsoft.SecurityInsights/hunts/comments",
    "systemData": {
        "createdAt": "2023-11-06T21:24:09.3874935Z",
        "createdBy": "garybushey@outlook.com",
        "createdByType": "User",
        "lastModifiedAt": "2023-11-06T21:24:09.3874935Z",
        "lastModifiedBy": "garybushey@outlook.com",
        "lastModifiedByType": "User"
    },
    "properties": {
        "message": "<p elementtiming=\"323\">Adding a comment for the <strong
elementtiming=\"358\">book</strong></p>"
```

```
    }
}
```

Delete Hunt Comment

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**/comment/**{commentId}**?**{apiVersion}**

This will delete a hunt comment. This is a simple call so I will not go into much detail.

Get Hunt Comment

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**/comment/**{commentId}**?**{apiVersion}**

Sample Request

```
$url = $baseUrl + "hunts/2f82ef7e-fa90-4079-9fed-bd839e49a5cf/comments/44cf6d91-0635-4b5b-9e4c-b6cfc303b1a0" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/hunts/2f82ef7e-fa90-4079-9fed-bd839e49a5cf/comments/44cf6d91-0635-4b5b-9e4c-b6cfc303b1a0",
    "name": "44cf6d91-0635-4b5b-9e4c-b6cfc303b1a0",
    "etag": "\"3600001a-0000-0100-0000-654959790000\"",
    "type": "Microsoft.SecurityInsights/hunts/comments",
    "systemData": {
      "createdAt": "2023-11-06T21:24:09.3874935Z",
      "createdBy": "garybushey@outlook.com",
      "createdByType": "User",
      "lastModifiedAt": "2023-11-06T21:24:09.3874935Z",
      "lastModifiedBy": "garybushey@outlook.com",
      "lastModifiedByType": "User"
    },
    "properties": {
      "message": "<p elementtiming=\"323\">Adding a comment for the <strong elementtiming=\"358\">book</strong></p>"
```

```
    }
  }
```

List Hunt Comments

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**/comments?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the hunts' comments. See the GET above.

Create/Update Hunt Relations

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**/relations/**{relationId}**?**{apiVersion}**

Hunt relations are the link between the hunt and the queries that belong to it. You will need to get the hunting query's resource ID (see below).

Sample Request

```
$body = @{
    "properties" = @{
        "relatedResourceId" = "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/savedSearches/0b407f0d-8703-4fa1-a1a8-dc5e9708992b"
    }
}
$guid = New-Guid
$url = $baseUrl + "hunts/2f82ef7e-fa90-4079-9fed-bd839e49a5cf/" + $guid +
$apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/hunts/2f82ef7e-
fa90-4079-9fed-bd839e49a5cf/relations/02de6bfb-223c-4b41-8934-96d41f8f968e",
    "name": "02de6bfb-223c-4b41-8934-96d41f8f968e",
```

```
    "etag": "\"3600d712-0000-0100-0000-654956c40000\"",
    "type": "Microsoft.SecurityInsights/hunts/relations",
    "systemData": {
        "createdAt": "2023-11-06T21:12:35.5267926Z",
        "createdBy": "garybushey@outlook.com",
        "createdByType": "User",
        "lastModifiedAt": "2023-11-06T21:12:35.5267926Z",
        "lastModifiedBy": "garybushey@outlook.com",
        "lastModifiedByType": "User"
    },
    "properties": {
        "relatedResourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/SavedSearches/0b407f0d-8703-4fa1-a1a8-dc5e9708992b",
        "relatedResourceName": "0b407f0d-8703-4fa1-a1a8-dc5e9708992b",
        "relatedResourceType": "Microsoft.OperationalInsights/SavedSearches"
    }
}
```


Delete Hunt Relation

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**/relations/**{relationId}**?**{apiVersion}**

This will delete a hunt relation. This is a simple call so I will not go into much detail.

Get A Hunt Relation

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**/relations/**{relationId}**?**{apiVersion}**

Sample Request

```
$url = $baseUrl + "hunts/2f82ef7e-fa90-4079-9fed-bd839e49a5cf/relations/02de6bfb-
223c-4b41-8934-96d41f8f968e" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
```

```
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/hunts/2f82ef7e-
fa90-4079-9fed-bd839e49a5cf/relations/02de6bfb-223c-4b41-8934-96d41f8f968e",
    "name": "02de6bfb-223c-4b41-8934-96d41f8f968e",
    "etag": "\"3600d712-0000-0100-0000-654956c40000\"",
    "type": "Microsoft.SecurityInsights/hunts/relations",
    "systemData": {
      "createdAt": "2023-11-06T21:12:35.5267926Z",
      "createdBy": "garybushey@outlook.com",
      "createdByType": "User",
      "lastModifiedAt": "2023-11-06T21:12:35.5267926Z",
      "lastModifiedBy": "garybushey@outlook.com",
      "lastModifiedByType": "User"
    },
    "properties": {
      "relatedResourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/SavedSearches/0b407f0d-8703-4fa1-a1a8-dc5e9708992b",
      "relatedResourceName": "0b407f0d-8703-4fa1-a1a8-dc5e9708992b",
      "relatedResourceType": "Microsoft.OperationalInsights/SavedSearches"
    }
  }
```


List Hunt Relations

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/hunts/**{huntId}**/relations?**{apiVersion}**

Filters Available: $filter, $orderby, $skipToken, $top

This will return a JSON array containing all the hunts' relations. See the GET above.

Incidents

We all know what Incidents are, right? If not, you may want to read some other documentation before reading this. For those that do know what an incident is, there are some new features in the preview REST API that are quite useful, including adding a Microsoft Teams' team to collaborate on incident investigation.

Create/Update

There are no changes from the stable Create/Update REST API

Delete

There are no changes from the stable Delete REST API

Get

There are no changes from the stable Get REST API
There may be more information returned, but the call is still the same.

List

There are no changes from the stable List REST API
There may be more information returned, but the call is still the same.

CreateTeam

Http Method: POST
REST API URL:
https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/createTeam?**{apiVersion}**

This will allow you to create a Microsoft Teams site where you can collaborate with your team members on an incident. For full disclosure, I have not tested this call as I do not have the ability to create a Teams site in my environment.

Sample Request

```
$body = @{
        "teamName"= "Incident 1634: Alert from ApplicationManagement"
        "teamDescription"= "This is a sample Teams site"
        "groupIds"= @()
        "memberIds"= @(
            "2fc92ec6-0d4c-4d31-a5ea-08364b7fca2e"
        )
}
$url = $baseUrl + "Incidents/3b5f312e-4da0-71d3-db46-185e2a5d987d/createTeam" + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method POST -Headers $authHeader -Body ($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

I cannot show this as I didn't get it to work. Based on the example JSON file, the return value will look something like

```
{
  "teamId": "99978838-9bda-4ad4-8f93-4cf7ebc50ca5",
  "primaryChannelUrl":
"https://teams.microsoft.com/l/team/19:80bf3b25485b4067b7d2dc4eec9e1578%40thread.
tacv2/conversations?groupId=99978838-9bda-4ad4-8f93-
4cf7ebc50ca5&tenantId=5b5a146c-eba8-46af-96f8-e31b50d15a3f",
  "teamCreationTimeUtc": "2021-03-15T17:08:21.995Z",
  "name": "Team name",
  "description": "Team description"
}
```

IncidentAlerts

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/alerts?**{apiVersion}**

Get a list of all the alerts for the specified incident.

Sample Request

```
$url = $baseUrl + "Incidents/3b5f312e-4da0-71d3-db46-185e2a5d987d/alerts" +
$apiVersion
$results = (Invoke-RestMethod -Method "Post" -Uri $url -Headers $authHeader )
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Entities/1028a1
d0-58a6-4a68-2c46-1f84fa73e087",
  "name": "1028a1d0-58a6-4a68-2c46-1f84fa73e087",
  "type": "Microsoft.SecurityInsights/Entities",
  "kind": "SecurityAlert",
  "properties": {
    "systemAlertId": "1028a1d0-58a6-4a68-2c46-1f84fa73e087",
    "tactics": [
      "Collection",
      "Reconnaissance"
    ],
    "alertDisplayName": "Alert from ApplicationManagement   ",
```

```
    "description": "Add service principal credentials occurred ",
    "confidenceLevel": "Unknown",
    "severity": "Medium",
    "vendorName": "Microsoft",
    "productName": "DemoSystem",
    "productComponentName": "Scheduled Alerts",
    "alertType": "230c86ca-abf2-48f4-b95e-8b977e67f4c6_d3c1e682-14f3-40a2-80b6-
34072cd9c272",
    "processingEndTime": "2023-11-09T17:17:46.0390825Z",
    "status": "New",
    "endTimeUtc": "2023-11-09T15:40:34.813635Z",
    "startTimeUtc": "2023-11-09T14:31:11.2493178Z",
    "timeGenerated": "2023-11-09T17:17:46.0836961Z",
    "providerAlertId": "6bf60b3a-0d47-464b-ac9e-804d9f306ac3",
    "resourceIdentifiers": [
      {
        "type": "LogAnalytics",
        "workspaceId": "230c86ca-abf2-48f4-b95e-8b977e67f4c6",
        "subscriptionId": "9790d913-b5da-460d-b167-ac985d5f3b83",
        "resourceGroup": "azuresentinel"
      }
    ],
    "additionalData": {
      "AlertMessageEnqueueTime": "2023-11-09T17:17:46.076Z",
      "Search Query Results Overall Count": "12",
      "OriginalProductName": "Azure Sentinel",
      "OriginalProductComponentName": "Scheduled Alerts"
    },
    "friendlyName": "Alert from ApplicationManagement   "
  }
}
```


Incident Bookmarks

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/bookmarks?**{apiVersion}**

Get a list of all the bookmarks for the specified incident.

Sample Request

```
$url= $baseUrl + "Incidents/3b5f312e-4da0-71d3-db46-185e2a5d987d/bookmarks" +
$apiVersion
```

```
$results = (Invoke-RestMethod -Method "Post" -Uri $url -Headers $authHeader )
```

Note that in the Sample Response below, I have removed most of the “queryResult” column’s value to save space.

