



1ST EDITION

Security Orchestration, Automation, and Response for Security Analysts

Learn the secrets of SOAR to improve MTTA and MTTR and strengthen your organization's security posture



BENJAMIN KOVACEVIC

Foreword by Nicholas DiCola, Vice President of Customers, Zero Networks

Security Orchestration, Automation, and Response for Security Analysts

Learn the secrets of SOAR to improve MTTA and MTTR and strengthen your organization's security posture

Benjamin Kovacevic



BIRMINGHAM-MUMBAI

Security Orchestration, Automation, and Response for Security Analysts

Copyright © 2023 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Group Product Manager: Pavan Ramchandani Publishing Product Manager: Prachi Sawant Senior Editor: Athikho Sapuni Rishana Technical Editor: Arjun Varma Copy Editor: Safis Editing Project Coordinator: Ashwin Kharwa Proofreader: Safis Editing Indexer: Hemangini Bari Production Designer: Nilesh Mohite Marketing Coordinator: Shruthi Shetty, Marylou De Mello Business Development Executive: Prathamesh Walse

First published: July 2023 Production reference: 1230623

Published by Packt Publishing Ltd. Livery Place 35 Livery Street Birmingham B3 2PB, UK.

978-1-80324-291-0 www.packtpub.com

Contributors

About the author

Benjamin Kovacevic is a cybersecurity enthusiast with hands-on experience with Microsoft XDR and SIEM platforms. Currently working with Microsoft Sentinel as a product manager, he focuses on the SOAR component of Microsoft Sentinel and works on new capabilities that help SOCs improve their investigations and responses. Benjamin constantly works to improve his knowledge about cybersecurity and also shares his knowledge about Microsoft SOAR. He is the author of Microsoft Sentinel Automation training blog, as well as many other blog posts containing tips and tricks to get started quickly with Microsoft Sentinel Automation.

Benjamin is originally from Bosnia and Herzegovina, but he currently resides in Ireland with his wife and two sons.

I want to thank my wife, Dzenana, and my sons, Adi and Mak. Thank you for all the sacrifices you have made and for supporting me through this journey. Also, a big thanks to all the people who have made a big impact on my security journey!

5 Introducing Microsoft Sentinel Automation

In the previous chapter, we introduced a few SOAR tools and some of the main features we can utilize in our day-to-day operations. We showcased what incident management, investigation, automation, and reporting look like in real tools and offered some directions on how to utilize them.

This chapter will focus on Microsoft Sentinel automation, and we will dive deep into each element when working with it. We will discuss automation rules, playbooks, their elements and permissions, and prepare you for hands-on examples that will be covered in *Chapters 6* to 8.

In this chapter, we will discuss the following:

- The purpose of Microsoft Sentinel automation
- All about automation rules
- All about playbooks
- Monitoring automation rules and playbook health

The purpose of Microsoft Sentinel automation

Microsoft Sentinel automation's purpose, like the purpose of all automation, is to take repetitive tasks and transform them into automated tasks. In the SOC, some of the topics automation focuses on are as follows:

• **Enrichment**: When an incident is created, we want to enrich it with additional data. This will save SOC analysts time as they will have this enrichment as soon as they pick up the incident. For example, when an incident with an IP address is created, we can run an automatic playbook to enrich the incident with TI data about whether the IP is known to be malicious or not.

- **Initial triage and incident suppression**: This accompanies enrichment as we can utilize the results of that to decide whether we want to auto-close an incident if the IP is internal and behavior is expected, or transfer it to tier 2 if the IP address is known to be malicious.
- Orchestration: This is more oriented to orchestrating incident assignments or notifying SOC analysts that an incident has been created or assigned to them. For example, we can create automation that will send a Microsoft Teams chat message to the user using adaptive cards on incident creation, from where we can utilize SOC analyst input to even auto-close incidents if the information that's shared warrants making that decision.
- **Response**: SOC analysts used to struggle when they needed to block an IP address, isolate a machine, block a user or reset their password, and so on. Because SOC analysts wouldn't usually have permission to access a firewall, active directory, or EDR solution, they would need to raise an internal ticket or ping the network or system administrator to help out. By running a playbook, that task can be done for them automatically. This is crucial for many modern threats, where the time it takes to contain the threat must be minimal.

To perform any of the preceding tasks, Microsoft Sentinel uses two different automation methods:

- Automation rules: These are used to manage automation in Microsoft Sentinel centrally. Automation rules contains triggers, conditions, and actions that dictate how an automation rule will respond. In the next section, *All about automation rules*, we will dive deep into this feature.
- **Playbooks**: Playbooks are a list of actions that will be performed on an incident. This can include enrichment, response, remediation, and much more. We will cover playbooks in more detail later, in the *All about playbooks* section.

All about automation rules

As mentioned previously, automation rules can be created to manage automation in Microsoft Sentinel centrally. But how can we do that?

Automation rules in Microsoft Sentinel have three main aspects:

- Triggers
- Conditions
- Actions

Automation rules are sorted in order, which is a critical element since all automation rules will run from the lowest order number (for example, 1) to the highest (for example, 55), and they will run sequentially.

However, before we go into more detail about triggers, conditions, and actions, let's familiarize ourselves with the **graphical user interface** (**GUI**) of Microsoft Sentinel automation rules and learn more about permissions.

Navigating the automation rule GUI

Microsoft Sentinel automation rules are located under the **Automation** tab in the **Automation rules** sub-menu. In this menu, we have the option to create an automation rule, edit an automation rule, enable or disable an automation rule, move it up or down, remove an automation rule, as well as filter automation rules by analytic rules, actions, triggers, statuses, who created them, and when they were last modified.

	+ 0	eate 🗸	🕐 Refresh 🕴 🧷 Edit 🕚	Enable =1 Move up =4 Mo	we down 🔋 Remove	🖗 Guides & Feedback				
General		2	4. 2							
Overview	Autom) ation rules	Enabled rules	[음] 111 Enabled playbooks	Conten	it hub				
P Logs										
News & guides	Auto	mation ru	les Active playbooks Pl	aybook templates (Preview)						
D Search										
Threat management	1× 56	arch		Analytic rules : All	Actions : All Creat	ed by : All Last more	atted by : All	tatus : All Trigge	er : All	
a Incidents		Order	Display name	Trigger	Analytic rule nam	Actions	Expiration date	Created by	Rule creation time	Last
Workbooks		1	Initial investigation	Incident created	AJI	Run playbook 'Send	Indefinite	Benji Kovacevic	12/02/2022, 18:44:53	Ben
D Hunting		2	When incident is updated	👸 Incident updated (Preview)	All	Change status, Assi	Indefinite	Benji Kovacevic	28/02/2022, 11:51:09	Ber
Notebooks		3	When incident is reopened	👸 Incident updated (Preview)	ILA	Run playbook 'Noti	Indefinite	Benji Kovacevic	16/05/2022, 11:56:13	Ber
Entity behavior		4	When incident severity chan	ncident updated (Preview)	ILA	Run playbook 'Noti	Indefinite	Benji Kovacevic	16/05/2022, 11:57:16	Ber
3 Threat intelligence		4	When incident is closed	🚯 Incident updated (Preview)	All	Run playbook 'Noti	Indefinite	Benji Kovacevic	16/05/2022, 13:57:04	Ben
MITRE ATT&CK (Preview)		5	Sync comments to M365D	🚯 Incident updated (Preview)	All	Run playbook 'Sync	Indefinite	Benji Kovacevic	17/05/2022, 12:50:14	Ber
Content management										
Content hub (Preview)										
Repositories (Preview)										
Community										
onfiguration										
Data connectors										
Analytics										
and the second se		_								

Figure 5.1 – Microsoft Sentinel automation rules

$+$ Create \vee (💙 Refresh 🛛 🖉 Edit 🕚	Enable =↑ Move up =↓ Mov	ve down 볩 Remove 🎗	Guides & Feedback
Automation rule Playbook with inc Playbook with ale	ident trigger rt trigger	{문} 111 Enabled playbooks	More con Content	ntent at hub
Blank playbook	playbooks F	Playbook templates (Preview)		
		Analytic rules : All	Actions : All Created	d by : All Last mo
Order	Display name	Trigger	Analytic rule nam	Actions
Order 1	Display name	Trigger	Analytic rule nam	Actions Run playbook 'Send
Order 1 2	Display name Initial investigation When incident is updated	Trigger Incident created Total Incident updated (Preview)	Analytic rule nam All All	Actions Run playbook 'Send Change status, Assi
Order 1 2 3	Display name Initial investigation When incident is updated When incident is reopened	Trigger Incident created To Incident updated (Preview) To Incident updated (Preview)	Analytic rule nam All All All	Actions Run playbook 'Send Change status, Assi Run playbook 'Noti
 Order 1 2 3 4 	Display name Initial investigation When incident is updated When incident is reopened When incident severity chan.	Trigger Incident created Incident updated (Preview) Incident updated (Preview) Incident updated (Preview) Incident updated (Preview)	Analytic rule nam All All All All	Actions Run playbook 'Send Change status, Assi Run playbook 'Noti Run playbook 'Noti
 Order 1 2 3 4 4 	Display name Initial investigation When incident is updated When incident is reopened When incident severity chan. When incident is closed	Trigger Incident created Incident updated (Preview) Incident updated (Preview)	Analytic rule nam All All All All All All	Actions Run playbook 'Send Change status, Assi Run playbook 'Noti Run playbook 'Noti Run playbook 'Noti

We need to click on **Create** and select **Automation rule** to create an automation rule.

