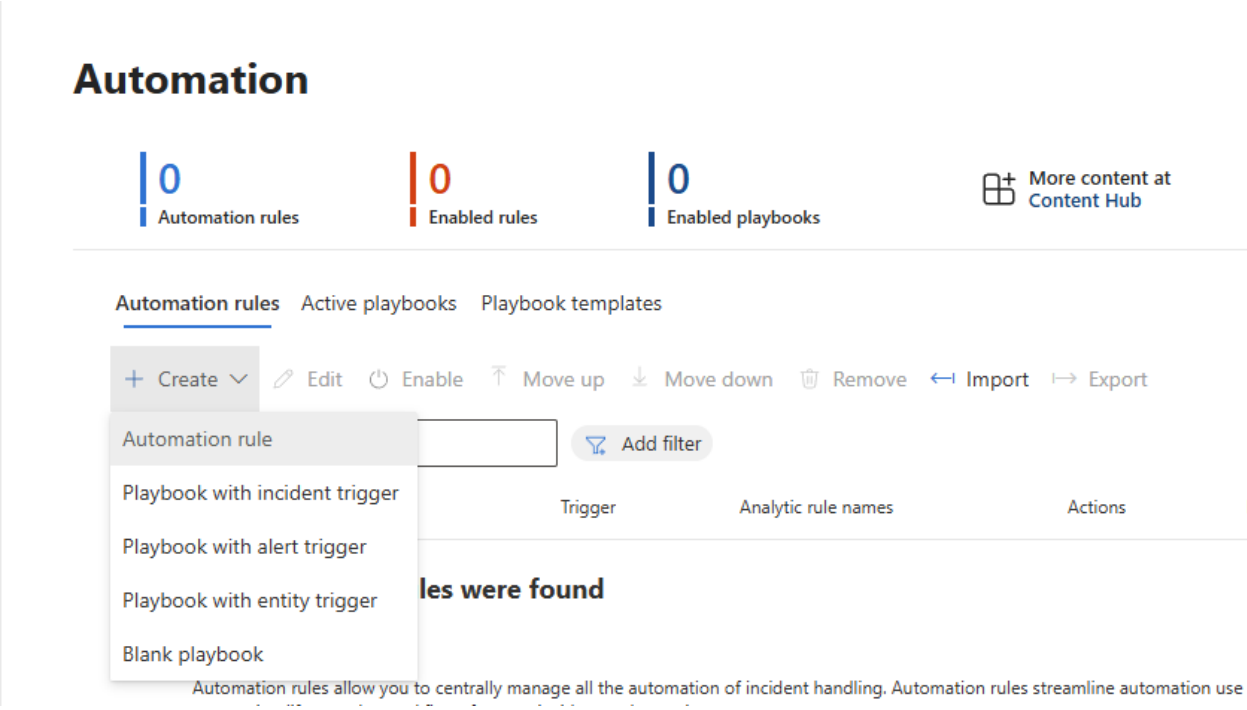
Playbooks and Logic Apps in MS Sentinel

Adrian Cortez

Overview

In Microsoft Sentinel, a playbook is an automated response plan for security incidents. It's built on top of Azure Logic Apps and defines what should happen when a certain alert or trigger occurs. Logic Apps is the underlying Azure service used to create automated workflows. This is a no-code platform where you can drag and drop connectors, steps, and conditions. Logic apps can be used to automate any workflow, not just for security. Playbooks are necessary for SOC analysts because they turn manual, repetitive, and time-sensitive tasks into fast, consistent, and automated workflows. This reduces human error and speeds up incident response.

Create an Automation Rule



Create new automation rule

Automation rule name *

Brute Force Alert Automation

Trigger

When incident is created

Conditions

If

Property: Analytic rule name | Operation: Contains | Value: Brute Force Attack (User has ...

