Summary

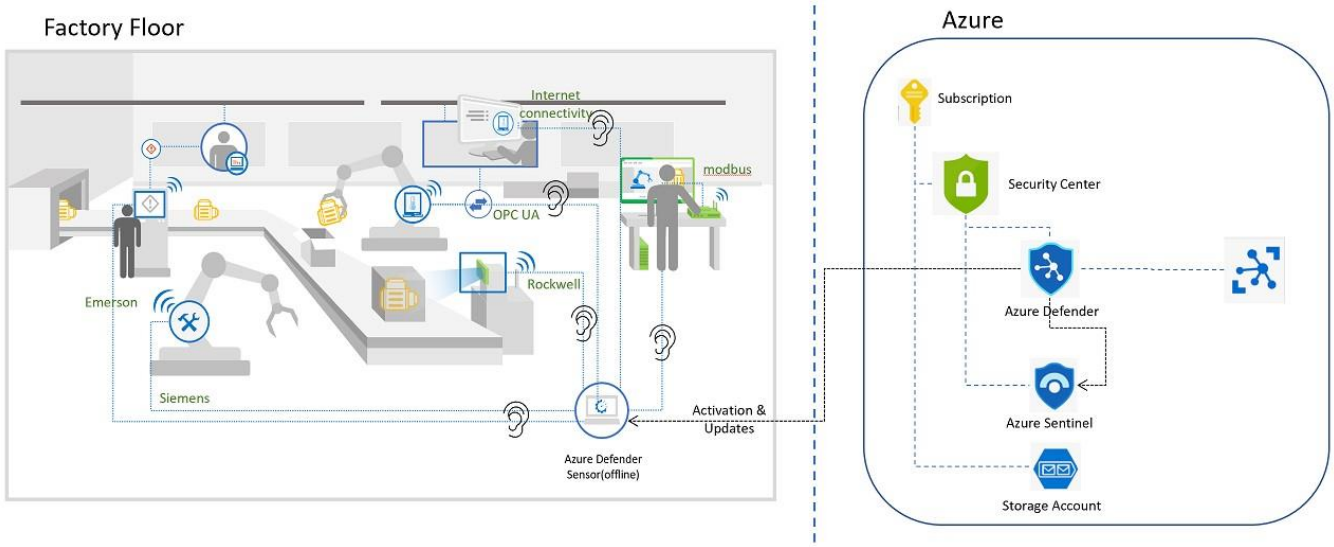
This Hands-on-Lab (HOL) will focus on securing your facilities. We will be simulating traffic by playing some Packet captures, visualizing and analyzing the data on the sensor console. Integrate our sensor with Microsoft Sentinel, to explore alert handling, and for writing queries to help with alert investigation.

Internet of Things - Microsoft Defender for IoT HOL

!! Since the PDF contains hyperlinks, please download the file before proceeding!!

Architecture Diagram

During this workshop we will be focusing on simulating traffic by playing some Packet captures, visualizing and analyzing the data on the sensor console. We will also integrate our sensor with Microsoft Sentinel, to explore alert handling, and for writing queries to help with alert investigation, This Hands-on-Lab (HOL) will focus on securing your facilities. The scenario below is one of many you would apply these lessons to, other scenarios are Oil, Gas, Utility, and Energy companies.