Figure 5.2 – Creating a new automation rule

From here, we must navigate to the **Create new automation rule** window; this is where we can start creating this new rule.

Automation rule name		
Trigger		
When incident is created		~
Conditions		
If		
—Analytic rule name	Contains V All	~
+ Add >/		
Actions ①		
		I
+ Add action		
Rule expiration ①		
Indefinite	Time	
Order ()		

Figure 5.3 – The Create new automation rule wizard

However, there are other ways to create or edit automation rules:

• When creating an analytic rule using the **Analytics rule wizard** area, under the **Automated response** tab, we can see what automation rules will be triggered when an incident is created. We can also create a new automation rule specific to this rule. We can choose between any trigger at this stage.

Home > Microsoft Sentinel And Analytics rule wizat Suspicious RDP activity Seneral Set rule logic Incide	nd - Edit existing scheduled rule	Create new automation rule × Automation rule name
Automation rules (Preview) View all automation rules that will	be triggered by this analytics rule and create new automation rules.	Trigger When incident is created
+ Add new Order	Automation rule name	Conditions
2	Initial investigation When incident is updated	Analytic rule name Contains Current rule + Add
3 4	When incident is reopened When incident severity changed	Actions O
4 5	When incident is closed Sync comments to M365D	+ Add action
✓ Alert automation (classic)		Rule expiration ① Indefinite Difference Time
		2
Previous Next : Review :		Apply Cancel

Figure 5.4 – Creating an automation rule when creating the analytic rule

• From the **Incidents** page, we can select an incident and, from the right menu, under **Actions**, select **Create automation rule**.

P Search ≪	+ Create incident (Pre	view) 🕐 Refresh 🕓	Last 24 hours 🗸 🞘 Actio	ns 📋 Delete 🛃 Sec	urity efficiency workboo	k 💷 Columns 🥀	Guides & Feedback			
eneral	- 1	250	01	Open incidents	by severity				100	
Overview	Open incidents	New incidents	Active incidents	High (1)	Media	m (0)	Elowr (0)	Informatio	nal (0)	
 Logs News & guides 	Search by ID, title, to	egs, owner or product	ରା Severity : All	Status : 2 selected		~ More (2)	RDP port scar	nning detected on	NebinarMach	ine
Search	Auto-refresh in	cidents					🚨 Benji Kova 🗸	C Active V	High	
nreat management	Severity †	Incident ID 14	Title ↑4	Alerts	Product names	Created time	Owner	Status	Severity	
Incidents	High	333	RDP port scanning	1	Microsoft Sentinel	11/02/22, 12:3-	Description Possible malicious PDE	out maning delarts	d on illiorteam	-11
Workbooks							Possible management	. Host scanning or over	a cu ll'estavani	w
Hunting							Alert product names Microsoft Sentinel			
Notebooks							Evidence			
Entity behavior							*1 01	R 2		
Threat intelligence							Events Alerts	Bookmarks		
MITRE ATT&CK (Preview)							La dillo	Construction of		
ntent management							11/18/22, 11:12 AM	11/02/22, 1	2:34 AM	
Content hub (Preview)							Entities (3)			
Repositories (Preview)							Benji Kovacevic WebinarMachi			
Community							20.232.133.192 View full details >			
figuration							lactic			
Data connectors							 S Investigat 	te		
Analytics							Run playt	book (Preview)		
and the second							Incide Create au	tomation rule		

Figure 5.5 – Creating an automation rule from the Incidents page

Using this method, automation rule conditions will be filled with the data that was detected in the incident itself.

Incidents			Create new automation rule Automation rule name	×
+ Create incident (Pre	eview) 🖒 Refresh 🕓	Last 24 hours 🗸 😤	RDP port scanning detected on WebinarMachine	
Den incidents	New incidents	C1 Active incident	Trigger When incident is created	
 >> Search by ID, title, t >> Auto-refresh in >> Severity ↑↓ >> High 	tags, owner or product ncidents Incident ID ↑↓ 333] ☐ Severity : Title ↑↓ RDP port scannin	Conditions If Analytic rule name Contains RDP port scanning detected RDP port scanning detected Account name Equals WebinarMachine (NO (NO (NO (NO (NO (NO (NO (NO	19 8 19 8 19 8
< 1	1 Naut -		Actions ① Change status Change status Closed Benign Positive - Suspicious but expected Comment	1
< Previous 1 -	1 Next >		Apply Cancel	

Figure 5.6 – Automation rule configuration

• We can follow the same steps to create an automation rule from the **Incident investigation** page.

Home > Microsoft Sentinel Incidents >	Create new automation rule	×
Incident ID 333	Automation rule name	
💍 Refresh 🗻 Delete incident	RDP port scanning detected on WebinarMachine	
RDP port scanning detected on WebinarMachine	incidents (Previe Trigger	-
▲ Benji Kovacevic ✓ ↓ High ✓ Owner Status Severity ✓	When incident is created	
Description Possible malicious RDP port scanning detected on ((Hostname)) Nov 17 R N Nov 17 R N Nov 17 R N Nov 17 R N No	tew bookmark iseated by Benji Ko H Anabelic rule name Contains V RDP port scanning detected V	
Alert product names Morosoft Sentinel Nov 16	łew bookmark	- 1
Evidence 11:18 C	reated by Benji Kos Account name V Equals V benji 💖 👔	
I I I I I Events Alerts Bookmarks 000	RDP port scanni Host name V Equals V WebinarMachine 12 [1
Last update time Creation time 11/18/22, 11:12 AM 11/02/22, 12:34 AM	IP address V Equals V 20232.133.192 149 1	1
Entities (3) Entities (3) Entities (3) WebinarMachine	+ Add ~	
= 20.232.133.192 View full details >	Actions ①	- 1
Tactics and techniques	Change status V	- 1
V 📕 Reconnaissance (1)	⊘ Closed ∨	
Incident workbook Incident Overview	Benign Positive - Suspicious but expected V	
Analytics rule RDP port scanning detected		
Investigate Actions V	Apply Cancel	

Figure 5.7 - Creating an automation rule from the Incident Overview page

To be able to create automation rules or playbooks, users must have the right permissions to create or edit them. Let's go through the permissions for Microsoft Sentinel automation.

Permissions

To create automation rules, a user needs to have a **Microsoft Sentinel Responder** or **Microsoft Sentinel Contributor** role assigned.

There is one more special role connected to Microsoft Sentinel automation rules – **Microsoft Sentinel Automation Contributor**. This is not a user role but instead a role that needs to be assigned to a Microsoft Sentinel identity so that an automation rule can run a playbook as an action. This is assigned to Microsoft Azure resource groups, which is where playbooks reside. For example, if we have five resource groups that contain playbooks, we want to have the option to attach them as an action; we need to assign this permission to all five Microsoft Azure resource groups.

To assign this permission, we need to go to the Microsoft Sentinel instance, go to **Settings**, then **Settings** again, and then, under **Playbook permissions**, click on **Configure permissions**. In the next window, choose the resource groups you want to assign the **Microsoft Sentinel Automation Contributor** role.

Home > Microsoft Sentinel	I Settings	Manage permissio	ons
Selected workspace: "cybsecsoc"	Pricing Settings Workspace settings >	Choose the resource groups that permissions to run Browse Current permission:	contain the playbooks you want to give Microsoft Se
🔗 Logs	Entity behavior analytics	Saarch	
les News & guides	~ Anomalies		Coleman al
P Search	V Workspace manager configuration	Name 14	Subscription 1
Threat management	 Playbook permissions 	Built-In-Identity-SG	T VS FTE
Incidents	What is it?	(i) doud-shell-storage-it.	• vsrie
Workbooks	Automation rules allow you to centrally manage all the automation of incident handling. Automation rules streamline		VSFIE
Hunting	Sentinel and enable you to simplify complex worknows for your incident orchestration processes.	(ii) DetautomourceGrou	with the second
Notebooks	Playbook permissions		• vorte
Entity behavior	Microsoft Sentinel automation rules can run Logic App playbooks to integrate with other services or create complex I handling. Explicit permissions are required to use this functionality.		Varia
3 Threat intelligence	Configure permissions		
MITRE ATT&CK (Preview)			
Content management	✓ How do we use your data?		
Content hub	✓ Auditing and health monitoring		
A Repositories (Preview)	Remove Microsoft Sentinel		
Community			
Configuration			
🐥 Workspace manager (Preview)			
Data connectors			
Analytics			
Watchlist			
Automation			
Settings	1	Apply Cancei	

Figure 5.8 – Microsoft Sentinel playbook permissions configuration

Once the permission is applied on the resource group level, we can attach playbooks from that resource group to an automation rule as an action.

Triggers

Triggers are used to define when an automation rule runs. For automation rules, we have three different triggers:

- When incident is created: This supports a complete list of conditions
- When incident is updated (Preview): This supports a complete list of conditions, plus conditions associated with information about updated data
- When alert is created (Preview): This supports only one condition (an analytic rule name)

Trigger		
When incident is created		\sim
	When incident is created	
Conditions	When incident is updated (Preview)	
lf	When alert is created (Preview)	

Figure 5.9 – Automation rule triggers

Conditions

Once a trigger has been set, we need to set conditions. Conditions are used to filter what incidents we want to run specific actions on, as we don't want the same actions on all incidents. What's important to note here is that actions will run only if all conditions are met. Automation rules support **OR** and **AND** condition grouping, which allows us to create more detailed automation.

