Isolate endpoint - MDE playbook

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

This playbook will isolate (full) the machine 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
```

Instructions on how to deploy