Sample Response


```
[
  {
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Entities/",
    "type": "Microsoft.SecurityInsights/Entities",
    "kind": "Bookmark",
    "properties": {
      "displayName": "AzureActivity - 03c0fdfba1d6 (1)",
      "created": "2023-11-09T17:17:34.9514219-05:00",
      "updated": "2023-11-09T17:17:34.9514219-05:00",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey"
      },
      "updatedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey"
      },
      "eventTime": "2023-11-09T17:07:07-05:00",
      "notes": "Added for book",
      "labels": [],
      "query": "AzureActivity\n",
      "queryResult":
"{\"OperationName\":\"\",\"OperationNameValue\":\"MICROSOFT.SECURITYINSIGHTS/INCI
DENTS/CREATETEAM/ACTION\"}",
      "additionalData": {
        "EntityMappings": "[]",
        "Tactics": "[]",
        "Techniques": "[]",
        "ETag": "\"09022c31-0000-0100-0000-654d5a7f0000\"",
        "EntityId": "e007dcdf-a352-4505-8f69-ddf24edbdcb8"
      },
      "friendlyName": "AzureActivity - 03c0fdfba1d6 (1)"
    }
  },
  {
```

```
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Entities/",
    "type": "Microsoft.SecurityInsights/Entities",
    "kind": "Bookmark",
    "properties": {
      "displayName": "AzureActivity - 03c0fdfba1d6",
      "created": "2023-11-09T17:17:35.132583-05:00",
      "updated": "2023-11-09T17:17:35.132583-05:00",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey"
      },
      "updatedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey"
      },
      "eventTime": "2023-11-09T17:07:07-05:00",
      "notes": "Added for book",
      "labels": [],
      "query": "AzureActivity\n",
      "queryResult":
"{\"OperationName\":\"\",\"OperationNameValue\":\"MICROSOFT.SECURITYINSIGHTS/INCI
DENTS/CREATETEAM/ACTION\"}",
      "additionalData": {
        "EntityMappings": "[]",
        "Tactics": "[]",
        "Techniques": "[]",
        "ETag": "\"09021c31-0000-0100-0000-654d5a7f0000\"",
        "EntityId": "88ad5015-200e-4fe1-ac8f-3f09f432768c"
      },
      "friendlyName": "AzureActivity - 03c0fdfba1d6"
    }
  }
]
```


Entities

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/entities?**{apiVersion}**

Get a list of all the entities for the specified incident.

Sample Request

```
$url= $baseUrl + "Incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/entities" +
$apiVersion
$results = (Invoke-RestMethod -Method "Post" -Uri $url -Headers $authHeader
).entities
```

Sample Response


```
[
  {
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Entities/41c57c
d2-a539-cc4e-89d0-38824a117a50",
    "name": "41c57cd2-a539-cc4e-89d0-38824a117a50",
    "type": "Microsoft.SecurityInsights/Entities",
    "kind": "Account",
    "properties": {
      "accountName": "Gary Bushey",
      "friendlyName": "Gary Bushey"
    }
  },
  {
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Entities/7e11e7
6f-53a9-a5e4-bb49-6480c6f9812a",
    "name": "7e11e76f-53a9-a5e4-bb49-6480c6f9812a",
    "type": "Microsoft.SecurityInsights/Entities",
    "kind": "Ip",
    "properties": {
      "address": "192.168.1.1",
      "friendlyName": "192.168.1.1"
    }
  }
]
```

Incident Comments

There are no changes from the stable Incident Comments REST API

Incident Relations

There are no changes from the stable Incident Relations REST API

Incident Tasks

Create/Edit

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentsId}**/tasks/**{incidentTaskId }**?**{apiVersion}**

Create a new task for the specified incident

Sample Request

```
$body = @{
    "properties" = @{
        "title" = "Book Demo"
        "description" = "<div><strong>This</strong> is a <em>demo</em>
<u>task</u> for the book</div>"
        "status" = "New"
    }
}
$guid = New-Guid
$url = $baseUrl + "incidents/3b5f312e-4da0-71d3-db46-185e2a5d987d/tasks/" + $guid
+ $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/3b5f3
12e-4da0-71d3-db46-185e2a5d987d/Tasks/f8f22c5a-9997-4a1a-9d1c-04ce5293da90",
  "name": "f8f22c5a-9997-4a1a-9d1c-04ce5293da90",
  "etag": "\"f10211df-0000-0100-0000-654d5ddd0000\"",
  "type": "Microsoft.SecurityInsights/Incidents/Tasks",
  "properties": {
    "title": "Book Demo",
    "description": "<div><strong>This</strong> is a <em>demo</em> <u>task</u> for
the book</div>",
    "status": "New",
    "createdTimeUtc": "2023-11-09T22:31:57Z",
    "lastModifiedTimeUtc": "2023-11-09T22:31:57Z",
    "createdBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
```

```
      "name": "Gary Bushey",
      "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
    },
    "lastModifiedBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey",
      "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
    }
  }
}
```

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/tasks/**{incidentTaskId}**?**{apiVersion}**

This REST API call will delete an existing incident's task where its Id matches the "taskId" being passed in. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/tasks/**{incidentTaskId }**?**{apiVersion}**

Get a specific task for an existing incident.

Sample Request

```
$url= $baseUrl + "incidents/3b5f312e-4da0-71d3-db46-185e2a5d987d/tasks/f8f22c5a-
9997-4a1a-9d1c-04ce5293da90" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/3b5f3
12e-4da0-71d3-db46-185e2a5d987d/Tasks/f8f22c5a-9997-4a1a-9d1c-04ce5293da90",
```

```
  "name": "f8f22c5a-9997-4a1a-9d1c-04ce5293da90",
  "etag": "\"f10211df-0000-0100-0000-654d5ddd0000\"",
  "type": "Microsoft.SecurityInsights/Incidents/Tasks",
  "properties": {
    "title": "Book Demo",
    "description": "<div><strong>This</strong> is a <em>demo</em> <u>task</u> for
the book</div>",
    "status": "New",
    "createdTimeUtc": "2023-11-09T22:31:57Z",
    "lastModifiedTimeUtc": "2023-11-09T22:31:57Z",
    "createdBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey",
      "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
    },
    "lastModifiedBy": {
      "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
      "email": "garybushey@outlook.com",
      "name": "Gary Bushey",
      "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
    }
  }
}
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/incidents/**{incidentId}**/tasks?**{apiVersion}**

Get a list of all the tasks for the specified incident.

Sample Request

```
$url= $baseUrl + "incidents/3b5f312e-4da0-71d3-db46-185e2a5d987d/tasks" +
$apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader
).value
```

Sample Response


```
[
```

```
  {
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/3b5f3
12e-4da0-71d3-db46-185e2a5d987d/Tasks/a5b3fdd3-519c-4299-8a8e-06c2c2e42167",
    "name": "a5b3fdd3-519c-4299-8a8e-06c2c2e42167",
    "etag": "\"f1024dbb-0000-0100-0000-654d5d740000\"",
    "type": "Microsoft.SecurityInsights/Incidents/Tasks",
    "properties": {
      "title": "Book Demo",
      "description": "<div><strong>This</strong> is a <em>demo</em> <u>task</u>
for the book</div>",
      "status": "New",
      "createdTimeUtc": "2023-11-09T22:30:12Z",
      "lastModifiedTimeUtc": "2023-11-09T22:30:12Z",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey",
        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
      },
      "lastModifiedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey",
        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
      }
    }
  },
  {
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Incidents/3b5f3
12e-4da0-71d3-db46-185e2a5d987d/Tasks/f8f22c5a-9997-4a1a-9d1c-04ce5293da90",
    "name": "f8f22c5a-9997-4a1a-9d1c-04ce5293da90",
    "etag": "\"f10211df-0000-0100-0000-654d5ddd0000\"",
    "type": "Microsoft.SecurityInsights/Incidents/Tasks",
    "properties": {
      "title": "Book Demo",
      "description": "<div><strong>This</strong> is a <em>demo</em> <u>task</u>
for the book</div>",
      "status": "New",
      "createdTimeUtc": "2023-11-09T22:31:57Z",
```

```
      "lastModifiedTimeUtc": "2023-11-09T22:31:57Z",
      "createdBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey",
        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
      },
      "lastModifiedBy": {
        "objectId": "4d737cb3-c7fe-40c6-bf21-05aad3a42c5e",
        "email": "garybushey@outlook.com",
        "name": "Gary Bushey",
        "userPrincipalName":
"garybushey_outlook.com#EXT#@garybusheyoutlook.onmicrosoft.com"
      }
    }
  }
]
```

Metadata

There are no changes from the stable Metadata REST API

Office Consents

I have no idea what this REST API is for. The example on the documentation website really doesn't provide any useful information. In all the instances I looked at, nothing was returned when I tried to list the entries. Because of this, I am not going to do any sample requests/responses. If I figure out what this is for and can find a Microsoft Sentinel instance that returns any data, I will modify this page.

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/officeConsents?**{apiVersion}**

Delete an office consent.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/officeConsents/**{officeConsentId}**?**{apiVersion}**

Get a specific office consent.

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/officeConsents?**{apiVersion}**

Get a JSON array of all the office consents.

Onboarding States

There are no changes from the stable Sentinel Onboarding States REST API

Recommendations

These REST APIs will return recommendations on how to improve your environment.

As of the time this document was written, this feature has not been released so it may change or not be released at all.

Update

Http Method: PATCH

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/recommendations/**{recommendationId}**?**{apiVersion}**

This will update an existing recommendation. It looks like there are only 2 fields you can update; state and hide until some specified time.

Sample Request

```
$body = @{
    "recommendationPatch" = @{
        "state" = "active"
        "hideUntilTimeUtc" = "2023-11-19T03:09:03.4888396+00:00"
    }
}
$url = $baseUrl + "recommendations/bfb6b71d-3ea0-426a-83f6-27238a64507d"
+  $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Patch -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Recommendations
/bfb6b71d-3ea0-426a-83f6-27238a64507d",
  "name": "bfb6b71d-3ea0-426a-83f6-27238a64507d",
  "type": "Microsoft.SecurityInsights/Recommendations",
  "properties": {
    "id": "bfb6b71d-3ea0-426a-83f6-27238a64507d",
    "instructions": {
```