An analytic rule name is one condition that cannot be removed and is used across all triggers. The evaluation supports **Contains** and **Does not contain** options, while for values, we can choose all analytic rules or run on only specific analytic rules created in Microsoft Sentinel. When we choose **All** as a value for incident creation and update, this will also run on synchronized incidents from tools such as Microsoft 365 Defender and Microsoft Defender for Cloud.

Since we have multiple triggers in automation rules, let's see what conditions are supported for each.

Conditions associated with the "When incident is created" trigger

The **When incident is created** trigger can only check the current state of the values of an incident. If we evaluate the same incident in multiple automation rules, the current state can change if we update the incident in a previous automation rule. For example, if the severity of incident creation is set to **Medium**, that will be the current state for the first automation rule. Suppose, in the automation rule, we take action to change the severity to **High**. In that case, the current value for severity in the following automation rule (that is, automation rule number 3) that will run on this same incident will be **High**.

The following conditions can be used with the When an incident is created trigger:

- **Incident properties**: For example, analytic rule name, title, description, severity, owner, status, tactics, and custom details
- Entity properties: For example, account name, account domain, filename, file hash, hostname, IP address, IoT device, mail message details, URL, and many more

Con	nditions	
lf		_
	Analytic rule name	
AND)	
	Tag V	
	Description	
-	Severity	F
Acti	Status	
L	Tactics	_
+ /	Тад	
-	Incident provider	ŀ
Rul	Custom details key (Preview)	
In	Alert product names	
Ord	Entity properties	
5	Account tenant id	Γ.
	Account AAD user id	
	Account name	
	Account NT domain	

Figure 5.10 – Automation rule condition values

Based on the condition selected, we can use one of the following evaluation methods:

- Equals or Does not equal
- Contains or Does not contain
- Starts with or Does not start with
- Ends with or Does not end with

	\sim
Equals	
Does not equal	
Contains	
Does not contain	
Starts with	Ī
Does not start with	
Ends with	
Does not end with	

Figure 5.11 – Automation rule condition options

The final element of the condition is the value itself. Here, we can have clear text input (such as an incident title or description) or the option to select pre-existing values (such as incident severity or status). We can also add multiple inputs to the same condition.

~	
+** 🛍	
Add o	onditio

Figure 5.12 – An automation rule condition example

Conditions associated with the "When incident is updated" trigger

If we update an incident with one of the supported conditions, we can trigger automation rules based on that. This gives us complete control over automation scenarios to support incident creation and updates.

Conditions with an incident update trigger support **current state** and **state changes**. Conditions include those from the incident creation trigger, plus the following:

- Owner
- Updated by
- Alerts
- Comments

They also include **state change** values for the following:

- Severity
- Status
- Tactics
- Tag

The following evaluation methods can be added with **state change**:

- Changed (owner, severity, and status)
- **Changed To** (severity and status)
- Changed From (severity and status)
- Added (alerts, comments, tactics, and tags)

The only difference is **Updated by**, which uses the current state for evaluation. We can select one of the following values from the dropdown:

- Application
- User (a manual change of a field by a specific user)
- Alert grouping (adding an alert to the incident)
- **Playbook** (a change made by a playbook run)
- Automation rule (a change made by an automation rule run)
- **Microsoft 365 Defender** (for updates to incidents made by bidirectional incident synchronization from Microsoft 365 Defender)

Updated by	✓ Equals	∽ 0 selected	\checkmark
		Search	
- + Add 🗸		Select all	
		Application	-
tions ①		User	
		Alert groupir	ng
Add action		Playbook	
		Automation	rule
le expiration ()		Microsoft 36	5 Defender

Figure 5.13 – The Updated by automation rule values

Conditions associated with the "When alert is created" trigger

The **When alert is created** trigger only supports analytic rules created in Microsoft Sentinel, and the only supported condition is **Analytic rule name**.

Trigger		
When alert is created (Previe	ew) 🗸 🗸]
Conditions If Analytic rule name	Contains V All	_]
Actions ① Run playbook	Select all (Preview) SAP - High - Activation or Deactivation of ICF Service (Preview) SAP - High - Change in Sensitive privileged user	Î
+ Add action	(Preview) SAP - High - Data has Changed during Debugging Activity	l
Rule expiration ①	(Preview) SAP - High - Deactivation of Security Audit Log (Preview) SAP - High - Execution of a Sensitive ABAP Program (Preview) SAP - High - Execution of a Sensitive Transaction Code	
Order ① 1	(Preview) SAP - High - Execution of Sensitive Function Module (Preview) SAP - High - Function Module tested	
	(Preview) SAP - High - HANA DB - Assign Admin Authorizations (Preview) SAP - High - HANA DB - Audit Trail Policy Changes (Preview) SAP - High - HANA DB - Deactivation of Audit Trail	
	 (Preview) SAP - High - HANA DB - User Admin actions (Preview) SAP - High - Login from unexpected network 	•

Figure 5.14 – An automation rule alert creation condition

After choosing one of the triggers (incident creation, incident update, or alert creation) and configuring the conditions, if all conditions we configured are met, we can run one or more actions on an incident.

Actions

The following actions are supported for automation rules:

• Run playbook:

		\sim	1
Run playbook	Search playbooks		Ŵ
Actions ()	UpdateTitle VS FTE / CyberSecurity	•	
⊢ + Add ∨	Unisolate-MDEMachine VS FTE / CyberSecurity		
	TipsAndTricks VS FTE / CyberSecurity		
If Analytic rule name	testOne VS FTE / CyberSecurity		1
Conditions	testEntity VS FTE / CyberSecurity		
When incident is created	Test-SharedMailbox VS FTE / CyberSecurity		I
Trigger	Test-incidentTrigger VS FTE / CyberSecurity	ľ	
	{P} test VS FTE / CyberSecurity	Î	

Figure 5.15 – Run playbook action

• Change status:

Actions 🛈			
Change status		\sim	Ŵ
		\checkmark	
+ Add action	NewActive		
Rule expiration ①	Closed		

Figure 5.16 – Change status action

• Change severity:

Actions ()

Change severity		\checkmark	Ŵ
		~	
+ Add action	Informational		
	Low		
Dula aurination ()	Medium		
	— High		
Indefinite			



• Assign owner:



Figure 5.18 – Assign owner action

• Add tags:

Actions (i)	
Add tags	∼ 🛍
+ Add tag	
OK Cancel	



Important note

The **Run playbook** action is the only action that's available when utilizing the **When alert is created** trigger.

While automation rule triggers, conditions, and actions are fields, we will always want to configure to have effective automation rules; we can also configure rule expiration and order.

Rule expiration and order

As mentioned previously, we have two additional steps we can configure when creating automation rules:

- **Rule expiration**: This is if we are creating an automation rule that will be active for only a specific period for example, if we are performing penetration testing. We want to auto-close incidents created by and during penetration testing and disable the automation rule at a specific date and time.
- **Order**: This is what execution order number we want to configure an automation rule as. To recall, all automation rules are run via an order number, from a lower number to a higher one, sequentially.

Rule expiration ()

11/25/2022	12:00 AM
Order ①	
5	



With that, we have covered all the major elements of automation rules and how they work. In the next section, we will look at playbooks and their main building blocks in Microsoft Sentinel automation in more detail.

All about playbooks

Playbooks are a list of actions that will be performed on the incident. They can include enrichment, response, remediation, and much more. To achieve this, Microsoft Sentinel utilizes a Microsoft Azure solution called **Logic Apps** – a platform used to create and run automated workflows. This platform uses low- or no-code and focuses more on visual design. However, those who prefer to code more can utilize coding mode as well. Because of this, it is common to hear people refer to Microsoft Sentinel playbooks as Logic Apps.

There are two different types of Logic Apps that Microsoft Sentinel supports:

- Logic Apps Consumption: This is a single playbook that has only one workflow. It supports templates and custom connectors and is widely integrated into Microsoft Sentinel with template support. Logic Apps Consumption shares the same backend resources across different customer tenants. We will use the Logic Apps Consumption model in our hands-on examples.
- Logic Apps Standard: This is a single Logic App that can have multiple workflows. It doesn't support templates and custom connectors, which is why Microsoft Sentinel doesn't have playbook templates created in Logic Apps Standard. In Logic Apps Standard, workflows in the same Logic App share the same backend resources, and they are not shared across different Logic Apps like they are with Logic Apps Consumption. It's also important to note that when creating a Logic Apps Standard playbook, it must be stateful and cannot utilize private endpoints Microsoft Sentinel does not support these scenarios at the time of writing.

Microsoft Sentinel is a unified way to run a playbook, and it will make no difference whether Logic Apps Consumption or Logic Apps Standard is used.

Navigating the playbooks GUI

Microsoft Sentinel playbooks are located under the **Automation** tab in the **Active playbooks** sub-menu. In this menu, we have the option to create a playbook, open playbook details to edit or manage it, enable or disable a playbook, delete a playbook, as well as to filter playbooks by status, trigger kind, subscription, resource group, plan, and source name. If we have deployed the playbook using built-in templates, we will also get information on whether an update is available.

