Programming Microsoft Sentinel using the REST APIs

By: 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.

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
     }

$subscriptionId = (Get-AzContext).Subscription.Id
```

"$subscriptionId" was added at the end since it will be needed for the calls, as you will see later.

Once you have this information, you 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 workspacename. 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.

```
$url="https://management.azure.com/subscriptions/$subscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/contentProductPackages?api-version=2023-04-01-preview"
$results = (Invoke-RestMethod -Method "Get" -Uri $url -Headers $authHeader )
```

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 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 “2023-07-01-preview”. This version will be updated almost monthly.

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 of 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.

Stable APIs

The stable APIs are the ones that have been thoroughly tested and are ready for general use. This does not mean that the preview APIs are not ready, just that they have not been thoroughly tested yet.

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!

Actions

This API is to set actions to an 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

```
$url="https://management.azure.com/subscriptions/$subscriptionId)/resourceGroups/$resourceGroupName)/providers/Microsoft.OperationalInsights/workspaces/$workspaceName)/providers/Microsoft.SecurityInsights//alertRuleTemplates/968358d6-6af8-49bb-aaa4-187b3067fb95?api-version=2023-02-01"
$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": {
```

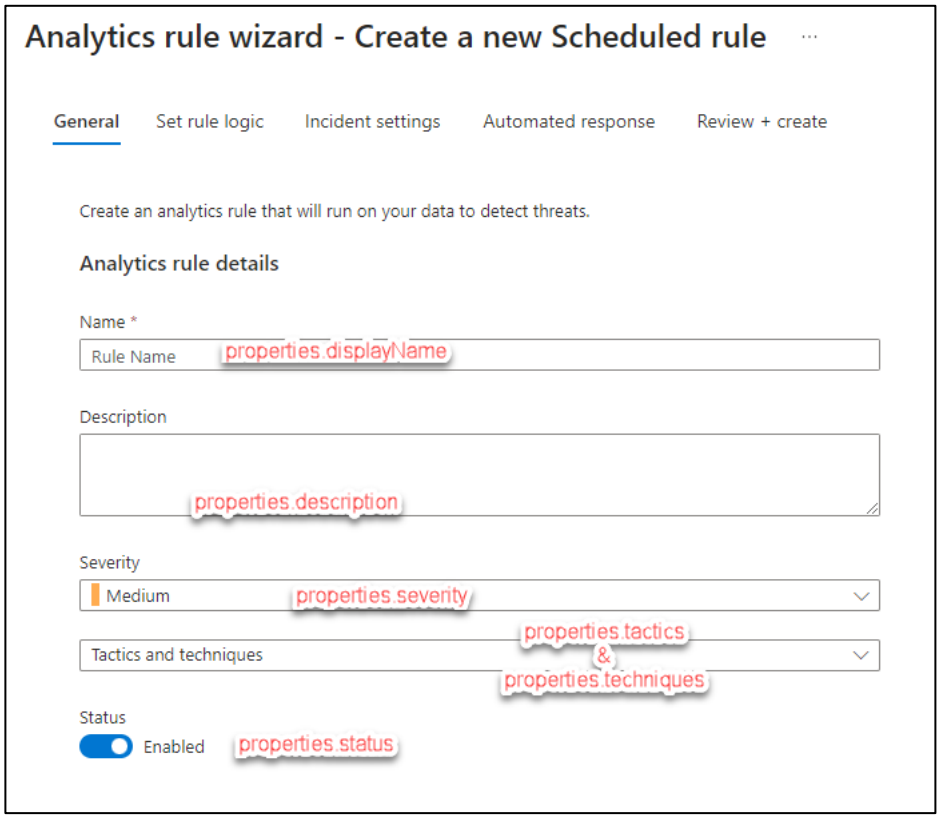
```
      "queryFrequency": "PT12H",
      "queryPeriod": "PT12H",
      "triggerOperator": "GreaterThan",
      "triggerThreshold": 0,
      "severity": "High",
      "query": "let successCodes = dynamic([200, 302, 401]);\nW3CIISLog\n| where
scStatus has_any (successCodes)\n| where ipv4_is_private(cIP) == 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
    }
  }
```

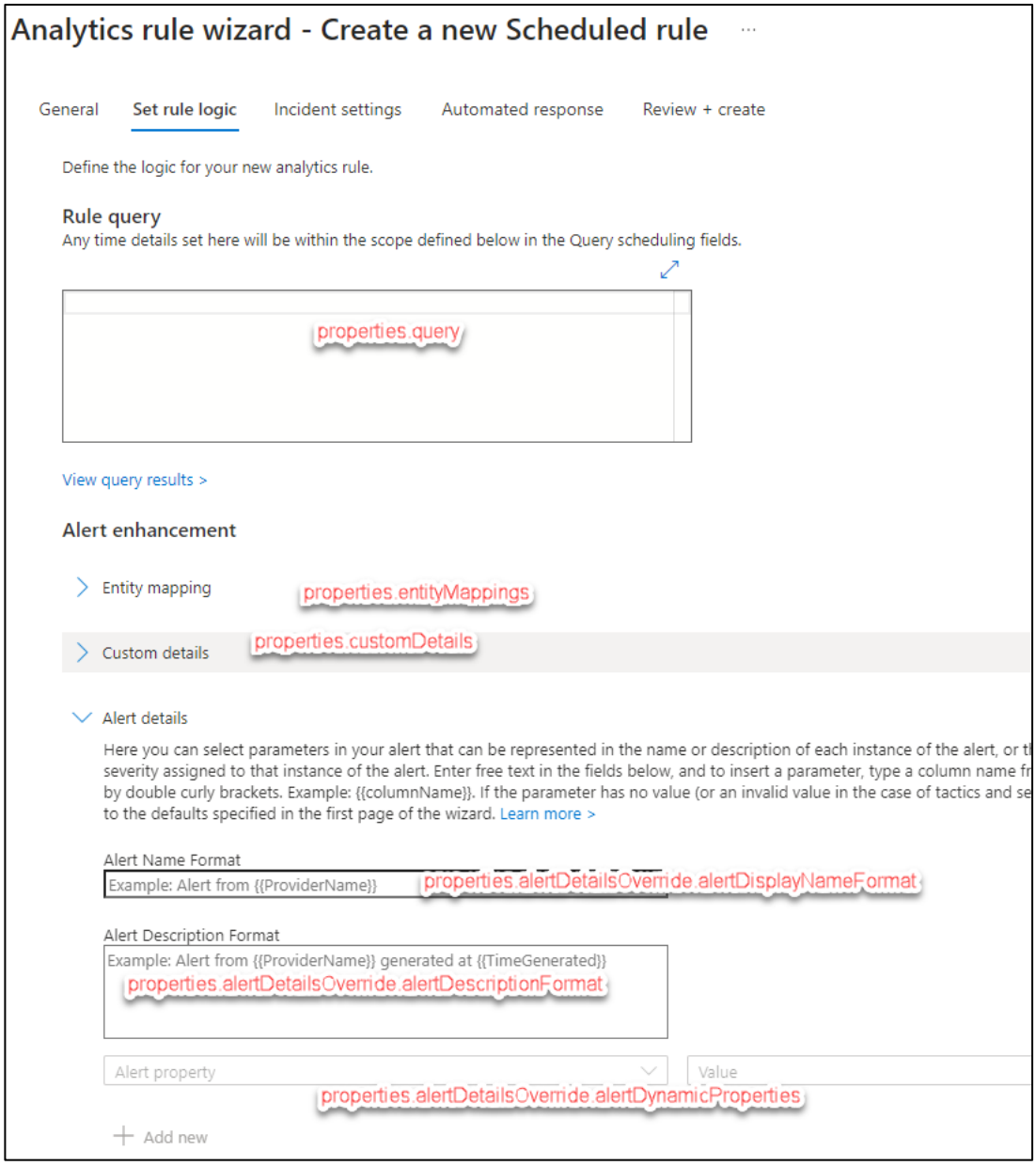

Scheduled Rule Mapping

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