```
      "actionsToBePerformed": "Go to content hub and install recommended analytic rules for this table, or change plan to improve value for ingestion from this table.",
      "recommendationImportance": "By adding analytic rules that run on this table, you will improve your organization's coverage against attacks while utilizing ingested data in a better and efficient way. If no analytic rules are recommended, or recommendations are not suitable for the organization's needs, consider changing the ingestion plan for this table.",
      "howToPerformActionDetails": "Install analytic rules templates to improve SOC coverage or change data plan"
    },
    "additionalProperties": {
      "TableName": "ApiManagementGatewayLogs",
      "CreationTimeUtc": "2023-11-09 15:26:11Z",
      "TemplateIds": "[]",
      "TableUsage": "Low",
      "ChangeToLowerLogTier": "True",
      "LastModifiedTimeUtc": "2023-11-09 15:26:13Z"
    },
    "title": "Data optimization - Data value",
    "description": "Improve coverage by utilizing this data source or disconnect the following connectors or stop the ingestion of the data sources.",
    "recommendationTypeTitle": "Data optimization - Data value",
    "recommendationTypeDescription": "Utilizing the data or move it to basic logs.",
    "recommendationTypeId": "Precision_DataValue",
    "category": "CostOptimization",
    "context": "None",
    "workspaceId": "8ecf8077-cf51-4820-aadd-14040956f35ee",
    "actions": [
      {
        "linkText": "DataValueAction",
        "linkUrl": "https://aka.ms/DataValueAction",
        "state": "Active"
      }
    ],
    "state": "Active",
    "priority": "Medium",
    "hideUntilTimeUtc": "2023-11-19T03:09:03.4888396+00:00",
    "lastEvaluatedTimeUtc": "2023-11-09T10:26:11.7695067-05:00",
    "displayUntilTimeUtc": "2024-02-07T10:26:11.7695067-05:00",
    "visible": true
  }
}
```

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/recommendations/**{recommendationId}**?**{apiVersion}**

Get a specific recommendation.

Sample Request

```
$url= $baseUrl + "recommendations/bfb6b71d-3ea0-426a-83f6-27238a64507d" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Recommendations/bfb6b71d-3ea0-426a-83f6-27238a64507d",
  "name": "bfb6b71d-3ea0-426a-83f6-27238a64507d",
  "type": "Microsoft.SecurityInsights/Recommendations",
  "properties": {
    "id": "bfb6b71d-3ea0-426a-83f6-27238a64507d",
    "instructions": {
      "actionsToBePerformed": "Go to content hub and install recommended analytic rules for this table, or change plan to improve value for ingestion from this table.",
      "recommendationImportance": "By adding analytic rules that run on this table, you will improve your organization's coverage against attacks while utilizing ingested data in a better and efficient way. If no analytic rules are recommended, or recommendations are not suitable for the organization's needs, consider changing the ingestion plan for this table.",
      "howToPerformActionDetails": "Install analytic rules templates to improve SOC coverage or change data plan"
    },
    "additionalProperties": {
      "TableName": "ApiManagementGatewayLogs",
      "CreationTimeUtc": "2023-11-09 15:26:11Z",
      "TemplateIds": "[]",
      "TableUsage": "Low",
      "ChangeToLowerLogTier": "True",
      "LastModifiedTimeUtc": "2023-11-09 15:26:13Z"
    },
```

```
    "title": "Data optimization - Data value",
    "description": "Improve coverage by utilizing this data source or disconnect
the following connectors or stop the ingestion of the data sources.",
    "recommendationTypeTitle": "Data optimization - Data value",
    "recommendationTypeDescription": "Utilizing the data or move it to basic
logs.",
    "recommendationTypeId": "Precision_DataValue",
    "category": "CostOptimization",
    "context": "None",
    "workspaceId": "8ecf8077-cf51-4820-aadd-14040956f35ee",
    "actions": [
      {
        "linkText": "DataValueAction",
        "linkUrl": "https://aka.ms/DataValueAction",
        "state": "Active"
      }
    ],
    "state": "Active",
    "priority": "Medium",
    "lastEvaluatedTimeUtc": "2023-11-09T10:26:11.7695067-05:00",
    "displayUntilTimeUtc": "2024-02-07T10:26:11.7695067-05:00",
    "visible": true
  }
}
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/recommendations?**{apiVersion}**

Get a list of all the recommendations.

Sample Request

```
$url= $baseUrl + "recommendations" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader
).value
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
```

```
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/Recommendations
/bfb6b71d-3ea0-426a-83f6-27238a64507d",
  "name": "bfb6b71d-3ea0-426a-83f6-27238a64507d",
  "type": "Microsoft.SecurityInsights/Recommendations",
  "properties": {
    "id": "bfb6b71d-3ea0-426a-83f6-27238a64507d",
    "instructions": {
      "actionsToBePerformed": "Go to content hub and install recommended analytic
rules for this table, or change plan to improve value for ingestion from this
table.",
      "recommendationImportance": "By adding analytic rules that run on this
table, you will improve your organization's coverage against attacks while
utilizing ingested data in a better and efficient way. If no analytic rules are
recommended, or recommendations are not suitable for the organization's needs,
consider changing the ingestion plan for this table.",
      "howToPerformActionDetails": "Install analytic rules templates to improve
SOC coverage or change data plan"
    },
    "additionalProperties": {
      "TableName": "ApiManagementGatewayLogs",
      "CreationTimeUtc": "2023-11-09 15:26:11Z",
      "TemplateIds": "[]",
      "TableUsage": "Low",
      "ChangeToLowerLogTier": "True",
      "LastModifiedTimeUtc": "2023-11-09 15:26:13Z"
    },
    "title": "Data optimization - Data value",
    "description": "Improve coverage by utilizing this data source or disconnect
the following connectors or stop the ingestion of the data sources.",
    "recommendationTypeTitle": "Data optimization - Data value",
    "recommendationTypeDescription": "Utilizing the data or move it to basic
logs.",
    "recommendationTypeId": "Precision_DataValue",
    "category": "CostOptimization",
    "context": "None",
    "workspaceId": "8ecf8077-cf51-4820-aadd-14040956f35ee",
    "actions": [
      {
        "linkText": "DataValueAction",
        "linkUrl": "https://aka.ms/DataValueAction",
        "state": "Active"
      }
    ],
    "state": "Active",
    "priority": "Medium",
```

```
    "lastEvaluatedTimeUtc": "2023-11-09T10:26:11.7695067-05:00",
    "displayUntilTimeUtc": "2024-02-07T10:26:11.7695067-05:00",
    "visible": true
  }
}
```

Security MLAnalytic Settings

There are no changes from the stable Security ML Analytics Settings REST API

Settings

This will show most of Microsoft Sentinel settings. You can see these in the Azure portal but going to "Settings" in the navigation and then "Settings" in the header bar.

As of the time I wrote this document, the options you can see/set are:

Name	*Description*
Anomalies	Are the Anomaly Analytic rules being used?
EyesOn	Is this Sentinel instance sharing data with Microsoft?
EntityAnalytics	Which systems is the instance getting its user information from?
Incident	This is not used in the Settings page, but it does list all the incident closing classifications. Maybe this is something we will be able to set in the future? One can hope!
IPSyncer	Not sure what this is for. I don't see anything that uses it
Ueba	Which data souces is this instance getting its data from?

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/settings/**{settingsName}**?**{apiVersion}**

This will create an entry, if it does not exist, or update an existing one. Keep in mind that if you want to disable it use the Delete call below.

In the call below I am enabling the Anomalies. Notice that I don't need to actually set anything, like the "IsEnabled" field. I just need to make the call.

Sample Request

```
$body = @{
    "kind" = "Anomalies"
    "properties" = @{
    }
}
$url = $baseUrl + "settings/EyesOn" + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/settings/Anomal
ies",
  "name": "Anomalies",
```

```
  "type": "Microsoft.SecurityInsights/settings",
  "kind": "Anomalies",
  "systemData": {
    "createdAt": "2023-11-10T22:44:50.3029353Z",
    "createdBy": "garybushey@outlook.com",
    "createdByType": "User",
    "lastModifiedAt": "2023-11-10T22:44:50.3029353Z",
    "lastModifiedBy": "garybushey@outlook.com",
    "lastModifiedByType": "User"
  },
  "properties": {
    "isEnabled": true
  }
}
```


I am going to do another sample here since it is so different than the first one. In this one, I will update which data sources I want to use with Entity Behavior. I had all but "SignInLogs" selected previously so you will need to submit the name of each and every source you want to connect. This also requires the "etag" field while the other call did not. Using the "*" works, and this is what the portal uses as well.

Sample Request

```
$body = @{
    "kind" = "Ueba"
    "etag" = "*"
    "properties" = @{
        "dataSources"= @(
            "AuditLogs",
            "AzureActivity",
            "SigninLogs",
            "SecurityEvent"
        )
    }
}
$url = $baseUrl + "settings/Ueba" + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/settings/Ueba",
  "name": "Ueba",
  "etag": "\"9c032f77-0000-0100-0000-654eb36f0000\"",
```

```
  "type": "Microsoft.SecurityInsights/settings",
  "kind": "Ueba",
  "systemData": {
    "createdAt": "2023-11-10T22:49:18.0502721Z",
    "createdBy": "garybushey@outlook.com",
    "createdByType": "User",
    "lastModifiedAt": "2023-11-10T22:49:18.0502721Z",
    "lastModifiedBy": "garybushey@outlook.com",
    "lastModifiedByType": "User"
  },
  "properties": {
    "dataSources": [
      "AuditLogs",
      "AzureActivity",
      "SigninLogs",
      "SecurityEvent"
    ]
  }
}
```

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/settings/**{settingsName}**?**{apiVersion}**

This is one time I will show a delete since it very useful with settings. If you want to deactivate a setting, you will just delete it.

Sample Request

```
$body = @{
    "kind" = "Anomalies"
    "properties" = @{
    }
}
$url = $baseUrl + "settings/Ueba" + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Delete -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Not much is being returned in the Sample Response, which makes sense since you have just deleted the entry.

Sample Response

```
{}
```

Get

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/settings/**{settingsName}**?**{apiVersion}**

Get a single setting using the setting name.

Sample Request

```
$url = $baseUrl + "settings/ueba" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/settings/Ueba",
  "name": "Ueba",
  "etag": "\"9c03bb81-0000-0100-0000-654eb5670000\"",
  "type": "Microsoft.SecurityInsights/settings",
  "kind": "Ueba",
  "systemData": {},
  "properties": {
    "dataSources": [
      "AuditLogs",
      "AzureActivity",
      "SigninLogs",
      "SecurityEvent"
    ]
  }
}
```

List

Http Method: Get

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/settings?**{apiVersion}**

Return an array of the various settings. Note that if some settings are not enabled, for instance if UEBA is not enabled, then those entries will not show up.

In the Sample Response below, I have the following settings enabled:

Anomalies: Enabled
EyesOn: Enabled
Entity Analytics: Azure AD selected (showing Microsoft Entra ID in the portal),
UEBA: Audit Logs, Azure Activity, Security Events, and Signin Logs enabled.

Sample Request

```
$url= $baseUrl + "settings" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader
).value
```

Sample Response