© Search 0	+ Create 🗸 🕐 Refresh	() Enable	🛇 Disable 🔳 Delete	R Guides & Feedback	API Connections				
ieneral	1 = c	d 2	(1) 110						
Overview	Automation rules	Enabled rules	Enabled plays	books	Content hub				
Logs									
News & guides	Automation rules Activ	e playbooks	Playbook templates (Pre	view)					
Search			-	-		ing the second se			
vreat management	D Search		Status : All	Trigger kind : All	Subscription : VS FTE	Resource group : All	Plan : All	Source name : All	
Incidents	Name 14	Status †↓	Plan ↑↓	Trigger kind 14	Subscription 1	Resource group †↓	Location \uparrow_\downarrow	Source name 14	Tags
Workbooks	UPDATE AVAILABLE ① U	🖒 Enabled	Consumption	🔷 Microsoft Senti	📍 VS FTE	(9) CyberSecurity	East US	Gallery Content	LogicAppsCate
Hunting	UPDATE ANNEARCE () PY_	🖒 Enabled	Consumption	Microsoft Senti	📍 VS FTE	() CyberSecurity	East US	Gallery Content	LogicAppsCate
Notebooks	test	O Disabled	Consumption	🚔 Microsoft Senti	📍 VS FTE	(•) CyberSecurity	East US	Custom Content	
Entity behavior	Test-alertTrigger	🔿 Enabled	Consumption	Vicrosoft Senti	📍 VS FTE	(•) CyberSecurity	East US	Custom Content	
Threat intelligence	test-createWatchlist	() Enabled	Consumption	Vicrosoft Senti	📍 VS FTE	(e) CyberSecurity	East US	Custom Content	
MITRE ATT&CK (Preview)	Test-incidentTrigger	C Enabled	Consumption	😫 Microsoft Senti	📍 VS FTE	(0) CyberSecurity	East US	Custom Content	
ontent management	Test-SharedMailbox	C Enabled	Consumption	😫 Microsoft Senti	🕈 VS FTE	() CyberSecurity	East US	Custom Content	
Content hub (Preview)	testEntity	() Enabled	Consumption	🚔 Microsoft Senti	🕈 VS FTE	() CyberSecurity	East US	Custom Content	
Repositories (Preview)	testOne	🖒 Enabled	Consumption	📫 Microsoft Senti	🕈 VS FTE	() CyberSecurity	East US	Custom Content	
Community	TipsAndTricks	() Enabled	Consumption	🖴 Microsoft Senti	🕈 VS FTE	(9) CyberSecurity	East US	Custom Content	
	Unisolate-MDEMachin	🖒 Enabled	Consumption	Vicrosoft Senti	🕈 VS FTE	(•) CyberSecurity	East US	Custom Content	LogicAppsCate
nfiguration	Update-VIPUsers-Wat	() Enabled	Consumption	Using Microsoft	🕈 VS FTE	() CyberSecurity	East US	Custom Content	LogicAppsCate
Data connectors	Update-Watchlist-Wit	🖒 Enabled	Consumption	Using Microsoft	📍 VS FTE	() CyberSecurity	East US	Custom Content	
Analytics	UpdateTitle	([†]) Enabled	Consumption	🚔 Microsoft Senti	YS FTE	(e) CyberSecurity	East US	Custom Content	

Figure 5.21 – Microsoft Sentinel playbooks

Playbooks support templates; all deployed templates can be found in the **Playbooks templates (Preview)** sub-menu. We can deploy any playbook, from templates to active state. We can filter templates by trigger, Logic App connector, entities, tags, and source name. If we have already deployed a playbook template, we will see a notification stating that a specific playbook is in use.

P Search	+ Create V 🖸 Refresh 🖾 A	utomation health workbool	k 🕴 🖗 Guides & Feedbr	ick					
P Logs	Automation rules	5 (A	157 bled playbooks	More content	ontent at t hub				
Search hreat management	Automation rules Active plays	pooks Playbook temp	lates (Preview)				$[\mathfrak{s}^{Q}_{\mathbf{k}}]$ Create Incident From Microsoft Forms Re	sponse (Pr.	
Incidents	P. Search by name	Trigger	: All Logic Apps Co	nnectors : All		✓ More (3)	IA) Other IA: Gallery Content 3 04 Trigger type Content source Last a	/09/2022, 0	
Workbooks	Name 1	Trigger †1	Logic Apps Connect	Entities	Tags	Last modifie	Description		
Hunting	Create Incident From Microsoft For.	A Other	Microsoft For +2 ①		Utilities	09/04/22	This playbook will create a new Microsoft Sentinel incid Microsoft Forms response is submitted.	kent when	
Notebooks	Create Incident From Shared Mailb.	A Other	Content Conv +2 🕥		Utilities	09/04/22	Constant in the		
 Entity behavior 	IP Enrichment - Virus Total report	Aicrosoft Senti	Virus Total +1 💿	IP IP	Enrichment	12/07/22	Microsoft Sentinel		
Threat intelligence	Reset Azure AD User Password - En.	💣 Microsoft Senti	Office 365 Ou +1 ()	Account	Remediation	12/07/22	Cffice 365 Dutlock		
MITRE ATT&CK (Preview)	IN USE Add Host To Watchlist - Inc.	Microsoft Senti	Microsoft Sentinel	Host.		04/25/22	Preneculates		
ontent management	IN USL Add IP Entity To Named Lo.	Microsoft Senti	Microsoft Sentinel	E IP	Remediation	08/12/21	1. Create Microsoft Forms from template.	day dealers the	
Content hub	IN USE Add IP To Watchlist - Incide	Microsoft Senti	Microsoft Sentinel			04/12/22	playbook.	9 am	
Repositories (Preview)	IN MR Add URL To Watchlist - Inci.	Microsoft Senti	Microsoft Sentinel	@ URL		04/25/22	 Prepare subscription ID, Resource Croup name, and Analytics Workspace name as it is needed for template 	.09	
Community	Add User To Watchlist - Incident Tri.	Microsoft Senti	Microsoft Sentinel	Account		04/25/22	deployment.		
onfiguration	IN VISE Block AAD user - Alert	V Microsoft Senti	Azure AD +2 ①	Account	Remediation	11/25/21	Post deployment steps 1. Add Microsoft Sentinel Responder role to the playbo	ck's	
Workspace manager (Preview)	IN USE Block AAD user - Incident	Aicrosoft Senti	Azure AD +2 ①	Account	Remediation	11/25/21	managed identity. 2. Authorize Microsoft Forms: Office 365 Outlook com	ertor and	
Data connectors	IN USE Block IP - Azure Firewall IP .	. 🔷 Microsoft Senti	AzureFirewall_ +3 ()	IP IP	Remediation Re	spo 07/28/21	Conversion Service connector (HTML to text).		
Analytics	Block IP - Cisco ASA	Microsoft Senti	CiscoASACon +2 ①	IP IP	Remediation Re	spo07/28/21		1	
Watehlist	1	-			-	. *	And and a second second		

Figure 5.22 – Microsoft Sentinel playbook templates

To access all templates in Microsoft Sentinel, we can utilize **Content hub** and the available solutions, where we can filter, among others, by the solution we need or solutions with playbook templates.

P Search	🗉 🕐 Refresh 🔗 Guides & Feedback				
General Overview	245 Solutions	1 6 Updates			
 News & guides Search 	P Search. Category : All	Status : All	Content type : Playbook (4	i) Support : All Provider : All	ĺ
Threat musiquement Indidents Workbooks Hunting Notebooks Instruction Threat intelligence MITRE ATTACK (Preview) Content management	Register cisco Cisco Umbrella Microsoft Sentine Microsoft Corporation Senting - Owed Senting Register set TIT: Des convents: Int	Cop4j Vulnerability Microsoft Sentinel, Mi Corporation Application, Security - Th Security - Whenability M Magnetic Add (M) - Rusing	Select All Analytics rule (114) Data connector (20) Data connector (20) Hunting query (59) Parser (107) Parser (107) Vischolst (7) Workbook (130) Apply Cance	ation	
Content hub (Preview) Repositories (Preview) Configuration Data connectors Analytics Watchist Automation	Atlassian Jira Audit Microsoft Corporation DerQu Redefice 24 (20) Determediar (3)	Azure Active Directo Microsoft Sentinel, Micro Corporation Kensty Magnesinal (M) Data cont	ey osoft Azure Identiti Micross Security	Active Directory Protection It Corporation Treat Preaction take Toda connection	No solution selected Select a solution to view more details

Figure 5.23 - Microsoft Sentinel - Content hub

More templates can be found on GitHub and can be easily deployed to Microsoft Sentinel since they utilize **Azure Resource Manager** (**ARM**) templates. Microsoft Sentinel has an official repository with lots of content available that is ready to be deployed. The link to the official repository is https://github.com/Azure/Azure-Sentinel.

