These playbooks automate the ingest of threat indicators into the ThreatIntelligenceIndicator table of an Azure Sentinel workspace. Sample data for Log4j IOC can be found at <https://raw.githubusercontent.com/Azure/AzureSentinel/master/Sample%20Data/Feeds/Log4j_IOC_List.csv>. You must deploy the BatchImportToSentinel playbook before deploying the Log4jIndicatorProcessor playbook. You must also make sure the Playbook2 Name parameter uses the exact name you chose when importing the Log4jIndicatorProcessor playbook.

Deploying these playbooks requires the following steps:

1. BatchImportToSentinel is deployed first, you need to provide following parameters –

Graphical user interface, text, application

Description automatically generated

1. BatchImportToSentinel will need connection for the Submit multiple tiIndicators action as shown below.

Graphical user interface

Description automatically generated with low confidence

Managed identity “azuresentinel-<playbookname>” is created as part of deployment. To configure the connection, You need to authenticate with as a user with an Azure Active Directory Limited Administrator Role of Global Administrator. Following script can be used to configure the connection –

Connect-AzureAD -TenantId <tenantid>

$graph = Get-AzureADServicePrincipal -Filter "AppId eq '00000003-0000-0000-c000-000000000000'"

$permissionlist = @( "Group.Read.All","SecurityActions.Read.All","SecurityActions.ReadWrite.All","SecurityEvents.Read.All","SecurityEvents.ReadWrite.All","ThreatIndicators.ReadWrite.OwnedBy" )

foreach( $permission in $permissionlist)

{

$groupReadPermission = $graph.AppRoles `

| where Value -Like ($permission) `

| Select-Object

# Use the Object Id as shown in the image above

$msi = Get-AzureADServicePrincipal -ObjectId <objid of managed identity>

New-AzureADServiceAppRoleAssignment `

-Id $groupReadPermission.Id `

-ObjectId $msi.ObjectId `

-PrincipalId $msi.ObjectId `

-ResourceId $graph.ObjectId

}

Log4jIndicatorProcessor is deployed after BatchImportToSentinel. You need to provide following parameters –

Graphical user interface, text, application

Description automatically generated

1. Log4jIndicatorProcessor Playbook performs the following steps:

* Triggered on a defined schedule
* Reads the indicators from GitHub
* Transforms the indicators from the text-based source to the appropriate tiIndicator JSON format
* Uses the Batch action to send the indicators to the second Playbook (BatchImportToSentinel)

1. Following configuration is needed in Log4jIndicatorProcessor Playbook after deployment

Graphical user interface, text, application, email

Description automatically generated

Query – This KQL query will get the external data from <https://raw.githubusercontent.com/Azure/AzureSentinel/master/Sample%20Data/Feeds/Log4j_IOC_List.csv>. This can be configured to any other data source.

Connection - Configuring this connection, you will be asked to login to Azure Active Directory and consent for the permissions needed for the Playbook to submit threat indicators to the Graph Security API. You need to authenticate with as a user with an Azure Active Directory Limited Administrator Role of Global Administrator.