AND

Property: Alert product names | Operation: Contains | Value: Microsoft Sentinel

+ Add

Actions

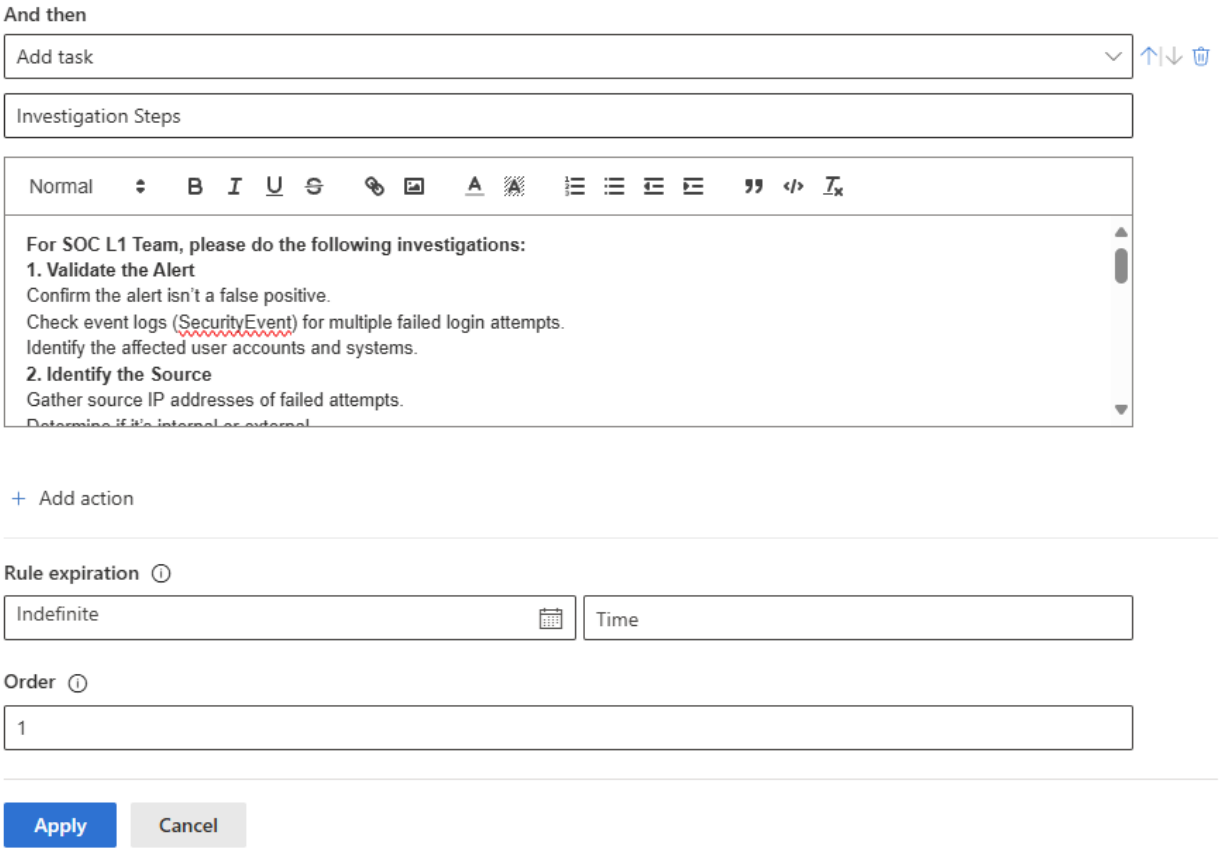
Change status

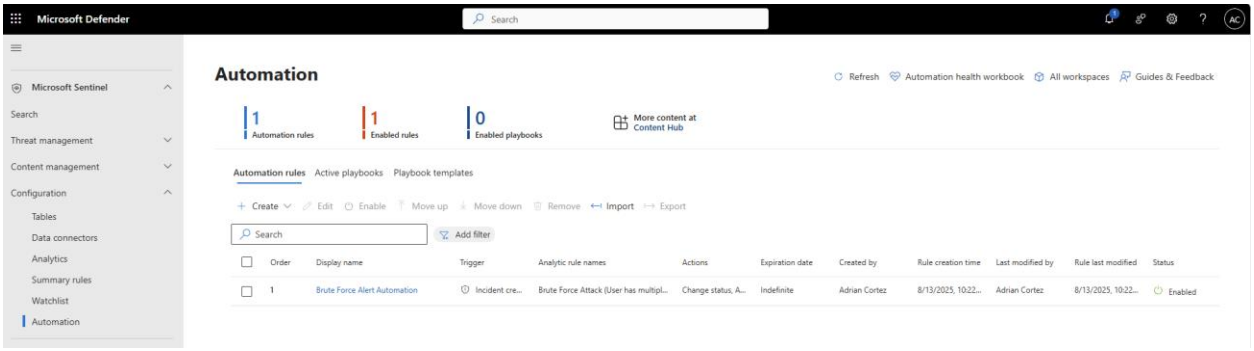
Active

And then

Assign owner

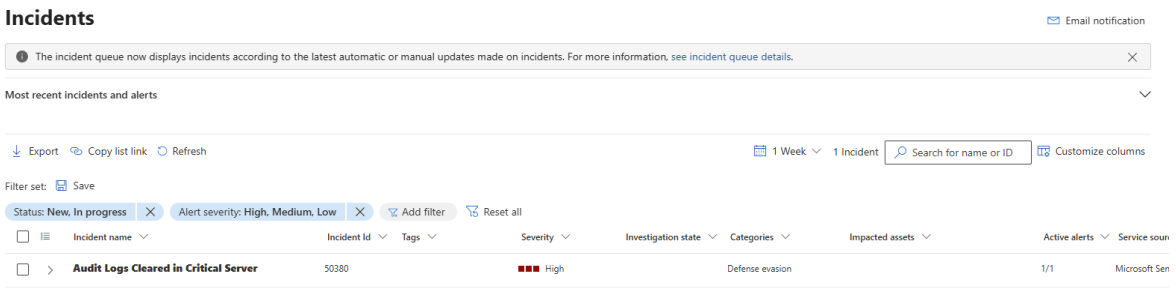
AC Adrian Cortez
amcortez@olivet.edu



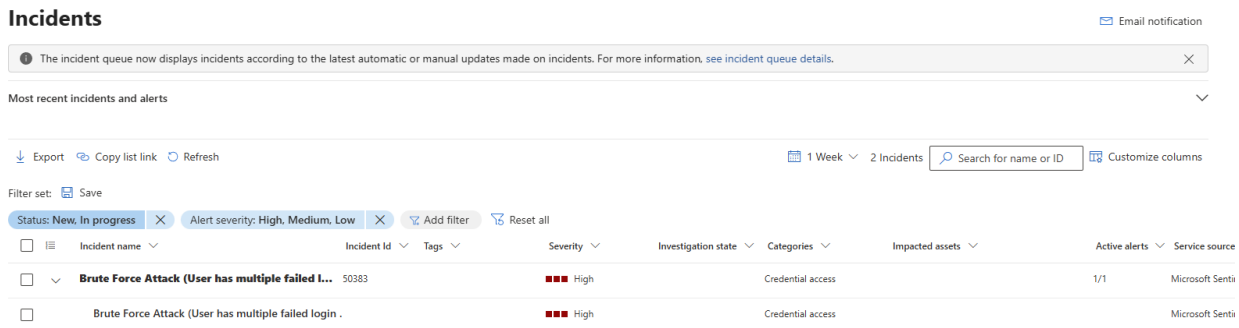


Manually brute force the VM and check whether our automation is working properly.

Before Brute Force Attempt:



After Brute Force Attempt



Observe the automation rules take action (Incident gets assigned, status changed, new task with investigation instructions)

Brute Force Attack (User has multiple failed login attempts)

High | Unknown | In progress

Manage alert | Move alert to another incident | ...

Incident

Brute Force Attack (User has multiple failed login attempts)

