# Laboratorio 5 - Defender for Cloud y Sentinel.

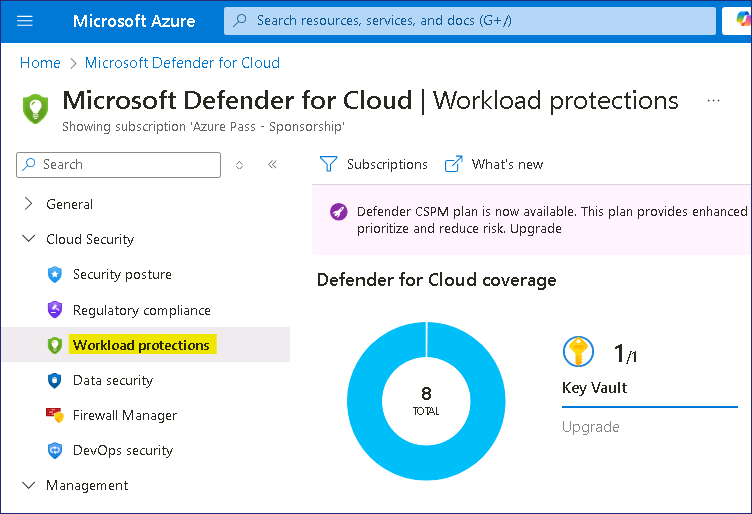
**Tarea 1: Habilite JIT en sus MVs desde Microsoft Defender for Cloud**

1. En el **Azure Portal** +++https://portal.azure.com+++ escriba +++Microsoft Defender for Cloud+++ en el cuadro de búsqueda y, a continuación, haga clic en **Microsoft Defender for Cloud** en **Services**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image1.png)

1. En el panel izquierdo de la página **Microsoft Defender for Cloud | Overview**, vaya a la sección **Cloud Security** y haga clic en **Workload Protections**.

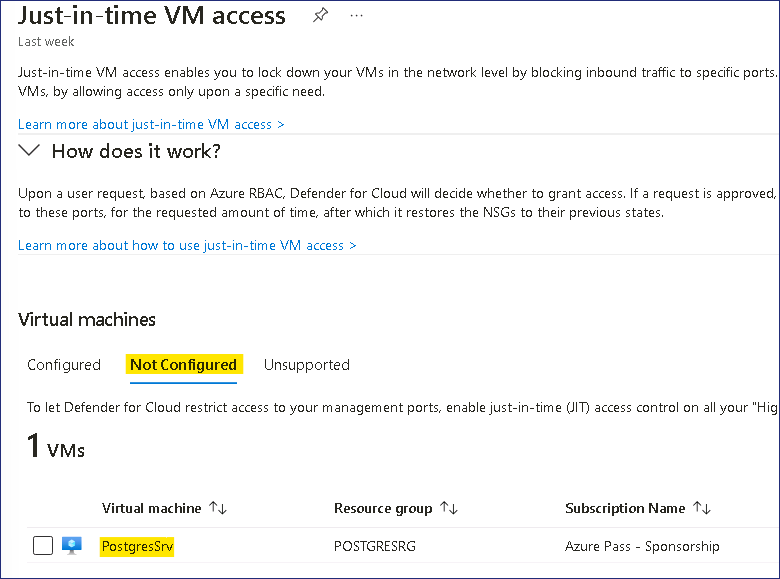
[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image2.png)

1. En la página **Microsoft Defender for Cloud | Workload protections**, desplácese hacia abajo y haga clic en **Just-in-time VM access** bajo la sección **Advanced protection** como se muestra en la siguiente imagen.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image3.png)

1. En la página de **Just-in-time VM access**, vaya a la sección **Virtual machines** y haga clic en la pestaña **Non Configured**. Verá las MVs - **PostgreSrv** que aparece en la pestaña **Non** **Configured**.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image4.png)

1. Seleccione una de las VMs disponibles y haga clic en el botón **Enable JIT on 1 VM** de la derecha.

[A screenshot of a computer

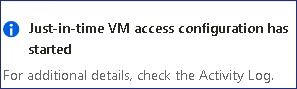
Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image5.png)

1. En la página de **JIT VM access configuration**, haga clic en **Save**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image6.png)

1. Recibirá una notificación, con el siguiente mensaje: **Just-in-time VM access configuration has started**.

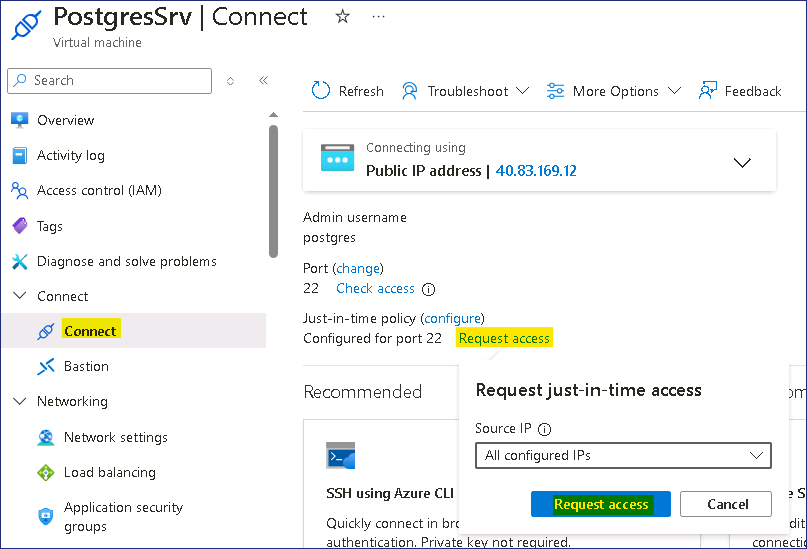
[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image7.png)

1. Haga clic en la pestaña **Configured** bajo la sección **Virtual machines**, verá que la VMs **PostgreSrv** está listada bajo la pestaña **Configured**.

[A screenshot of a computer

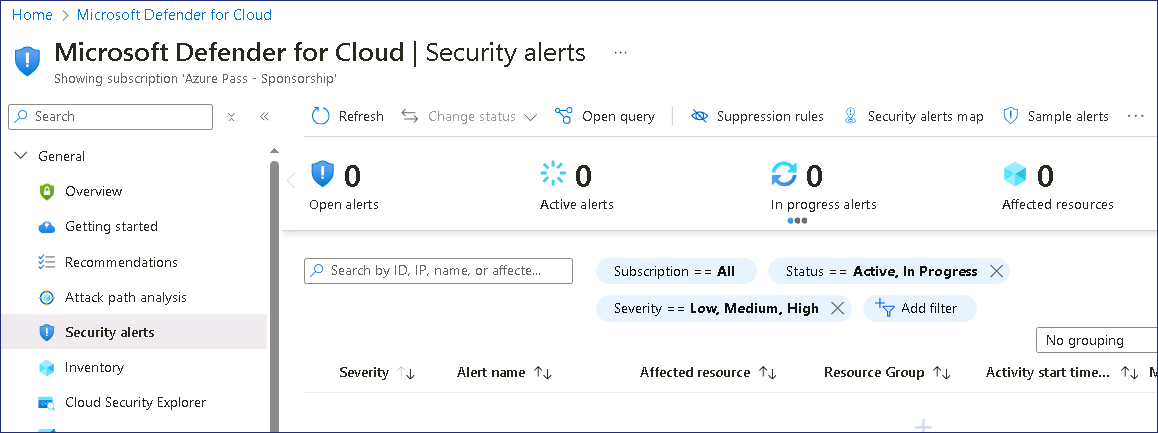
Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image8.png)