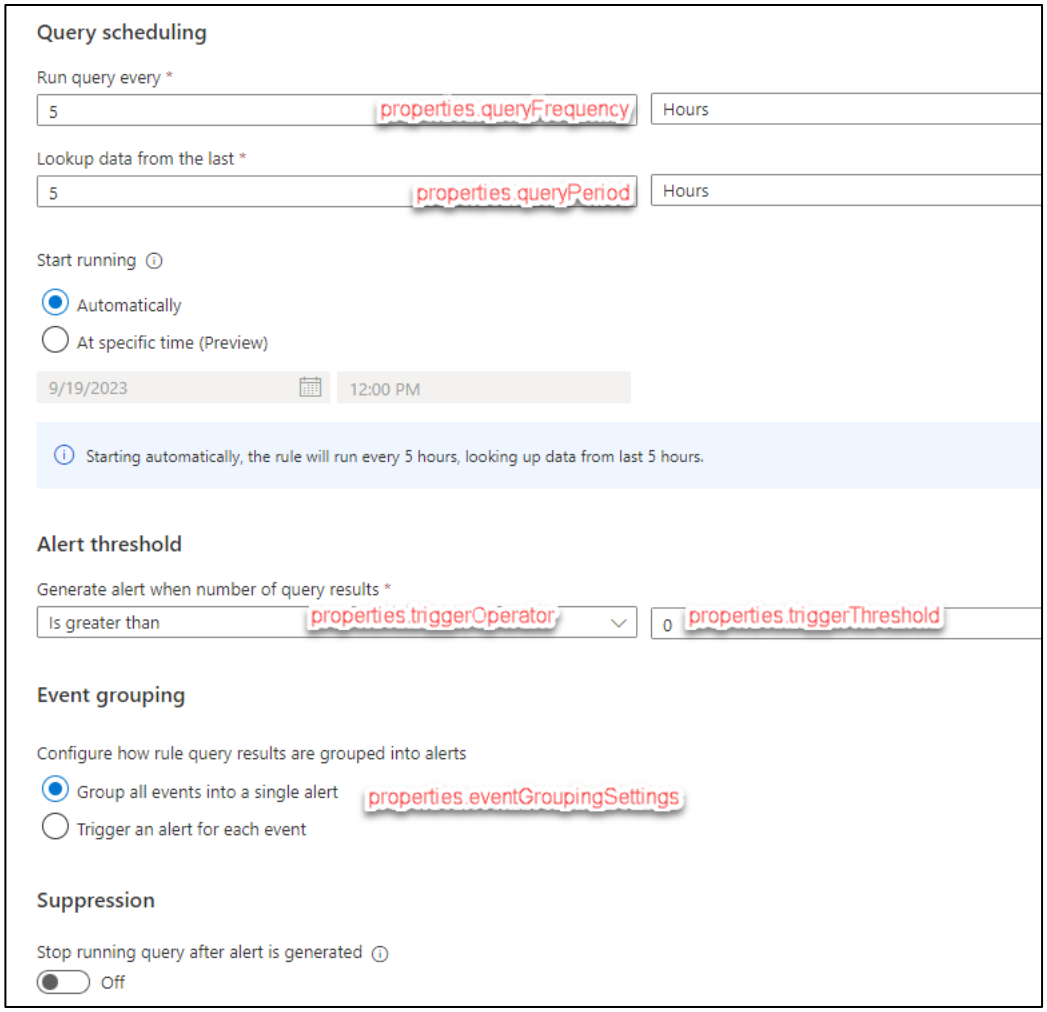


Set rule logic (top part of the page)



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.

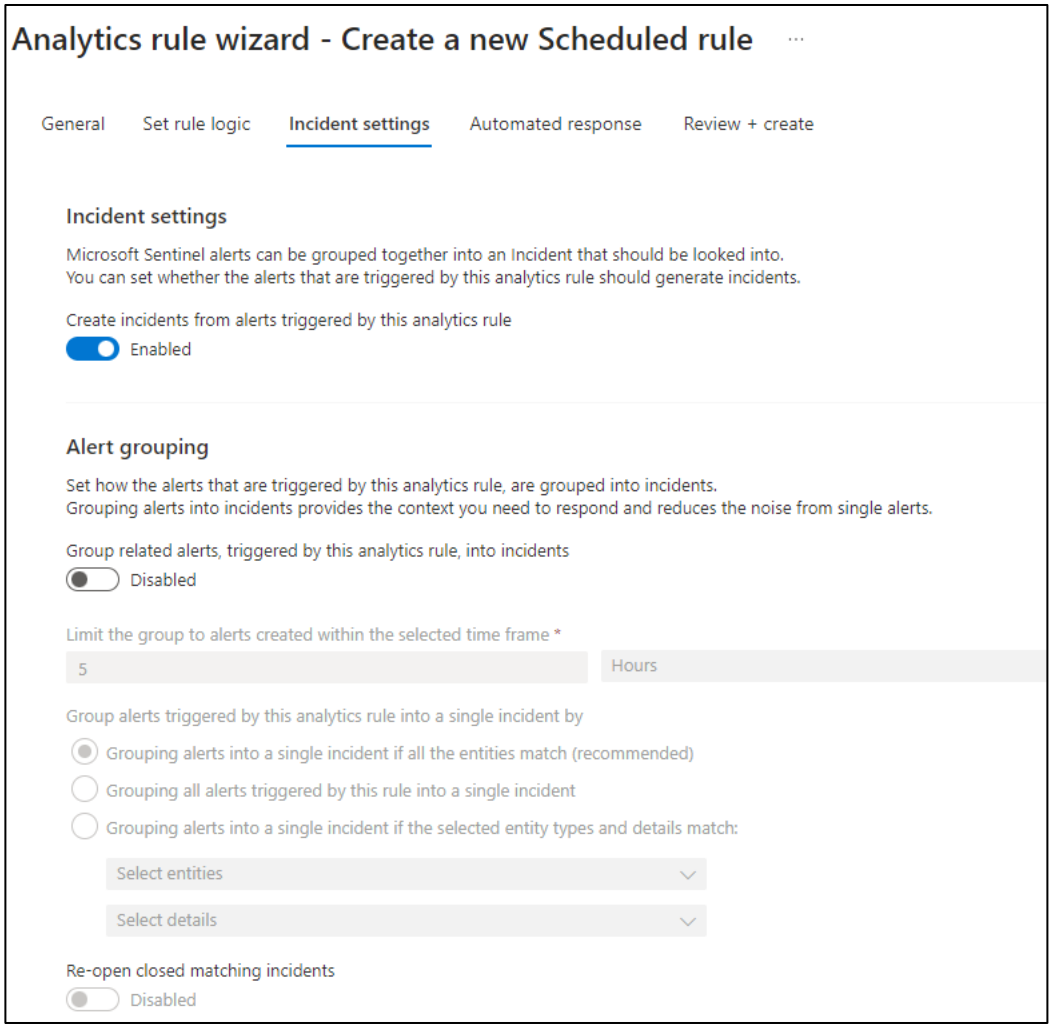
Set rule logic (bottom part of the page)



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.

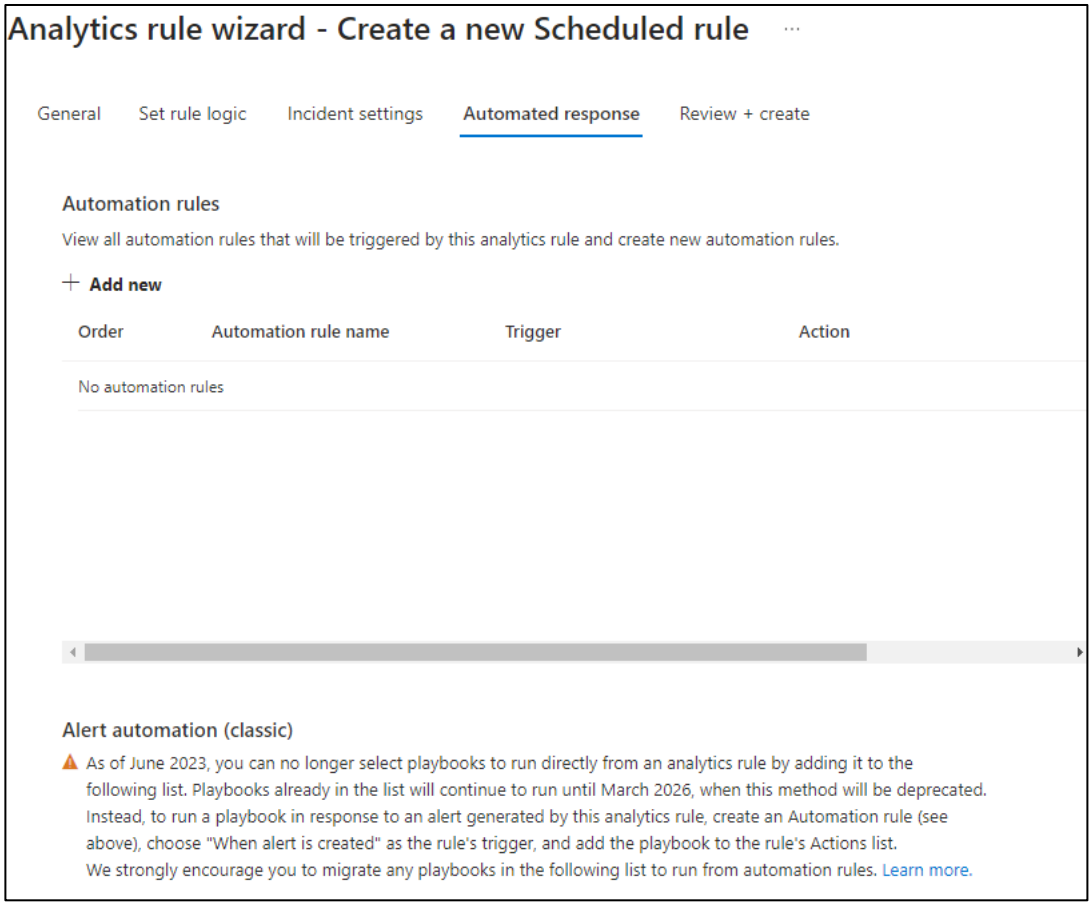
There is also no support in the template for alert suppression.

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)

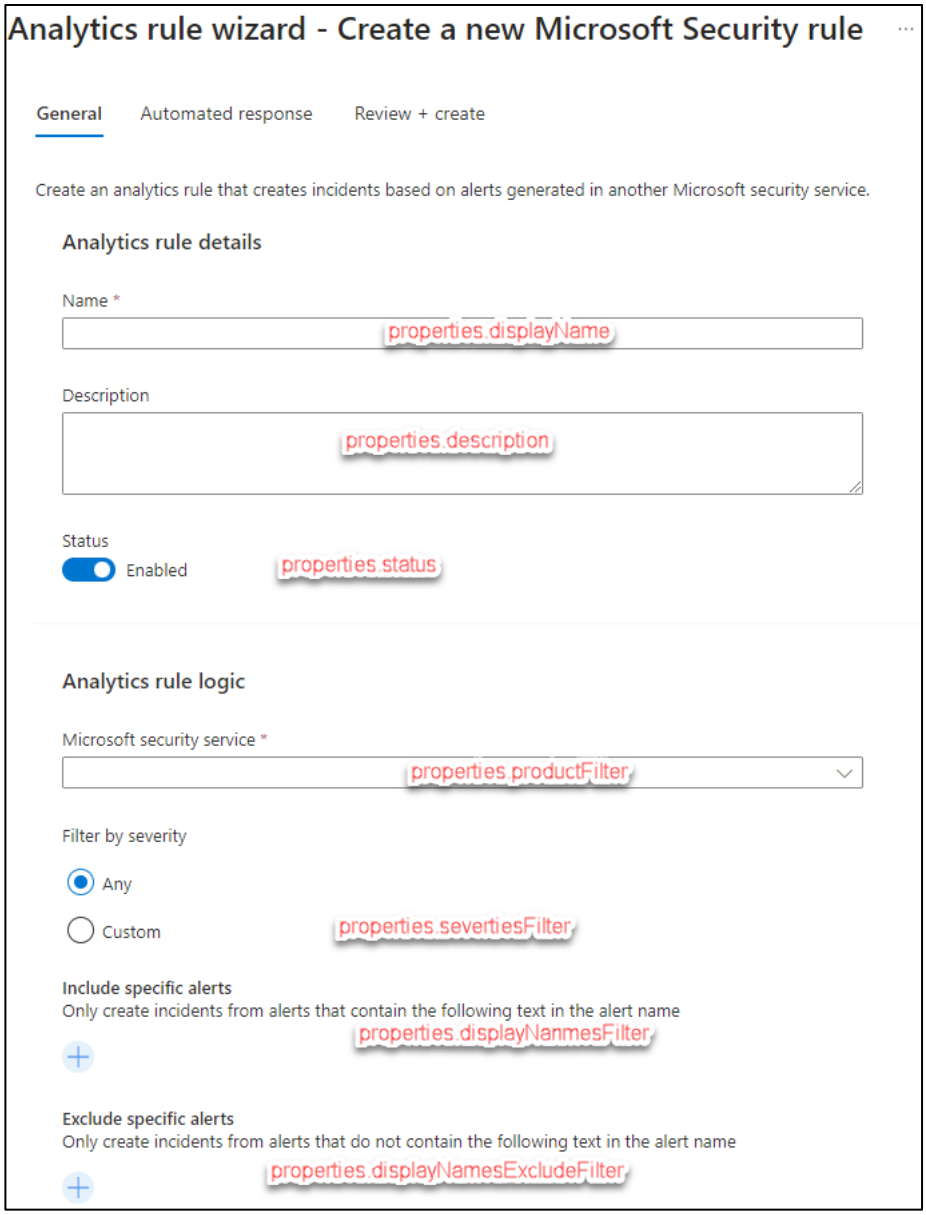
NRT

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.