Incident severity

High

Active alerts	Devices	Users	Mailboxes	Apps
1/1	0	0	0	0

Comments & history

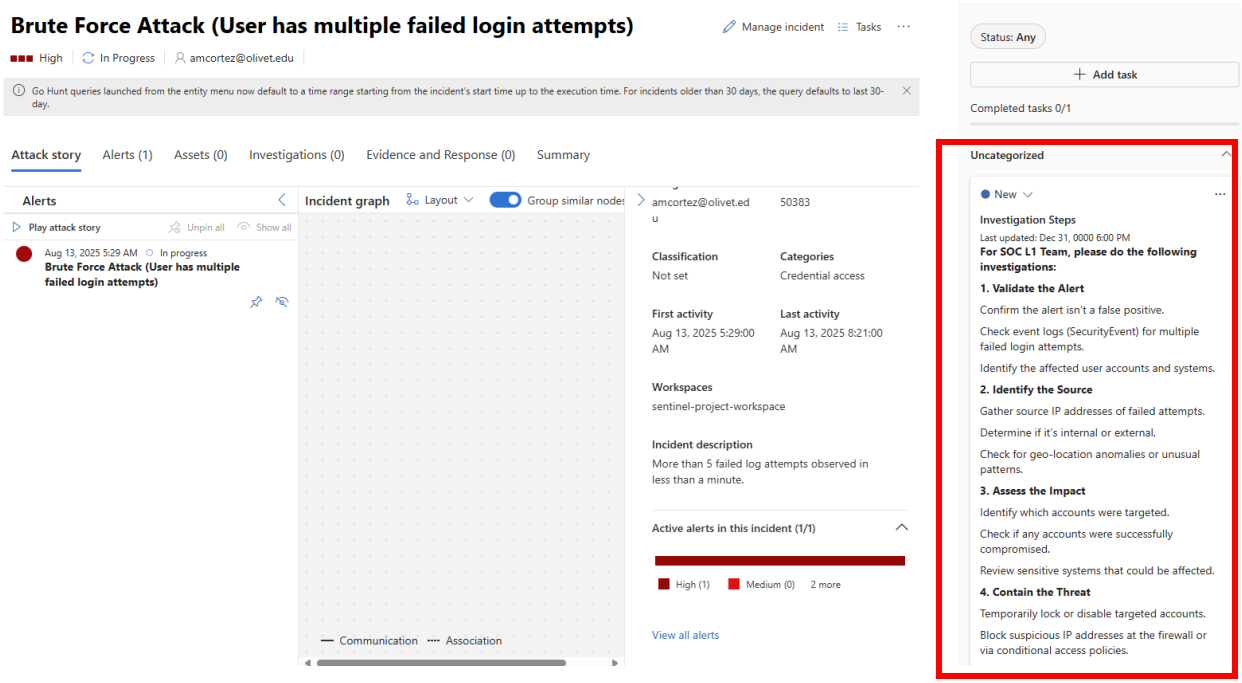
Add a new comment

Save

Automation rule-Brute Force Alert Automation
Alert was assigned to amcortez@olivet.edu.
Aug 13, 2025 10:34:45 AM

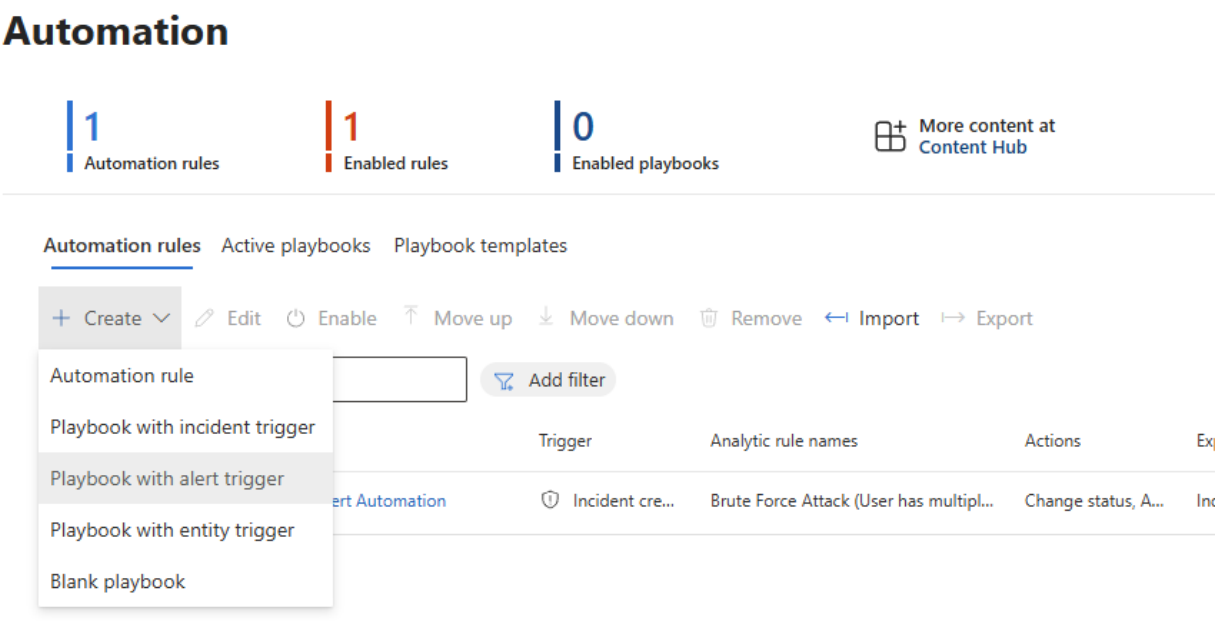
Automation rule-Brute Force Alert Automation
Status changed from 'New' to 'In progress'.
Aug 13, 2025 10:34:40 AM

Automation
Alert linked to incident #50383
Aug 13, 2025 10:32:18 AM



Creating a Playbook in MS Sentinel

Now we will build a basic playbook in MS Sentinel that automatically sends an email notification.



Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Azure for Students

Resource group

Sentinel-Project

Create new

Region *

(US) East US

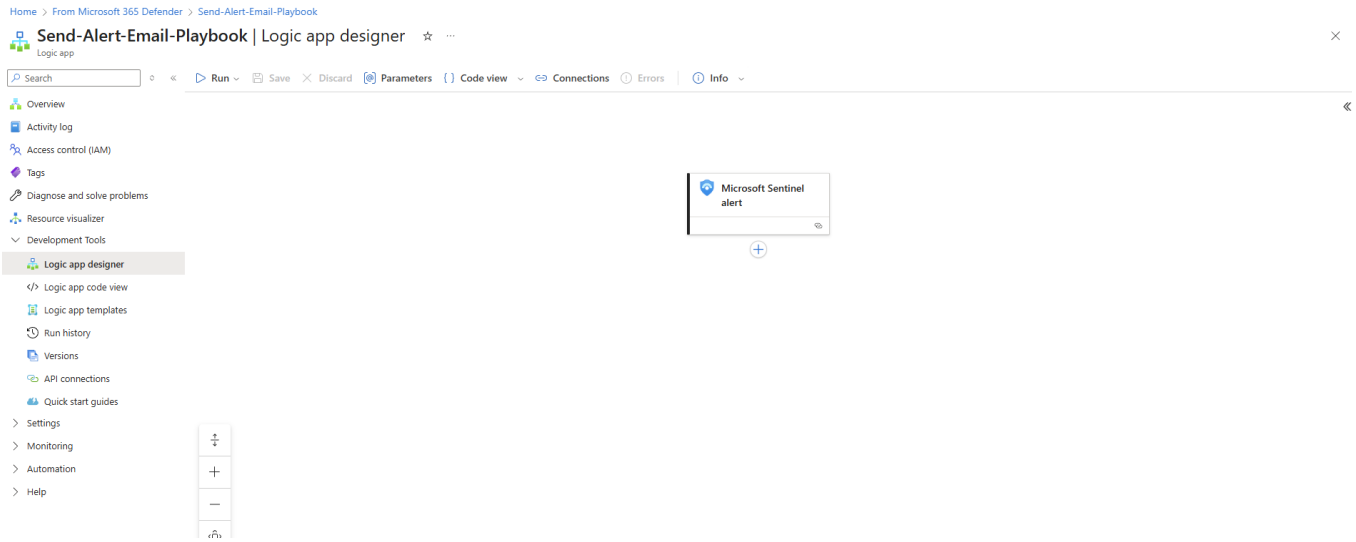
Playbook name *

Send-Alert-Email-Playbook

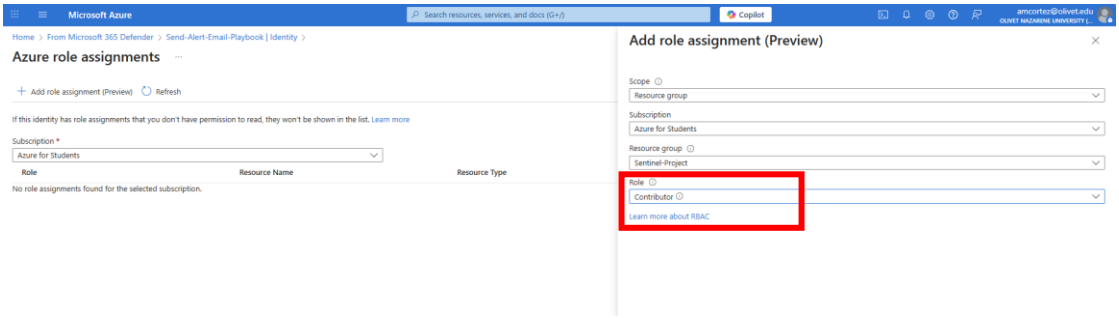
Enable diagnostics logs in Log Analytics