1. Ahora, para conectarse a esta VM, el acceso se concede previa solicitud.

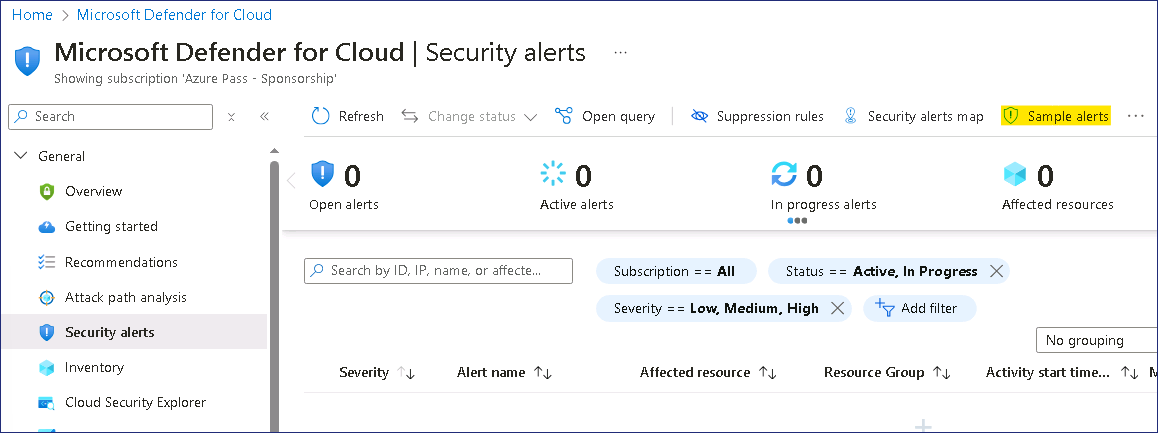
[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image9.png)

**Tarea 2: Genere e investigue alertas de seguridad**

1. En **Microsoft Defender for Cloud**, en la sección **General**, seleccione **Security alerts.**

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image10.png)

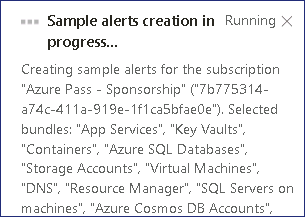
1. Haga clic en el botón **Sample alerts** para generar alertas.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image11.png)

1. Haga clic en el botón **Create sample alerts**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image12.png)

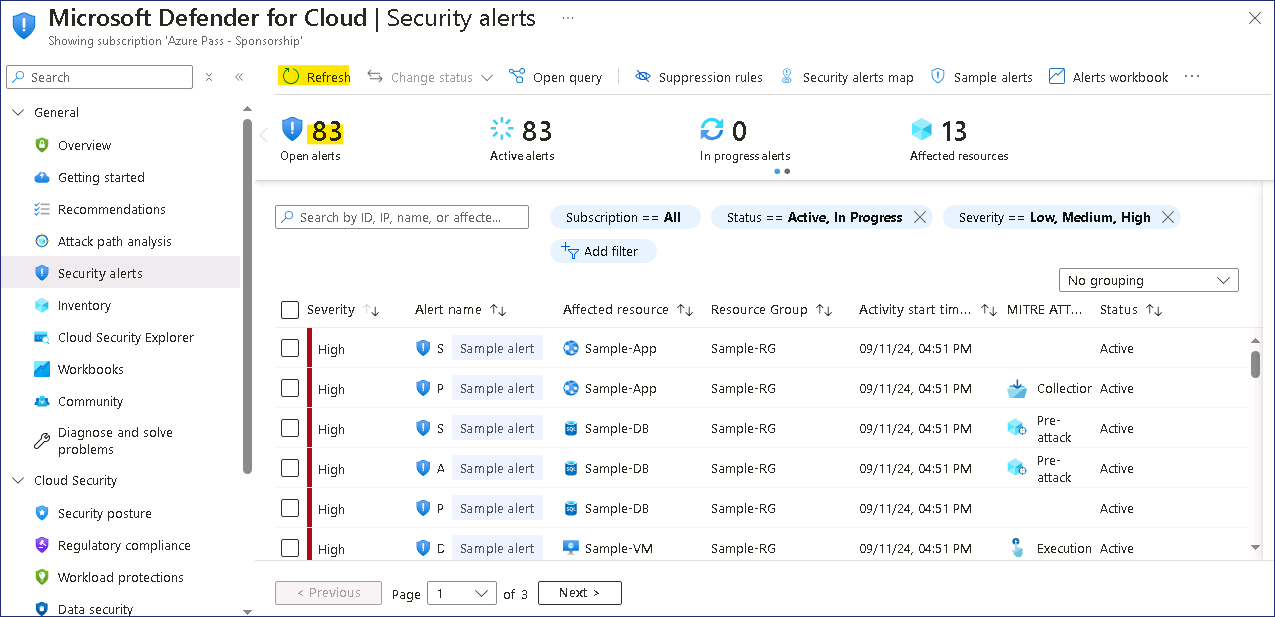
[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image13.png)

1. Se generarán descripciones de muestra

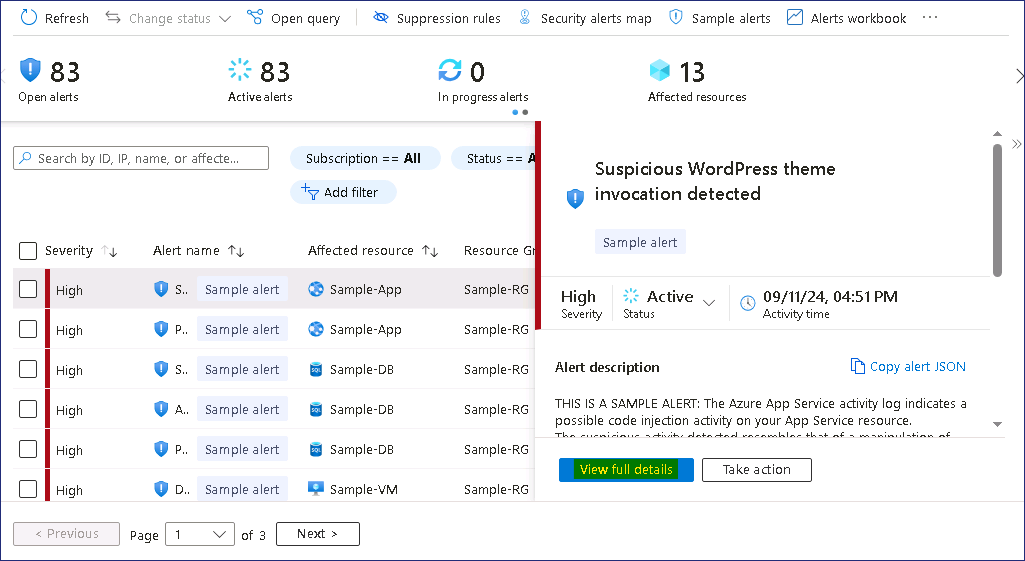
[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image14.png)