To create a new playbook, go to the Automation tab, click Create, and select one of the following options:

- Playbook with incident trigger
- Playbook with alert trigger
- Blank playbook

P Search a	+ Create 🗸 🜔 Refresh	() Enable	🛇 Disable 📋 Delete	e 🔗 Guides & Feedbac	k 😒 API Connections				
General Overview P	Automation rule Playbook with incident trigger Playbook with alert trigger	C 2 Enabled rules	(A) 110 Enabled play) 🗳	More content at Content hub				
News & guides	Blank playbook	playbooks	Playbook templates (Pr	review)					
Search	Search		Status : All	Trigger kind : All	Subscription : VS FTE	Resource group : All	Plan : All	Source name : All	
fhreat management	-	8 8			999923 52				
Incidents	Name Ti	Status ↑↓	Plan ⊤↓	Trigger kind T‡	Subscription 14	Resource group ↑↓	Location ↑↓	Source name 1	Tags
Workbooks	UPDATE AVAILABLE 🔾 U.,	C Enabled	Consumption	Microsoft Senti	Y VS FTE	() CyberSecurity	East US	Gallery Content	LogicAppsCateg
Hunting	UPDATE AVAILABLE O PT	C Enabled	Consumption	Microsoft Senti	Y VS FTE	(•) CyberSecurity	East US	Gallery Content	LogicAppsCate
Notebooks	test	O Disabled	Consumption	Microsoft Senti	Y VS FTE	() CyberSecurity	East US	Custom Content	
Entity behavior	Test-alertTrigger	C Enabled	Consumption	Microsoft Senti	📍 VS FTE	() CyberSecurity	East US	Custom Content	
Threat intelligence	test-createWatchlist	C Enabled	Consumption	Microsoft Senti	📍 VS FTE	() CyberSecurity	East US	Custom Content	
MITRE ATT&CK (Preview)	Test-incidentTrigger	🖒 Enabled	Consumption	Microsoft Senti	Y VS FTE	() CyberSecurity	East US	Custom Content	
	Test-SharedMailbox	C Enabled	Consumption	Microsoft Senti	Y VS FTE	() CyberSecurity	East US	Custom Content	
Control by Maniant	testEntity	C Enabled	Consumption	Microsoft Senti	Y VS FTE	(CyberSecurity	East US	Custom Content	
Coment nuo (Preview)	testOne	C Enabled	Consumption	Alicrosoft Senti	Y VS FTE	(e) CyberSecurity	East US	Custom Content	
 Repositories (Preview) 	TipsAndTricks	C Enabled	Consumption	Alicrosoft Senti	Y VS FTE	(9) CyberSecurity	East US	Custom Content	
Community	Unisolate-MDEMachin	() Enabled	Consumption	V Microsoft Senti	Y VS FTE	(9) CyberSecurity	East US	Custom Content	LogicAppsCateg
onfiguration	Update-VIPUsers-Wat	C Enabled	Consumption	Q Using Microsoft	* VS FTE	() CyberSecurity	East US	Custom Content	LogicAppsCateg
Data connectors	Update-Watchlist-Wit	() Enabled	Consumption	Using Microsoft	Y VS FTE	() CyberSecurity	East US	Custom Content	
Analytics	UndataTitle	(h) Enabled	Consumption	Microsoft Centi	· WE FTE	(a) Coherfaquilty	East 115	Curtom Content	

Figure 5.24 – Creating a new Microsoft Sentinel playbook

If we select **Playbook with incident trigger** or **Playbook with alert trigger**, we will create a **Logic Apps Consumption** Logic App. The first view is where we enter basic information, such as what subscription and resource we want to deploy the playbook in, the region, and the playbook's name. We can also enable diagnostic settings, which we will cover in the *Monitoring automation rules and playbook health* section:

Home > Microsoft Sentinel Auton	nation >	
Create playbook		
Basics ② Connections (3 Review and create	
Select the subscription to manage dep organize and manage all your resourc	oloyed resources and costs. Use reso es.	ource groups like folders to
Subscription *	VS FTE	\checkmark
Resource group *	CyberSecurity Create new	~
Region *		
East US		\sim
Playbook name *		
SOAR		~
Enable diagnostics logs in Log Ar	nalytics ()	
Log Analytics workspace		
cybsecsoc		\checkmark
Associate with integration service	environment ①	
Integration service environment		
		\sim
Next : Connections >		

Figure 5.25 – The Create playbook wizard

In the next window, we can select how we want to authenticate a Microsoft Sentinel connection. By default, playbook creation will enable a **system-assigned managed identity** from the playbook and utilize it (the recommended method). However, we can utilize any pre-existing connection or change it once the playbook has been deployed.

Basics	2 Connections (3) Review and	d create
or each cor laybook. O ogic Apps o	nnector this playbook uses, you can cho therwise, you must create a new connec designer after your playbook is deployed	ose to use an existing connection from another tion and authenticate when you are brought to the d.
^ 📀	Microsoft Sentinel	Connect with managed identity
	Connect with managed identity	
	FailedTrigger	
	benji@cybsec.guru	
	ttt	

Figure 5.26 – Creating a new playbook – Connections

Next : Review and create >

The last step is to review the configuration and create our playbook.

Previous

Previous

Home > Microsoft Sentinel Aut	omation >
Create playbook	
Sasics Connections	3 Review and create
Basics	
Subscription	VS FTE
Resource group	CyberSecurity
Region	East US
Playbook name	SOAR
Diagnostics logs workspace	Disabled
Integration service environment	Disabled
Connections	
Microsoft Sentinel Connect with managed identity	,
1 Note: Grant permissions to the second s	he managed identity after deployment.

Figure 5.27 – Creating a new playbook – Review and create

Create and continue to designer

Once the playbook has been deployed, we can navigate to **Logic app designer**, where we can start our playbook design.



Figure 5.28 – The Logic app designer view

From here, we can also access the code view of the playbook if we prefer to work with code.



Figure 5.29 – The Logic App designer code view

We will go through the whole process of creation and explanation in *Chapters 6* to 8, where we will cover hands-on examples.

When we want to create a blank playbook, we can choose between creating a **Logic Apps Standard** or **Logic Apps Consumption** Logic App. We can also utilize any other trigger available in Logic Apps, such as a recurrence to perform a regular playbook run, and a Microsoft Forms trigger to create an incident when a new form is filled in and when an email is received.

Home > Create Logic App Basics Hosting Monitoring Tags Review + create Create a logic app, which lets you group workflows as a logical unit for easier management, deployment and sharing of resources. Workflows let you connect your business-critical apps and services with Azure Logic Apps, automating your workflows without writing a single line of code. **Project Details** Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources. Subscription * ① VS FTE \sim Resource Group * ① CyberSecurity \sim Create new Instance Details Logic App name * SOARStandard \checkmark .azurewebsites.net Workflow O Docker Container Publish * Central US Region * \sim 1 Not finding your App Service Plan? Try a different region or select your App Service Environment. Plan The plan type you choose dictates how your app scales, what features are enabled, and how it is priced. Learn more Standard: Best for enterprise-level, serverless applications, with Plan type * event-based scaling and networking isolation. Consumption: Best for entry-level. Pay only as much as your workflow runs. Windows Plan (Central US) * ① (New) ASP-CyberSecurity-8dfe \sim Create new Pricing plan * Workflow Standard WS1 210 total ACU, 3.5 GB memory Change size Zone redundancy An App Service plan can be deployed as a zone redundant service in the regions that support it. This is a deployment time only decision. You can't make an App Service plan zone redundant after it has been deployed Learn more

	(
Review + create	< Previous	Next : Hosting >	



To run the created playbook, we have a few options:

- Attach the playbook to an automation rule for automatic triggering (which will require the **Microsoft Sentinel Automation Contributor** role to be assigned to a Microsoft Sentinel identity; more about this in the subsequent *Permissions* section)
- Run the playbook manually on the incident (which will require the **Microsoft Sentinel Automation Contributor** role assigned to a Microsoft Sentinel identity)
- Run the playbook manually on the alert

To create, edit, and run playbooks in Microsoft Sentinel, you will need certain permissions to perform these actions. Let's go through the different permissions users can have and what users can perform with these actions.

Permissions

Important note

To understand this segment better, I suggest that you have a basic understanding of permissions on Azure and Azure RBAC. A great starting point is the official documentation: https://learn.microsoft.com/azure/role-based-access-control/.

There are a few different permissions that users can utilize based on the actions they need to perform when working with Microsoft Sentinel playbooks:

- Logic Apps Contributor: This gives you permission to manage Logic Apps and run playbooks, but you cannot change access to them (there is standard role separation in Azure, and only the Owner or User Access Administrator role can perform this action).
- Logic App Operator: This gives you permission to read, enable, or disable a playbook, but you cannot edit, update, or run playbooks.
- **Microsoft Sentinel Contributor**: This permits you to attach a playbook to an analytic rule, among other Microsoft Sentinel permissions.
- **Microsoft Sentinel Responder**: This permits you to run playbooks manually, among other Microsoft Sentinel permissions.
- Microsoft Sentinel Playbook Operator: This permits you to list and run playbooks manually.

We covered the **Microsoft Sentinel Automation Contributor** role earlier in this chapter, so we will not look at it in detail again.

To be able to create and utilize playbooks, it is important to understand how they work. In the next section, we will cover the main aspects of Logic Apps.

Logic Apps connectors and authentication

Under the hood, Logic Apps uses API calls to connect with Microsoft and non-Microsoft solutions. Those API calls can be wrapped in a Logic Apps connector, giving us more straightforward configuration and authentication. These connectors are as follows:

- Managed connectors: These are available in a Logic App out of the box. They contain triggers and actions for specific products or services, such as the Microsoft Sentinel connector. There are hundreds of managed connectors for Microsoft products and services, as well as for non-Microsoft products and services.
- **Custom connectors**: If some product or service still doesn't have a built-in connector in Logic Apps, you have the option to create and utilize a custom connector in your environment. It is also possible to share those custom connectors with others, and some of them are utilized with Microsoft Sentinel. When using custom connectors, you must utilize the Logic App Consumption model since Logic App Standard doesn't support custom connectors at the time of writing.

But what if there is neither a built-in nor custom connector?