```
$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.

So that will create the actual rule, however, it does not map back to the solution, so that we can see if there is an update. There is another call that you must make to do that. Note that you cannot do this if you used the Rule Templates REST API that was described above. 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.

HTTP Method: PUT

REST API URL:

https://management.azure.com/subscriptions/**{subscriptionId}**/resourceGroups/**{resourceGroupName}**/providers/Microsoft.OperationalInsights/workspaces/**{workspaceName}**/providers/Microsoft.SecurityInsights/metadata/analyticsrule-{$verdict.name}?api-version=2022-01-01-preview

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.

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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId)/resourceGroups/
$resourceGroupName)/providers/Microsoft.OperationalInsights/workspaces/$workspace
Name/providers/Microsoft.SecurityInsights/alertRules/99ce9db5-41b3-4cf9-b909-
d408e21f277d?api-version=2023-02-01"
$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

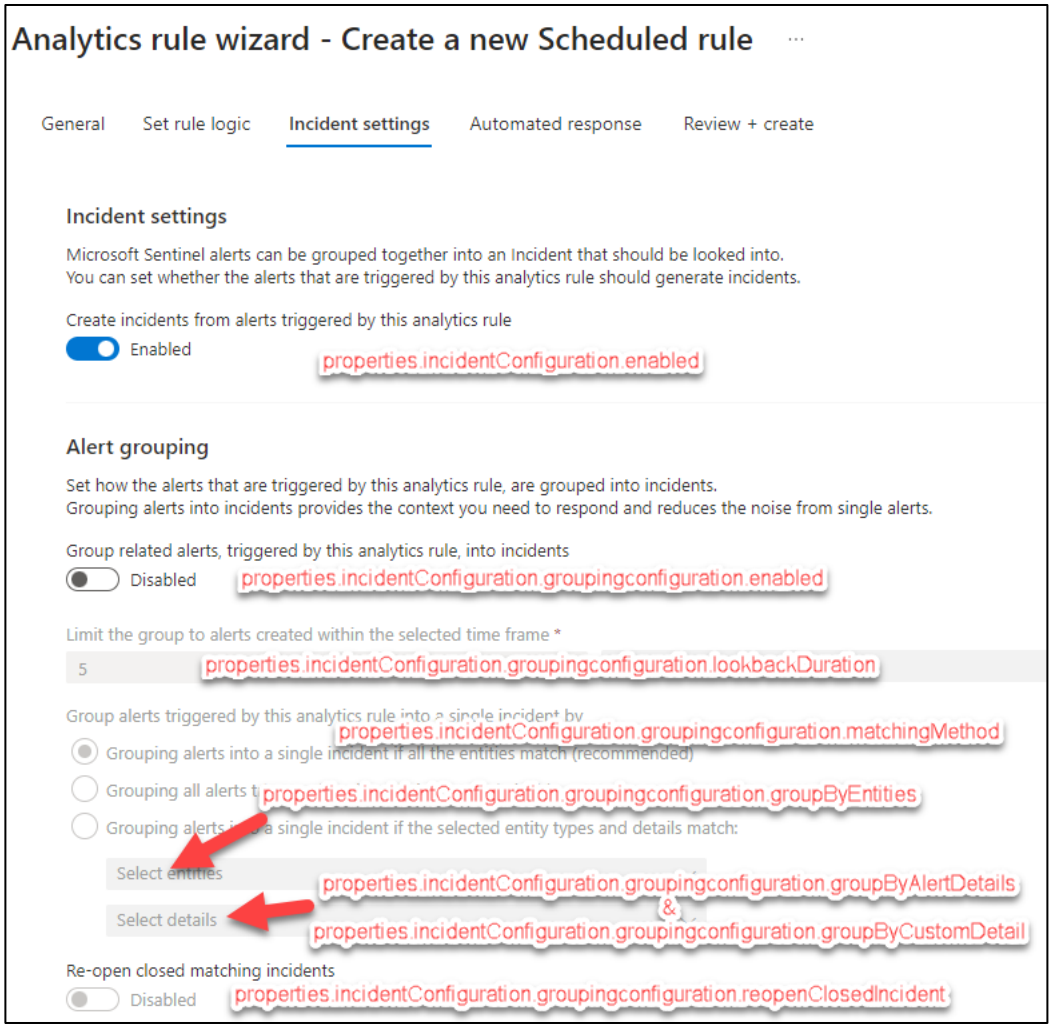

```
{
    "id": "/subscriptions/34bdcce3-c06f-416b-aaa0-
24683117cc68/resourceGroups/devbookrg/providers/Microsoft.OperationalInsights/wor
kspaces/devbookwg/providers/Microsoft.SecurityInsights/alertRules/99ce9db5-41b3-
4cf9-b909-d408e21f277d",
    "name": "99ce9db5-41b3-4cf9-b909-d408e21f277d",
    "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"

                }
            }
```

```
        )
    }
}
$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

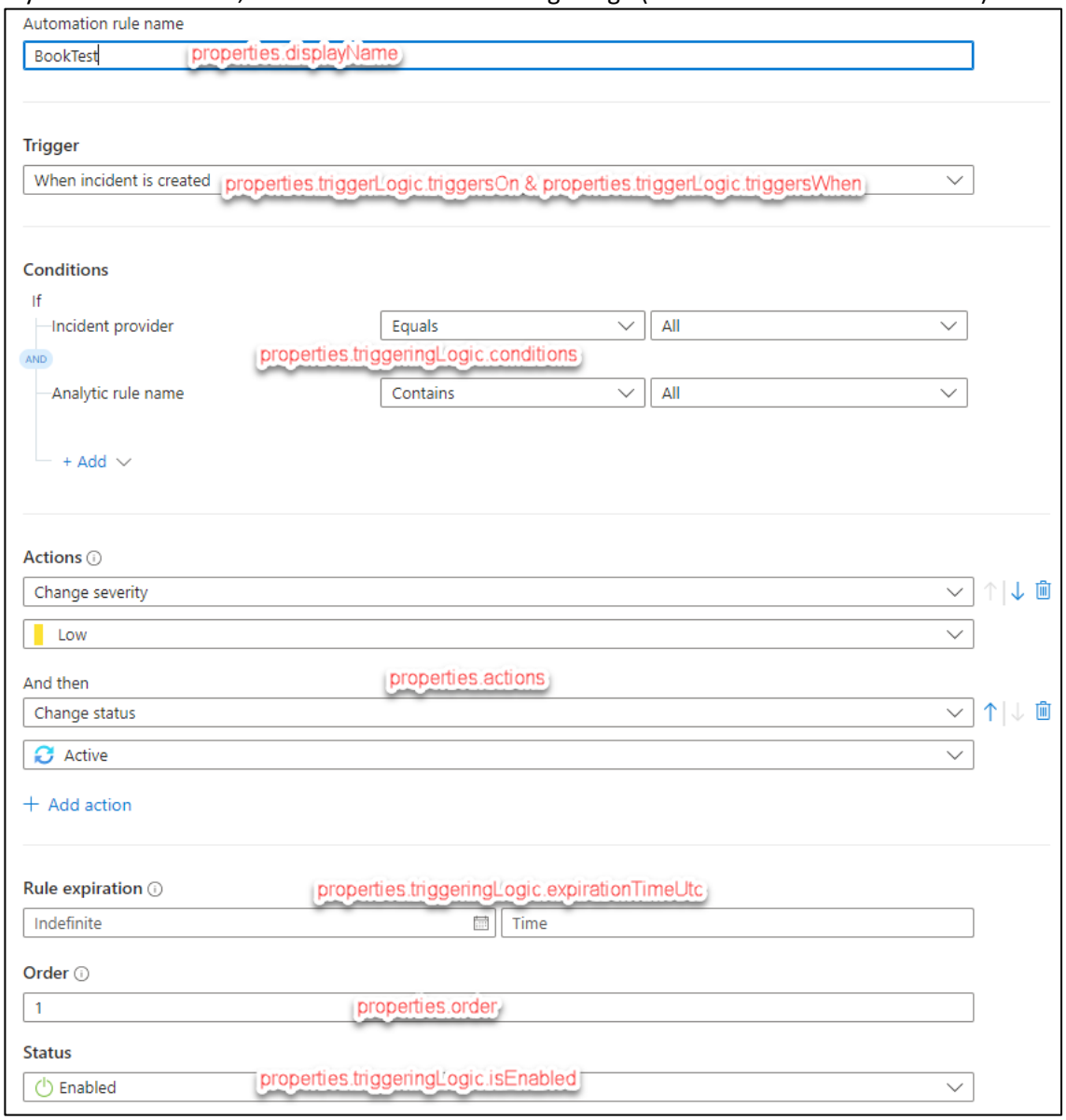
Sample response