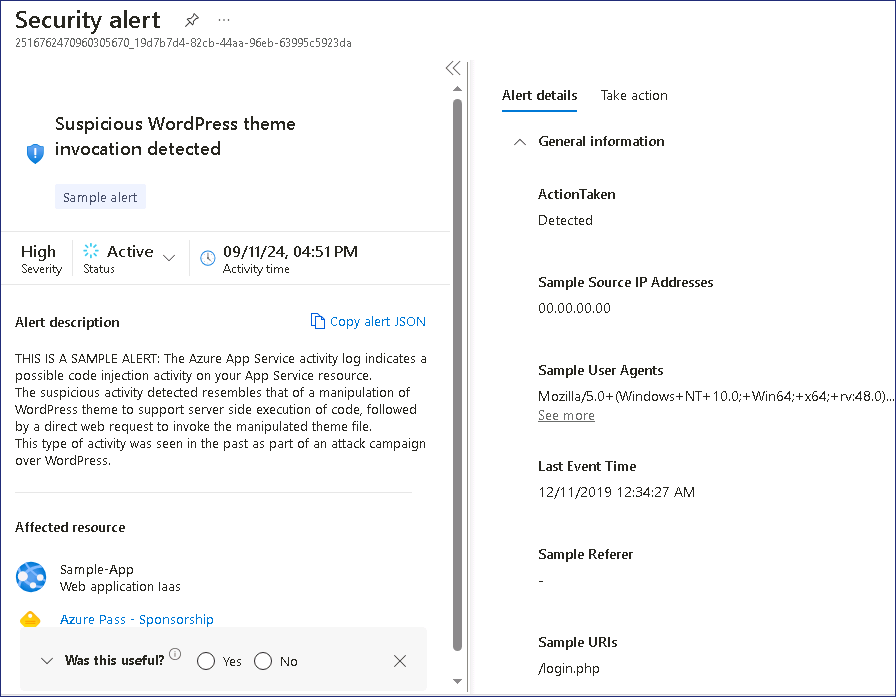
1. Haga clic en el botón **Refresh** y podrá ver las alertas de muestra.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image15.png)

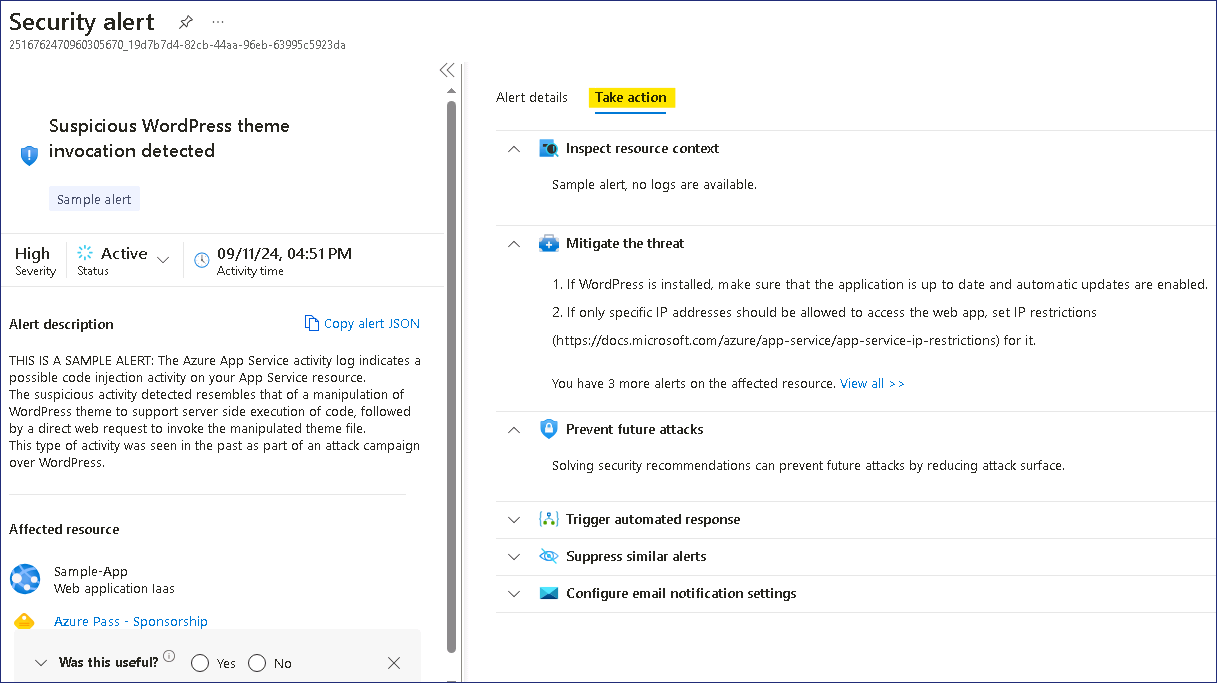
1. Puede hacer clic en cualquier alerta que desee investigar
2. En el panel de resumen de alertas, investigue los siguientes detalles.
   1. **Severity, Status, and Activity time**
   2. **Description** que explica con precisión la actividad detectada
   3. **Affected resources**
   4. **Kill chain intent** de la actividad en la matriz ATT&CK de MITRE.
3. Para obtener información más detallada que pueda ayudarle a investigar la actividad sospechosa, haga clic en el botón **View full details**.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image16.png)

1. Revise la información en la pestaña **Alert details**.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image17.png)

1. Haga clic en el botón **Take action** y revise las opciones disponibles

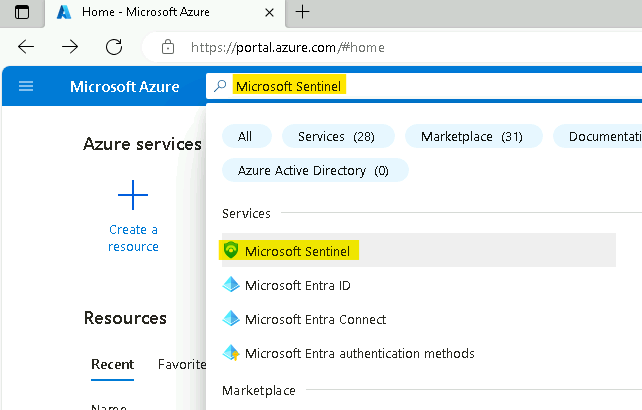
[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image18.png)

**Ejercicio 2 - Implementación de Sentinel**

**Tarea 1: Espacio de trabajo de Microsoft Sentinel**

En este ejercicio veremos cómo crear un área de trabajo de Microsoft Sentinel.

1. Vaya a +++https://portal.azure.com+++ e inicie sesión con las credenciales **MOD Administrator** proporcionadas con los recursos de laboratorio de su entorno de laboratorio.
2. En la barra de búsqueda superior, escriba +++Microsoft Sentinel+++ y haga clic en **Microsoft Sentinel**.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image19.png)

1. En la pantalla de **Microsoft Sentinel**, haga clic en **Create** en la parte superior izquierda.

[A screenshot of a computer

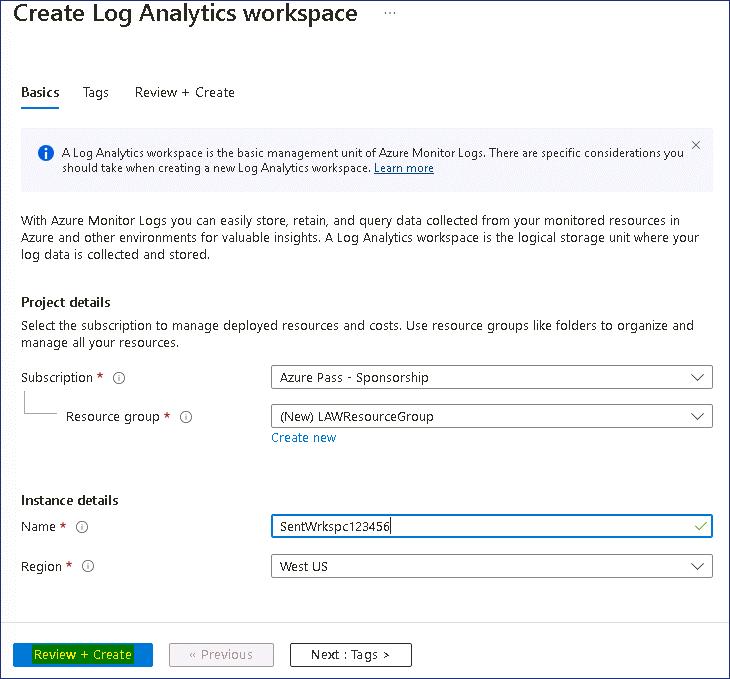
Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image20.png)

1. Puede elegir entre añadir **Microsoft Sentinel** a un **Log Analytics** **workspace** existente o crear uno nuevo. Vamos a crear uno nuevo, así que haga clic en **Create a new workspace**.

