**Lab Details**

1. In this lab, you will learn how to deploy the Microsoft Sentinel Training Lab solution.
2. Duration: **45 minutes**

**Introduction**

**What is Microsoft Sentinel?**

* Microsoft Sentinel is a cloud-native security information and event manager (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise—fast.
* Microsoft Sentinel SIEM can be considered as SaaS (Security-as-a-Service) based on its high scalability when meeting the security needs of various organizations.
* It is a SIEM (Security Information and Event Management) and Security Orchestration and Automated Response (SOAR) system in Microsoft's public cloud platform.
* It can provide a single solution for alert detection, threat visibility, proactive hunting, and threat response. It collects data from different data sources, performs data correlation, and Data Visualization the processed data in a single dashboard. It helps to collect, detect, investigate and respond to security threats and incidents.Thus delivering intelligent security analytics and threat intelligence all across the enterprise ecosystem.
* It natively incorporates Azure Logic Apps and Log Analytics that enhances its capabilities. It also has built-in advanced machine learning capabilities that can detect actors of threats and suspicious behaviors that can significantly help security analysts to analyze their environment.

**Architecture Diagram**

**Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media**

**Task Details**

1. Sign in to Azure Portal
2. Create a Microsoft Sentinel workspace
3. Deploy the Microsoft Sentinel Training Lab Solution
4. Configure Microsoft Sentinel Playbook
5. Validation test
6. Delete the Resources

**Lab Steps**

**Task 1: Sign in to Azure Portal**

1. Go to the Azure portal by clicking on the **Open Console** button or by using URL [https://portal.azure.com](https://portal.azure.com/).
   * **Note**: It is recommended to use incognito mode to avoid Azure portal cache related issues.
2. If it automatically logs into any other azure account, please logout of it and clear cache.
3. Sign in with your given ***username*** and ***password*** on Azure portal.
4. If login is not working. Click on **End Lab** and start the lab again.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Task 2: Create a Microsoft Sentinel workspace**

1. At the top of the Azure portal, in the search box, enter **Microsoft Sentinel**. Select **Microsoft Sentinel** in the search results.

**Microsoft sentinel es una solución de gestion de eventos y seguridad que permite detectar, responder y prevenir ataques.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Click on **+ Create**.

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. On the **Add Microsoft Sentinel to a workspace** tab, click on **+ Create a new workspace**.

**Crear un workspace en sentinel nos sirve para poder editar y ejecutar consultas de los registros que recopila Microsoft sentinel y así poder analizar los resultados de una forma interactiva.**

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

1. On the **Create Log Analytics workspace** tab, enter or select the following information in the **Basics** tab:

* Resource group : Select **resource group\_XXXXX**
* Instance details :
  + Name : Enter ***whizworkspace[your name]***
  + Region : Select **West Europe**

Texto

Descripción generada automáticamente

1. Click on **Review + create**. Then, click on **Create**. Your deployment will be completed after a few minutes.

Interfaz de usuario gráfica, Diagrama, Texto

Descripción generada automáticamente

1. You will be redirected back to the ***Add Microsoft Sentinel to a workspace***tab. Select your workspace which is listed there.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Click **Add** at the bottom.

Diagrama

Descripción generada automáticamente

1. Now, your Microsoft Sentinel workspace is ready to use.

**Hemos añadido el workspace a Microsoft Sentinel.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Task 3: Deploy the Microsoft Sentinel Training Lab Solution**

1. Now go to the top of the Azure portal, in the search box, enter **Microsoft Sentinel Training**. Select **Microsoft Sentinel Training Lab Solution (Preview)** marketplace item in the search results.

**Microsoft Sentinel Training es una solución de Microsoft Sentinel que incorpora datos de muestra en su espacio de trabajo se Sentinel, lo que nos hará explorer las características de Microsoft Sentinel.**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. Click on **Create**.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. On the **Create Microsoft Sentinel Training Lab Solution (Preview)** tab, enter or select the following information in the **Basics** tab:

* Resource group : Select **resource group\_XXXXX**
* Instance details :
  + Workspace : Select your workspace

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Click on **Review + create**. Then, click on **Create**. The deployment process takes about 15 minutes, this is because we want to make sure that all the ingested data is ready for you to use once finished.

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Sitio web

Descripción generada automáticamente

1. Now, go to Microsoft Sentinel and select your workspace.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. You will see some ingested data and several recent incidents. Don't worry if you don't see 3 incidents like in the screenshot below, they might take a few minutes to be raised.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Task 4: Configure Microsoft Sentinel Playbook**

1. Navigate to your resource group where the resources has been deployed.
2. In the resource group you should see an API Connection resource called **azuresentinel-Get-GeoFromIpAndTagIncident**, click on it.  
   Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

   Descripción generada automáticamente
3. Click on **Edit API connection** under **General**.

Interfaz de usuario gráfica

Descripción generada automáticamente

1. Click on **Authorize** and a new window will open to choose an account. Pick the user that you want to authenticate with. This should normally be the same user that you're logged in with.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Click on **Save**.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Task 6: Delete the Resources**

1. In the search box at the top of the Azure portal, enter **Resource groups**. Select **Resource groups** from the search results.
2. Click on the name of **Resource groups**
3. Select all the Resoures in that **Resource groups**
4. Go to Three dots to the right and then click **Delete** button
5. Now type **delete**
6. Confirm delete

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Completion and Conclusions**

1. You have successfully logged into Azure Portal.
2. You have successfully created a Microsoft Sentinel workspace.
3. You have successfully deployed the Microsoft Sentinel Training Lab Solution.
4. You have successfully configured Microsoft Sentinel Playbook.
5. You have successfully tested the validation.
6. You have successfully deleted the resources.