In this case, we can utilize an HTTP connector that will allow us to connect to a product or solution using direct API calls. Examples of these HTTP calls will be covered in *Chapter 9*.

Important note

Data connectors in Microsoft Sentinel aren't the same as Logic Apps connectors.

Data connectors in Microsoft Sentinel are used to ingest logs into a Log Analytics workspace, and we can utilize those logs to create detection rules, hunt for data, and so on. Some examples of these logs include Syslog data, security event data from Windows Server, and sign-in logs from Azure AD.

Logic Apps connectors are API calls to products and services so that we can perform specific actions. Examples of these API calls are a call to Azure AD to block a user, a call to an EDR solution to isolate the machine, and an API call to the TI solution to get IP address information.

But wait! When making an API call, don't we need to provide authentication? Is this supported in Microsoft Sentinel playbooks?

Yes! If we need to authenticate managed or custom connectors, there is a way to do this. For non-Microsoft products and services, these can be usernames and passwords, API tokens, and so on. These authentications are saved as API connections and can be accessed from a playbook. Once created, these API connections can also be utilized in other playbooks; they are not specific to one playbook.

Home > Microsoft Sentinel Automa	tion > SNOW-CreateAndUpdateIncident API conn	ections > snow-CreateSNOWRecord	
SNOW-CreateAnd	UpdateIncident API «	API Connection	VRecord Edit API connection * ···· ×
	O Refresh		Edit API connection
Activity log Activity log Access control (IAM) Tags Diagnose and solve problems	API connections associated with the logic app • azuresentinel-Create/Iralssue • snow-CreateSNOWRecord	Activity log Access control (IAM) Tags Diagnose and solve problems	Edit API connection lets you update the display name and refresh the authorization for this SaaS provider. API ServiceNow Display Name SNOW
Development Tools		Settings	Instance * () http://
Logic app code view Versions ABL connections		General	Username * ©
Quick start guides Settions		Edit API connection Monitoring	Password * O
Workflow settings Authorization Access keys Identify If Properties		Automation Automation	5ave Discard
A Locks		R New Support Request	
Alerts Metrics Diagnostic settings			
P Logs	•		

Figure 5.31 – Managing an API connection in a playbook

If we use HTTP calls, this information will be inserted into the header or body of the API call, as per the instructions of the product or service.

In terms of Microsoft services and products, playbooks support three types of API authentication. Let's look at them in detail.

System-assigned managed identity

This is the preferred option and is utilized by default when creating playbooks using **Create playbook** with an incident trigger or **Create playbook with an alert trigger**. Each playbook has its own systemassigned managed identity that can be enabled, and this identity can be utilized only by this specific playbook. This connection cannot be shared among playbooks. A managed identity also provides an option for the least privileged approach.

It's important to note that not all connectors in Logic Apps support managed identities. For example, a Microsoft Sentinel connector supports them, while Microsoft Teams and Office 365 Outlook do not.

To add permissions to a managed identity, you will need to go to the **Identity** tab in Logic Apps.

Home > Microsoft Sentinel Auto	mation > SOAR
SOAR Identity	
🔎 Search	⁴ System assigned Liker assigned
Activity log	A system analysis dentity is restricted to one per resource and is tired to the Breycle of this resource. You can grant permissions to the managed identity by using Asure role-based access control (Asure RBAC). The managed identity is authenticated with Asure AD, so you don't have to store any credentials in code. Learn more about Managed identities.
Access control (IAM)	Serve X Discard () Refresh R Got feedback?
 Lings Diagnose and solve problems Development Tools 	Statun () Off ()
む Logic app designer	Object (principal) (D 🔘
Versions API connections	Permissions ③ Azure role assignments
Quick start guides Settings	This resource is registered with Asure Active Directory. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures. Learn more
(i) Workflow settings	
Authorization	
Access keys	
🐛 Identity	
III Properties	
A Locks	
Monitoring	
Merts	
in Metrics	
Diagnostic settings	
🚅 Logs	

Figure 5.32 – Enabling a playbook's managed identity

Once you are in the **Identity** section, you need to select **Azure role assignments** and then **Add role assignments** to assign an Azure permission to the managed identity.

Home > Microsoft Sentinel Automation > SOAR Identity > Azure role assignments	Add role assignmer	nt (Preview) ×
+ Add role assignment (Preview) O Refresh If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more	Scope ③ Resource group Subscription VS FTE	~] ~
Subscription *	Resource group	
VS FTE V	CyberSecurity	~
Kele Name Resource Ty No role assignments found for the selected subscription.	Role O Select a role Learn more about RBAC	Microsoft Sentinel Microsoft Sentinel Automation Contributor © Microsoft Sentinel Contributor © Microsoft Sentinel Playbook Operator © Microsoft Sentinel Responder © Microsoft Sentinel Responder ©
	Save Discard	

Figure 5.33 – Assigning a permission to a playbook's managed identity

To authenticate a playbook trigger or action with a managed identity, first, fill in **Connection name**, then for connecting, select **System-assigned managed identity** from the drop-down list, and click **Create**.

O Microsoft Senti	nel	(j)
* Connection name	Enter name for connection	
* Managed identity	System-assigned managed identity	~
	Create Cancel	
Connect with sign in	Connect with service principal ⁽ⁱ⁾	

Figure 5.34 – Connecting to a Logic Apps connector using a managed identity

Service principals

Service principals can be created on the Azure AD administrator page by registering an application. Once we have created an application, we will need to save a **Tenant ID** and **Application ID** in a secure space. These will be needed for authentication purposes, as well as to create a secret for the application and save it in a secure space, such as Azure Key Vault.

To register an application, we need to enter the application's name and specify whether the application is single- or multi-tenant.

Dashboard > CybSec Guru App registrations >
Register an application
* Name
The war facing display name for this application (this can be shanged later)
The user-facing display name for this application (this can be changed later).
SOAR
Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (CybSec Guru only - Single tenant)
O Accounts in any organizational directory (Any Azure AD directory - Multitenant)
O Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
O Personal Microsoft accounts only
Help me choose
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Select a platform
Crect a particiting of the participation of the partipation of the partipation of the participation of the partici
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.
By proceeding, you agree to the Microsoft Platform Policies 📴
Register

Figure 5.35 – Creating a new service principal using Azure AD App registrations

Once the service principal has been created, we can assign API permissions to it, such as the Microsoft Graph Security API and Microsoft 365 Defender.

SOAR API perr	nissions 🖈 …	Request API permissions	
		< All APIs	
P Search «	🕐 Refresh 🛛 🖗 Got feedback?	Microsoft Graph	
Overview		https://graph.microsoft.com/ Docs C*	
Chicketer		What type of permissions does your application require?	
Integration assistant	The "Admin consent required" column shows the default value fo in organizations where this app will be used. Learn more	Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
anage	Configured permissions		-
Branding & properties	Applications are authorized to call APIs when they are granted perr	Select permissions	expand a
Authentication	all the permissions the application needs. Learn more about permis	Start typing a permission to filter these results	
Certificates & secrets	+ Add a permission 🗸 Grant admin consent for CybSec Gun	Permission	Admin consent required
Token configuration	API / Permissions name Type Description	Accure Benime	
API permissions	✓Microsoft Graph (1)	/ Mutessnellew	
Expose an API	User.Read Delegated Sign in and res	> Acronym	
App roles		N	
Owners .	To view and manage consented permissions for individual apps, as	AdministrativeUnit	
Roles and administrators		> AgreementAcceptance	
Manifest			
pport + Troubleshooting		> Agreement	
* Troubleshooting		> APIConnectors	
New support request			
		> AppCatalog	
		> Application	

Figure 5.36 – Assigning API permissions to a service principal

We can also assign any Azure AD or Azure **Role Based Access Control (RBAC)** role to a service principal. For example, suppose we want the option to query data in a Log Analytics workspace. In that case, we can utilize the **Azure Monitor Logs** connector, which does not support a managed identity at the time of writing but does support service principals. Therefore, we will assign the Log Analytics Reader permission to the service principal and authenticate our connector with it. Another important note about using a service principal is that it can be reused across multiple playbooks as it is not playbook-specific. This is because it's a system-assigned managed identity.

😥 Azure Monitor Log	gs	(j) ···	
*Connection name	Enter name for connection		
Client ID	Client (or Application) ID of the Azure Active Directory application.		
Client Secret	Client secret of the Azure Active Directory application.		
Tenant	The tenant ID of the Azure Active Directory application.		
	Create		
Connect with sign in			

Figure 5.37 – Connecting to the Logic Apps connector using a service principal

User identity

The last option that we will cover is user identity. This option allows any user from your organization to authenticate the connection. The user carrying out the authentication must have the permission to perform the needed action (for example, to block a user in Azure Active Directory or to isolate a host in EDR) to authenticate the API connection. If the user doesn't have the permission, the playbook will fail on this step. This is also a shared connection. Once we create this API connection, it can be utilized across multiple playbooks – by a specific user or any user with permission to create and edit playbooks.



Figure 5.38 - Connecting to the Logic Apps connector using a user's identity

What's important to note here is that the user who authenticates this connection must have permission to perform the action (for example, to block a user in Azure Active Directory or isolate a host in EDR) when the playbook is running. Some organizations use **Privileged Identity Management (PIM)** and users are only assigned permission when needed. In this scenario, it is advisable to not use user identity for any action that can run while the user doesn't have permission active.

With that, let's shift focus and get to know triggers a little better.