```
{
    "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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/automationRules/7d46439e-e8b4-41f9-b71f-7ad1399cad05?api-version=2023-02-01"

$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"
        }
    }
}
```

```
$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

```
$url="https://management.azure.com/subscriptions/$subscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/bookmarks/479f1d9a-6771-466f-918e-d78a71a0078f?api-version=2023-02-01"
$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/479f1d9a-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

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>"
    }
}
$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

```
$url="https://management.azure.com/subscriptions/$subscriptionId/resourceGroups/$
resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceNa
me/providers/Microsoft.SecurityInsights/incidents/a60ef091-61ae-4e4c-aabf-
7423c33318c3/comments/4e280bb6-91bd-46e9-b2a6-f983f8287821?api-version=2023-02-
01"
$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}**

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"
    }
}
$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

```
$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"
    }
}
$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/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}**

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

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"
```

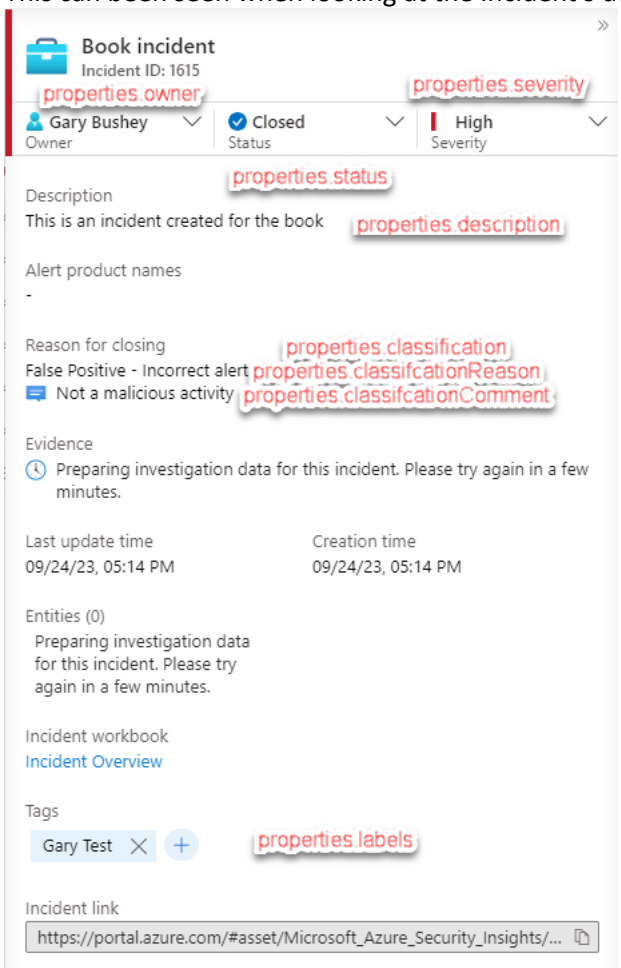
```
    }
}
```

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 been 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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4?api-version=2023-02-01"
$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",
  "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}**

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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/alerts?api-version=2023-02-01"
$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}**/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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$
resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceNa
me/providers/Microsoft.SecurityInsights/incidents/7752c995-4e1c-d0a1-3d07-
f3c90ca48bf4/bookmarks?api-version=2023-02-01
$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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/incidents/7752c995-4e1c-d0a1-3d07-f3c90ca48bf4/entities?api-version=2023-02-01"
$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/41c57cd2-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/7e11e76f-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"
    }
```

```
  }
]
```

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 we have seen this call in action when creating an Analytic Rule (it was the second call that was made after the rule was defined to map the Analytic Rule to the Solution).

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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/metadata/analyticsrule-f32ad97a-b6a7-4be9-84ea-cd7ca448fb6c?api-version=2023-02-01"
```

```
$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}**

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
    }
}
$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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/securityMLAnalyticsSettings/2fd3b6aa-0aec-40c6-8f3c-a647cc97e934?api-version=2022-11-01-preview"
$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
    }
}
$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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/onboardingStates/default?api-version=2022-11-01-preview"
$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/onboardingStates/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"
    )
}
$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/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"
    }
}
$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": "\"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"         = ""
    }
}
$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/threatIntelligence/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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/threatIntelligence/main/indicators/2d86220d-2772-885c-733f-5cc62798fb72?api-version=2023-02-01"
$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"
        }
    )
}
$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"
        )
    }
}
$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": "\"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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights/threatIntelligence/main/metrics?api-version=2023-02-01"
$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 group.

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}**

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.

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"     = ""
        }
    }
}
$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": {}
  }
}
```


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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights//watchlists/SolutionData/watchlistitems/fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13?api-version=2023-02-01"
$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}**

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

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" = "testingforbook"
        "displayName"= "booktest"
        "sourceType" = "Local"
        "contentType"= "Text/Csv"
        "source"= "Network Addresses.csv"
        "description"= "Just a simple test for the book"
        "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"
    }
}
$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": {}
    }
  }
```


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>
  }
}
$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"
  }
}
```


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

```
$url="https://management.azure.com/subscriptions/$SubscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.OperationalInsights/workspaces/$workspaceName/providers/Microsoft.SecurityInsights//watchlists/SolutionData/watchlistitems/fe77ad22-62c6-4f8f-b3ec-1c81e5ee3e13?api-version=2023-02-01"
$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/Solu
tionData/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}**

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