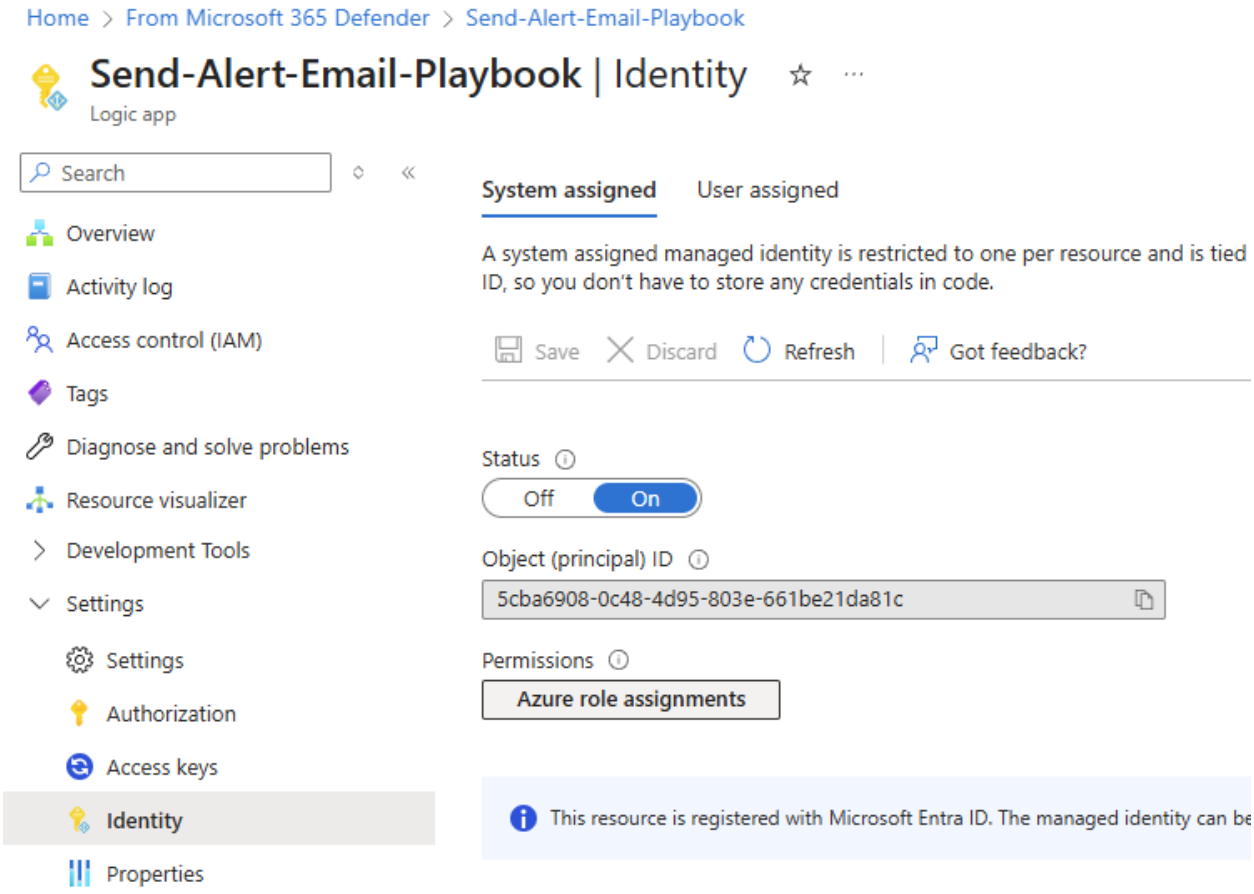
Log Analytics workspace

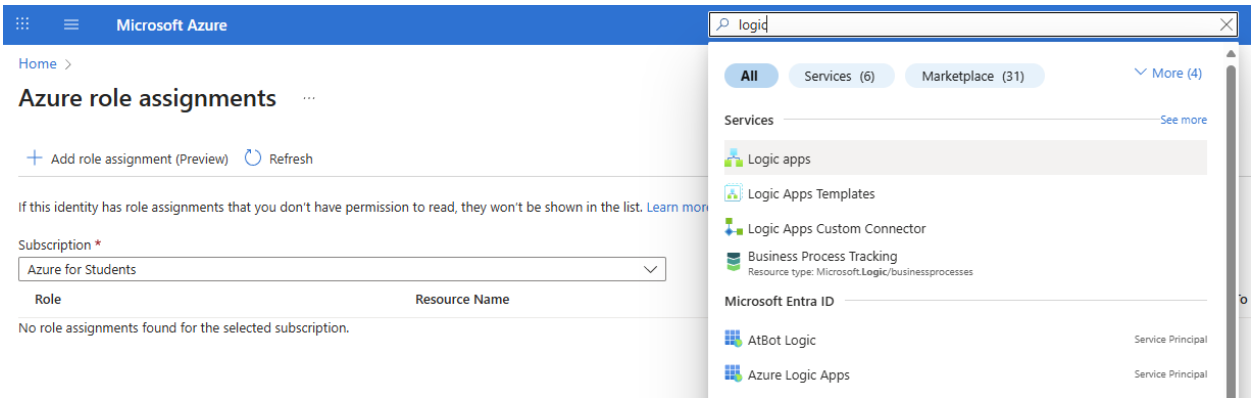
Sentinel-Project-Workspace

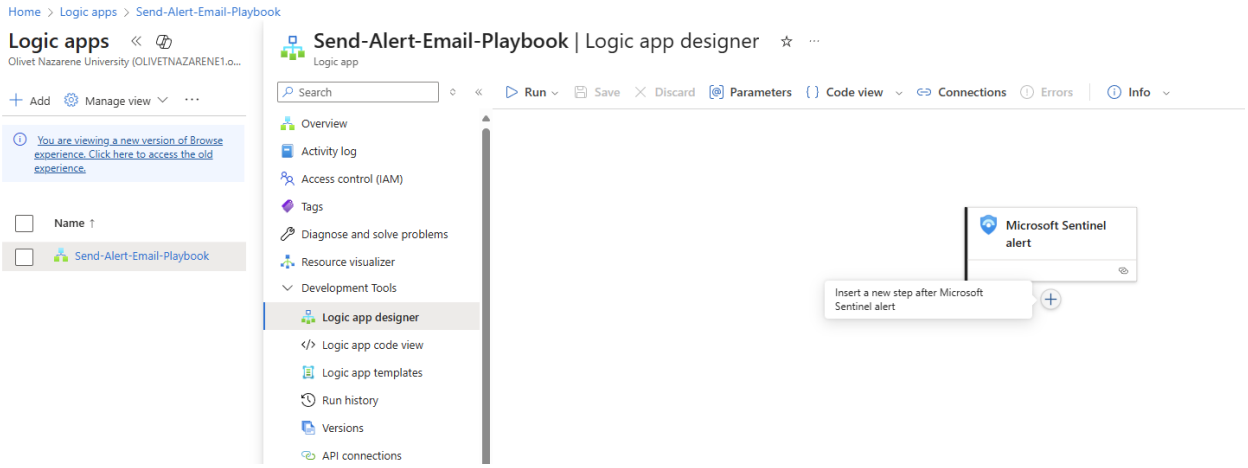


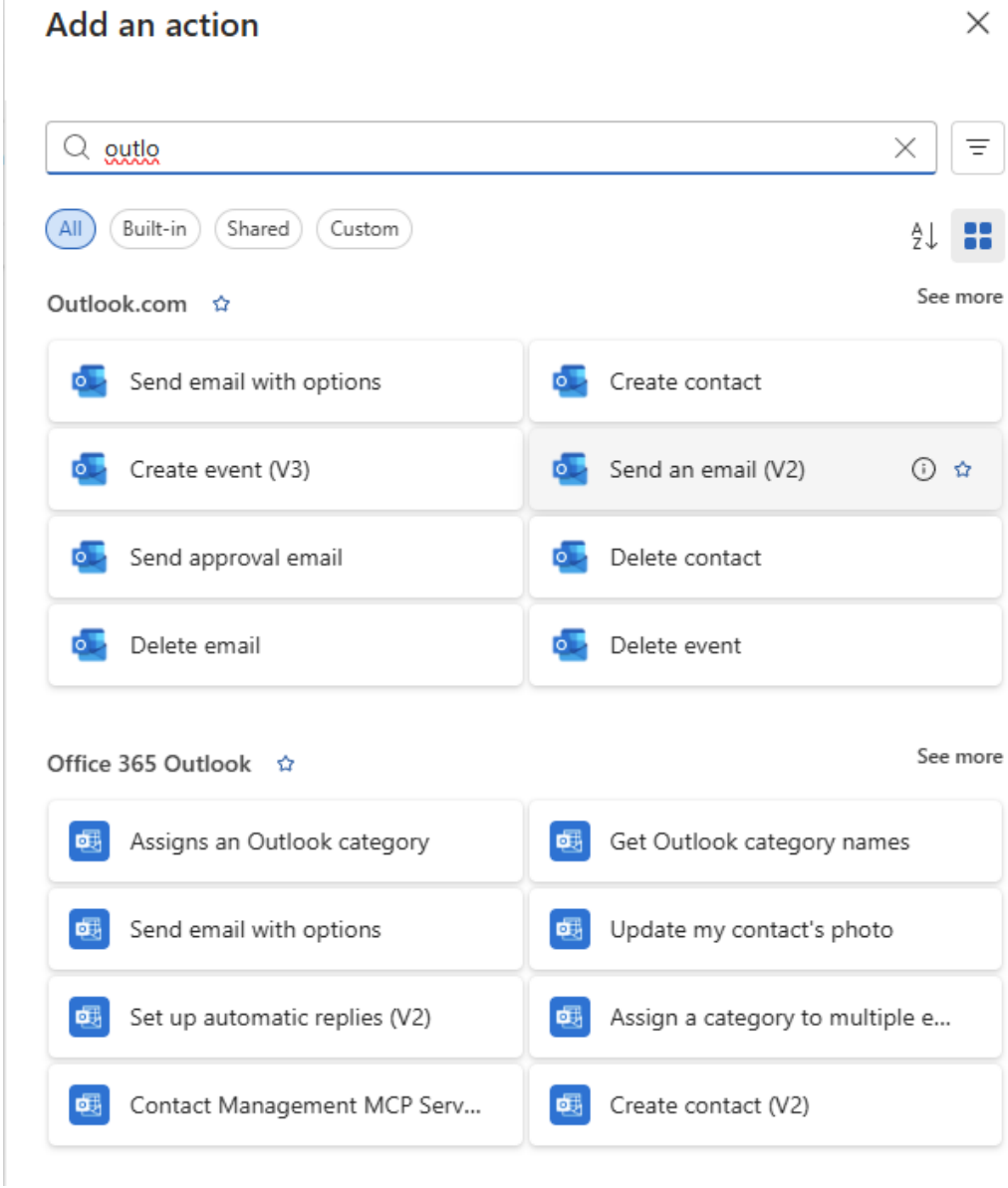
Make sure to add Contributor as a role.