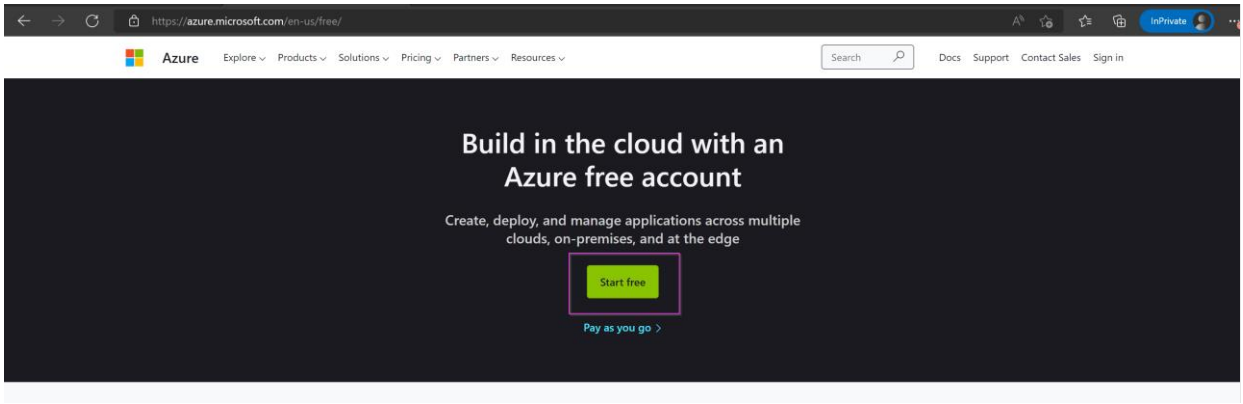


Contents

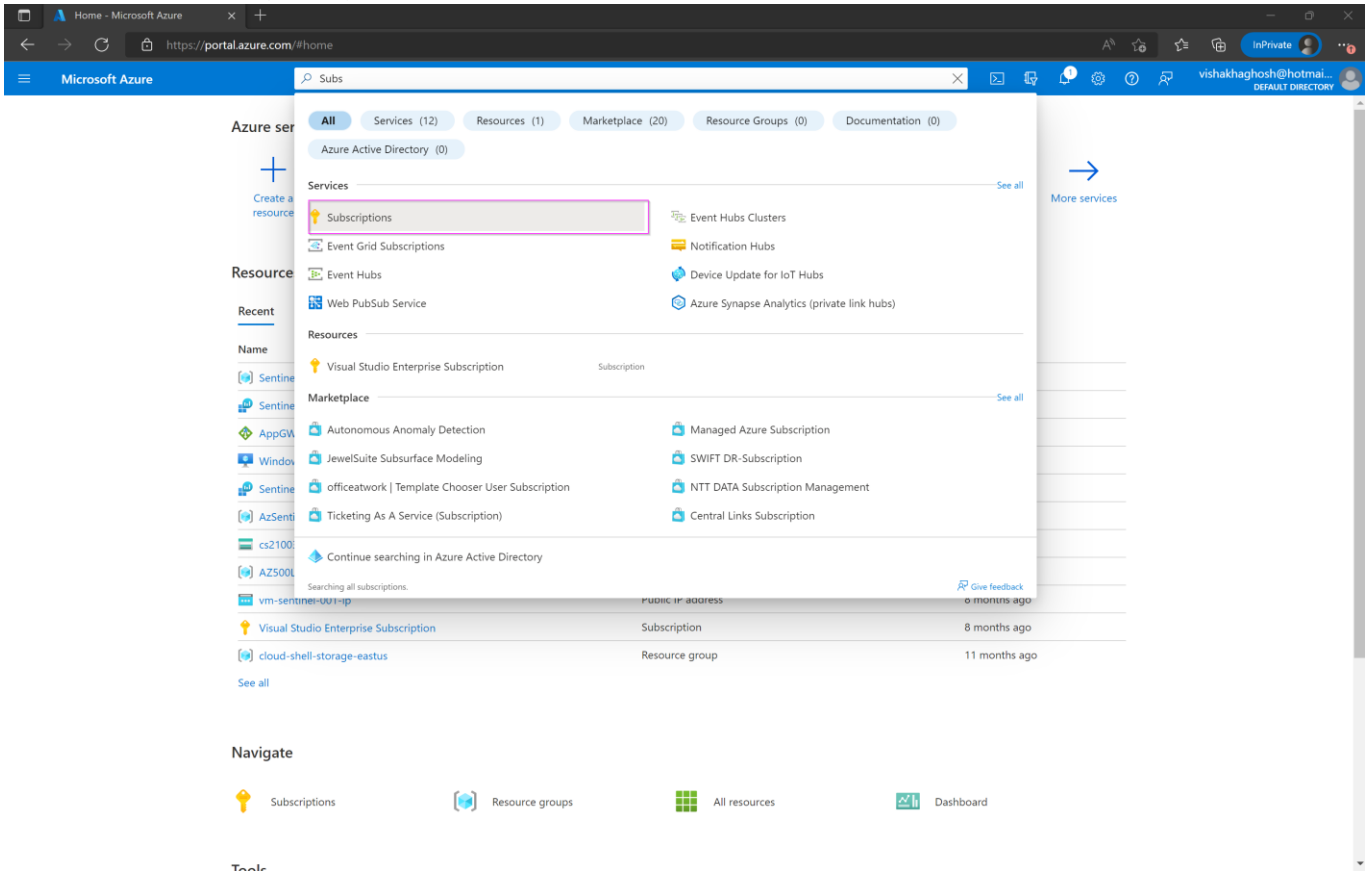
Exercise 1: Enabling Defender

Task 1: Create an Azure Subscription

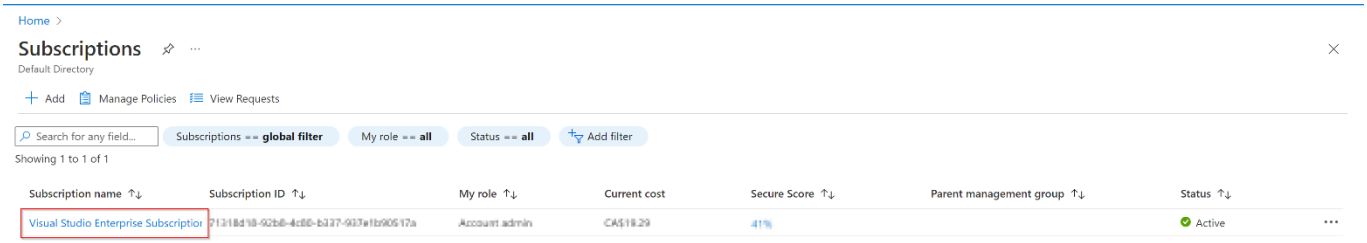
1. Use this link to set up your free trial: https://azure.microsoft.com/en/free.
2. Click on **"Start Free"** as shown in the image



3. Follow the prompts to **Create your Account** and **Sign in.**
4. On the Azure Portal, go to type **"Subscriptions"** on the search bar on top.