```
[
  {
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/settings/Entity
Analytics",
    "name": "EntityAnalytics",
    "etag": "\"9c039d5e-0000-0100-0000-654ead640000\"",
    "type": "Microsoft.SecurityInsights/settings",
    "kind": "EntityAnalytics",
    "systemData": {},
    "properties": {
      "entityProviders": [
        "AzureActiveDirectory"
      ]
    }
  },
  {
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/settings/EyesOn
",
    "name": "EyesOn",
    "etag": "\"ea005c20-0000-0300-0000-654eaccb0000\"",
    "type": "Microsoft.SecurityInsights/settings",
    "kind": "EyesOn",
    "systemData": {},
    "properties": {
      "isEnabled": true
    }
  },
  {
```

```
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/settings/IPSync
er",
    "name": "IPSyncer",
    "etag": "\"0500560f-0000-0300-0000-6006c2760000\"",
    "type": "Microsoft.SecurityInsights/settings",
    "kind": "IPSyncer",
    "systemData": {},
    "properties": {
      "isEnabled": true
    }
  },
  {
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/settings/Anomal
ies",
    "name": "Anomalies",
    "etag": "\"ea004120-0000-0300-0000-654eacc80000\"",
    "type": "Microsoft.SecurityInsights/settings",
    "kind": "Anomalies",
    "systemData": {},
    "properties": {
      "isEnabled": true
    }
  },
  {
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/settings/Ueba",
    "name": "Ueba",
    "etag": "\"9c039d5e-0000-0100-0000-654ead640000\"",
    "type": "Microsoft.SecurityInsights/settings",
    "kind": "Ueba",
    "systemData": {},
    "properties": {
      "dataSources": [
        "AuditLogs",
        "AzureActivity",
        "SecurityEvent",
        "SigninLogs"
      ]
    }
  },
```

```
  {
    "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/settings/Incide
nt",
    "name": "Incident",
    "type": "Microsoft.SecurityInsights/settings",
    "kind": "Incident",
    "systemData": {},
    "properties": {
      "customStatuses": [],
      "customClassificationReasons": [
        {
          "name": "suspiciousactivity",
          "description": null,
          "mappedClassification": 1
        },
        {
          "name": "suspiciousbutexpected",
          "description": null,
          "mappedClassification": 2
        },
        {
          "name": "incorrectalertlogic",
          "description": null,
          "mappedClassification": 3
        },
        {
          "name": "inaccuratedata",
          "description": null,
          "mappedClassification": 3
        }
      ]
    }
  }
]
```

Source Controls

These REST APIs will work provide you the information regarding the Microsoft Sentinel Repositories.

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/sourceControls/**{sourceControlId}**?**{apiVersion}**

This will create a new Microsoft Sentinel repository, using an existing code repository.

Sample Request

```
$body = @{
    "properties" = @{
        "description"  = "Testing for the book"
        "displayName"  = "Book Test"
        "repository"   = @{
            "url"    = "https=//github.com/garybushey/CreateMultiRulesGUI"
            "branch" = "master"
        }
        "repoType"     = "GitHub"
        "contentTypes" = @(
            "AnalyticsRule"
            "AutomationRule"
            "HuntingQuery"
            "Parser"
            "Playbook"
            "Workbook"
        )
        "repositoryAccess"= @{
            "kind"= "OAuth"
            "clientId"= "******"
            "code"= "******"
            "state"= "******"
        }
    }
}
$guid = New-Guid
$url = $baseUrl + "sourceControls/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Post -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/SourceControls/
51bc62f7-b54e-41e1-8fba-13cf46d5beac",
  "name": "51bc62f7-b54e-41e1-8fba-13cf46d5beac",
  "type": "Microsoft.SecurityInsights/SourceControls",
  "systemData": {
    "createdAt": "2023-11-11T13:09:07.8841225Z",
    "createdBy": "garybushey@outlook.com",
    "createdByType": "User",
    "lastModifiedAt": "2023-11-11T13:09:07.8841225Z",
    "lastModifiedBy": "garybushey@outlook.com",
    "lastModifiedByType": "User"
  },
  "properties": {
    "id": "51bc62f7-b54e-41e1-8fba-13cf46d5beac",
    "version": "V1",
    "repoType": "GitHub",
    "displayName": "Book Test",
    "description": "Testing for the book",
    "contentTypes": [
      "AnalyticsRule",
      "AutomationRule",
      "HuntingQuery",
      "Parser",
      "Playbook",
      "Workbook"
    ],
    "repository": {
      "url": "https://github.com/garybushey/CreateMultiRulesGUI",
      "displayUrl": null,
      "branch": "main",
      "deploymentLogsUrl":
"https://github.com/garybushey/CreateMultiRulesGUI/actions/workflows/sentinel-
deploy-51bc62f7-b54e-41e1-8fba-13cf46d5beac.yml"
    },
    "servicePrincipal": {
      "id": "a2e99505-c986-47b2-bc6b-a5a3fc867a69",
      "tenantId": "ae0818a0-ede8-4da6-9786-2d9d5fd5295f",
      "appId": "4fdb8497-5a73-4311-928f-a50d6e233432"
    },
    "repositoryResourceInfo": {
      "webhook": null,
      "gitHubResourceInfo": {
```

```
        "appInstallationId": "18576607"
      },
      "azureDevOpsResourceInfo": null
    },
    "lastDeploymentInfo": null,
    "pullRequest": null
  }
}
```


Delete

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/sourceControls/**{sourceControlId}/**delete?**{apiVersion}**

This will delete a Microsoft Sentinel repository, using an existing source control Id. Unlike other delete REST API calls, this one requires a POST command and that you pass in the repository access.

Sample Request

```
$body = @{
    "properties" = @{
        "repositoryAccess"= @{
            "kind"= "OAuth"
            "clientId"= "******"
            "code"= "******"
            "state"= "******"
        }
    }
}
$url = $baseUrl + "sourceControls/70a10097-9127-4082-8c6b-7759c862ad26/delete"  +
$apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Post -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{}
```

Get

Http Method: Get

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/sourceControls/**{sourceControlId}**?**{apiVersion}**

This will get a single source code entry.

Sample Request

```
$url = $baseUrl + "sourcecontrols/79a06b5c-7705-4622-8675-1e3034f38943" +
$apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/SourceControls/
79a06b5c-7705-4622-8675-1e3034f38943",
  "name": "79a06b5c-7705-4622-8675-1e3034f38943",
  "etag": "\"75027295-0000-0100-0000-652710590000\"",
  "type": "Microsoft.SecurityInsights/SourceControls",
  "systemData": {
    "createdAt": "2023-10-11T21:14:55.8974123Z",
    "createdBy": "garybushey@outlook.com",
    "createdByType": "User",
    "lastModifiedAt": "2023-10-11T21:14:55.8974123Z",
    "lastModifiedBy": "garybushey@outlook.com",
    "lastModifiedByType": "User"
  },
  "properties": {
    "id": "79a06b5c-7705-4622-8675-1e3034f38943",
    "version": "V1",
    "repoType": "GitHub",
    "displayName": "Gary GitHub",
    "description": "This is a Github repo that I want to connect to",
    "contentTypes": [
      "AnalyticsRule",
      "AutomationRule",
      "HuntingQuery",
      "Parser",
      "Playbook",
      "Workbook"
    ],
    "repository": {
      "url": "https://github.com/garybushey/AzSentinelAnalyticsRules",
      "displayUrl": null,
      "branch": "master",
      "deploymentLogsUrl":
"https://github.com/garybushey/AzSentinelAnalyticsRules/actions/workflows/sentine
l-deploy-79a06b5c-7705-4622-8675-1e3034f38943.yml"
```

```
    },
    "servicePrincipal": {
      "id": "<Guid>",
      "tenantId": "<guid>",
      "appId": "<guid>"
    },
    "repositoryResourceInfo": {
      "webhook": null,
      "gitHubResourceInfo": {
        "appInstallationId": "18576607"
      },
      "azureDevOpsResourceInfo": null
    },
    "lastDeploymentInfo": {
      "deploymentFetchStatus": "Success",
      "deployment": {
        "deploymentId": "6488097986",
        "deploymentState": "Completed",
        "deploymentResult": "Success",
        "deploymentTime": "2023-10-11T21:15:09Z",
        "deploymentLogsUrl":
"https://github.com/garybushey/AzSentinelAnalyticsRules/actions/runs/6488097986"
      },
      "message": "Workflow run triggered by push with status completed and
conclusion success"
    },
    "pullRequest": null
  }
}
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/sourceControls/?**{apiVersion}**

This will return a JSON array of all the source controls that are part of your Microsoft Sentinel instance.

List Repositories

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/listRepositories?**{apiVersion}**

I was not able to get this to work correctly. Based on the example that is in the GitHub repository, this should return all the repositories for a given type, either “GitHub” or “AzureDevOps”. You can get this information by getting the source controls and filtering so it may be that this REST API just doesn’t work.

Threat Intelligence

There are no changes from the stable Threat Intelligence Indicator REST API

Triggered Analytics Rule Runs

These REST API calls will allow you to get a list of when the Analytics rules were last run or trigger the rule to start. The GET and LIST do not appear to work correctly. They are actually used in the Microsoft Sentinel portal, but no data is returned. Instead, there is a query against the "SentinelAudit" table that returns the needed information.

Create

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/alertRules/**{ruleId}**/triggerRuleRun?**{apiVersion}**

This will kick off the Analytic rule to run again immediately. In the Sample Request below, I am telling the run that kicked off at "11/05/2023 4:19:56 PM" EST to run again. While the Microsoft Sentinel portal only allows you to rerun an existing rule run, you can use any "executionTimeUtc" to run the rule again at that time.

Sample Request

```
$body = @{
    "properties" = @{
        "executionTimeUtc"= "2023-11-05T21:19:56.731Z"
    }
}
$url = $baseUrl + "alertRules/32fcb127-6c57-41f5-8db5-
3181525a7919/triggerRuleRun"  + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Post -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
  "properties": {
      "executionTimeUtc": "2023-11-05T21:19:56.731Z"
  }
}
```

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/triggeredAnalyticsRuleRuns/**{ruleRunId}**?**{apiVersion}**

This call does not currently work.

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/triggeredAnalyticsRuleRuns?**{apiVersion}**

This call does not currently work.

Watchlists

There are no changes from the stable Watchlists REST API.

Watchlist Items

There are no changes from the stable Watchlist Items REST API

Workspace Manager Assignments

The Workspace Manager assignments are the actual items that are going to be copied to the various other Microsoft Sentinel instances. These are the items that you add when creating or updating a Workspace Manager group in the "Select Content" tab.

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerAssignments.**{workspaceManagerAssignmentName}**?**{apiVersion}**

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerAssignments.**{workspaceManagerAssignmentName}**?**{apiVersion}**

This REST API call will delete an existing workspace manager assignment. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerAssignments.**{workspaceManagerAssignmentName}**?**{apiVersion}**

Get a single Workspace Manager assignment.

