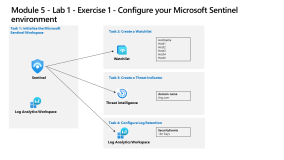
Module 5 - Lab 1 - Exercise 1 - Configure your Microsoft Sentinel environment

**Scenario**



You are a Security Operations Analyst working at a company that is implementing Microsoft Sentinel. You are responsible for setting up the Microsoft Sentinel environment to meet the company requirement to minimize cost, meet compliance regulations, and provide the most manageable environment for your security team to perform their daily job responsibilities.

Task 1: Initialize the Microsoft Sentinel Workspace

In this task, you will create a Microsoft Sentinel workspace.

1. Log in to [**WIN1**](urn:gd:lg:a:select-vm) virtual machine as [**Admin**](urn:gd:lg:a:send-vm-keys) with the password: [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. Open the **Edge browser**.
3. In the Edge browser, navigate to the Azure portal at [**https://portal.azure.com**](urn:gd:lg:a:send-vm-keys).
4. In the **Sign in** dialog box, copy, and paste in the tenant Email account for the admin username [**admin@WWLx470898.onmicrosoft.com**](urn:gd:lg:a:send-vm-keys) and then select **Next**.
5. In the **Enter password** dialog box, copy, and paste in the admin's tenant password provided [**42LG~xlgD==I56^n**](urn:gd:lg:a:send-vm-keys) and then select **Sign in**.
6. In the Search bar of the Azure portal, type [**Sentinel**](urn:gd:lg:a:send-vm-keys), then select **Microsoft Sentinel**.
7. Select **+ Create**.
8. Next, select the Log Analytics workspace you created earlier, for example **uniquenameDefender** and select **Add**. The activation could take a few minutes.

**Note:** If you do not see a Log Analytics workspace here, please refer to Module 3, Exercise 1, Task 2 to create one.

1. Navigate around the newly created Microsoft Sentinel workspace to become familiar with the user interface options.

Task 2: Create a Watchlist

In this task, you will create a watchlist in Microsoft Sentinel.

1. In the search box at the bottom of the Windows 11 screen, enter [**Notepad**](urn:gd:lg:a:send-vm-keys). Select **Notepad** from the results.
2. Type [**Hostname**](urn:gd:lg:a:send-vm-keys) then enter for a new line.
3. From row 2 of the notepad, copy the following hostnames, each one in a different line:
4. Host1
5. Host2
6. Host3
7. Host4
8. Host5
9. From the menu select, **File - Save As**, Name the file [**HighValue.csv**](urn:gd:lg:a:send-vm-keys), change the **save as type** **All files(*.*)** and select **Save**.

**Hint:** The file can be saved in the **Documents** folder.

1. Close Notepad.
2. In Microsoft Sentinel, select the **Watchlist** option under the **Configuration** area.
3. Select **+ New** from the command bar.
4. In the Watchlist wizard, enter the following:

| **General setting** | **Value** |
| --- | --- |
| Name | [**HighValueHosts**](urn:gd:lg:a:send-vm-keys) |
| Description | [**High Value Hosts**](urn:gd:lg:a:send-vm-keys) |
| Watchlist alias | [**HighValueHosts**](urn:gd:lg:a:send-vm-keys) |

1. Select, **Next: Source >**.
2. Select **Browse for files** under **Upload file** and browse for the **HighValue.csv** file you just created.
3. In the **SearchKey field** select **Hostname**.
4. Select **Next: Review and Create >**.
5. Review the settings you entered and select **Create**.
6. The screen returns to the Watchlist page.
7. Select the **HighValueHosts** watchlist and on the right pane, select **View in logs**. To see the right pane, you may need to expand it by clicking on the **<<** icon

**Important:** It could take up to ten minutes for the watchlist to appear. **Please continue to with the following task and run this command on the next lab**.

**Note:** You can now use the \_GetWatchlist('HighValueHosts') in your own KQL statements to access the list. The column to reference would be *Hostname*.

1. Close the **Logs** window by selecting the 'x' in the top-right and select **OK** to discard the unsaved edits.

Task 3: Create a Threat Indicator

In this task, you will create an indicator in Microsoft Sentinel.

