Unisolate MDE Machine playbook

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

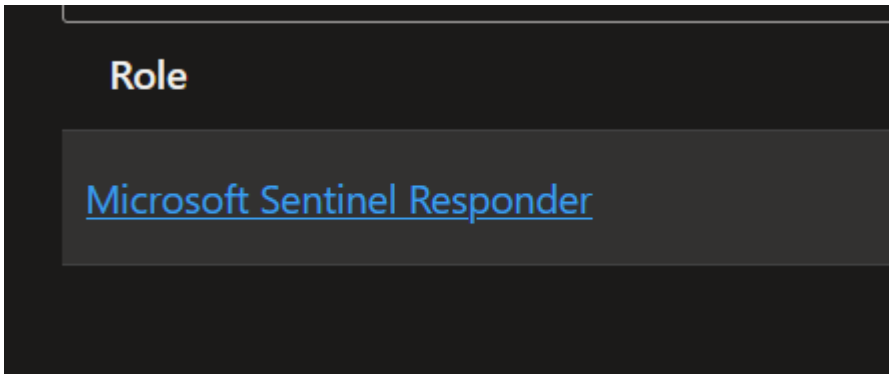
This playbook will release a machine from isolation in Microsoft Defender for Endpoint.

Prerequisites:

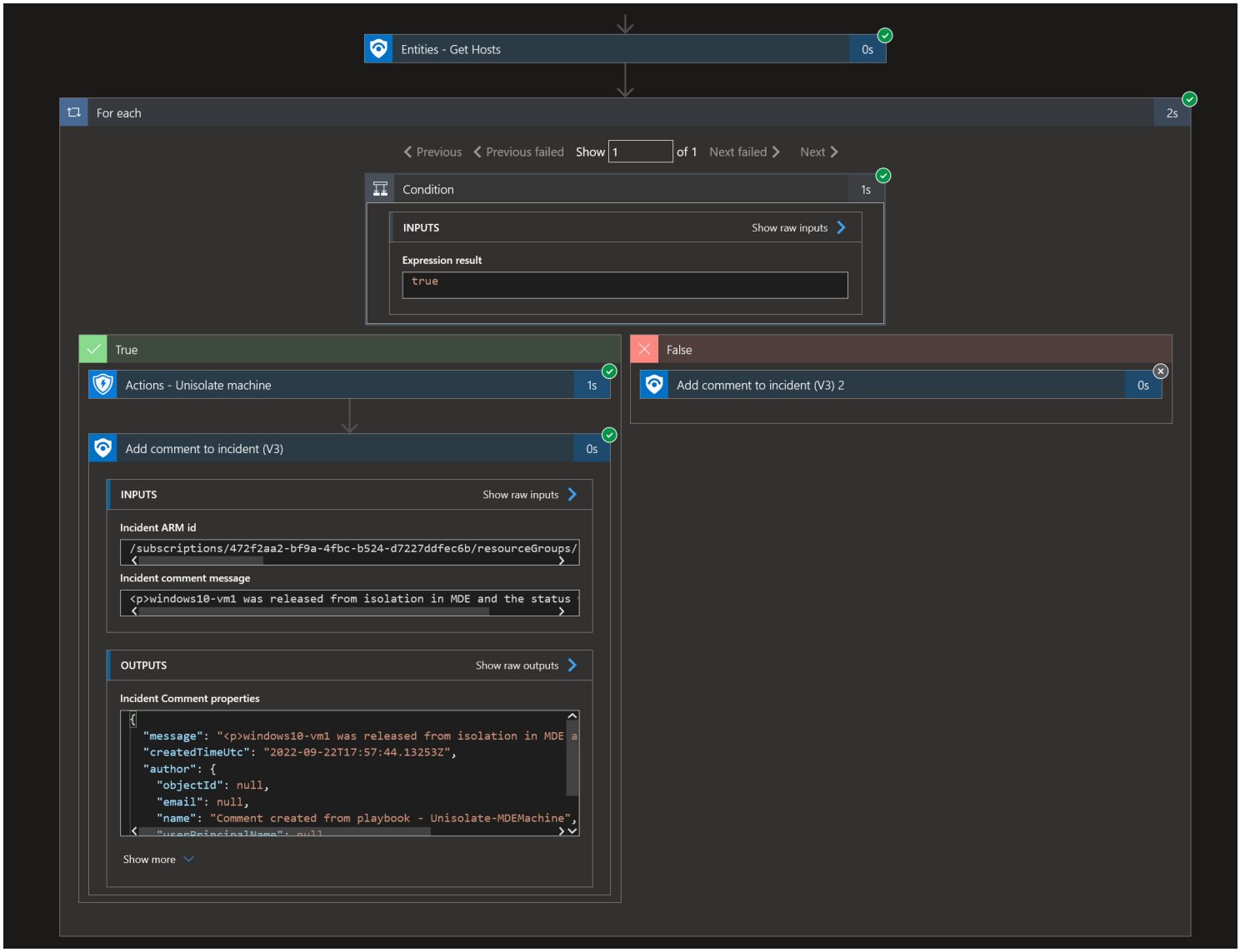
1. Grant Machine.Isolate permissions to the managed identity. Run the following command in cloud shell.

```
$MIGuid = "enter the managed identity id here"
$MI = Get-AzureADServicePrincipal -ObjectId $MIGuid

$MDEAppId = "fc780465-2017-40d4-a0c5-307022471b92"
$PermissionName = "Machine.Isolate"

$MDEServicePrincipal = Get-AzureADServicePrincipal -Filter "appId eq '$MDEAppId'"
$AppRole = $MDEServicePrincipal.AppRoles | Where-Object {$_.Value -eq $PermissionName -and $_.AllowedMemberTyp
New-AzureAdServiceAppRoleAssignment -ObjectId $MI.ObjectId -PrincipalId $MI.ObjectId `
-ResourceId $MDEServicePrincipal.ObjectId -Id $AppRole.Id
```

2. Add Microsoft Sentinel Responder role to the managed identity.



Expected Result:


Entities - Get Hosts
0s
For each
2s
Previous
Previous failed
Show 1 of 1
Next failed
Next
Condition
1s
INPUTS
Show raw inputs
Expression result
true
True
Actions - Unisolate machine
1s
Add comment to incident (V3)
0s
INPUTS
Show raw inputs
Incident ARM id
/subscriptions/472f2aa2-bf9a-4fbc-b524-d7227ddfec6b/resourceGroups/
Incident comment message
<p>windows10-vm1 was released from isolation in MDE and the status
OUTPUTS
Show raw outputs
Incident Comment properties
{
"message": "<p>windows10-vm1 was released from isolation in MDE a
"createdTimeUtc": "2022-09-22T17:57:44.1325Z",
"author": {
"objectId": null,
"email": null,
"name": "Comment created from playbook - Unisolate-MDEMachine",
Show more
False
Add comment to incident (V3) 2
0s

Action center

For submitted actions to take effect, device must be connected to the network.

Investigation package collection

Status

Package collection package available

Package collection submitted

Collect investigation package from playbook for Azure Sentinel Incident: 82

By Get-MDEInvestigationPackage on Sep 13, 2022 1:01:29 PM

Device isolation

Status

Release from isolation pending

Cancel action

Release from isolation submitted

Relased from isolation from playbook for Azure Sentinel Incident: 755 - Unusual number of failed sign-in attempts on one endpoint

By Unisolate-MDEMachine on Sep 22, 2022 10:57:43 AM