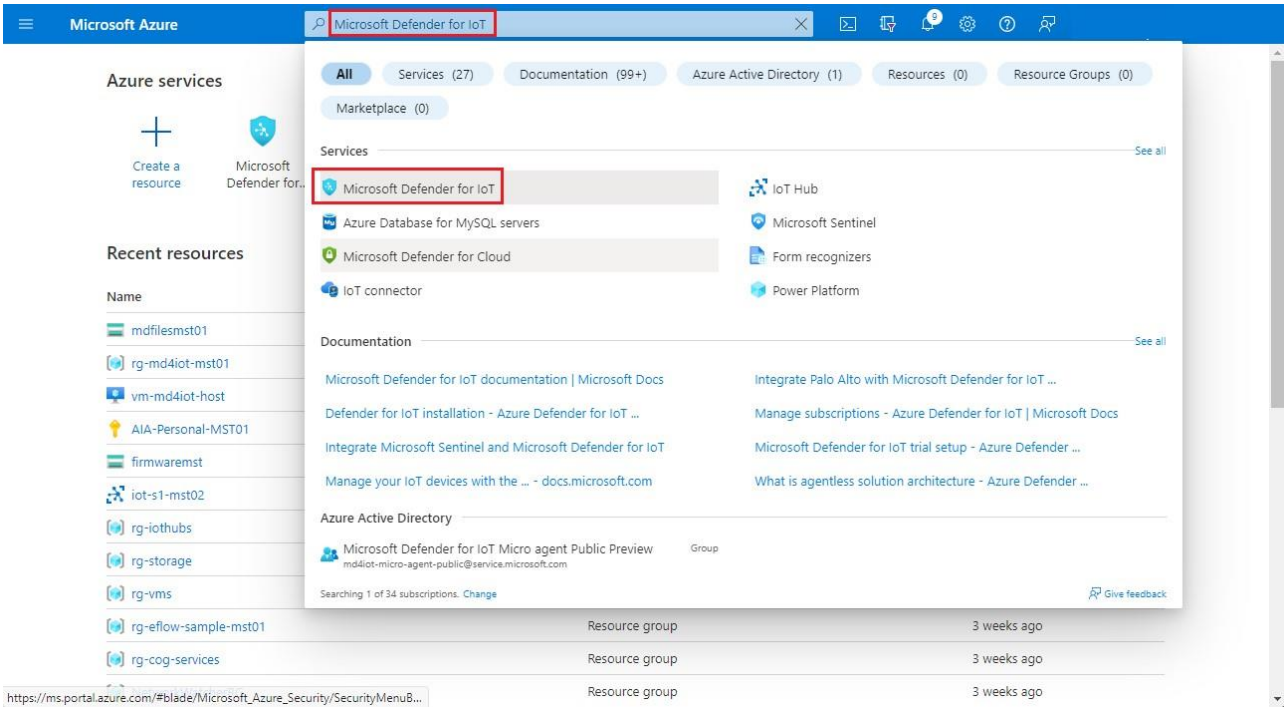


5. Your subscription will show up on the list of **"Subscriptions".**

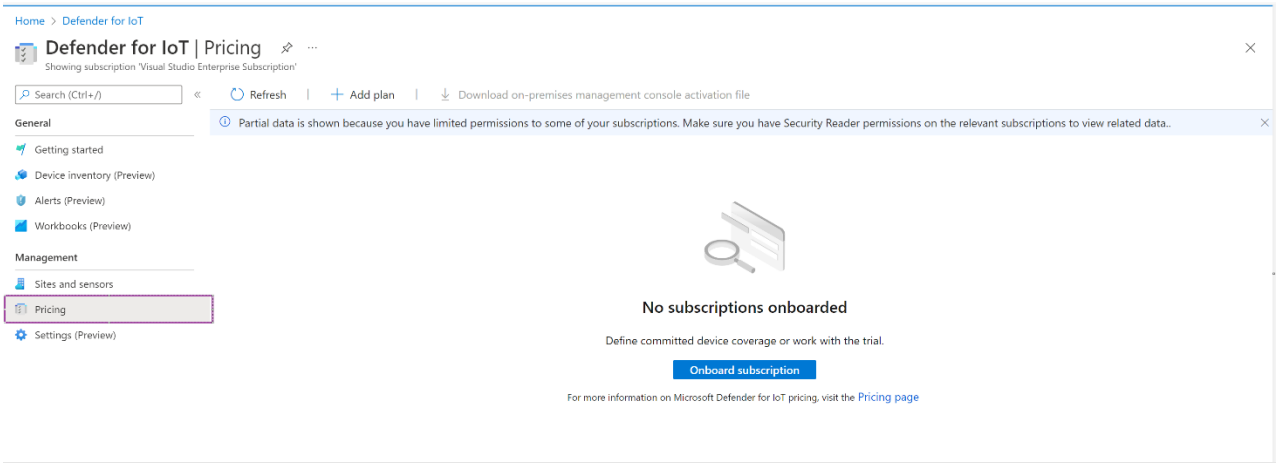


Task 2: Enabling Microsoft Defender for IoT on the Subscription

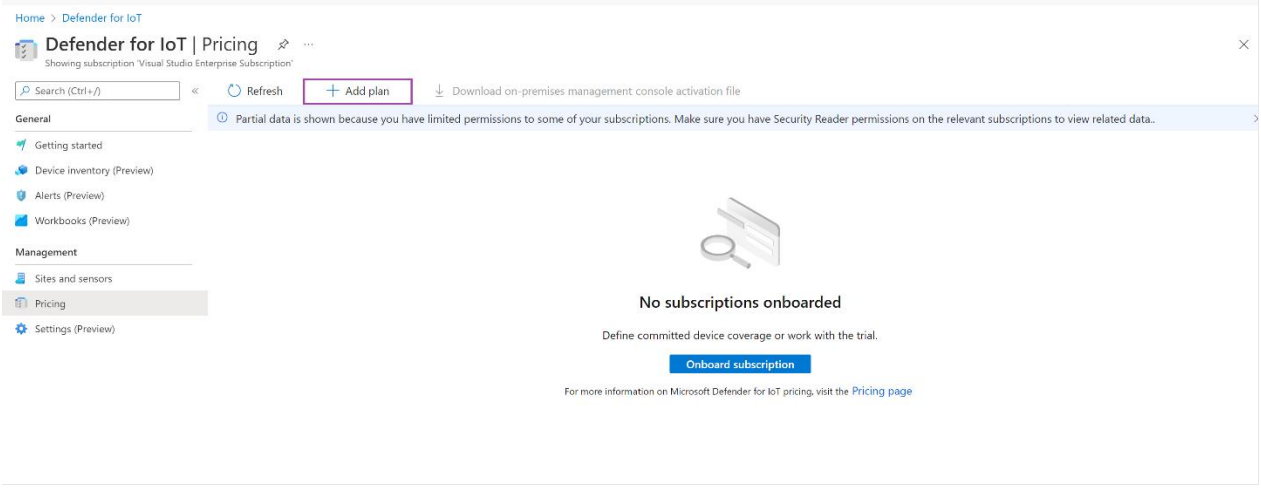
1. In the Azure Portal, search for **Microsoft Defender for IoT**. Select **Microsoft Defender for IoT** in the popup window, to open the Microsoft Defender for IoT Page.



2. On the Defender for IoT page, in the **Getting Started** section, select **Pricing**.

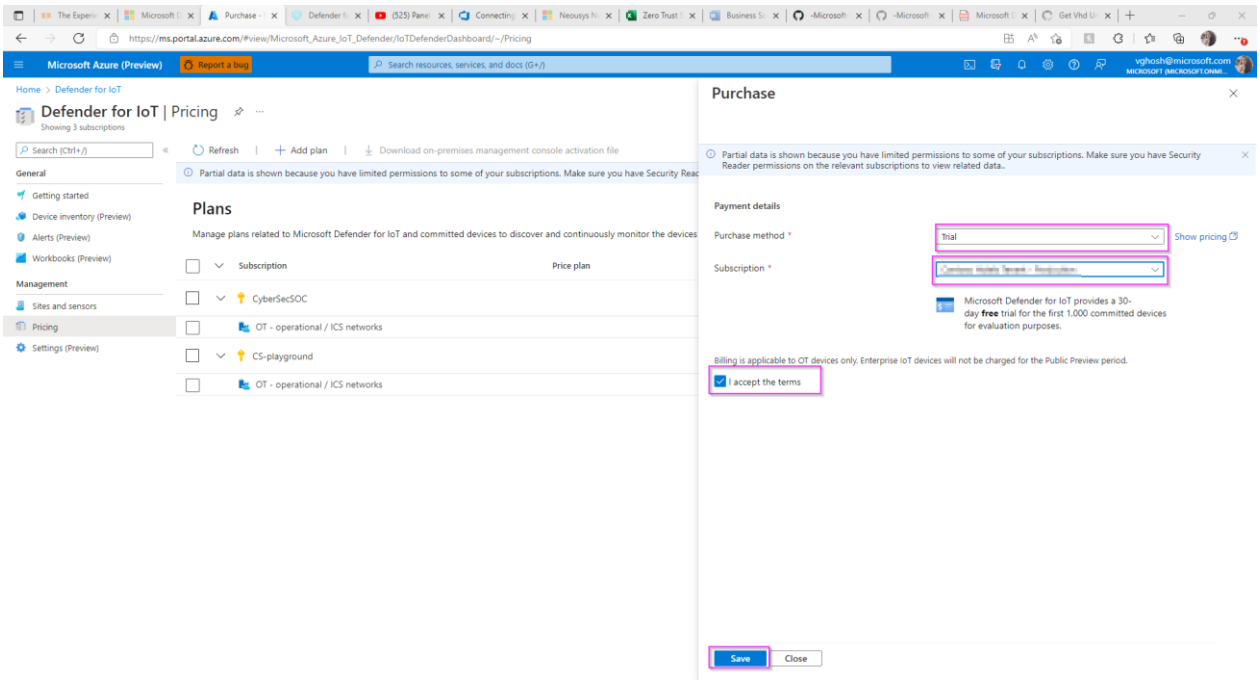


3. On the **Pricing** page, select **+Add Plan**.



4. In the popup screen, select:

   a. **Purchase Method:** Trail
   b. **Subscription:** pick the trial subscription you created
   c. Click **"I accept the terms"**, followed by "**Save"**.



