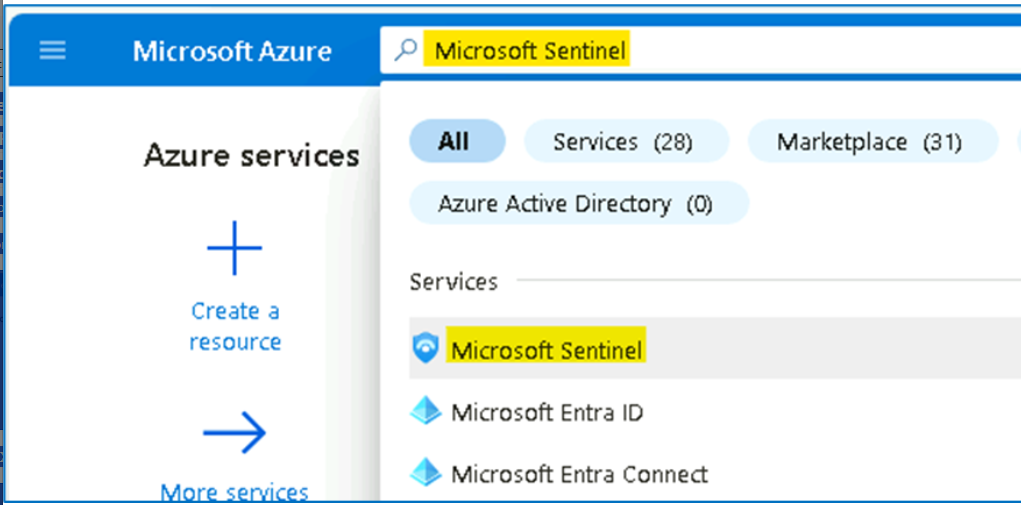
# Lab 8 - Repositories in Microsoft Sentinel

## Exercise 1: Explore Repositories in Microsoft Sentinel

### Task 1: Creating and exporting an analytical rule

In this task, you will enable Entity behaviour analytics in Microsoft Sentinel.

1. On the Azure Portal [**http://portal.azure.com**](urn:gd:lg:a:send-vm-keys), search for [**Microsoft Sentinel**](urn:gd:lg:a:send-vm-keys) and click on **Microsoft Sentinel**.

