

Playbook - Send email when a Sentinel Automation rule is created

Last updated by | Paulo Santana | Mar 24, 2023 at 2:29 PM CDT


Contents

- [Playbook - Send email when a Sentinel Automation rule is ...](#)
 - [Description](#)
 - [Requirements](#)
 - [Instructions](#)
 - [Testing](#)

Playbook - Send email when a Sentinel Automation rule is created

Description

This article outlines the procedure for creating a playbook in Microsoft Sentinel to send an email upon the creation of an automation rule.

We will use a Sentinel Analytic Rule to query the Azure Activity logs table for an Automation rule created in the last 5 minutes. Because the query will return only an Automation rule ID, we will use the [Automations - Get](#)  API to get the Automation rule name and send an email with this information.

Requirements




- ☒ Azure Activity Logs data connector enabled.

Instructions

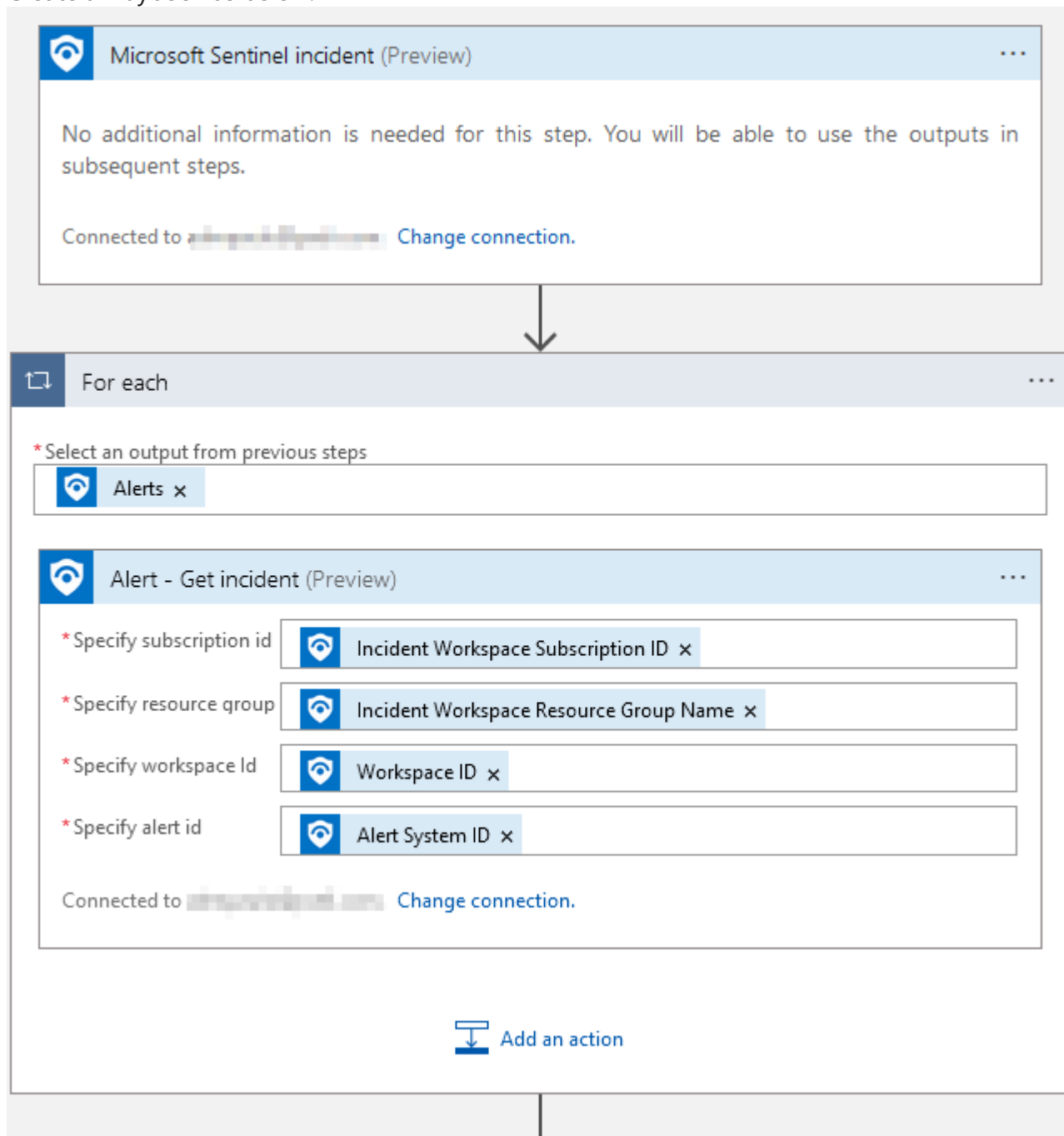
1. Enable Azure Activity Logs data connector in Sentinel.
2. Create a Sentinel Analytics rule to generate an incident when an Automation rule is created with the query below:

```
AzureActivity | where OperationNameValue == "MICROSOFT.SECURITYINSIGHTS/AUTOMATIONRULES/WRITE" | where ActivityStatusValue == "Success" | where ActivitySubstatusValue == "Created" | extend automationRuleId = substring(split(_ResourceId, '/')[12], 0, 36)
```