Triggers

Triggers are used to define on what event a playbook will be triggered to run. It is always the first step when we create our playbook. Triggers also define the scheme that the playbook expects when it is triggered.

In Microsoft Sentinel, we have two primary triggers, with the third one still under development at the time of writing and, therefore, it will not be covered in this book.

The following triggers are available in Microsoft Sentinel:

- Microsoft Sentinel alert: This receives alert data as input
- Microsoft Sentinel incident: This receives incident data as input
- Microsoft Sentinel entity: Under development

\leftarrow β earch connectors and triggers	
Triggers Actions	
Microsoft Sentinel alert (preview) Microsoft Sentinel	(i)
Microsoft Sentinel entity (Private Preview) (preview) Microsoft Sentinel	()
Microsoft Sentinel incident (preview) Microsoft Sentinel	0
Don't see what you need?	

Figure 5.39 – Microsoft Sentinel playbook triggers

Since Microsoft Sentinel utilizes Logic Apps to create playbooks, we can utilize many more triggers that are not connected to Microsoft Sentinel. Some of them are as follows:

- Schedule triggers: Runs a playbook every *n* minutes, hours, or days, or at a specific time on specific days
- Microsoft Forms triggers: Creates a manual incident when a Microsoft Forms form is submitted
- Office 365 Outlook: Creates a manual incident when an email is received in a shared mailbox, and so on

Let's now focus on the rest of the playbook steps.

Actions

Once we have configured a trigger, we need to configure actions that will be performed when a playbook is triggered. We can utilize data that arrives with the trigger (incident data alongside the incident trigger, for example) to focus on specific information from it. These actions can be run sequentially, in parallel, or under complex conditions.

Microsoft Sentinel's native actions, among others, include the following:

- Add comment to incident
- Bookmarks: Create or update a bookmark
- Create incident
- Entities: Get accounts/hosts/IPs/URLs
- Watchlist: Create a new watchlist with data (raw content) and so on

Microsoft Sentinel	>
 Search connectors and actions 	
Triggers Actions	
Alert - Get incident (preview) Microsoft Sentinel	0
Bookmarks - Creates or updates a bookmark (preview) Microsoft Sentinel	Ū
Sookmarks - Delete a bookmark (preview) Microsoft Sentinel	Ū
Bookmarks - Get a bookmark (preview) Microsoft Sentinel	Ū
Bookmarks - Get all bookmarks (preview) Microsoft Sentinel	Ū
Create incident (preview) Microsoft Sentinel	Ū
This - Get Accounts (preview) Microsoft Sentinel	Ū
Entities - Get DNS (preview) Microsoft Sentinel	Ū
Tritities - Get FileHashes (preview) Microsoft Sentinel	0



It's important to know that each action defines its scheme, and we can utilize data from triggers and previous actions to define data in the action we are working on now. To access this data, we can utilize dynamic content. This will be covered in the next section.

Some other actions we can create are as follows:

- Azure Active Directory: An action to block a user, reset their password, and revoke the session
- Azure Firewall: An action to block an IP
- Palo Alto/Fortinet/CheckPoint...: An action to block an IP
- ServiceNow/Jira: Sends incident data and creates a record
- VirusTotal: Gets the IP/URL/file hash enrichment data

Some other actions native to Logic Apps that we need to be aware of are as follows:

- **Condition**: Here, we can define which block of actions to execute based on condition evaluation. For example, if the host starts with *admin*, we can auto-close the incident; if not, we can isolate the device.
- For each: If the data that we are working on is an array (set of data) and we want to act on each piece of data in the dataset.
- Switch: Similar to Condition, but we can have multiple paths.
- HTTP: To make an API call to a product or service if a native action is not available in Logic Apps.
- **Parse JSON**: To parse a result received by an HTTP call.
- **Create HTML table**: To be used when creating an email response and you want to create an HTML table containing data.
- Set variable: If we want to set a variable that can be used on multiple instances in a playbook.

We will cover these actions in more depth in *Chapter 9*.

To make playbook actions utilize dynamic data, we can utilize dynamic content in Logic Apps.

Dynamic content

Dynamic content refers to temporary fields in a playbook run; these are created by triggers and actions. The only rule is that using these temporary fields is only possible for triggers and actions that happened before the action we are working on occurred. For example, when a playbook is triggered with a Microsoft Sentinel incident trigger, the output that's received will contain all the necessary data about the incident, such as its severity, status, incident number, incident URL, entities, and alerts. Using dynamic content, we can specify these values in the next action. For example, we might want to get a list of IPs, so we can use the **Entities - Get IPs** action; as input, we can use the **Entities** dynamic content that we received from the Microsoft Sentinel incident trigger.

Microsoft Sentinel incident (Preview)	
C Entities - Get IPs (Preview) ····	
*Entities list 🛛 🐼 Entities 🗙	
Add dynamic content	Dynamic content Expression
Connected to azuresentinel-TestBookmark. Change connection.	
	Search dynamic content
+ New step	Microsoft Sentinel incident See more
The sep	Incident updates Alert Display Name
	Incident updates Alert URI This is the link to the alert in the orignal vendor.
	Incident updates Alert Description The description of the alert.
	Incident updates Alert Friendly Name The graph item display name which is a short humanly re
	Incident updates Alert Product Name The name of the product which published this alert.
	Incident updates Incident Tags Name The name of the tag
	The type of the tag
	Incident updates Incident Tactics Item

Figure 5.41 – Dynamic content in Microsoft Sentinel playbooks

If some data is not exposed in **Dynamic content** or we want to join two values, we can use expressions. An example of an expression is when we have an array containing alerts and we want to list alert names from that dataset; we can use a **join** expression to perform this action.

We will cover more on dynamic content and expressions in the hands-on examples in *Chapters 6* to 9, which will feature common tips and tricks for working with Microsoft Sentinel playbooks.

Monitoring automation rules and playbook health

Microsoft Sentinel automation has a native way of monitoring the health of automation rules and playbook triggers. This monitoring can be enabled from the **Settings** page of Microsoft Sentinel, under **Health monitoring**.

≡ Microsoft Azure			Ģ	Ø	۲	0	8	
Home > Microsoft Sentinel Microsoft Sentinel Selected workspace: 'cybsecsoc'	Settings ····							×
	Pricing Settings Workspace settings >							
General	Entity behavior analytics							
Overview								
🧬 Logs	✓ Anomalies							
🌰 News & guides	 Playbook permissions 							
🔎 Search	✓ How do we use your data?							
Threat management	∧ Health monitoring							
Incidents	What is it?							
🞽 Workbooks	Microsoft Sentinel's health monitoring allows you to keep an eye on data connect	tor activity a	nd on s	cheduk	ed anal	ytics ru	les' ope	rations.
Hunting	How to anable it?							
Notebooks	To turn on Microsoft Sentinel's health monitoring feature, select Configure diagn	ostic settin	gs belo	w. Mari	k the cł	neck bo	xes for	the logs and
💞 Entity behavior	metrics you want to collect, and select your Log Analytics workspace as the destin can find and query your Sentinel health monitoring data in the SentinelHealth tab	ation for the	e data (alytics.	you can Learn n	n select nore >	additio	mal des	tinations too). You
O Threat intelligence	Configure diagnostic settings							
MITRE ATT&CK (Preview)								
Content management	✓ Remove Microsoft Sentinel							
Content hub (Preview)								
 Repositories (Preview) 								
dia Community								
Configuration								
Data connectors								
 Analytics 								
Watchlist								
- Cattle -								
🔽 Settings	¥							

Figure 5.42 – Microsoft Sentinel – Health Monitoring configuration

We need to enable the **Automation** diagnostic settings and send them to the Log Analytics workspace where Microsoft Sentinel is enabled.

Home > Microsoft Sentinel Settings >	Diagnostic settings >		
Diagnostic setting			\times
🔚 Save 🗙 Discard 🗊 Delete 🔗	Feedback		
A diagnostic setting specifies a list of categor and one or more destinations that you wou more about the different log categories and	ries of platform logs and/or metrics that you d stream them to. Normal usage charges for contents of those logs	a want to collect from a resource, the destination will occur. Learn	JSON View
Diagnostic setting name *	Automation Health	×	
Logs		Destination details	
Category groups ①		Send to Log Analytics workspace	
Categories		Subscription	7
V Automation		Log Analytics workspace	1
Data Collection - Connectors		CybSecSOC (eastus)	-
		Archive to a storage account	
		Stream to an event hub	
		Send to partner solution	

Figure 5.43 – The Automation Health monitoring configuration wizard

These diagnostic settings will be saved in the **SentinelHealth** table in Microsoft Sentinel so that we can query statuses using KQL.

A sample KQL query that you can use to get this data is as follows:



Figure 5.44 - Querying the SentinelHealth table in the Microsoft Sentinel | Logs tab

We can also utilize the **Automation Health** workbook that's available in workbook templates to get a detailed report about our automation health in Microsoft Sentinel.



Figure 5.45 – Utilizing the Microsoft Sentinel Automation Health workbook

Automation Health only monitors a playbook trigger – in other words, it only checks whether the playbook triggered successfully, not the whole playbook run. To monitor whether the playbook runs successfully or not, we have to utilize diagnostic settings at the playbook level. A diagnostic setting can be configured when creating a playbook.

