## Microsoft Defender for Cloud

| **Steps** | **View** |
| --- | --- |
| Navigate to [**https://portal.azure.com**](https://portal.azure.com)portal and open **Microsoft Defender for Cloud**  From there, navigate to the **Data and security blade**  Review the page and note it offers a starting point for your Cloud Data and AI assets |  |
| Scroll down to the **AI closer look** section, click on **services**. This will open the *Cloud Security Explorer* blade.  Note that the query options are pre-populated, hit **Search**.  The outcome is all the AI Services and Platforms in your Cloud environment, you can drill down further if needed.  This solution helps you to have visibility of current and new AI deployments happening in your environment |  |
| Back to the **Data and security blade** and to the **AI closer look** section in the middle pane you’ll see **AI threat detection**, click on **View all AI alerts**.  This will open all the alerts already filtered for your AI workloads.  Select any and view details  For our example we are using “*A Jailbreak attempt on your Azure AI model deployment was blocked by Prompt Shields”* |  |
| With the alert open, review all details provided like:   1. Status 2. Alert description 3. Affected resources 4. MITRE ATT&CK mapping 5. Alert details 6. Take action |  |
| Now, change to the [**https://security.microsoft.com/**](https://security.microsoft.com/) portal, navigate to **Investigation & response -> Incidents & alerts -> Incidents**  Search for **Incident ID 31421**  <https://security.microsoft.com/incident2/31421/overview?tid=0527ecb7-06fb-4769-b324-fd4a3bb865eb>  Note that we have the same Jailbreak alert now contextualized and with the Attack story.  You can navigate the Incident to understand further. |  |
| Back to the **Microsoft Defender for Cloud** main console, navigate to the **Attack path analysis blade.**  Note there are different attack paths listed.  For our AI workloads example click on **“***Internet exposed Azure VM with high severity vulnerabilities allows lateral movement to Critical Storage with sensitive data used by Azure AI Foundry”* |  |
| With the Attack path open, review all details provided like:   1. Status 2. Description 3. Attack story 4. Resource types 5. Graphical view of the attack path |  |
| Navigate to the end of the graph, click on the **Storage Account**, then click on **Insights.**  Note that very important information is provided including the sensitive info types |  |
| **References:**   * [Overview - AI threat protection - Microsoft Defender for Cloud | Microsoft Learn](https://learn.microsoft.com/en-us/azure/defender-for-cloud/ai-threat-protection) * [AI and agents Insights | Microsoft Security Blog](https://www.microsoft.com/en-us/security/blog/topic/ai-and-machine-learning/?msockid=1e08ff6a60ef6d1520ffeb9861e06cb9) |  |