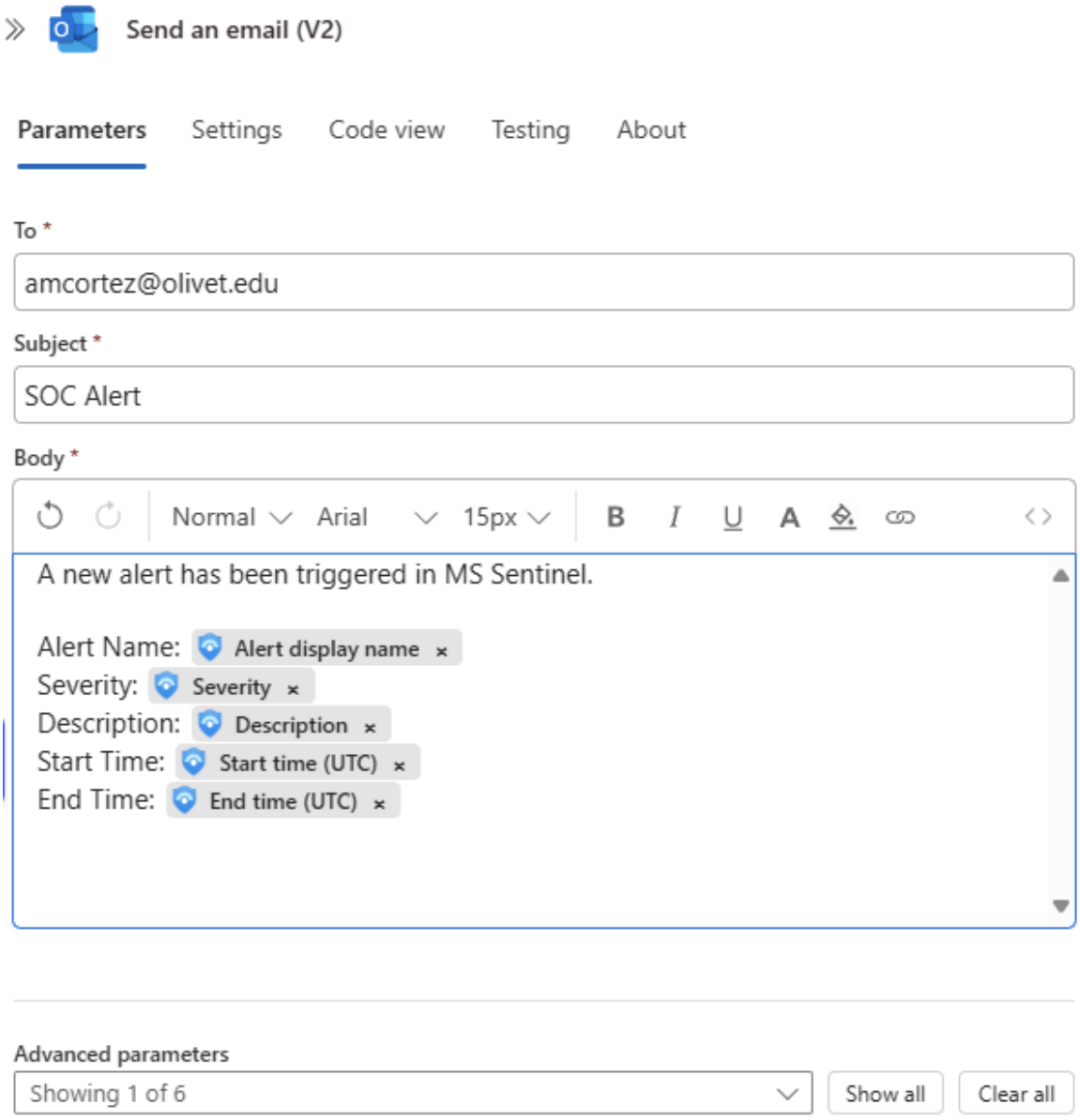

Microsoft Azure
Azure role assignments
Add role assignment (Preview)
Refresh
Subscription *
Azure for Students
Role
Resource Name
Resource Type
No role assignments found for the selected subscription.
Add role assignment (Preview)
Scope
Resource group
Subscription
Azure for Students
Resource group
Sentinel-Project
Role
Contributor
Learn more about RBAC


Home > From Microsoft 365 Defender > Send-Alert-Email-Playbook
Send-Alert-Email-Playbook | Identity
Logic app
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Development Tools
Settings
Settings
Authorization
Access keys
Identity
Properties
System assigned
User assigned
A system assigned managed identity is restricted to one per resource and is tied
ID, so you don't have to store any credentials in code.
Save
Discard
Refresh
Got feedback?
Status
Off
On
Object (principal) ID
5cba6908-0c48-4d95-803e-661be21da81c
Permissions
Azure role assignments
This resource is registered with Microsoft Entra ID. The managed identity can be