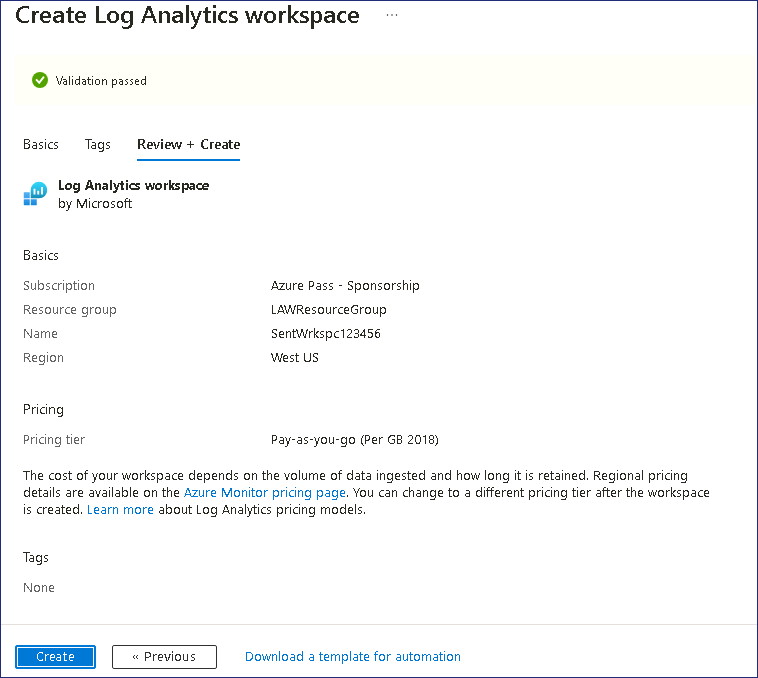
[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image21.png)

1. En la página **Create Log Analytics workspace**, diligencie el formulario como se indica a continuación:
   1. Subscription: **Azure Pass - Sponsorship**
   2. Resource Group: haga clic en **Create new** +++LAWResourceGroup+++.
   3. Workspace Name: +++SentWrkspcXXXXXX+++ [sustituya **XXXXXX** por un número aleatorio].
   4. Region: **West US**
   5. Haga clic en **Review + create**.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image22.png)

1. Haga clic en **Create** una vez completada la validación. La creación tarda unos segundos.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image23.png)

1. Se le redirigirá de nuevo a la página **Add Microsoft Sentinel** a un área de trabajo, haga clic en el botón **Refresh**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image24.png)

1. Selecciona el espacio de trabajo que acaba de crear y haga clic en **Add**, ubicadaen la parte inferior.

[A screenshot of a computer

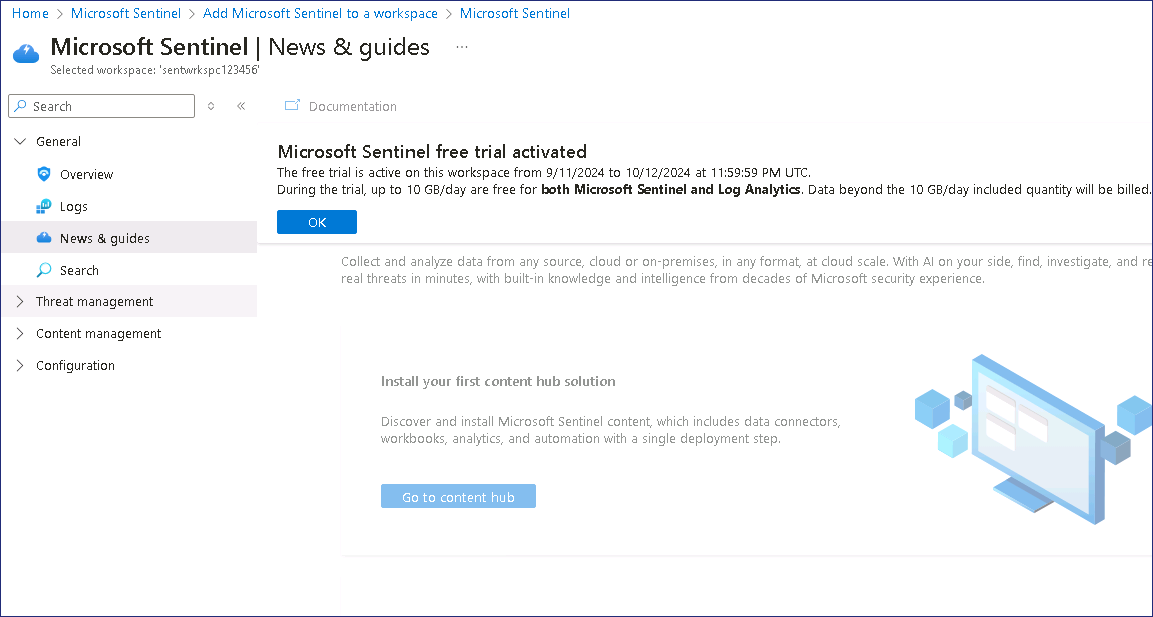
Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image25.png)

1. Debería recibir una notificación como la que se muestra en la siguiente imagen

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image26.png)

1. Su espacio de trabajo Microsoft Sentinel ya está listo para ser utilizado, haga clic en el botón **OK** para continuar.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image27.png)

**Tarea 2: Habilite los conectores de datos.**

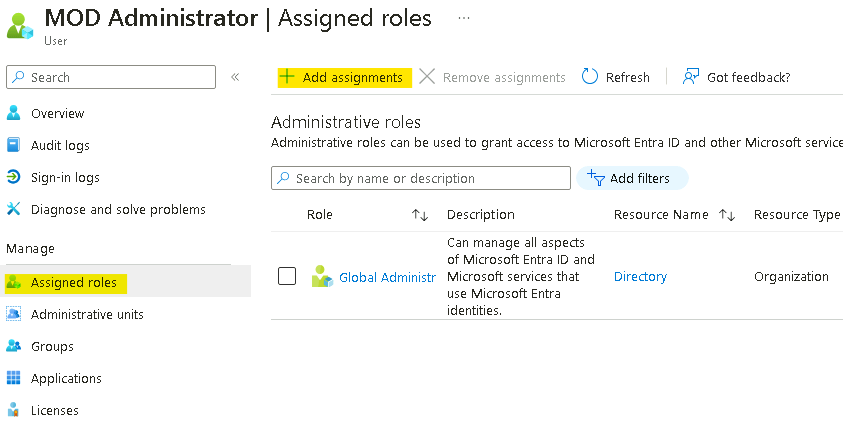
Este ejercicio muestra cómo activar los conectores de datos.