Home > Microsoft Sentinel Automati	ion >	
Create playbook		
Basics ② Connections ③	Review and create	
Select the subscription to manage deploy organize and manage all your resources.	red resources and costs. Use resource groups	like folders to
Subscription *	VS FTE	\sim
Resource group *	CyberSecurity Create new	\sim
Region *		
East US		\sim
Playbook name *		
Enable diagnostics logs in Log Analy	tics ①	
Log Analytics workspace		
cybsecsoc		\sim
Associate with integration service en	vironment ①	
Integration service environment		
		\sim
Next : Connections >		

Figure 5.46 – Enabling diagnostic settings when creating a new playbook

A diagnostic setting can also be created in the playbook itself.



Figure 5.47 – Adding a diagnostic setting to an existing playbook

Once we've done this, we need to select the **Send to Log Analytics workspace** box, where we have Microsoft Sentinel enabled.

Home > Microsoft Sentinel Automation	n > SOAR Diagnostic settings >		
Diagnostic setting			
🔚 Save 🗙 Discard 🗊 Delete 🔗	Feedback		
A diagnostic setting specifies a list of categor and one or more destinations that you woul more about the different log categories and	ories of platform logs and/or metrics that you Id stream them to. Normal usage charges for I contents of those logs	want to collect from a resource, the destination will occur. Learn	
Diagnostic setting name *	SOAR playbook diagnostic settings	✓	
Logs		Destination details	
Category groups 🛈		Send to Log Analytics workspace	
Categories		Subscription	
Workflow runtime diagnostic eve	ents	VS FIE	<u> </u>
Metrics		CybSecSOC (eastus)	\sim
AllMetrics		Archive to a storage account	
		Stream to an event hub	
		Send to partner solution	

Figure 5.48 – The Diagnostic setting configuration wizard of a playbook

This data will be saved in the **AzureDiagnostics** table. We can query it using KQL:

```
AzureDiagnostics
| where OperationName == "Microsoft.Logic/workflows/
workflowRunCompleted"
```

The preceding KQL query will give you the following output:

Microsoft Sentin Selected workspace: "cybsecsoc"	nel Logs							
P Search «	₽ New Query 1* × +					(Feedback	Queries 🛞 🔟
eneral	P CybSecSOC	Þ R	in Time range : Custon	n) 🔚 Save 🗸 🕜 Share 🗸	+ New alert rule	✓ → Export ✓	🖈 Pin to 🗸 🔤	Format query
Overview	Tabler Queries Eurotions	1	AzureDiagnostics					
Logs		2	where OperationName ==	"Microsoft.Logic/workflows/wor	<pre>ckflowRunComplet</pre>	ed"		
News & auides	,O Search							
Sauch	(😵 Filter) 📳 Group by: Solution 🗸							
Search	P. Colored	Re	sults Chart [2] Add b	pokmarie				2
reat management	Conapse an		TimeGenerated [UTC]	Resourceld		Category	ResourceGroup	SubscriptionId
Incidents	Favorites		✓ 11/4/2022, 2:59:43.740 PM	/SUBSCRIPTIONS/	-	WorkflowRuntime	CYBERSECURITY	80314059-666a
Workbooks	You can add favorites by clicking on the \$ icon		Tenantid					1
Hunting	h Antimolucion Accordinate		TimeGenerated [UTC]	2022-11-04T14:59:43.7406564Z				
Notebooks	+ LooMonormont		Resourceld	/SUBSCRIPTIONS/		RESOURCEGRO	UPS/ /	PROVIDERS/MICROSO
Entity behavior	 Logiwanagement Missessfit Continuel 		Category	WorkflowRuntime				
Thread intrificence	Microsoft Sentinel (168A		ResourceGroup	с ү				
inreat mengence	Security and Audit		SubscriptionId					
MITRE ATT&CK (Preview)	Security and Addit		ResourceProvider	MICROSOFTLOGIC				
tent management	Custom Logs		Resource	0851	JU34			
Content hub (Preview)			ResourceType	WORKFLOWS/RUNS				
Repositories (Preview)			OperationName	Microsoft,Logic/workflows/workf	lowRunCompleted			
Community			Level	Error				
			status_s	Falled				
liguration			startTime_t [UTC]	2022-11-04714:59:41:50328862				
Data connectors			endTime_t [UTC]	2022-11-04714:59:43.74057622				
Analytics			workflowid_s	/SUBSCRIPTIONS/		/RESOURCEGRO	UPS/ /	PROVIDERS/MICROSO
Watchlist			resource_location_s	eastus				
Automation			Madde	Maria 100 al Inter 1990 a 1990 Charles	Malace March			

Figure 5.49 - The queried playbook's diagnostic settings in the Microsoft Sentinel | Logs tab

We can also join and compare data from the **AzureDiagnostics** and **SentinelHealth** tables to check whether the playbook triggered by the automation rule or the one we triggered manually had a successful run. This can be done by comparing the **runId** columns in both tables and joining them on the same **runId** since it is unique for each playbook run.

Here is a KQL example:

```
SentinelHealth
where SentinelResourceType == "Automation rule"
mv-expand TriggeredPlaybooks = ExtendedProperties.TriggeredPlaybooks
extend runId = tostring(TriggeredPlaybooks.RunId)
join (AzureDiagnostics
     where OperationName == "Microsoft.Logic/workflows/
workflowRunCompleted"
    project
        resource_runId_s,
       playbookName = resource_workflowName_s,
       playbookRunStatus = status s)
    on $left.runId == $right.resource runId s
project
   RecordId,
    TimeGenerated,
   AutomationRuleName= SentinelResourceName,
   AutomationRuleStatus = Status,
```

```
Description,
workflowRunId = runId,
playbookName,
playbookRunStatus
```

The preceding KQL query will give you the following output:

Selected workspace: 'cybsecso	c 1-5-						
© Search 0	* New Query 1* * +					🗢 Feedback 👷 Queries	© Ш ~
eneral	CybSecSOC	► Run (Time range : Cust	om) 🔠 Sa	ve \checkmark 🕼 Share \checkmark $+$ Ne	w alert rule 🗸 🗁 Export 🗸	🖈 Pin to 🗸 🛛 🖅 Format	query
Overview	Tables Queries Functions #	1 SentinelHealth					
Logs		3 mv-expand TriggeredPl	aybooks = Ex	tendedProperties.Triggere	dPlaybooks		9
News & guides	P Search :	4 extend runId = tostri 5 join (AzureDiagnostic	ng(Triggered	Playbooks.RunId)			
Search	Filter IB Group by: Solution 🤝	6 where OperationNa 7 project	me == "Micro	soft.Logic/workflows/work	flowRunCompleted"		
	E College di	8 resource_runId	S,	kElmAlmo x			
hreat management	1 Conspie au	10 playbookRunStat	us = status_	s)			
Incidents	Favorites	11 on Slett.runid == 3 12 project	right.resour	ce_runId_s			*
Workbooks	You can add favorites by clicking on the \$\overline{x}\$ icon	Results Chart 1 10 Add	bookmark				Q
Hunting	Antimalware Assessment	RecordId		TimeGenerated [UTC]	AutomationRuleName	AutomationRuleStatus	Des
Notebooks	+ LogManagement		-096371de65c2	9/26/2022, 3:27:55.353 PM	Update Test	Success	
Entity behavior	Microsoft Sentinel	Recordid	b4805a31-9b9	J 1-4ea5-8872-096371de65c2			
Threat intelligence	Microsoft Sentinel UEBA	TimeGenerated [UTC]	2022-09-2671	5:27:55.3536564Z			
MITRE ATT&CK (Preview)	Security and Audit	AutomationRuleName	Update Test				
	Custom Logs	AutomationRuleStatus	Success				
ntent management		Description	Rule executed	successfully, triggering all actions.			
Content hub (Preview)		workflowRunld	085853740081	\$3596575593236339CU12			
Repositories (Preview)		playbookName	UpdateTitle				- 1
Community		pleybookRunStatus	Failed				
infiguration		> 70a26e68-4c6b-448b-ada2	87ddcd16a205	10/4/2022, 1.31:32.067 PM	Update Test	Success	
Data consectors		> 31cd9e98-d102-48d2-8afc	da9c2f8304e3	10/4/2022, 1:32:55:904 PM	Update Test	Success	1
Data comectors		> 1c479eb6-918f-4150-9303-	140833d960e9	10/7/2022, 1:30:25:211 PM	Update Test	Success	R
Analytics		> f7139689-054e-48e9-9551-	186610855604	10/7/2022, 2:42:37:713 PM	Update Test	Success	
Watchlist		d118de8a-15c5-4ddf-8dae	2f218e3a17d9	10/7/2022 1:28:28:860 PM	Update Test	Success	R

Figure 5.50 – Querying AzureDiagnostics and SentinelHealth in the Microsoft Sentinel | Logs tab

With automation rule and playbook health monitoring covered, let's wrap up this chapter.

Summary

In this chapter, we dug deep into Microsoft Sentinel automation and dissected each element. First, we focused on automation rules and their main elements – triggers, conditions, and actions – and how they define automation rule runs. We also covered permissions and ways to create automation rules. Then, we moved on to the topic of playbooks, where we focused on their main elements – triggers, actions, and dynamic content – as well as underlying information such as connectors, permissions, and authentication methods.

At the end of this chapter, we focused on the critical topic of automation health and how to monitor it using Microsoft Sentinel functionalities.

In the next chapter, we will begin our hands-on examples. We will focus on enriching incidents so that we can speed up MTTA and MTTR in Microsoft Sentinel.