You now have a valid Microsoft Defender for IoT Trial with ***1000 committed devices***. These devices represent all those equipment/sensors connected to your network in the facility you are analyzing. This configuration allows you a ***30-day trial for free.***

Exercise 2: Deploy the Sensor in Azure

Task 1: Create a Resource group to automatically deploy your sensor, storage account and network security group to

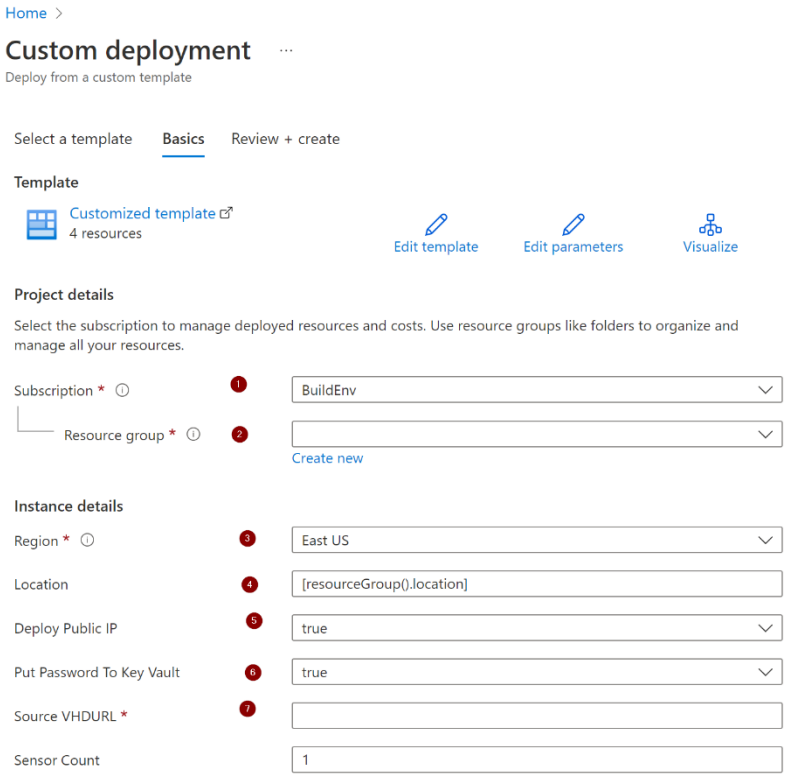
For the deployment, a **VHD file is used**. Please send a request to HOL_D4IOT@microsoft.com for a link for the IoT sensor installation. You will receive an email with the link once your request has been received.

Please note - This link is private and will expire in 5 days.

1. Click the link below to generate a template deployment installation

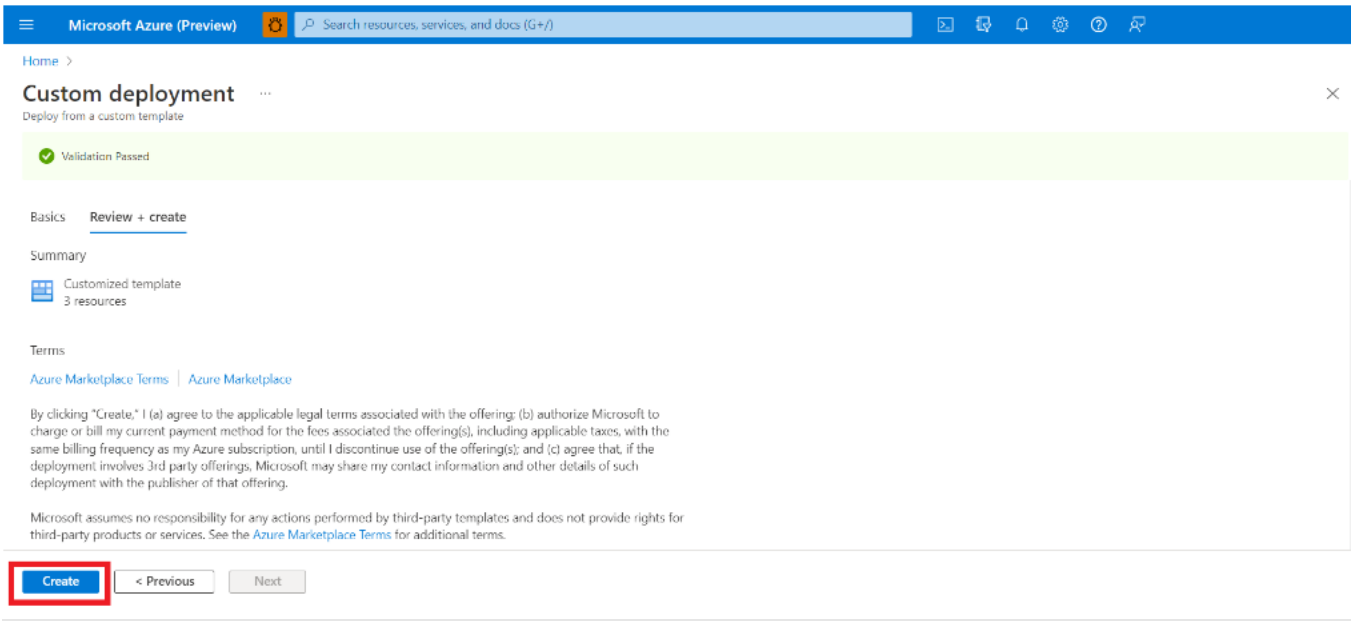
   https://ms.portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2FAzure%2F-Microsoft-Defender-for-IoT%2Fmain%2FHands%2520on%2520Lab%2520Documents%2FAzureDeploy.json

2. You will be taken to a custom deployment page that looks like the image below:



   1) Please select your **Subscription** liked to the trail service.
   2) Please create a new **Resource Group** (Use the hyperlink below the box). We recommend creating a new one to easily identify the relevant resources of the trail service.
   3) Please select the **Region** (Time zone) to which you are deploying the trail service to.
   4) Please leave the **Location** box with its default value, no need to change it.
   5) **[OPTIONAL]** Set the **Public IP** option to **"true". However, doing this will open your sensor to the internet. If you have alternate ways to publish the sensor to end users, then just use the internal ip by setting "Deploy Public IP" to "false".**
   6) Set this field to true if you want to store your secrets in keyvault.
   7) Please paste the link of the **VHD** copied from the email into the **Source VHDURL** field. **Please make sure there are no extra spaces after the link when you paste it.**