1. En la pestaña del navegador, vaya a +++https://portal.azure.com/#view/Microsoft\_AAD\_UsersAndTenants/UserManagementMenuBlade/~/AllUsers+++ y seleccione **Tenant Administrator account.**

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image28.png)

1. Seleccione las **Assigned roles** en Manage y, a continuación, haga clic en **+ Add assignments.**

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image29.png)

1. Busque y seleccione **Security Administrator** y, a continuación, haga clic en el botón **Add**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image30.png)

[A close-up of a black text

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image31.png)

1. En el Azure Portal https://portal.azure.com, busque Microsoft Sentinel y haga clic en **Microsoft Sentinel**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image32.png)

1. Seleccione **SentWrkspcXXXXXX**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image33.png)

1. Ahora seleccione **Data Connectors** en la sección **Configuration**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image34.png)

1. Debería aparecer el mensaje **Data Connector with "content source = gallery content" have been removed.** En ese mensaje seleccione el enlace **Click here**

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image35.png)

1. En la página de **Out-of-the-box Content Centralization**, haga clic en **Continue.**

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image36.png)

1. Haga clic en el botón **Complete centralization**

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image37.png)

1. Debería recibir la notificación como se muestra en la siguiente imagen

[A close-up of a sign

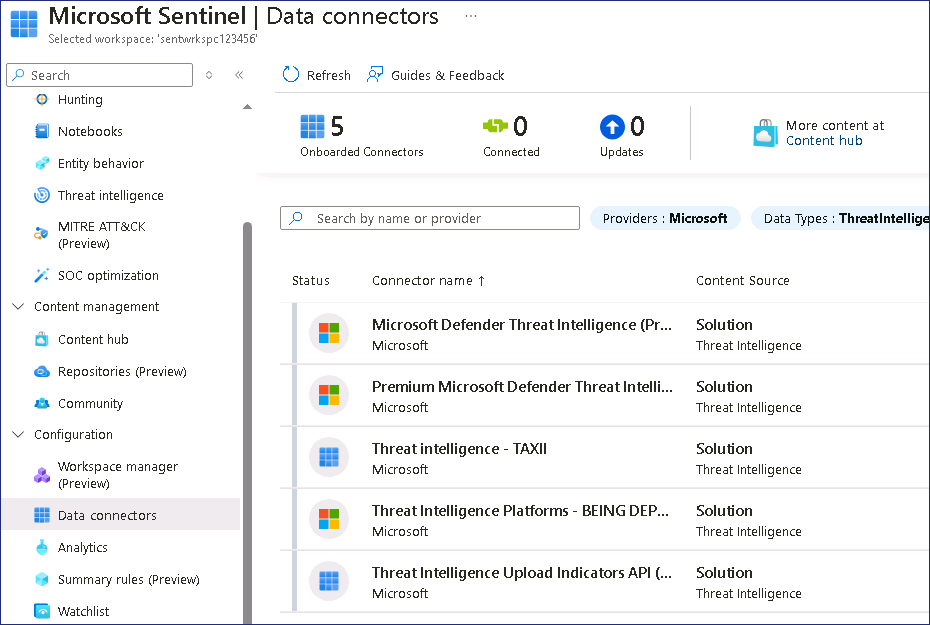
Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image38.png)

1. En la parte superior, haga clic en el enlace de **Microsoft Sentinel** o vuelva a la página de Sentinel.

[A screen shot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image39.png)

1. Haga clic en el botón **Refresh** y debería poder ver algunos conectores de datos visibles.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image40.png)

**Nota** - En ocasiones, es posible que no se instale ningún conector, lo cual también está bien para continuar con los laboratorios.

1. Haga clic en **Content hub,** debajo de **Content management**

[A screenshot of a computer

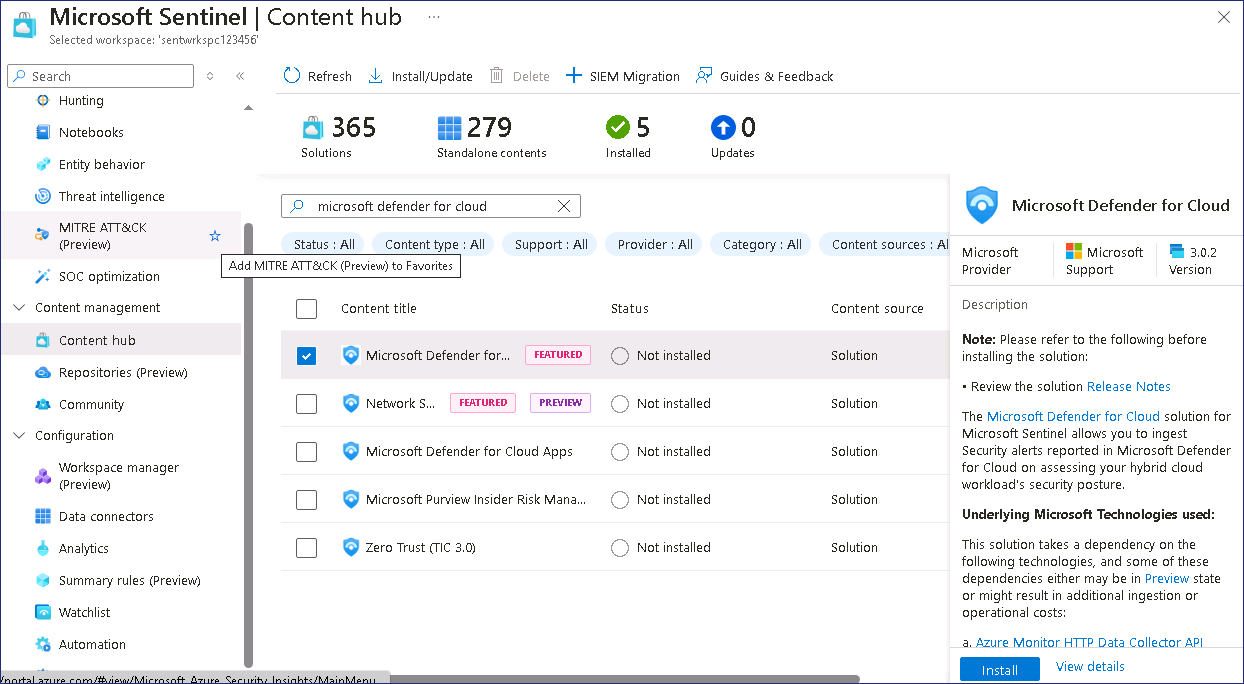
Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image41.png)

1. En la página Content hub, busque Azure Activity, luego seleccione el contenido **de Azure Activity** y haga clic en el botón **Install.**

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image42.png)

1. En la página Content hub, busque Microsoft Defender forCloud, luego seleccione el contenido de **Microsoft Defender for Cloud** y haga clic en el botón **Instalar.**

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image43.png)

**Tarea 3: Habilite el conector de datos Azure Activity**

Este ejercicio muestra cómo habilitar el conector de datos Azure Activity. Este conector traerá todos los eventos de auditoría, para las acciones realizadas en Azure subscription, a su espacio de trabajo de Microsoft Sentinel.

1. En la página de **Microsoft Sentinel**, haga clic en **Data Connectors** en la sección **Configuration**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image44.png)

1. En la pantalla de conectores de datos, escriba activity en la barra de búsqueda, seleccione el conector **Azure Activity** y haga clic en **Open connector page**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image45.png)

1. En la página **Azure Activity connector**, vaya a la opción número **2. Connect your subscriptions through diagnostic settings new pipeline**. Este método aprovecha Azure Policy y ofrece muchas mejoras en comparación con el método anterior (se pueden encontrar más detalles sobre estas mejoras aquí). Haga clic en el asistente **Launch Azure Policy Assignment**, esto le redirigirá a la página de creación de políticas.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image46.png)

1. En la selección **Scope** seleccione **Azure Pass – Sponsorship**. Haga clic en **Select**.

[Screens screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image47.png)

1. Vaya a la pestaña **Parameters**. En el **Primary Log Analytics workspace**, seleccione **MicrosoftSentinelWorkspace**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image48.png)

1. En la pestaña **Remediation**, seleccione la casilla junto a **Create a remediation task** y, a continuación, haga clic en el botón **Review + create**

[A screenshot of a computer screen

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image49.png)

1. En la pestaña **Review + create**, haga clic en el botón **Create**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image50.png)