3. In the Analytics Rule, under entities, map **File Hash** with **automationRuleId**

Analytics rule details	
Name	PS-AutomationRuleCreated
Description	
Tactics and techniques	 Impact
Severity	 Medium
Status	 Enabled
Analytics rule settings	
Rule query	AzureActivity where OperationNameValue == "MICROSOFT.SECURITYINSIGHTS/AUTOMATIONRULES/WRITE" where ActivityStatusValue == "Success" where ActivitySubstatusValue == "Created" extend automationRuleId = substring(split(_ResourceId, '/')[12], 0, 36)
Rule frequency	Run query every 5 minutes
Rule period	Last 5 minutes data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns more than 0 results
Event grouping	Group all events into a single alert
Suppression	Not configured
Entity mapping	
Entity 1:	FileHash Identifier: Value, Value: automationRuleId

4. Create a Playbook as below:



Entities - Get FileHashes (Preview) ...

* Entities list Entities x

Connected to ██████████ [Change connection.](#)

For each 3 ...

* Select an output from previous steps

FileHashes x

HTTP ...

* Method GET

* URI

`https://management.azure.com/subscriptions/
Incident Workspace Subscription ID x /resourceGroups/
Incident Workspace Resource Group Name x /providers
/Microsoft.Operationallnsights/workspaces/
Incident Workspace Workspace Name x /providers
/Microsoft.SecurityInsights/automationRules/FileHashes Value x ?api-
version=2022-11-01`

Headers



Enter key	Enter value	
-----------	-------------	--

Queries

Enter key	Enter value	
-----------	-------------	--

Body

Cookie



Authentication  

* Authentication type

* Managed identity

Audience



 Parse JSON 

* Content  Body x

* Schema

```
},
  "required": [
    "order",
    "actionType",
    "actionConfiguration"
  ],
  "type": "object"
},
"type": "array"
```

[Use sample payload to generate schema](#)

Click here and paste a sample output from the API call to generate a schema.



Send an email (V2)

* Body

Font 12 B I U [Rich Text Editor Icons]

Automation rule { } displayName x was created by { } name x on { } createdTimeUtc x

* Subject

Automation Rule Created

* To

paulosantana@microsoft.com

Add new parameter

Connected to [Connection Name] Change connection.

Add an action

5. Attach this playbook to the Analytic rule created in step 2.
6. Done.

Testing

Action: Create a new automation rule.

Expected Result: After approx. 5 minutes, an email will be sent with the information below:

Subject: [EXTERNAL] Automation Rule Created

Importance: Low

Automation rule AR-RunPlaybook-SentEmail was created by Paulo Santana on 2023-03-23T22:21:38Z

Contributor Name	Details	Date
Paulo Santana	Created this section	2023-03-24