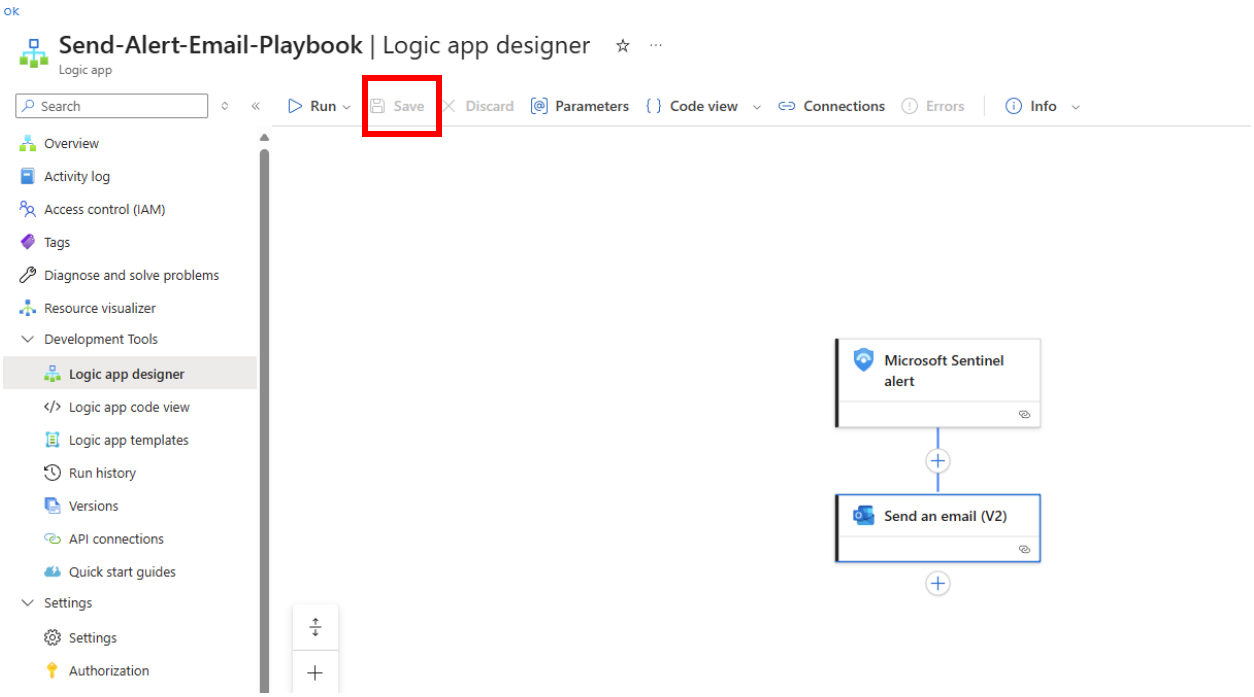

Microsoft Azure
logic
Home
Azure role assignments
Add role assignment (Preview)
Refresh
If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn mor
Subscription *
Azure for Students
Role
Resource Name
No role assignments found for the selected subscription.
All
Services (6)
Marketplace (31)
More (4)
Services
See more
Logic apps
Logic Apps Templates
Logic Apps Custom Connector
Business Process Tracking
Resource type: Microsoft.Logic/businessprocesses
Microsoft Entra ID
AtBot Logic
Service Principal
Azure Logic Apps
Service Principal


Home > Logic apps > Send-Alert-Email-Playbook
Logic apps
Olivet Nazarene University (OLIVETNAZARENE1.o...
Add
Manage view
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
Send-Alert-Email-Playbook
Send-Alert-Email-Playbook | Logic app designer
Logic app
Search
Run
Save
Discard
Parameters
Code view
Connections
Errors
Info
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Development Tools
Logic app designer
Logic app code view
Logic app templates
Run history
Versions
API connections
Microsoft Sentinel alert
Insert a new step after Microsoft Sentinel alert


Add an action
outlo
All
Built-in
Shared
Custom
Outlook.com
See more
Send email with options
Create contact
Create event (V3)
Send an email (V2)
Send approval email
Delete contact
Delete email
Delete event
Office 365 Outlook
See more
Assigns an Outlook category
Get Outlook category names
Send email with options
Update my contact's photo
Set up automatic replies (V2)
Assign a category to multiple e...
Contact Management MCP Serv...
Create contact (V2)