1. En el panel de **Notification** podrá ver las notificaciones ‘**Role Assignments creation succeeded**’, ‘**Remediation task creation succeeded**’ y ‘**Creating policy assignment succeeded**’.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image51.png)

1. En la página **Azure Activity connector** podrá ver el estado de la conexión.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image52.png)

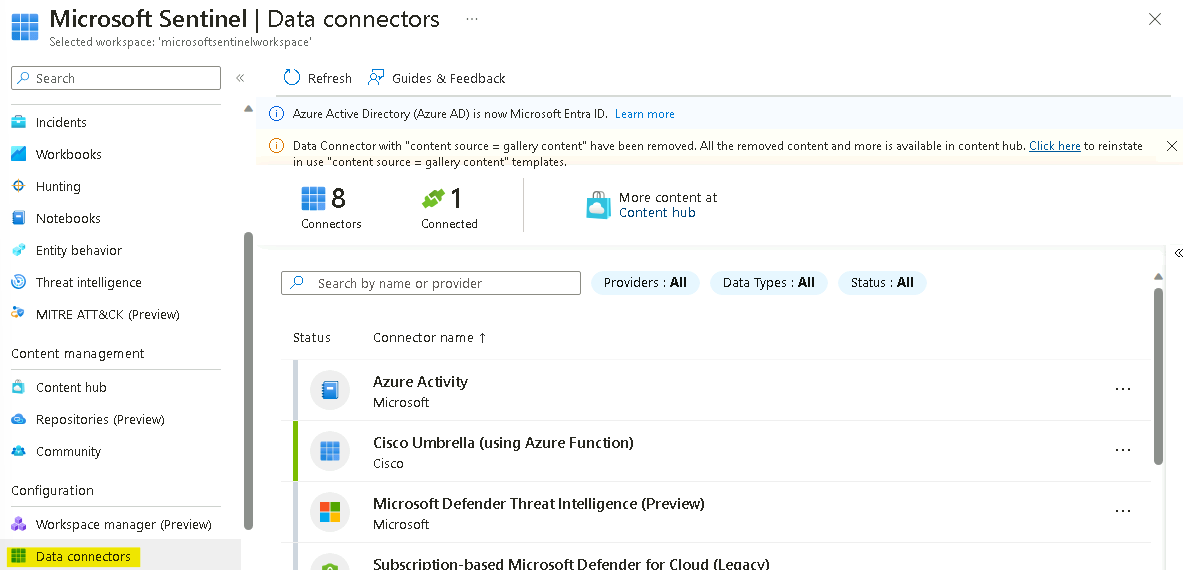
**Nota**: Es normal que el conector no aparezca inmediatamente como **Connected** y en color verde, el proceso tarda unos 30 minutos en completarse.

1. Continúe con el siguiente ejercicio y vuelva a verificar al cabo de 30 minutos.

**Tarea 4: Habilite el conector de datos de Microsoft Defender for Cloud.**

Este ejercicio muestra cómo habilitar el conector de datos de Microsoft Defender for Cloud. Este conector le permite transmitir sus alertas de seguridad de Microsoft Defender for Cloud a Microsoft Sentinel, para que pueda ver los datos de Defender en libros de trabajo, consultarlos para producir alertas e investigar y responder a incidentes.

1. En la página de **Microsoft Sentinel**, haga clic en **Data Connectors** en la sección **Configuration**.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image44.png)

1. En la pantalla **Data connectors**, escriba tenant en la barra de búsqueda, seleccione el conector **Tenant-based Microsoft Defender for Cloud** **(Preview)** y haga clic en **Open connector page**.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image53.png)

**Nota** - Si recibe el error **Data Connector Not Found**, vaya a **Content Hub** y vuelva a instalar **Microsoft Defender for Cloud Connector**.

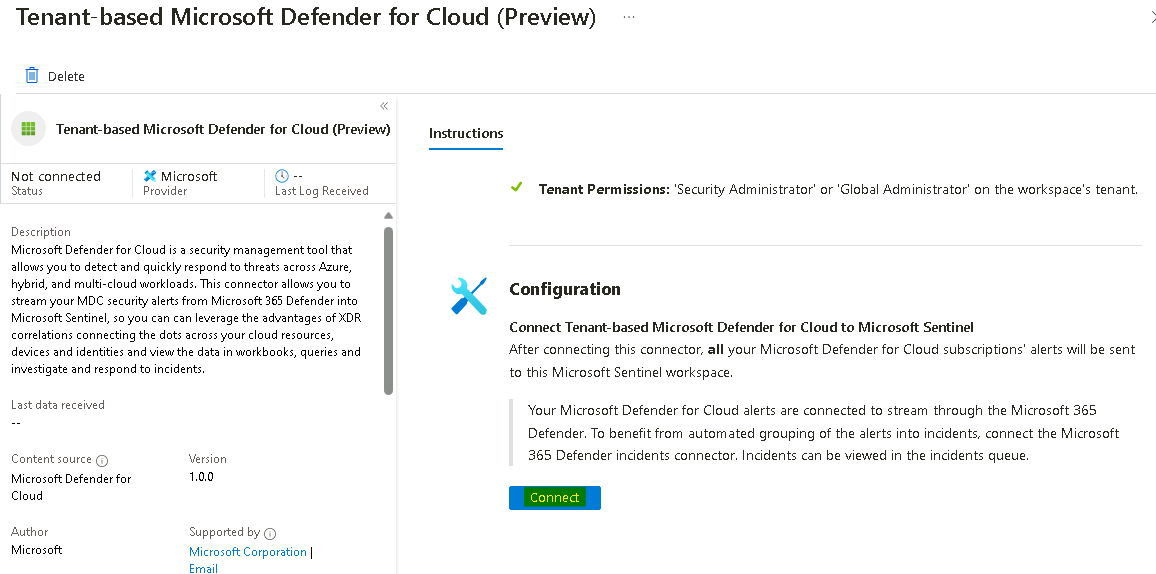
[A black text on a white background

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image68.png)

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image69.png)

1. En la página del conector **Tenant-based Microsoft Defender for Cloud** **(Preview)**, en la sección **Configuration**, haga clic en el botón **Connect**.

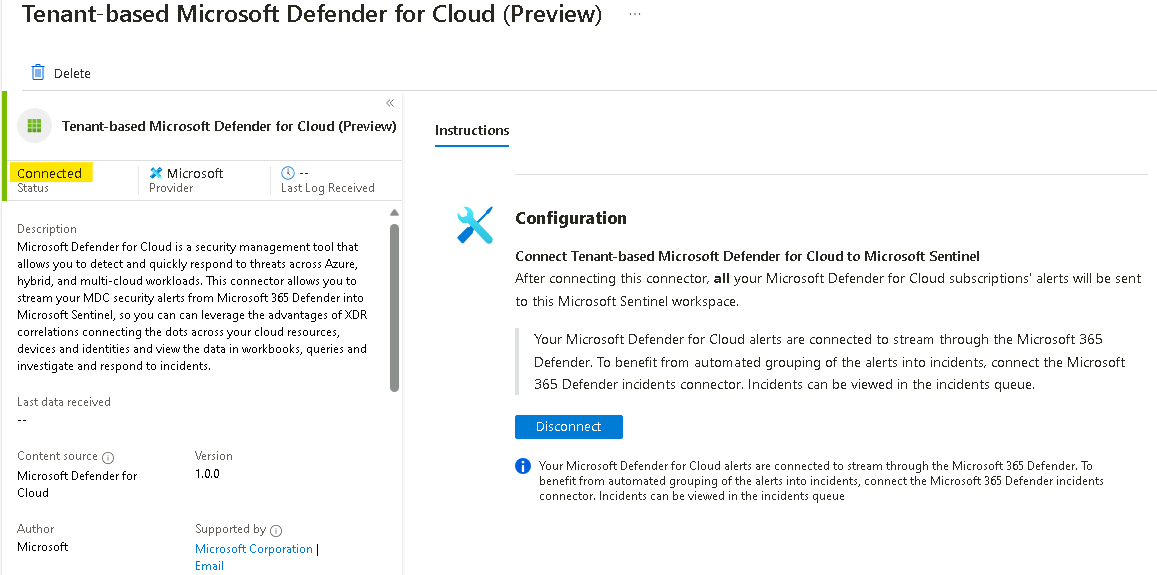
[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image54.png)