Sample Request

```
$url = $baseUrl + "workspaceManagerAssignments/9d2bf63a-ecbf-4704-b60e-f9162382d36d" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Note that in the Sample Response below. I removed some of the resources to save space.

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/workspaceManagerAssignments/9d2bf63a-ecbf-4704-b60e-f9162382d36d",
  "name": "9d2bf63a-ecbf-4704-b60e-f9162382d36d",
```

```
  "etag": "\"bf025626-0000-0100-0000-651330ad0000\"",
  "type": "Microsoft.SecurityInsights/workspaceManagerAssignments",
  "properties": {
    "items": [
      {
        "resourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/alertRules/Buil
tInFusion"
      },
      {
        "resourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/alertRules/fb46
c6e2-fb77-4373-bbf0-192a0cbf4f00"
      }
    ],
    "targetResourceName": "7097ccf5-0bdd-4696-be28-de586e81edcb",
    "lastJobEndTime": "2023-09-26T15:27:41.8571034-04:00",
    "lastJobProvisioningState": "Failed"
  }
}
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerAssignments?**{apiVersion}**

Filters Available: $orderby, $skipToken, $top

This will return a JSON array of the Workspace Manager assignments. See the GET call above.

Workspace Manager Configurations

This REST API will tell you if the Microsoft Sentinel installation has the Workspace Manager enabled.

Documentation:

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerConfigurations/**{workspaceManagerConfigurationName}**?**{apiVersion}**

This will either enable or disable Workspace Manager in your Microsoft Sentinel environment. In the example below, the Workspace Manager has been enabled. You can set "mode" to "Disabled" to disable Workspace Manager or you can Delete the entry using the DELETE command below

Sample Request

```
$body = @{
    "properties" = @{
        "mode" = "Enabled"
    }
}
$guid = New-Guid
$url = $baseUrl + "workspaceManagerConfigurations" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/workspaceManage
rConfigurations/5dcbd802-8223-4287-b15c-11685b26e211",
  "name": "5dcbd802-8223-4287-b15c-11685b26e211",
  "etag": "\"d800e58b-0000-0100-0000-654fc1030000\"",
  "type": "Microsoft.SecurityInsights/workspaceManagerConfigurations",
  "properties": {
    "mode": "Enabled"
  }
}
```

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerConfigurations/**{workspaceManagerConfigurationName}**?**{apiVersion}**

This REST API call will delete an existing workspace manager configuration. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerConfigurations/**{workspaceManagerConfigurationName}**?**{apiVersion}**

This will return a single Workspace Manager Configuration. Now, there will only be one Workspace Manager Configuration so you could either use this call or the LIST call below.

Sample Request

```
$url = $baseUrl + "workspaceManagerConfigurations/5dcbd802-8223-4287-b15c-11685b26e211" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/workspaceManagerConfigurations/5dcbd802-8223-4287-b15c-11685b26e211",
  "name": "5dcbd802-8223-4287-b15c-11685b26e211",
  "etag": "\"d800e58b-0000-0100-0000-654fc1030000\"",
  "type": "Microsoft.SecurityInsights/workspaceManagerConfigurations",
  "properties": {
    "mode": "Enabled"
  }
}
```

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerConfigurations?**{apiVersion}**

Filters Available: $orderby, $skipToken, $top

This will return a list of Workspace Manager Configurations. Since there will only be one (there can only be one!), it will work just like the GET above, except you do not need to add the Workspace Manager Configuration Name to the URL.

Workspace Manager Groups

The REST APIs will work with the Workspace Manager Groups which contain the definitions of the which content will be pushed and where it will go.

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerGroups/**{workspaceManagerGroupName}**?**{apiVersion}**

This will create a new Workspace Manager Group. While in the Microsoft Sentinel portal, you create the group as well as add the content that will be copied, this REST API will only create the Workspace Manager Group. To add the resources, use the Workspace Manager Assignments REST API call discussed above.

Sample Request

```
$body = @{
    "properties" = @{
        "description"= "This is being created for the book"
        "displayName"= "Book Test"
        "memberResourceNames"= @(
            "a454293d-0945-4b0d-b01e-d2076c8785ca"
            "8f52ff2b-2629-4f9e-a19f-823f4caea51f"
        )
    }
}
$guid = New-Guid
$url = $baseUrl + "workspaceManagerGroups/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/workspaceManage
rGroups/2adacf59-fd78-4b4d-9a1e-07442b02082f",
  "name": "2adacf59-fd78-4b4d-9a1e-07442b02082f",
  "etag": "\"4400bd66-0000-0100-0000-654fc72c0000\"",
  "type": "Microsoft.SecurityInsights/workspaceManagerGroups",
  "properties": {
    "displayName": "Book Test",
    "description": "This is being created for the book",
```

```
    "memberResourceNames": [
      "a454293d-0945-4b0d-b01e-d2076c8785ca",
      "8f52ff2b-2629-4f9e-a19f-823f4caea51f"
    ]
  }
}
```

Delete

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerGroups/**{workspaceManagerGroupName}**?**{apiVersion}**

This REST API call will delete an existing Workspace Manager Group. This is a simple call so I will not go into much detail.

Get

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerGroups/**{workspaceManagerGroupName}**?**{apiVersion}**

This will get a single Workspace Manager Group.

Sample Request

```
$url = $baseUrl + "workspaceManagerGroups/c4a29f23-653a-486f-90ee-ec33204f3c27" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/workspaceManagerGroups/c4a29f23-653a-486f-90ee-ec33204f3c27",
  "name": "c4a29f23-653a-486f-90ee-ec33204f3c27",
  "etag": "\"0e00f154-0000-0100-0000-653a5b880000\"",
  "type": "Microsoft.SecurityInsights/workspaceManagerGroups",
  "properties": {
    "displayName": "GABTEst",
    "description": "Testing how new rules are created",
    "memberResourceNames": [
      "a454293d-0945-4b0d-b01e-d2076c8785ca",
```

```
        "8f52ff2b-2629-4f9e-a19f-823f4caea51f"
      ]
    }
}
```

List

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerGroups?**{apiVersion}**

Filters Available: $orderby, $skipToken, $top

This will return a JSON array of all the Workspace Manager Groups. See the GET above.

Workspace Manager Jobs

These REST APIs will work with the jobs that will perform the replication tasks.

Create/Update

Http Method: POST

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerAssignments/**{workspaceManagerAssignmentName}**/jobs?**{apiVersion}**

This will create a new job for the specified Workspace Manager Assignment.

Note, unlike most other REST APIs that are used to create a new entry, this one requires the new job's GUID as part of the body rather than as part of the URL.

Sample Request

```
$guid = New-Guid
$body = @{
    "name" = "$guid"
}
$url = $baseUrl + "workspaceManagerAssignments/9d2bf63a-ecbf-4704-b60e-f9162382d36d/jobs" + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Post -Headers $authHeader -Body ($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/workspaceManagerAssignments/9d2bf63a-ecbf-4704-b60e-f9162382d36d/jobs/c9bf7993-6c66-4862-bffa-b18bd0176197",
  "name": "c9bf7993-6c66-4862-bffa-b18bd0176197",
  "etag": "\"6b004b1c-0000-0100-0000-654fbc9a0000\"",
  "type": "Microsoft.SecurityInsights/workspaceManagerAssignments/jobs",
  "properties": {
    "items": [],
    "endTime": null,
    "startTime": "2023-11-11T12:40:42.4170045-05:00",
    "provisioningState": "InProgress",
    "errorMessage": null
```

```
    }
}
```

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerAssignments.**{workspaceManagerAssignmentName}**/jobs/**{jobName}**?**{apiVersion}**

This REST API call will delete an existing workspace manager assignment's job. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerAssignments/**{workspaceManagerAssignmentName}**/jobs/**{jobName}**?**{apiVersion}**

This will return a single Workspace Manager job for the given Workspace Manager Assignment.

Sample Request

```
$url = $baseUrl + "workspaceManagerAssignments/9d2bf63a-ecbf-4704-b60e-f9162382d36d/jobs/e9fdedef-0606-42d2-b4e5-51acd38c4402" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Note that in the Sample Response below, I have removed some the "resourceId" entries to save space.

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/workspaceManagerAssignments/9d2bf63a-ecbf-4704-b60e-f9162382d36d/jobs/e9fdedef-0606-42d2-b4e5-51acd38c4402",
  "name": "e9fdedef-0606-42d2-b4e5-51acd38c4402",
  "etag": "\"2901f998-0000-0100-0000-651330ad0000\"",
  "type": "Microsoft.SecurityInsights/workspaceManagerAssignments/jobs",
  "properties": {
    "items": [
      {
```

```
        "resourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/alertRules/Buil
tInFusion",
        "status": "Succeeded",
        "executionTime": "2023-09-26T15:27:40.0023988-04:00",
        "errors": []
      },
      {
        "resourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/alertRules/fb46
c6e2-fb77-4373-bbf0-192a0cbf4f00",
        "status": "Failed",
        "executionTime": "2023-09-26T15:27:40.8376617-04:00",
        "errors": [
          {
            "memberResourceName": "a454293d-0945-4b0d-b01e-d2076c8785ca",
            "errorMessage": "Failed to publish content item - content item was
not found. Please verify that the content item exists, or edit and update the
Group to remove reference to this content item. Correlation request id: 42ceeecc-
2611-42de-bfda-44600e79a779."
          }
        ]
      },
      {
        "resourceId": "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/alertRules/cfb7
5437-7e99-432e-ba68-4efab0e6c9a0",
        "status": "Failed",
        "executionTime": "2023-09-26T15:27:40.9549376-04:00",
        "errors": [
          {
            "memberResourceName": "a454293d-0945-4b0d-b01e-d2076c8785ca",
            "errorMessage": "Failed to publish content item - content item was
not found. Please verify that the content item exists, or edit and update the
Group to remove reference to this content item. Correlation request id: 42ceeecc-
2611-42de-bfda-44600e79a779."
          }
        ]
      }
    ],
    "endTime": "2023-09-26T15:27:41.8571034-04:00",
    "startTime": "2023-09-26T15:27:39.5286058-04:00",
```

```
    "provisioningState": "Failed",
    "errorMessage": null
  }
}
```


List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerAssignments/**{workspaceManagerAssignmentName}**/jobs?**{apiVersion}**

Filters Available: $orderby, $skipToken, $top

This will return a JSON array of all the different jobs for the specified Workspace Manager Assignment. See the GET above.

Workspace Manager Members

These REST API calls will allow you to work with the Microsoft Sentinel instances that the Workspace Manager will send the content.

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerMembers/**{workspaceManagerMemberName}**?**{apiVersion}**

In the Sample Request below, add your own tenant's GUID and the Resource Id for the workspace you want to add.

Sample Request

```
$body = @{
    "properties" = @{
        "targetWorkspaceResourceId"= "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azureml/providers/Microsoft.OperationalInsights/workspaces/azureml9236226029",
        "targetWorkspaceTenantId"= "<GUID>"
    }
}
$guid = New-Guid
$url = $baseUrl + "workspaceManagerMembers/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body ($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Note that in the Sample Response below, your tenant's actual GUID will be shown.