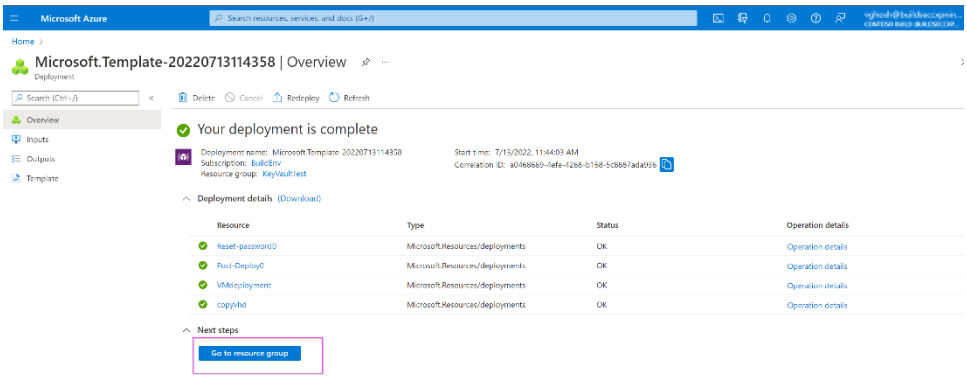
3. Once complete please click on the **Review + Create** button Upon validation completion, proceed to click on the **Create** button to initiate the process. The process runs for approx. 30 to 60 minutes.



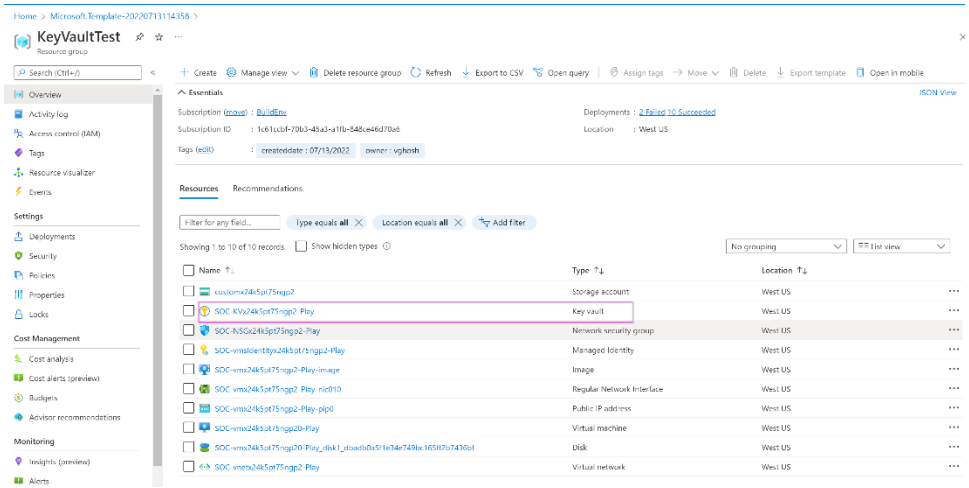
Task 2: Access your Virtual Machine.

Option #1: If you deployed with Keyvault

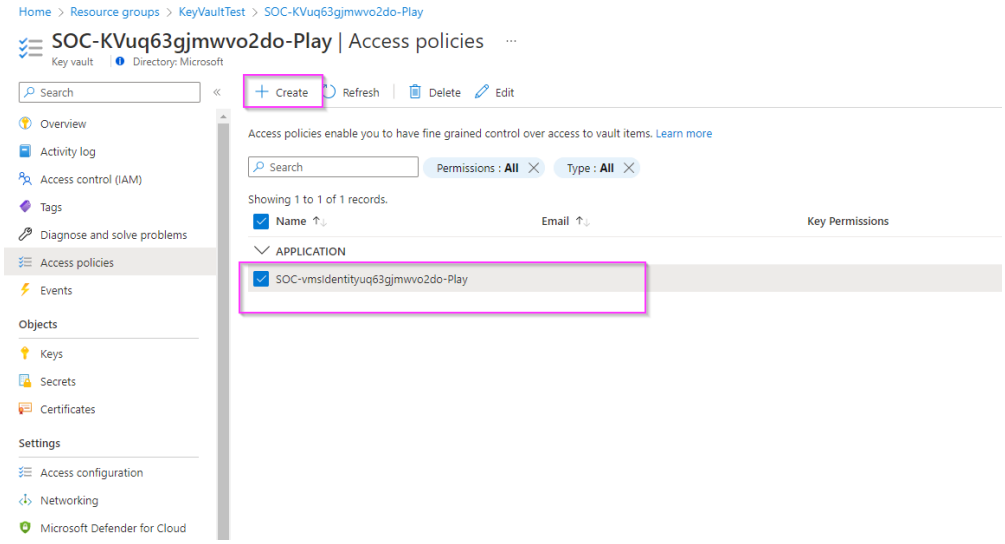
1. Once the deployment is complete, click on "Go to resource group" as shown in the image below.



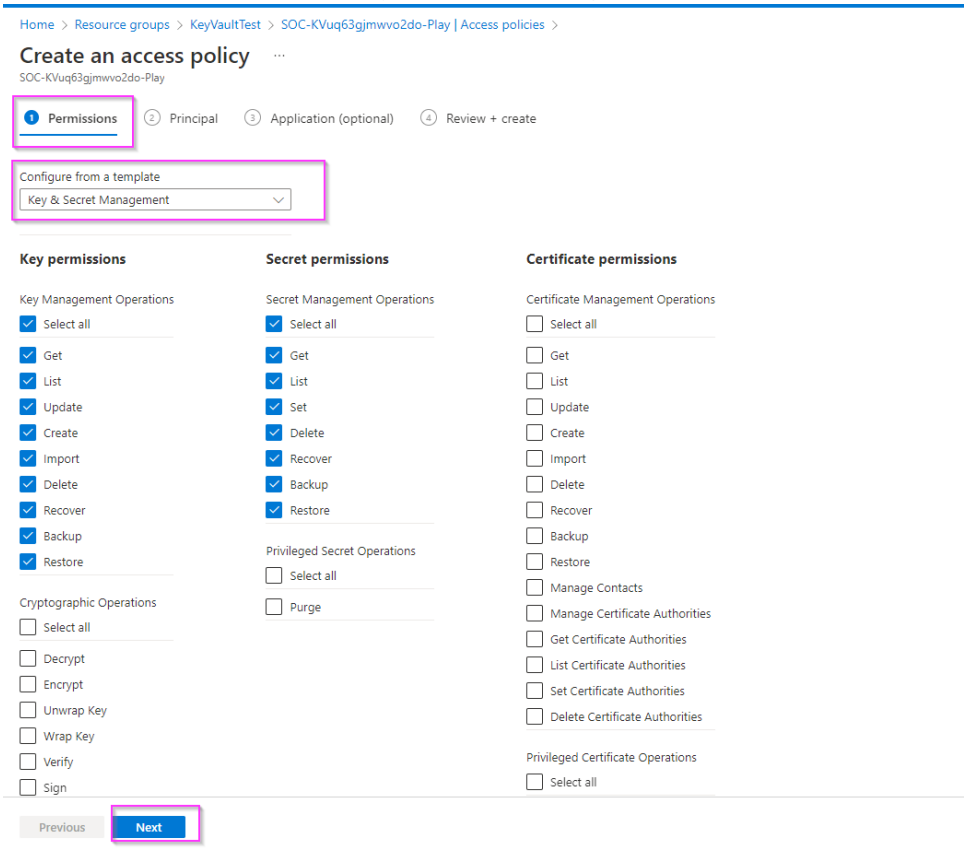
2. Go to the keyvault resource from the list.



