Case study

Sam's Scoops is benefiting from using several Azure services. They have virtual machines with Azure Bastion, JIT, and Azure firewalls protecting their environment. They are also using Office 365 and recently started using Microsoft 365 Defender to protect the services and users in the business.

Instructions

You have been tasked with bringing the generated data from all these services to a central place. You will do this by deploying Microsoft Sentinel and using the built-in data connectors to connect the different services Sam's Scoops is using.

Step 1: Deploy Microsoft Sentinel and a log analytics workspace

1. From the **Azure portal home** page, search for and select **Microsoft Sentinel**.
2. Select **Create Microsoft Sentinel**.
3. Select **Create a new workspace**.
4. Your current subscription will be already selected. Fill in the following deployment details for a log analytics workspace:

- Resource group: **RG_Web_Server**.
- Instance name: **SamScoops**.
- Region: The region will be prepopulated with the Resource group's current region.

1. Select **Review + Create**.
2. Select **Create**.
3. After a few seconds, a new workspace will be created. Select **SamScoops**.
4. Select **Add**.
5. Select **OK** when the notification of the activation of Microsoft Sentinel's free trial appears.

Step 2: Configure data connectors

1. On the **Get started** page select **Go to content hub.**
2. On the **Content Hub** page select **Azure Active Directory** from the list and select **Install**.
3. After a few seconds, the connector will install. Select **Manage** for Azure Active Directory.

4. You now need to configure the connector. To do this, select **Azure Active Directory** from the list.
5. Select **Open connector page**.
6. Scroll down and select each log from the list and select **Apply Changes**. Data will now be collected from Azure Active Directory.
7. Navigate back by selecting **Microsoft Sentinel | Content hub** at the top of the page.
8. Type **Defender** in the search bar.
9. Select **Microsoft 365 Defender** and Select **Install**.
10. After a few seconds, the connector will install. Then select **Manage** for Microsoft 365 Defender.
11. You now need to configure the connector. To do this, select **Microsoft 365 Defender**.
12. Select **Open connector page**.
13. Scroll down and select **Connect incidents & alerts**.
14. Scroll down and select the tick box next to **Name** under Microsoft Defender for Endpoint.
15. Scroll down and select the tick box next to **Name** under Microsoft Defender Alerts.
16. Select **Apply Changes**.
17. Navigate back to the **Content hub** page **Microsoft Sentinel | Content hub** at the top of the page.

Step 3: Review implementation

1. Select **Data connectors** from the left-hand menu.
2. Filter the output by selecting **Status** and then selecting **Connected** and **Apply**.
3. Record how many connectors have been connected.

Clean-up

If you are using your own Azure subscription, it is recommended that you follow the clean-up instructions to stop compute resources after completing each lesson. When you're working in your own subscription, it's also a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

Please refer to the reading, Clean up resources for instructions on how to delete resources after you've completed the exercise.

Conclusion

You have successfully configured Microsoft Sentinel to collect data from Sam's Scoop's Azure AD and Microsoft 365 Defender tenants. Any events that now happen within these products will be captured by the Sentinel portal, offering one place for Sam's Scoops to access all incidents and alerts.