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/workspaceManagerMembers/507f970b-517e-46de-a272-1e9a946c3e15",
  "name": "507f970b-517e-46de-a272-1e9a946c3e15",
  "etag": "\"1701e163-0000-0100-0000-654fc9a30000\"",
  "type": "Microsoft.SecurityInsights/workspaceManagerMembers",
  "properties": {
      "targetWorkspaceResourceId": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azureml/providers/Microsoft.OperationalInsights/workspaces/azureml9236226029",
      "targetWorkspaceTenantId": "<GUID>"
```

```
  }
}
```

Delete

Http Method: DELETE

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerMembers/**{workspaceManagerMemberName}**?**{apiVersion}**

This REST API call will delete an existing Workspace Manager Member. This is a simple call so I will not go into much detail.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerMembers/**{workspaceManagerMemberName}**?**{apiVersion}**

This will return a single Workspace Manager Member

Sample Request

```
$url = $baseUrl + "workspaceManagerMembers/a454293d-0945-4b0d-b01e-d2076c8785ca" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Note that in the Sample Response below, your tenant's actual GUID will be shown.

Sample Response

```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/workspaceManagerMembers/a454293d-0945-4b0d-b01e-d2076c8785ca",
  "name": "a454293d-0945-4b0d-b01e-d2076c8785ca",
  "etag": "\"54001a5b-0000-0100-0000-6398fa7f0000\"",
  "type": "Microsoft.SecurityInsights/workspaceManagerMembers",
  "properties": {
    "targetWorkspaceResourceId": "/subscriptions/34bdcce3-c06f-416b-aaa0-24683117cc68/resourceGroups/mssentinel/providers/Microsoft.OperationalInsights/workspaces/MSSentinel",
    "targetWorkspaceTenantId": "<GUID>"
  }
}
```

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/workspaceManagerMembers?**{apiVersion}**

Filters Available: $orderby, $skipToken, $top

This will return a JSON array of all the Workspace Manager Members. See the GET call above.

Data Connector Definitions

These REST API calls do not appear to be working yet. I can see them being used in the Microsoft Sentinel portal but nothing gets returned.

Data Connectors

This will work with the installed data connectors. All the information that is presented on the Data Connectors page can be obtained here.

Note. I have found that some of the "sampleQueries" entries are not correct so I would not trust them.

Create/Update

Http Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/dataConnectors/**{dataConnectorId}**?**{apiVersion}**

This REST API call only works on the Microsoft first-party data connectors. You are better off deploying the solution that contains this data connector to get it installed.

Get

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/dataConnectors/**{dataConnectorId}**?**{apiVersion}**

This will return a single Data Connector definition.

Sample Request

```
$url = $baseUrl + "dataConnectors/d4830f7e-fb84-4526-b18d-eb38366e471d" + $apiVersion
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

Sample Response


```
{
  "id": "/subscriptions/9790d913-b5da-460d-b167-ac985d5f3b83/resourceGroups/AzureSentinel/providers/Microsoft.OperationalInsights/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/dataConnectors/d4830f7e-fb84-4526-b18d-eb38366e471d",
  "name": "d4830f7e-fb84-4526-b18d-eb38366e471d",
  "etag": "\"16007ade-0000-0100-0000-622fc47b0000\"",
  "type": "Microsoft.SecurityInsights/dataConnectors",
  "kind": "APIPolling",
```

```
  "properties": {
    "pollingConfig": {
      "auth": {
        "authType": "APIKey",
        "APIKeyName": "Authorization",
        "APIKeyIdentifier": "token"
      },
      "request": {
        "apiEndpoint":
"https://api.github.com/organizations/{{placeHolder1}}/audit-log",
        "rateLimitQPS": 50,
        "queryWindowInMin": 15,
        "httpMethod": "Get",
        "queryTimeFormat": "yyyy-MM-ddTHH:mm:ssZ",
        "retryCount": 2,
        "timeoutInSeconds": 60,
        "headers": {
          "Accept": "application/json",
          "User-Agent": "Scuba"
        },
        "queryParameters": {
          "phrase": "created:{_QueryWindowStartTime}..{_QueryWindowEndTime}"
        }
      },
      "paging": {
        "pagingType": "LinkHeader",
        "pageSizeParaName": "per_page"
      },
      "response": {
        "eventsJsonPaths": [
          "$"
        ]
      },
      "isActive": false
    },
    "connectorUiConfig": {
      "title": "GitHub Enterprise Audit Log",
      "publisher": "GitHub",
      "descriptionMarkdown": "The GitHub audit log connector provides the
capability to ingest GitHub logs into Microsoft Sentinel. By connecting GitHub
audit logs into Microsoft Sentinel, you can view this data in workbooks, use it
to create custom alerts, and improve your investigation process.",
      "graphQueriesTableName": "GitHubAuditLogPolling_CL",
      "graphQueries": [
        {
```

```
          "metricName": "Total events received",
          "legend": "GitHub audit log events",
          "baseQuery": "{{graphQueriesTableName}}"
        }
      ],
      "sampleQueries": [
        {
          "description": "All logs",
          "query": "{{graphQueriesTableName}}\n | take 10"
        }
      ],
      "dataTypes": [
        {
          "name": "{{graphQueriesTableName}}",
          "lastDataReceivedQuery": "{{graphQueriesTableName}}\n            |
summarize Time = max(TimeGenerated)\n            | where isnotempty(Time)"
        }
      ],
      "connectivityCriterias": [
        {
          "type": "SentinelKindsV2",
          "value": [
            "{{graphQueriesTableName}}\n | summarize LastLogReceived =
max(TimeGenerated)\n | project IsConnected = LastLogReceived > ago(30d)"
          ]
        }
      ],
      "availability": {
        "status": 1,
        "isPreview": true
      },
      "permissions": {
        "resourceProvider": [
          {
            "provider": "Microsoft.OperationalInsights/workspaces",
            "permissionsDisplayText": "read and write permissions are required.",
            "providerDisplayName": "Workspace",
            "scope": "Workspace",
            "requiredPermissions": {
              "write": true,
              "read": true,
              "delete": true
            }
          }
        ],
```

```
        "customs": [
          {
            "name": "GitHub API personal token Key",
            "description": "You need access to GitHub personal token, the key
should have 'admin:org' scope"
          }
        ]
      },
      "instructionSteps": [
        {
          "title": "Connect GitHub Enterprise Audit Log to Microsoft Sentinel",
          "description": "Enable GitHub audit Logs.",
          "instructions": [
            {
              "parameters": {
                "enable": "true",
                "userRequestPlaceHoldersInput": [
                  {
                    "displayText": "Organization Name",
                    "requestObjectKey": "apiEndpoint",
                    "placeHolderName": "{{placeHolder1}}"
                  }
                ]
              },
              "type": "APIKey"
            }
          ]
        }
      ]
    }
  }
}
```

List

Http Method: GET

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/dataConnectors?**{apiVersion}**

This will return a JSON array of all the installed data connector's information.

Use Cases

In this section, I am going to list some different use cases and then show the various REST API calls I have made to solve the problem. For the most part, I will not post the entire PowerShell script, just the REST API calls and any special processing that would be needed.

Create a new Analytic rule from a rule template.

This will probably happen quite a bit. You can extract a rule JSON and use that with repositories, but that isn't what this book is about 😊

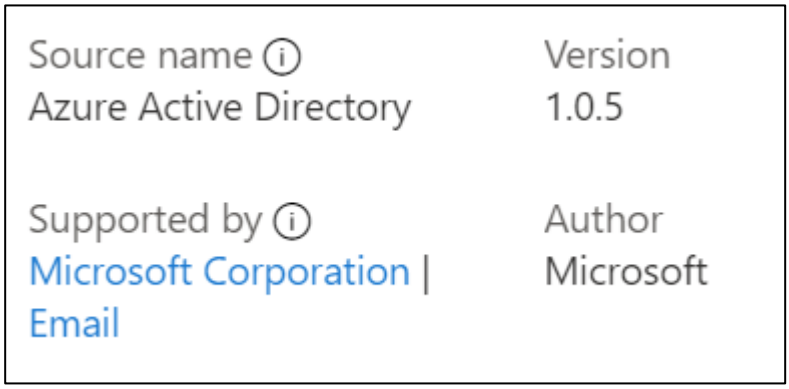
Assumptions

1. You have a Microsoft Sentinel environment where you have at least Microsoft Sentinel Contributor rights.
2. You know the name of the template you want to use.
3. You have deployed the solution that contains the template (see the use case "How to find the solution that contains the template" on how to do find the solution)

```
<use the code to connect to Azure>
$baseUrl = "https://management.azure.com/subscriptions/$SubscriptionId" +
"/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights" +
"/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/"

$apiVersion = "?api-version=2023-09-01-preview"
$templateName = "User Assigned Privileged Role"
#Get the list of all installed templates
$url = $baseUrl + "contentTemplates" + $apiVersion
$templates = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader
).value
#Find the exact template
$foundTemplate = $templates | Where-Object { $_.properties.displayName -eq
$templateName }
#$foundTemplate does not actually contain the data we need so now we need to make
#the call to load the individual template.  The "name" field contains
#the GUID that we need to pass into the URL to load.
$url = $baseUrl + "contentTemplates/" + $foundTemplate.name + $apiVersion
$template = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
# Assign the properties from the template
$properties = $template.properties.mainTemplate.resources[0].properties
#Some templates have this field and others don't
if ($null -eq $properties.enabled) {
  $properties | Add-Member -NotePropertyName "enabled" -NotePropertyValue $true
}
else {
  $properties.enabled = $true  #Added this to make sure each rule was enabled
}
#Add the field to link this rule with the rule template so that the rule template
will show up as used
```

```
#We had to use the "Add-Member" command since this field does not exist in the
rule template that we are copying from.
$properties | Add-Member -NotePropertyName "alertRuleTemplateName" -
NotePropertyValue $template.properties.contentId
$properties | Add-Member -NotePropertyName "templateVersion" -NotePropertyValue
$template.properties.version

