Dependencies to deploy a custom Playbook - Powershell Utility

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

Customer asked about documentation to check dependencies to deploy a custom playbook in a new environment:

Export

Export Microsoft Sentinel Playbooks (Azure LogicApps) in the quickest amount of time by sanitizing the JSON contains organizational information such as tenant ID, subscription information, connection strings, and other items that makes sharing a Playbook (Azure LogicApps) a daunting technical challenge.

Powershell utility

This PowerShell utility first evaluates your Azure logic app and any API connections that the logic app uses then generates template resources with the necessary parameters for deployment.

ARM template

You can use this ARM template for your own business scenarios or customize the template to meet your requirements. You can share it safely knowing that your organization's information is stripped from the JSON and that it will work correctly in the recipient environment.

Documentation

Blog: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/export-microsoft-sentinel-playbooks-or-azure-logic-apps-with/ba-p/3275898 ⤢

Demo: https://www.youtube.com/watch?v=scTtVHVzrQw ⤢

Github: https://github.com/Azure/Azure-Sentinel/tree/master/Tools/Playbook-ARM-Template-Generator ⤢