1. Debería recibir la notificación **Connected successfully.**

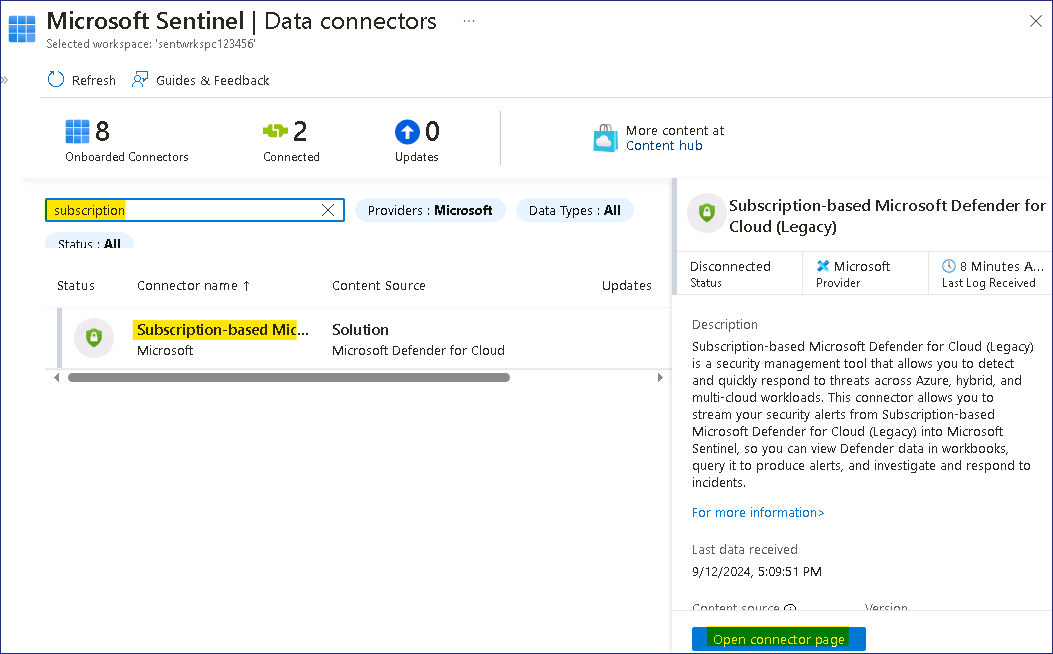
[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image55.png)

1. Espere 1-2 minutos y luego actualice la página. El estado del conector también debería actualizarse a **Connected.**

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image56.png)

1. Regrese a la pantalla **Data connectors**, escriba subscription en la barra de búsqueda, seleccione el conector **Subscription-based Microsoft Defender for Cloud** **(legacy)**, luego haga clic en **Open connector page**.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image57.png)

1. En la página del conector **Subscription-based Microsoft Defender for Cloud** **(legacy)**, en la sección **Configuration**, seleccione la suscripción **Azure Pass – Sponsorship** y, a continuación, haga clic en el botón **Connect**.

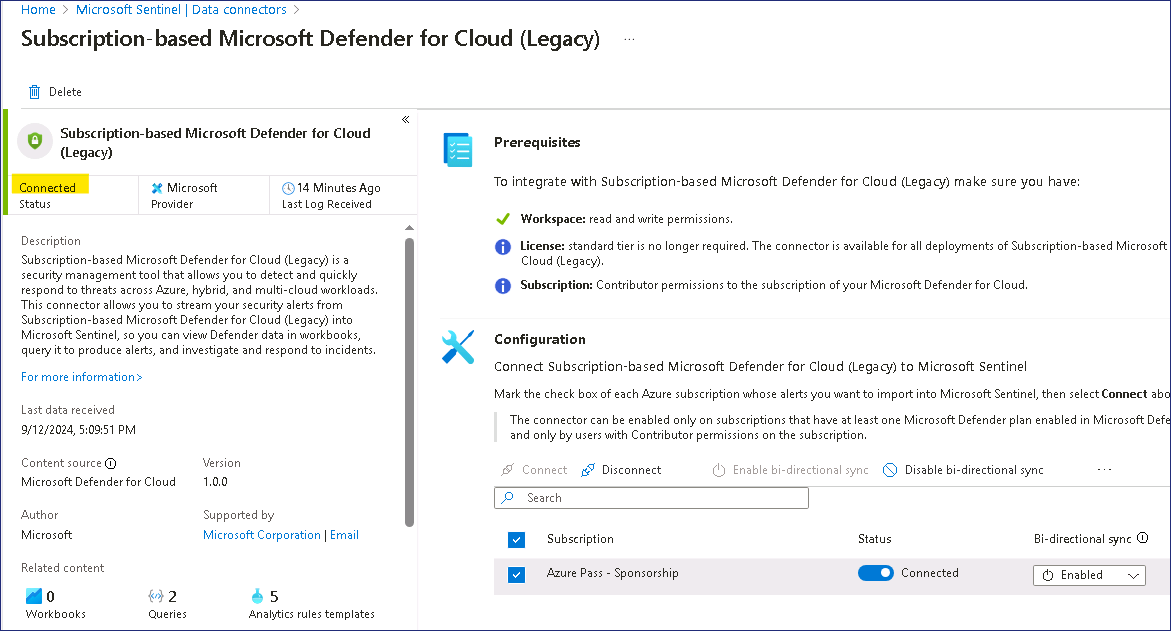
[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image58.png)

1. Debería recibir la notificación **Connected successfully**.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image59.png)

1. El estado del conector también debería actualizarse a **Connected.**

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image60.png)

**Ejercicio 3- Integración**

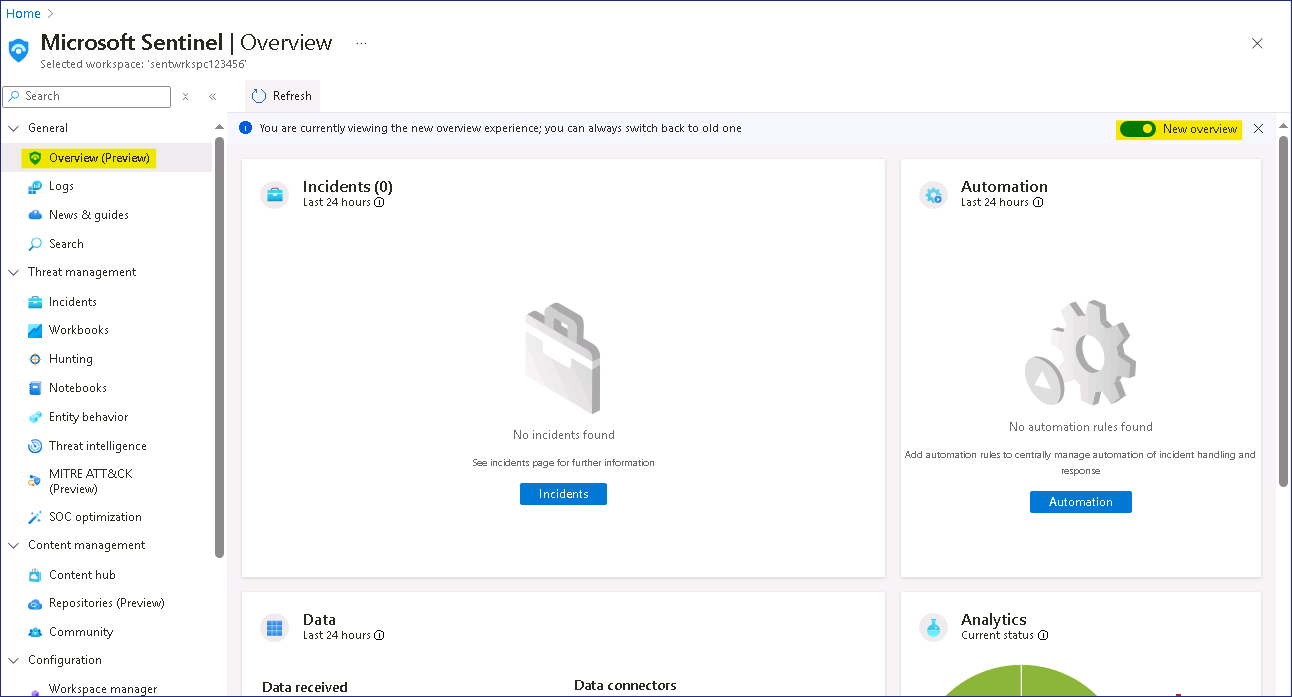
Como hemos instalado el conector Defend for Cloud, deberíamos poder ver el Incidente de Microsoft Defender for Cloud generado, utilizando las Alertas de ejemplo.

