Converting a Sentinel Playbook to a Template

Ref:

<https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks#instructions-for-templatizing-a-playbook>

1. Export your playbook from Sentinel:

Graphical user interface, application

Description automatically generated

1. Unzip the exported file and edit template.json in your preferred editor (Visual studio Code is recommended).
   1. Throughout this procedure pay careful attention to the json syntax. If you see a red highlighted error, immediately fix it before moving to the next step.
2. Delete the entire parameters section:

Timeline

Description automatically generated

1. Replace the parameters section with the information below. NOTE you may need additional parameters, but these are the most common values.

Matt, can we provide an appendix with more parameter examples?

"parameters": {

"PlaybookName": {

"defaultValue": "Mitre\_Mappings",

"type": "String"

},

"SubscriptionID": {

"defaultValue": "Enter your subscription ID.",

"type": "string"

},

"WorkspaceResourceGroup": {

"defaultValue": "Enter workspace resource group name.",

"type": "string"

},

"WorkspaceName": {

"defaultValue": "Enter Azure Sentinel workspace name.",

"type": "string"

},

"WorkspaceID": {

"defaultValue": "Enter Azure Sentinel workspace ID.",

"type": "string"

}

},

1. Replace Variables with this:

"variables": {

"azuresentinelConnectionName": "[concat('azuresentinel-', parameters('PlaybookName'))]",

"azuremonitorlogsConnectionName": "[concat('azuremonitorlogs-', parameters('PlaybookName'))]"

},

A picture containing shape

Description automatically generated

Matt, can we add more parameter options to the Appendix?

1. Add the required ‘connectors’ at the beginning of the ‘Resources’ section:

{

"apiVersion": "2016-06-01",

"name": "[variables('azuremonitorlogsConnectionName')]",

"properties": {

"customParameterValues": {},

"displayName": "[variables('azuremonitorlogsConnectionName')]",

"api": {

"id": "[concat('/subscriptions/', subscription().subscriptionId, '/providers/Microsoft.Web/locations/', resourceGroup().location, '/managedApis/azuremonitorlogs')]"

}

},

"location": "[resourceGroup().location]",

"type": "Microsoft.Web/connections",

"kind": "V1"

},

{

"apiVersion": "2016-06-01",

"name": "[variables('azuresentinelConnectionName')]",

"properties": {

"customParameterValues": {},

"displayName": "[variables('azuresentinelConnectionName')]",

"api": {

"id": "[concat('/subscriptions/', subscription().subscriptionId, '/providers/Microsoft.Web/locations/', resourceGroup().location, '/managedApis/azuresentinel')]"

}

},

"location": "[resourceGroup().location]",

"type": "Microsoft.Web/connections",

"kind": "V1"

},

Matt, can we add more connector options to the Appendix?

Text

Description automatically generated with medium confidence

1. Under the Microsoft.Logic/workflows, replace the name and location lines, and add in the ‘dependsOn’ section as shown here:

"name": "[parameters('PlaybookName')]",

"location": "[resourceGroup().location]",

"dependsOn": [

"[resourceId('Microsoft.Web/connections', variables('azuremonitorlogsConnectionName'))]",

"[resourceId('Microsoft.Web/connections', variables('azuresentinelConnectionName'))]"

],

Diagram

Description automatically generated

1. Scroll down to the very bottom of the json file and replace the connector with this:

"azuremonitorlogs": {

"connectionId": "[resourceId('Microsoft.Web/connections', variables('azuremonitorlogsConnectionName'))]",

"connectionName": "[variables('azuremonitorlogsConnectionName')]",

"id": "[concat('/subscriptions/', subscription().subscriptionId, '/providers/Microsoft.Web/locations/', resourceGroup().location, '/managedApis/azuremonitorlogs')]"

},

"azuresentinel": {

"connectionId": "[resourceId('Microsoft.Web/connections', variables('AzureSentinelConnectionName'))]",

"connectionName": "[variables('AzureSentinelConnectionName')]",

"id": "[concat('/subscriptions/', subscription().subscriptionId, '/providers/Microsoft.Web/locations/', resourceGroup().location, '/managedApis/azuresentinel')]"

}

Text

Description automatically generated with low confidence

Search and replace for any connectors NOT named azuremonitorlogs and azuresentinel.

For example, if you see azuresentinel\_1, replace it with azuresentinel.

Graphical user interface, application

Description automatically generated

1. Replace all the ‘query’ parameters with variables like this:

"queries": {

"resourcegroups": "[parameters('WorkspaceResourceGroup')]",

"resourcename": "[parameters('WorkspaceName')]",

"resourcetype": "Log Analytics Workspace",

"subscriptions": "[parameters('SubscriptionID')]",

"timerange": "Last hour"

}

Matt, are there other common variable that could be added to the Appendix?