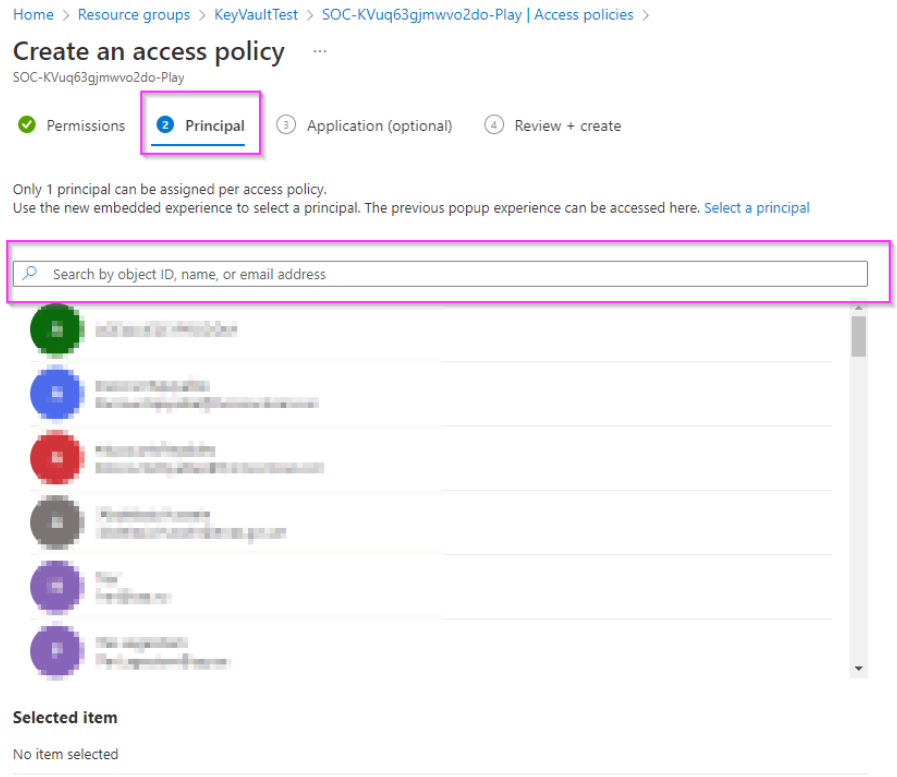
3. Select the application and click on “Access Policies” -> “+Create”.



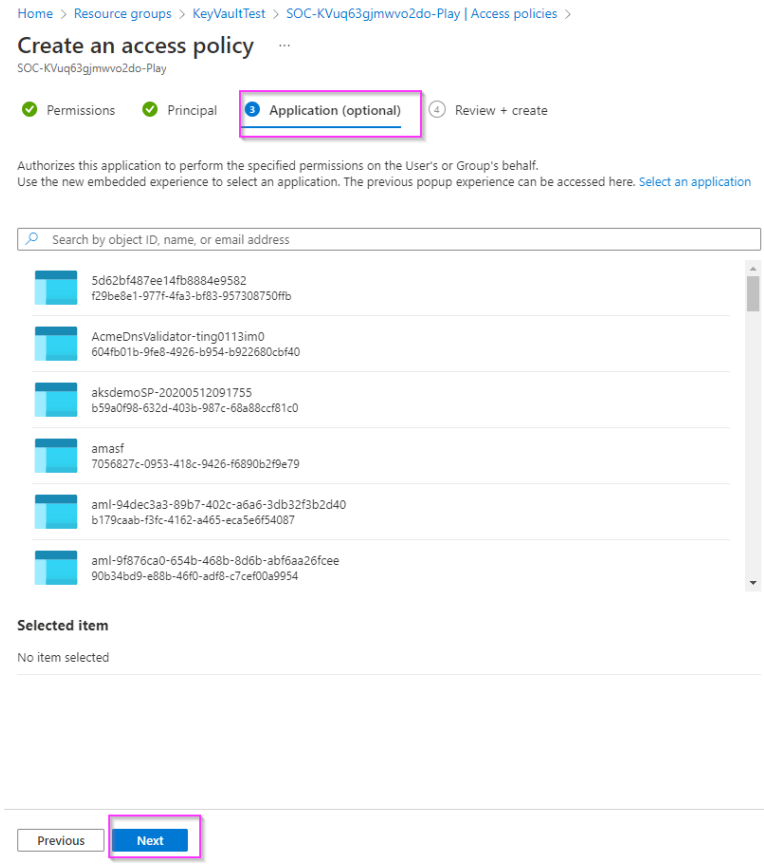
4. Under “Permissions” select “Key & Secret Management” template.