#Depending on the type of alert we are creating, the body has different
parameters but this should cover all types
$body = @{
  "kind"       = $template.properties.mainTemplate.resources[0].kind
  "properties" = $properties
}
#Create the rule.
$guid = New-Guid
$url = $baseUrl + "alertRules/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
#We need to load the solution that this rule template belongs to so we can
populate the metadata
$url = $baseUrl + "contentpackages/" + $template.properties.packageId +
$apiVersion
$solution = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )

#Add the metadata to link it to the solution
$metabody = @{
  "apiVersion" = "2022-01-01-preview"
  "name"       = "analyticsrule-" + $verdict.name
  "type"       = "Microsoft.OperationalInsights/workspaces/providers/metadata"
  "id"         = $null
  "properties" = @{
    "contentId" = $verdict.name
    "parentId"  = $verdict.id
    "kind"      = "AnalyticsRule"
    "version"   = $template.properties.Version
    "source"    = $solution.properties.source
    "author"    = $solution.properties.author
    "support"   = $solution.properties.support
  }
}
$url = $baseUrl + "metadata/analyticsrule-" + $verdict.name + $apiVersion
$metaVerdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($metabody | ConvertTo-Json -EnumsAsStrings -Depth 5)
```

That will do it. If you run all the code up to the last line, you will see that the analytic rule exists, but if you look at the details pane, you will not see any of the solution information like shown below:



Create a new Analytic rule manually.

Chances are this will not happen too often, but you never know.

Assumptions

1. You have a Microsoft Sentinel environment where you have at least Microsoft Sentinel Contributor rights.
2. You have all the values you need to create the rule.

For this example. I am going to use the values I want to use and then show you how it will look in the Microsoft Sentinel's GUI. It will be a scheduled rule, since this is what you will create most of the time.

```
<use the code to connect to Azure>
$baseUrl = "https://management.azure.com/subscriptions/$SubscriptionId" +
"/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights" +
"/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/"

$apiVersion = "?api-version=2023-09-01-preview"
$properties = @{
  "displayName"           = "Book Test"
  "description"           = "This is for the book"
  "severity"              = "Medium"
  "enabled"               = $true
  "query"                 = "AuditLogs | extend ProductName = 'DemoSystem'"
  "queryFrequency"        = "PT5H"
  "queryPeriod"           = "PT5H"
  "triggerOperator"       = "GreaterThan"
  "triggerThreshold"      = 0
  "suppressionDuration"   = "PT5H"
  "suppressionEnabled"    = $false
  "tactics"               = @(
```

```
    "Reconnaissance"
    "Collection"
  )
  "techniques"            = @(
    "T1595"
    "T1557"
  )
  "incidentConfiguration" = @{
    "createIncident"        = $true
    "groupingConfiguration" = @{
      "enabled"               = $true
      "reopenClosedIncident" = $true
      "lookbackDuration"     = "PT5H"
      "matchingMethod"       = "AllEntities"
      "groupByEntities"      = @()
      "groupByAlertDetails"  = @()
      "groupByCustomDetails" = @()
    }
  }
  "eventGroupingSettings" = @{
    "aggregationKind" = "SingleAlert"
  }
  "alertDetailsOverride"  = @{
    "alertDisplayNameFormat" = "Alert from {{{Category}} "
    "alertDescriptionFormat" = "{{OperationName}} occurred "
    "alertDynamicProperties" = @(
      @{
        "alertProperty" = "ProductName"
        "value"         = "ProductName"
      }
    )
    "customDetails"          = @{
      "TenantId" = "TenantId"
    }
    "entityMappings"         = @(
      @{
        "entityType"    = "Host"
        "fieldMappings" = @(
          @{
            "identifier" = "HostName"
            "columnName" = "SourceSystem"
          }
        )
      }
    )
```

```
  }
}
$body = @{
  "kind"       = "Scheduled"
  "properties" = $properties
}
#Create the rule
$guid = New-Guid
$url = $baseUrl + "alertRules/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Create an Automation Rule using the incident creation trigger

This rule will trigger when an incident was created when:

- The incident was created by any Incident provider
- AND Created by any Analytic Rule
- AND when the entity Host Name contains “Gary”

When those conditions are met, the Automation rule will:

1. Add a new task called “This is a test task” and the description will be “**Look** *at* this ~~description~~. Isn't it amazing?”
2. Add another task called “Second task” with the description of “The first amazing task”.

The rule will not expire and the run order is 1

```
$body = @{
  "properties" = @{
    "displayName"     = "Book Test"
    "order"           = 1
    "triggeringLogic" = @{
      "isEnabled"         = $true
      "expirationTimeUtc" = $null
      "triggersOn"        = "Incidents"
      "triggersWhen"      = "Created"
      "conditions"        = @(
        @{
          "conditionType"       = "Property"
          "conditionProperties" = @{
            "propertyName"   = "HostName"
            "operator"       = "Contains"
            "propertyValues" = @(
              "Gary"
            )
          }
        }
```

```
      )
    }
    "actions"         = @(
      @{
        "order"               = 1
        "actionType"          = "AddIncidentTask"
        "actionConfiguration" = @{
          "title"       = "This is a test task"
          "description" = "<div><strong>Look </strong><em>at </em><u>this
</u><s>description</s>. Isn't it amazing?</div>"
        }
      }
      @{
        "order"               = 2
        "actionType"          = "AddIncidentTask"
        "actionConfiguration" = @{
          "title"       = "Second task"
          "description" = "<div>The first amazing task</div>"
        }
      }
    )

  }
}
$guid = New-Guid
$url = $baseUrl + "automationRules/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Create an Automation Rule using the incident update trigger

This rule will trigger when an incident was updated when:

- When the incident provider equals “Microsoft Sentinel”
- AND when the Analytic rule name contains “Book Test”
- AND
    - When the Status has changed to “Closed”
    - OR when the Severity has changed from “Low”

When those conditions are met, the Automation rule will:

1. Assign the incident to “Gary Test” user
2. Add then run the playbook called “CreateJiraIssue”

The rule will expire on November 30, 2023 at 08:00AM EST (which has to be converted to UTC when using it in the body) and it will be the second Analytic rule to be run.

```
$body = @{
  "properties" = @{
      "displayName"     = "Use Case Automation Rule"
      "order"           = 2
      "triggeringLogic" = @{
          "isEnabled"          = $true
          "expirationTimeUtc" = "2023-11-30T13:00:00.000Z"
          "triggersOn"         = "Incidents"
          "triggersWhen"       = "Updated"
          "conditions"         = @(
              @{
                  "conditionType"       = "Property"
                  "conditionProperties" = @{
                      "propertyName"    = "IncidentProviderName"
                      "operator"        = "Equals"
                      "propertyValues" = @(
                          "Azure Sentinel"
                      )
                  }
              }
              @{
                  "conditionType"       = "Property"
                  "conditionProperties" = @{
                      "propertyName"    = "IncidentRelatedAnalyticRuleIds"
                      "operator"        = "Contains"
                      "propertyValues" = @(
                          "/subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/providers/Microsoft.SecurityInsights/alertRules/d3c1
e682-14f3-40a2-80b6-34072cd9c272"
```

```
                    )
                }
            }
            @{
                "conditionType"       = "Boolean"
                "conditionProperties" = @{
                    "operator"        = "Or"
                    "innerConditions" = @(
                        @{
                            "conditionType"       = "PropertyChanged"
                            "conditionProperties" = @{
                                "propertyName"    = "IncidentStatus"
                                "operator"        = "Equals"
                                "changeType"      = "ChangedTo"
                                "propertyValues" = @(
                                    "Closed"
                                )
                            }
                        }
                        @{
                            "conditionType"       = "PropertyChanged"
                            "conditionProperties" = @{
                                "propertyName"    = "IncidentSeverity"
                                "operator"        = "Equals"
                                "changeType"      = "ChangedFrom"
                                "propertyValues" = @(
                                    "Low"
                                )
                            }
                        }
                    )
                }
            }
        )
    }
    "actions"         = @(
        @{
            "order"               = 1
            "actionType"          = "ModifyProperties"
            "actionConfiguration" = @{
                "owner" = @{
                    "objectId"          = "2fc92ec6-0d4c-4d31-a5ea-
08364b7fca2e"
                    "email"             = $null
                    "userPrincipalName" = $null
```

```
                }
            }
        }
        @{
            "order"                = 2
            "actionType"           = "RunPlaybook"
            "actionConfiguration" = @{
                "logicAppResourceId" = "/subscriptions/34bdcce3-c06f-416b-aaa0-
24683117cc68/resourceGroups/MSSentinel/providers/Microsoft.Logic/workflows/Create
JiraIssue"
                "tenantId"           = "ae0818a0-ede8-4da6-9786-2d9d5fd5295f"
            }
        }
    )
  }
}
$guid = New-Guid
$url = $baseUrl + "automationRules/" + $guid + $apiVersion
$verdict = Invoke-RestMethod -Uri $url -Method Put -Headers $authHeader -Body
($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
```

Obtain a list of Hunting queries to use with my Hunts.

Hunting queries are considered to be "saved queries" by Microsoft Sentinel. This is quite easy actually as there is a REST API call to get the saved queries.

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$
resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceNa
me/savedSearches?api-version=2017-04-26-preview"
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader
).value
$huntingQueries = $results | Where-Object {$_.properties.category -eq "Hunting
Queries"}
```

This call returns a JSON array of all the saved searches. Unfortunately, there does not appear to be anyway to do a filter using the URL. So, the last line is to filter to see just those saved searches that are for Hunting Queries. Each entry in the "$huntingQueries" will look like what is shown below:

```
{
  "id": "subscriptions/9790d913-b5da-460d-b167-
ac985d5f3b83/resourceGroups/azuresentinel/providers/Microsoft.OperationalInsights
/workspaces/gabazuresentinel/savedSearches/01146dd7-9404-4ecf-8ec9-0a0cbe6ed7d2",
  "etag": "W/\"datetime'2023-11-06T20%3A48%3A38.6371781Z'\"",
  "properties": {
    "Category": "Hunting Queries",
    "DisplayName": "Linux security related process termination activity
detected",
```

```
    "Query": "Syslog ",
    "Tags": [
      {
        "Name": "description",
        "Value": "This query will alert on any attempts to terminate processes
related to security monitoring on the host. \nAttackers will often try to
terminate such processes post-compromise as seen recently to exploit the remote
code execution vulnerability in Log4j ..."
      },
      {
        "Name": "tactics",
        "Value": "DefenseEvasion"
      },
      {
        "Name": "techniques",
        "Value": "T1489"
      },
      {
        "Name": "createdBy",
        "Value": "garybushey@outlook.com"
      },
      {
        "Name": "createdTimeUtc",
        "Value": "11/06/2023 20:48:41"
      }
    ],
    "Version": 2
  },
  "name": "01146dd7-9404-4ecf-8ec9-0a0cbe6ed7d2",
  "type": "Microsoft.OperationalInsights/savedSearches"
}
```


Obtain a list of resources that make up a solution.