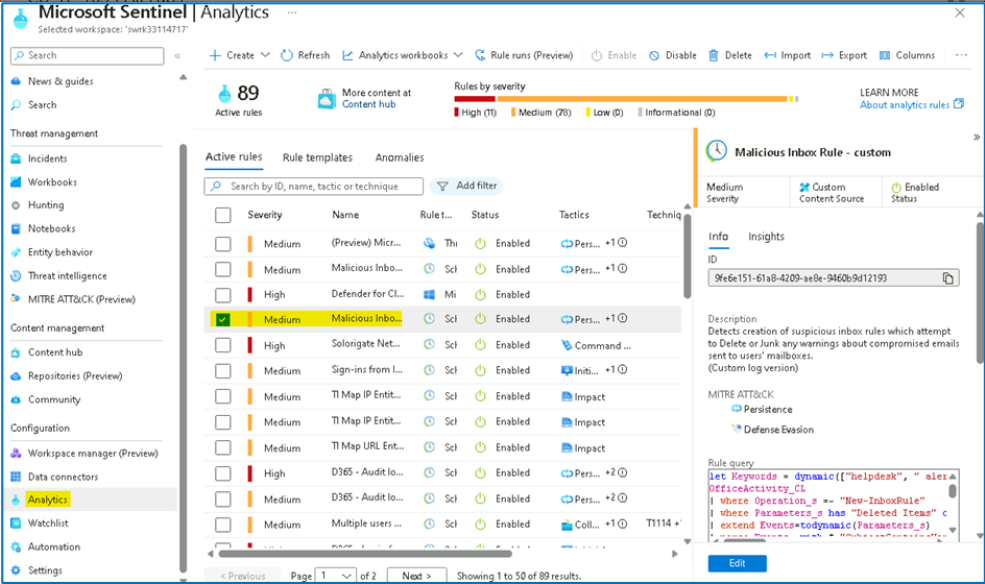


1. Select **SwrkXXXXXXX**.

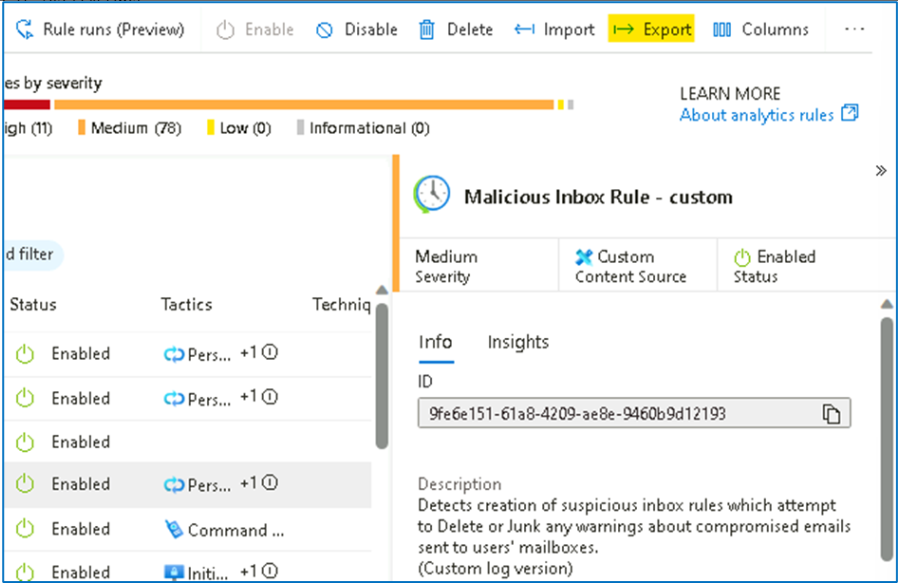
A screenshot of a computer

Description automatically generated

1. Now click on **Analytics** under the **Configuration** area from the left blade. Select the **Malicious Inbox Rule** that you created earlier.



1. Select the **Export** from the toolbar. **Hint:** You might need to select the ellipsis icon **(...)** to see it.



1. The rule is exported to a text file named **Azure\_Sentinel\_analytic\_rule.json**. Select **Open file** below the name of the downloaded file.

A screenshot of a computer

Description automatically generated

1. Select **More apps** and then select **Notepad** and then select **OK**.

A screenshot of a computer

Description automatically generated

1. Review the **Azure Resource Manager** template and the close it when done.

A screenshot of a computer program

Description automatically generated

### Task 2: Creating our Azure DevOps environment

In this task, you will create an Azure DevOps repository.

1. Open another tab in the browser and navigate to [**https://aexprodcus1.vsaex.visualstudio.com/me?mkt=en-US**](urn:gd:lg:a:send-vm-keys)
2. On the **We need a few more details** page, select **Continue**.

A screenshot of a computer

Description automatically generated

1. On the **Get started with Azure DevOps** page, select **Create new organization** and then select **Continue**.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. On the **Almost done...** page, enter a name for your DevOps organization that you would not want to use in the future, like for example, your tenant suffix [number at the end of **m365x**]. Under **We'll host your projects in**, select **United States**. Enter characters you see, then **Continue**.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. On the **Create a project to get started** page, enter **My Sentinel Content** and then select **Create project**.

A screenshot of a computer

Description automatically generated

1. Navigate to **Repos** on the left pane. At the bottom of the page in the area **Initialize main branch with a README or gitignore**, select **Initialize**.

A screenshot of a computer

Description automatically generated

1. The page should show the Files for the Repo. The only file is README.md. On the Files (right side of the page) blade, the toolbar include options *Set up build*, *Clone*, ... Select the colon icon **(:)** to show more options. Select **Upload Files**.

A screenshot of a computer

Description automatically generated

1. Select **Browse** and select the file **Azure\_Sentinel\_analytic\_rule.json** from your **Downloads** directory. Select **Commit**.

A screenshot of a computer

Description automatically generated

1. Select **Azure DevOps** on the top left corner of the page. This display your organization and projects. Select **Organization settings** from the bottom left of the page.

A screenshot of a computer

Description automatically generated

1. Select **Policies** under the **Security** area of the left blade. Toggle **On** **Third-party application access via OAuth** under the **Application connection policies** area.

A screenshot of a computer

Description automatically generated

### Task 3: Connecting Sentinel to Azure DevOps.

1. On the Azure Portal [**http://portal.azure.com**](urn:gd:lg:a:send-vm-keys) and search for **Microsoft Sentinel** and click on **Microsoft Sentinel**.

A screenshot of a computer service

Description automatically generated

1. Select **SwrkXXXXXXX**.

A screenshot of a computer

Description automatically generated

1. Now click on **Repositories (Preview)** in the **Content Management** section.

A screenshot of a computer

Description automatically generated

1. Select **+ Add new** button from the toolbar.

A screenshot of a computer

Description automatically generated

1. For the name enter [**My Content**](urn:gd:lg:a:send-vm-keys). For Source control, select **Azure DevOps**. Select **Authorize**.

A screenshot of a computer

Description automatically generated

1. On the **Azure Sentinel V3 (Prod) by Microsoft** page scroll down the permissions request and then select **Accept**.

A screenshot of a computer

Description automatically generated

1. Select the **Organization** your created earlier. Select the Project you created earlier, **My Sentinel Content**. Select the Repository you created earlier, **My Sentinel Content**. Select the Branch **main**. Select all content types. Then select **Create**.

A screenshot of a computer

Description automatically generated

1. The Connection creation error can occur, close the page and return back to Repositories (Preview) page.

A close-up of a message

Description automatically generated

1. On the **Repositories** *(Preview)* page, select **Refresh**. Wait **until *Last* deployment status** is **Failed**.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Note**: The Failed status is due to limitations in the hosted lab environment. You would normally see Succeeded. Then you can see in the Analytics the imported rule Rule from Azure DevOps.

**Congratulation** you have completed Lab 8. In this lab, we had explored the advanced features of Microsoft Sentinel.