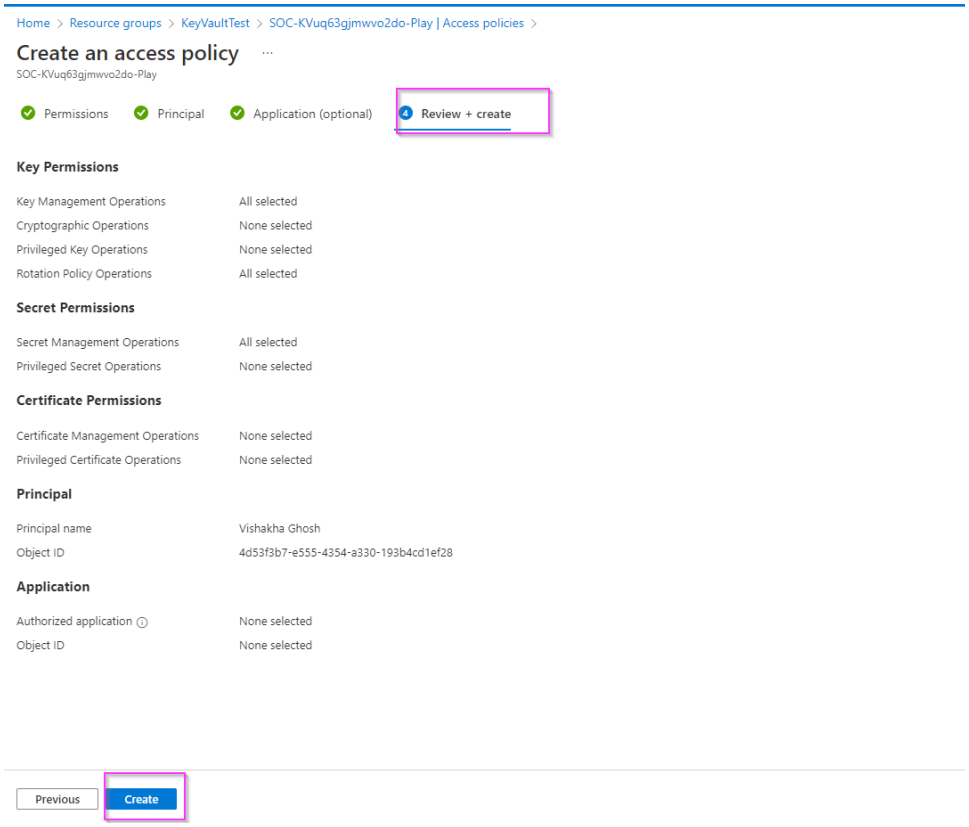
5. Under “Principle” select a principle



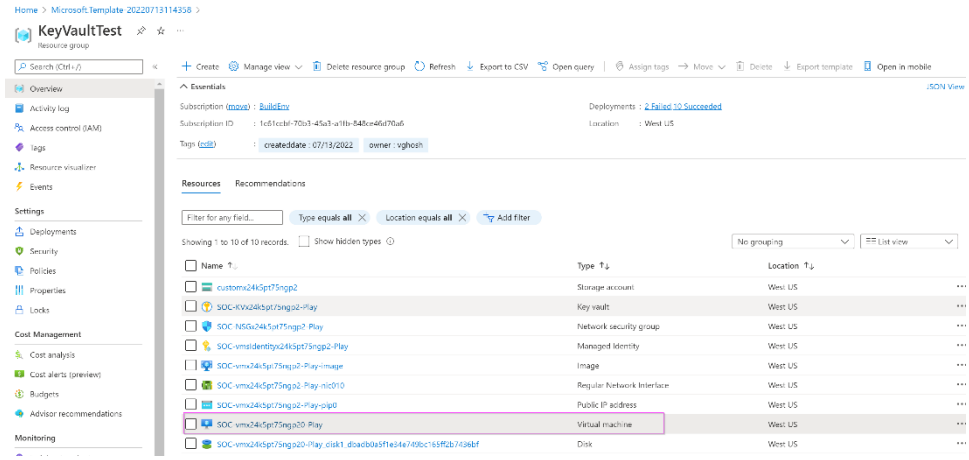
6. You can skip over “Application”.



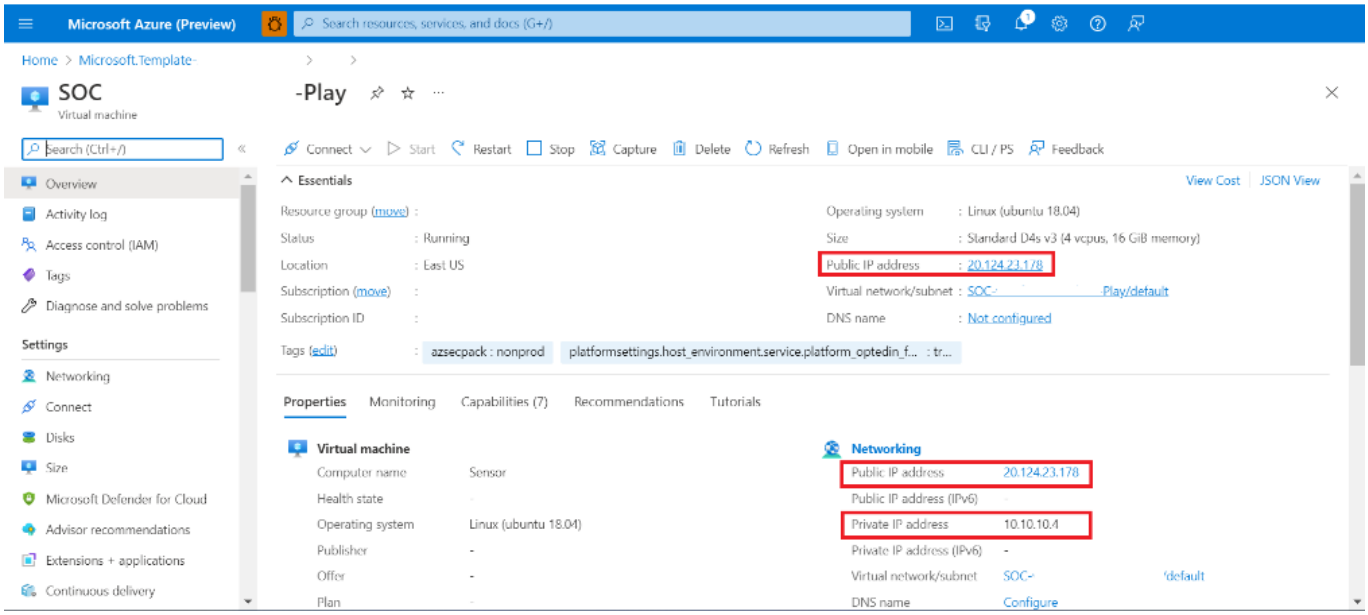
7. Click on “Create”.