1. En la página de **Microsoft Sentinel**, haga clic en **Incidents** en Threat management.

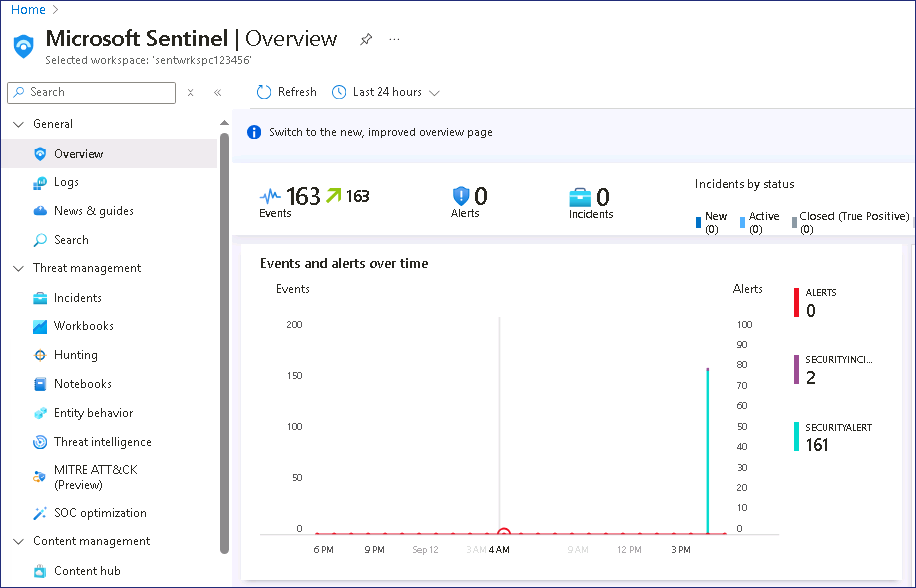
[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image61.png)

1. Como acabamos de activar el conector de **Microsoft Defender for Cloud**, los incidentes tardarán entre 20 y 30 minutos en aparecer.
2. Haga clic en **Overview** en **General** y, a continuación, **desactive** la opción **New overview.**

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image62.png)

1. Una vez desactivado el interruptor, deberíamos poder ver los **Sample events** de Microsoft Defender for Cloud.

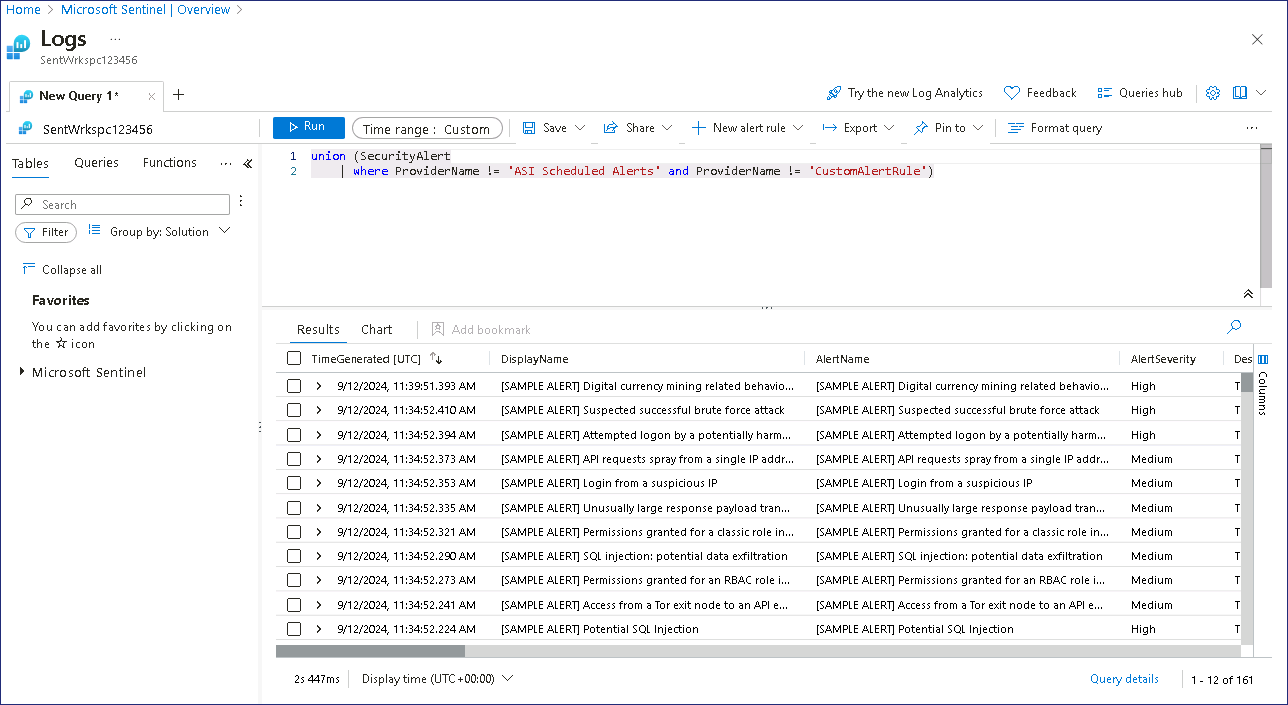
[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image63.png)

1. Haga clic en **SecurityAlerts**

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image64.png)

1. Debería abrir el espacio de trabajo Log Analytic y listar todos los registros de **Alertas** generados y sincronizados desde **Microsoft Defender for Cloud**.

[](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image65.png)

1. Haga clic en cualquier **Alerta** para ampliar y listar los detalles de la misma.

[A screenshot of a computer

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image66.png)

1. En los detalles ampliados de la alerta se puede ver.
   1. TimeGenerated [UTC]
   2. Displayname
   3. AlertName
   4. AlertSeverity
   5. Description, que explica con precisión la actividad detectada
   6. ProviderName, Azure Security Center, el nombre anterior de Microsoft Defender for Cloud.
   7. RemeditalSteps
   8. Y otras filas con información adicional.

[A screenshot of a computer error

Description automatically generated](https://github.com/technofocus-pte/migrt2Innovregdepth/blob/main/Lab%20Guides/Lab%205%20-%20Defender%20for%20Cloud%20%26%20Sentinel/media/image67.png)