There are three different scenarios that we need to consider here; Standalone entries, solutions added either through the REST API or the Content Hub in the Microsoft Sentinel portal, and those solutions that were installed automatically by the system when Microsoft Sentinel switched to using solutions.

First, you need to load all the installed solutions. Sadly, this is not as easy as it should be either.

```
$url = $baseUrl + "contentProductPackages" + $apiVersion
        $allSolutions = (Invoke-RestMethod -Method "Get" -Uri $url -Headers
$authHeader ).value
        $solutions = $allSolutions | Where-Object { $null -ne
$_.properties.installedVersion }
```

In this case, you load all the solutions and then check for the “installedVersion” column to see if there is a value. If there is, then the solution has been installed.

Next, iterate through all the “$solutions” to get each individual solution.

```
foreach ($solution in $solutions | Sort-Object { $_.properties.displayName }) {
   …
   }
```

Now that we have the individual solution, we can start looking at the code to determine the resources. This is what we would place instead of the “…” code above.

First, we check to see if the solution is a standalone. If it is, there will only be one resource in it.

```
if ($solution.properties.contentKind -eq "StandAlone") {
    switch ($solution.properties.dependencies.criteria.kind) {
        #Do what you want with the resources
    }
}
```

If this is not a standalone solution, we will then check to see if what was installed using the REST API or the portal.

```
 $contentId = $solution.properties.contentId
#try to load using the new way.
$url = $baseUrl + "contentTemplates" + $apiVersion
$url += "&%24filter=(properties%2FpackageId%20eq%20'$contentId')%20and%20" +
"(properties%2FcontentKind%20eq%20'AnalyticsRule'%20or%20properties%2FcontentKind
%20eq%20'DataConnector'%20or%20properties" +
"%2FcontentKind%20eq%20'HuntingQuery'%20or%20properties%2FcontentKind%20eq%20'Pla
ybook'%20or%20properties%2FcontentKind" +
"%20eq%20'Workbook'%20or%20properties%2FcontentKind%20eq%20'Parser')"
$singleSolutionTemplates = (Invoke-RestMethod -Method "Get" -Uri $url -Headers
$authHeader ).value
if ("" -eq $singleSolutionTemplates) {}
else {
    #Do what you want with the resources
}
```

The “If” statement will see if any data was returned. If there is no data, we have the last way to load the resources, otherwise we have the solution’s resources.

Finally, if all the other code fails, we then need to use the Resource Graph to load the solution and its resources.

```
$body = @{
    "subscriptions" = @(
        "$SubscriptionId"
    )
    "query"         = "Resources | where type =~
'Microsoft.Resources/templateSpecs/versions' " +
    "| where tags['hidden-sentinelWorkspaceId'] =~
'/subscriptions/$SubscriptionId/resourcegroups/$resourceGroupName/providers/micro
soft.operationalinsights/workspaces/$workspaceName' " +
```

```
    "| extend version = name | extend parsed_version = parse_version(version)  "
+
    "| extend content_kind = tags['hidden-sentinelContentType'] " +
    "| extend resources =
parse_json(parse_json(parse_json(properties).template).resources)  " +
    "| extend metadata = parse_json(resources[array_length(resources)-
1].properties) " +
    "| extend contentId=tostring(metadata.contentId) " +
    "| where metadata.source.sourceId == '$contentId'  " +
    "| extend resource = parse_json(resources[0].properties)  " +
    "| extend displayName = case(content_kind == `"DataConnector`",
resource.connectorUiConfig['title'], content_kind == `"Playbook`",
properties['template']['metadata']['title'] , resource.displayName)  " +
    "| where content_kind in ('Workbook', 'AnalyticsRule', 'DataConnector',
'Playbook', 'Parser', 'HuntingQuery')  " +
    "| extend additional_data = case(content_kind == 'Parser',
resource['functionAlias'], '')  " +
    "| summarize arg_max(id, parsed_version, version, displayName, content_kind,
properties, additional_data) by contentId, tostring(content_kind) " +
    "| project id, contentId, version, displayName, content_kind,
additional_data"
}
$url =
"https://management.azure.com/providers/Microsoft.ResourceGraph/resources?api-
version=2019-04-01"
$singleSolutionTemplates = Invoke-RestMethod -Uri $url -Method POST -Headers
$authHeader -Body ($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
foreach ($row in $singleSolutionTemplates.data.rows) {
    switch ($row[4]) {
        #do what you want with the resources
    }
}
```

Below is the entire code in one place.

```
$url = $baseUrl + "contentProductPackages" + $apiVersion
$allSolutions = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader
).value
$solutions = $allSolutions | Where-Object { $null -ne
$_.properties.installedVersion }
foreach ($solution in $solutions | Sort-Object { $_.properties.displayName }) {
    if ($solution.properties.contentKind -eq "StandAlone") {
        switch ($solution.properties.dependencies.criteria.kind) {
            #Do what you want with the resources
        }
    }
```

```
    else {
        $contentId = $solution.properties.contentId
        #try to load using the new way.
        $url = $baseUrl + "contentTemplates" + $apiVersion
        $url +=
"&%24filter=(properties%2FpackageId%20eq%20'$contentId')%20and%20" +
        "(properties%2FcontentKind%20eq%20'AnalyticsRule'%20or%20properties%2Fcon
tentKind%20eq%20'DataConnector'%20or%20properties" +
        "%2FcontentKind%20eq%20'HuntingQuery'%20or%20properties%2FcontentKind%20e
q%20'Playbook'%20or%20properties%2FcontentKind" +
        "%20eq%20'Workbook'%20or%20properties%2FcontentKind%20eq%20'Parser')"
        $singleSolutionTemplates = (Invoke-RestMethod -Method "Get" -Uri $url -
Headers $authHeader ).value
        if ("" -eq $singleSolutionTemplates) {
            $body = @{
                "subscriptions" = @(
                    "$SubscriptionId"
                )
                "query"         = "Resources | where type =~
'Microsoft.Resources/templateSpecs/versions' " +
                "| where tags['hidden-sentinelWorkspaceId'] =~
'/subscriptions/$SubscriptionId/resourcegroups/$resourceGroupName/providers/micro
soft.operationalinsights/workspaces/$workspaceName' " +
                "| extend version = name | extend parsed_version =
parse_version(version)  " +
                "| extend content_kind = tags['hidden-sentinelContentType'] " +
                "| extend resources =
parse_json(parse_json(parse_json(properties).template).resources)  " +
                "| extend metadata =
parse_json(resources[array_length(resources)-1].properties) " +
                "| extend contentId=tostring(metadata.contentId) " +
                "| where metadata.source.sourceId == '$contentId'  " +
                "| extend resource = parse_json(resources[0].properties)  " +
                "| extend displayName = case(content_kind == `"DataConnector`",
resource.connectorUiConfig['title'], content_kind == `"Playbook`",
properties['template']['metadata']['title'] , resource.displayName)  " +
                "| where content_kind in ('Workbook', 'AnalyticsRule',
'DataConnector', 'Playbook', 'Parser', 'HuntingQuery')  " +
                "| extend additional_data = case(content_kind == 'Parser',
resource['functionAlias'], '')  " +
                "| summarize arg_max(id, parsed_version, version, displayName,
content_kind, properties, additional_data) by contentId, tostring(content_kind) "
+
                "| project id, contentId, version, displayName, content_kind,
additional_data"
```

```
            }
            $url =
"https://management.azure.com/providers/Microsoft.ResourceGraph/resources?api-
version=2019-04-01"
            $singleSolutionTemplates = Invoke-RestMethod -Uri $url -Method POST -
Headers $authHeader -Body ($body | ConvertTo-Json -EnumsAsStrings -Depth 50)
            foreach ($row in $singleSolutionTemplates.data.rows) {
                switch ($row[4]) {
                    #do what you want with the resources
                }
            }
        }
        else {
            #Do what you want with the resources
        }
    }
```

Install a solution

While there are REST APIs to handle solutions, the one to actually install the solutions does not work. Because of that, the code below is used to install a solution.

In the code below "$Solutions" will contain an array of the solution names to be deployed. Make sure that the entries being passed in match the "displayName" of the solution.

```
$url = $baseUri + "contentProductPackages" + $apiVersion
$allSolutions = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader
).value
foreach ($deploySolution in $Solutions) {
    $singleSolution = $allSolutions | Where-Object { $_.properties.displayName -
Contains $deploySolution }
    if ($null -eq $singleSolution) {
        Write-Error "Unable to get find solution with name $deploySolution"
    }
    else {
        $solutionURL = $baseUri +
"/providers/Microsoft.SecurityInsights/contentProductPackages/$($singleSolution.n
ame)?api-version=2023-04-01-preview"
        $solution = (Invoke-RestMethod -Method "Get" -Uri $solutionURL -Headers
$authHeader )
        $packagedContent = $solution.properties.packagedContent
        #Some of the post deployment instruction contains invalid characters and
since this is not displayed anywhere
        #get rid of them.
        foreach ($resource in $packagedContent.resources) {
            if ($null -ne
$resource.properties.mainTemplate.metadata.postDeployment ) {
```

```
                $resource.properties.mainTemplate.metadata.postDeployment = $null
            }
        }
        $installBody = @{"properties" = @{
                "parameters" = @{
                    "workspace"          = @{"value" = $Workspace }
                    "workspace-location" = @{"value" = $Region }
                }
                "template"   = $packagedContent
                "mode"       = "Incremental"
            }
        }
        $deploymentName = ("allinone-" + $solution.name)
        if ($deploymentName.Length -ge 64){
            $deploymentName = $deploymentName.Substring(0,64)
        }
        $installURL =
"https://management.azure.com/subscriptions/$($SubscriptionId)/resourcegroups/$($
ResourceGroup)/providers/Microsoft.Resources/deployments/" + $deploymentName +
"?api-version=2021-04-01"
        try{
            Invoke-RestMethod -Uri $installURL -Method Put -Headers $authHeader -
Body ($installBody | ConvertTo-Json -EnumsAsStrings -Depth 50 -EscapeHandling
EscapeNonAscii)
        }
        catch {
            $errorReturn = $_
            Write-Error $errorReturn
        }
    }
}
```