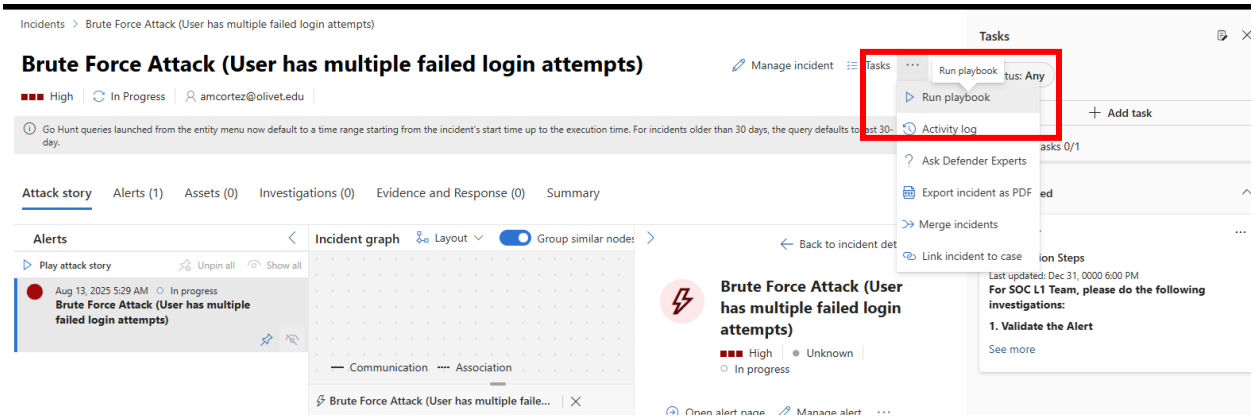


Make sure to save your logic app design

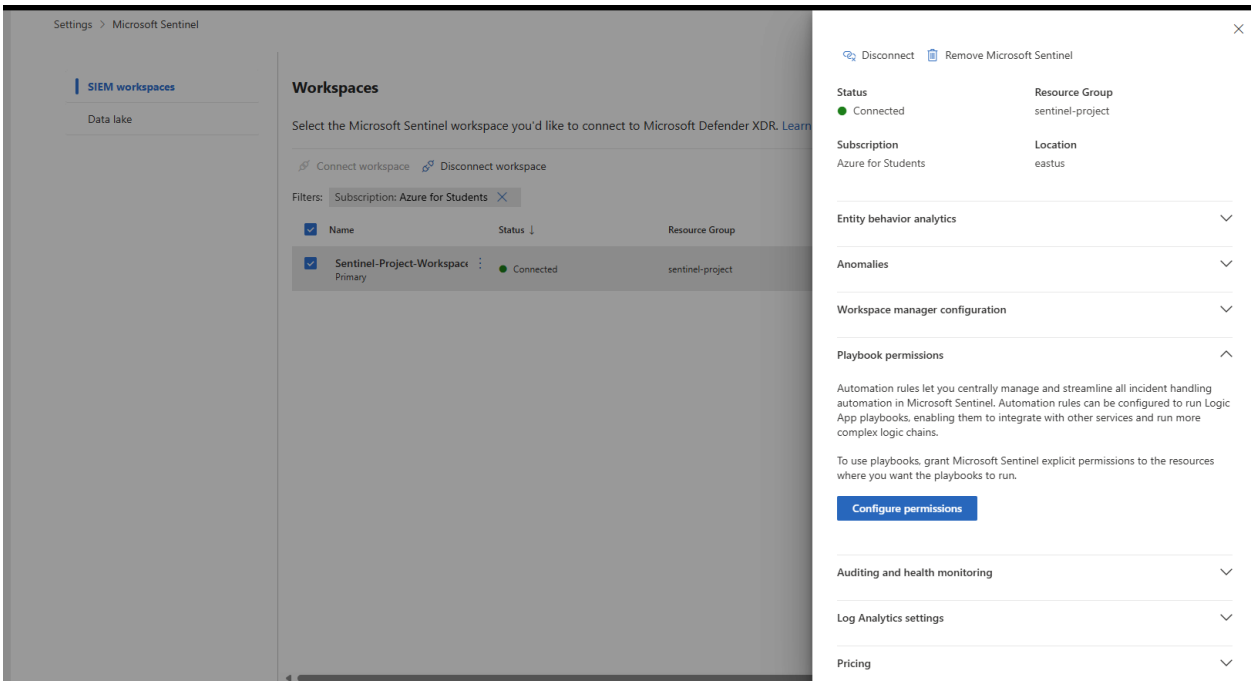


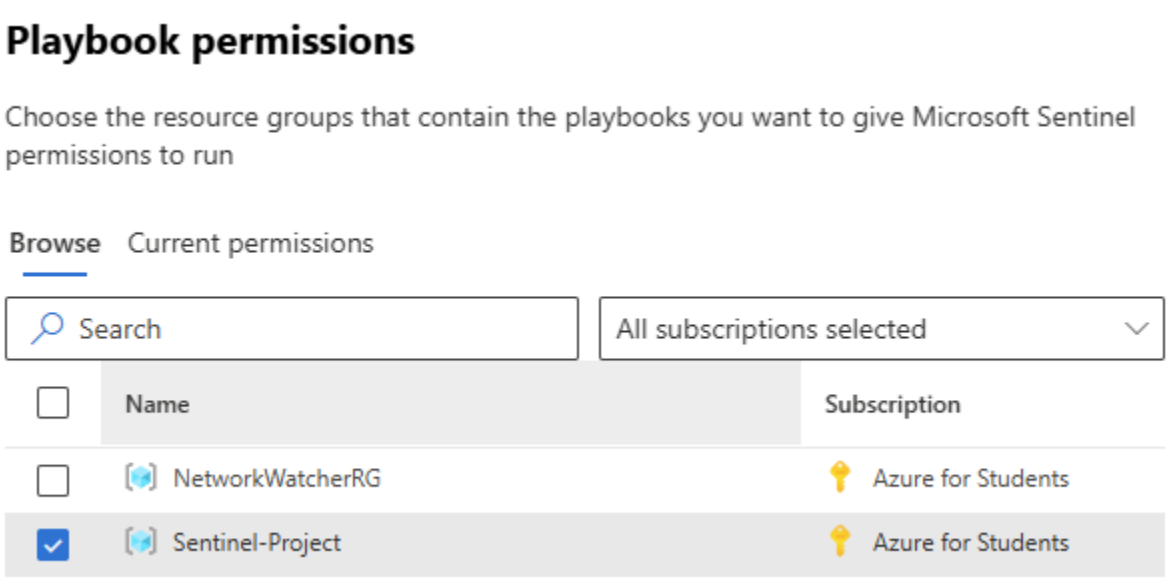
Test the Playbook

I will use the previous generated incident to run the playbook manually

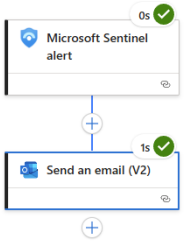


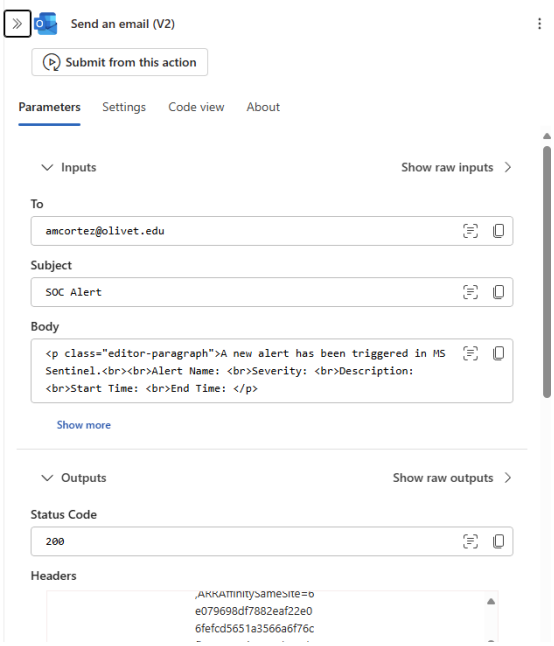
We will run into an error, because MS Sentinel doesn't give access to the resource group for running the playbook by default. So, we need to give access to the resource group for running the playbook.





Now we can run the playbook without error.


0s
Microsoft Sentinel alert
1s
Send an email (V2)


Send an email (V2)
Submit from this action
Parameters
Settings
Code view
About
Inputs
Show raw inputs
To
amcortez@olivet.edu
Subject
SOC Alert
Body
A new alert has been triggered in MS Sentinel.

Alert Name:
Severity:
Description:
Start Time:
End Time:
Show more
Outputs
Show raw outputs
Status Code
200
Headers
e079698df7882eaf22e0
6fefcd5651a3566a6f76c