1. In Microsoft Sentinel, select the **Threat intelligence** option in the **Threat management area**.
2. Select **+ Add New** from the command bar.
3. Review the different indicator types available in the **Types** dropdown. Select the **domain-name**. Enter [**WWLx470898.onmicrosoft.com**](urn:gd:lg:a:send-vm-keys).
4. On the New indicator blade, under **Threat types**, select **+ Add**, type [**malicious-activity**](urn:gd:lg:a:send-vm-keys) and select **OK**.
5. For the **Name**, enter the same value used for the Domain. [**WWLx470898.onmicrosoft.com**](urn:gd:lg:a:send-vm-keys)
6. Enter a **Description**
7. For the **Name**, enter the same value used for the Domain.
8. Set the **Valid from** field to today's date.
9. Select **Apply**.
10. Select the **Logs** option under the General area. You might want to disable the "Always show queries" option and close the **Queries** window to run the KQL statements.
11. Run the following KQL statement.
12. ThreatIntelligenceIndicator

**Note:** It could take up to five minutes for the indicator to appear.

1. Scroll the results to the right to see the DomainName column. You can also run the following KQL statement to just see the DomainName column.
2. ThreatIntelligenceIndicator
3. | project DomainName

Task 4: Configure log retention

In this task, you will change the retention period for the SecurityEvent table.

1. In Microsoft Sentinel, select the **Settings** option under **Configuration** in the left navigation pane.
2. Select **Workspace settings**.
3. In Log Analytics workspace, select the **Tables** option in the *Settings* area.
4. Search and select the table **[SecurityEvent](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)**, and then select the ellipsis button (...).
5. Select **Manage Table**.
6. Select **180 days** for **Total retention period**. Then **Save**.

**06:03:256 hours and 3 minutes remaining on your lab session**

Module 7 - Lab 1 - Exercise 4 - Explore Entity Behavior Analytics

**Scenario**

You are a Security Operations Analyst working at a company that implemented Microsoft Sentinel. You already created Scheduled and Microsoft Security Analytics rules.

You need to configure Microsoft Sentinel to perform Entity Behavior Analytics to discover anomalies and provide entity analytic pages.

Task 1: Explore Entity Behavior

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

1. Log in to [**WIN1**](urn:gd:lg:a:select-vm) virtual machine as [**Admin**](urn:gd:lg:a:send-vm-keys) with the password: [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. In the Edge browser, navigate to the Azure portal at [**https://portal.azure.com**](urn:gd:lg:a:send-vm-keys).
3. In the **Sign in** dialog box, copy and paste in the [**admin@WWLx470898.onmicrosoft.com**](urn:gd:lg:a:send-vm-keys) account provided by your lab hosting provider and then select **Next**.
4. In the **Enter password** dialog box, copy and paste in the [**42LG~xlgD==I56^n**](urn:gd:lg:a:send-vm-keys) provided by your lab hosting provider and then select **Sign in**.
5. In the Search bar of the Azure portal, type [**Sentinel**](urn:gd:lg:a:send-vm-keys), then select **Microsoft Sentinel**.
6. Select your Microsoft Sentinel Workspace you created earlier.
7. Select the **Entity behavior** under **Threat Management** in the left hand navigation pane.
8. On the popup from **Entity behavior settings**, select **Set EUBA**.
9. On the next page, select **Set UEBA**.
10. Review the three pre-requisite steps to enable entity behavior analytics.
11. Close the Entity behavior configuration page by selecting the **x** at the top right of the page.
12. Scroll down the **Settings** page and read through the **Anomalies** paragraph.
13. Select **Go to analytics** in order to configure the anomalies.

Task 2: Confirm and review Anomalies rules

In this task, you will confirm Anomalies analytics rules are enabled.

1. You should be now at the Analytics page, Anomalies tab.
2. Confirm status column of the rules is **Enabled**.
3. Select any rule. Then select **Edit** on the rule blade.

**Note:** If you do not see an edit button, scroll across and select the **...** icon on the right of the rule name.

1. Review the **General** tab information. Then select **Next : Configuration**
2. Review the **Configuration** tab information. Notice that you cannot change the **Anomaly score threshold**.
3. Then select **X** in the top right corner to exit the Analytics rule wizard.
4. Scroll right to the analytics rule you selected until see and select the ellipsis **(...)** icon.
5. Select **Duplicate** and scroll left to review the new rule with the **FLGT** tab at the beginning of the name.
6. Select **FLGT** rule and then select **Edit** again.
7. Review the **General** tab information. Notice the **Mode** is **Flighting** and then select **Next: Configuration**.
8. Review the **Configuration** tab information. Notice that you can now change the **Anomaly score threshold**.
9. Set the value to [**1**](urn:gd:lg:a:send-vm-keys) and then select **Next: Submit Feedback**.
10. Select **Next: Review** and then **Save** to update the rule.

**Note:** You can upgrade the **Flighting** rule to **Production** by changing the setting on this rule and save the changes. The **Production** rule will become the **Flighting** rule afterwards.

**06:01:016 hours and 1 minute remaining on your lab session**