8. Go back to your resource group and select the Virtual Machine resource.

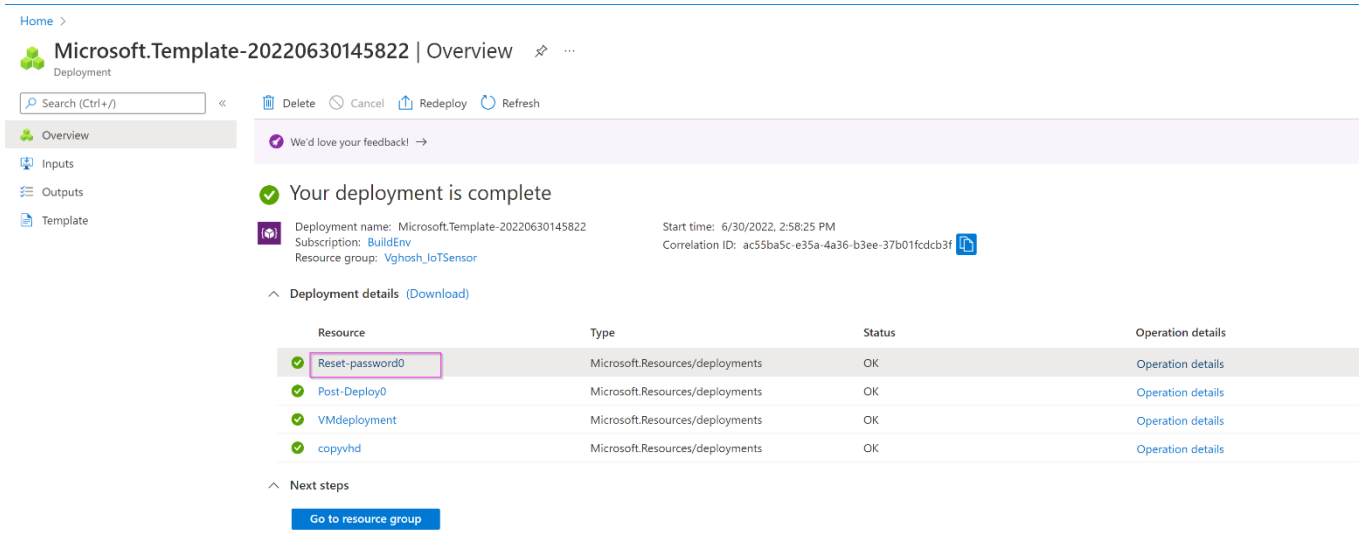


9. Make a note of the Public IP address.



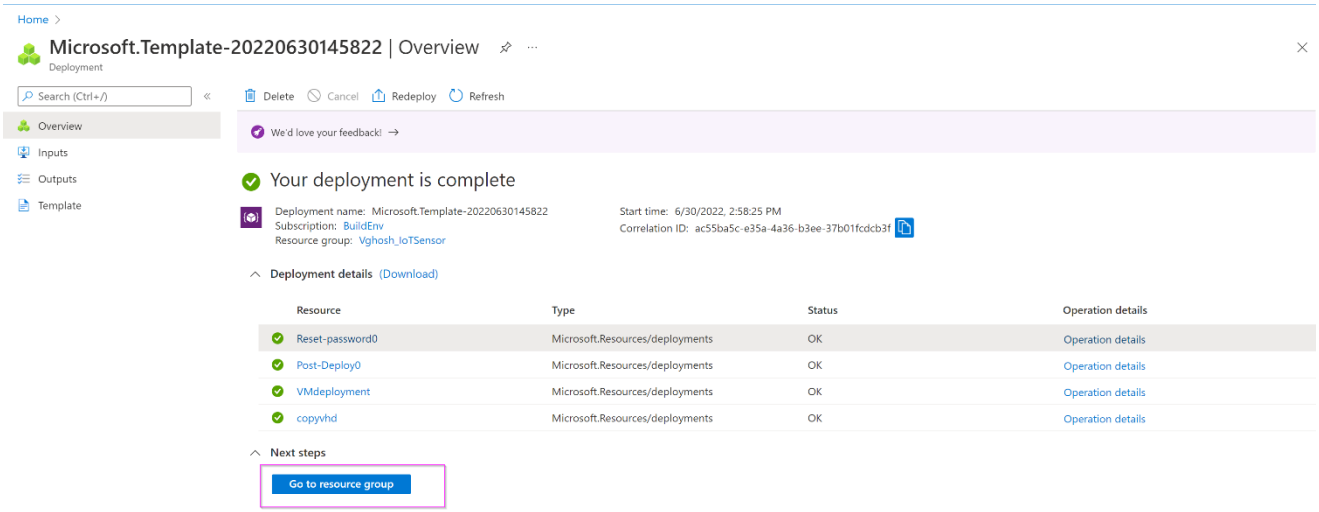
Option #2: If you deployed without Keyvault.

1. Once the deployment is complete, go to “Reset-password0” by clicking the button.

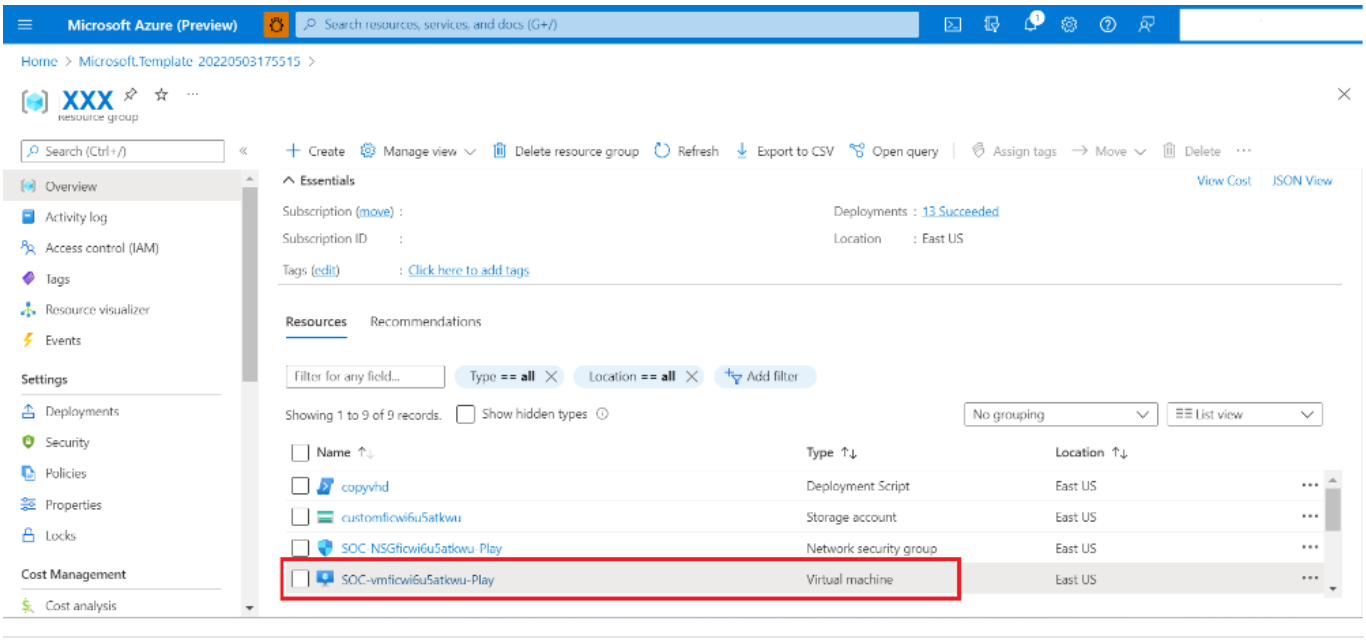


2. Copy the system generated random password from the “Password” field and make a note of the VMName.

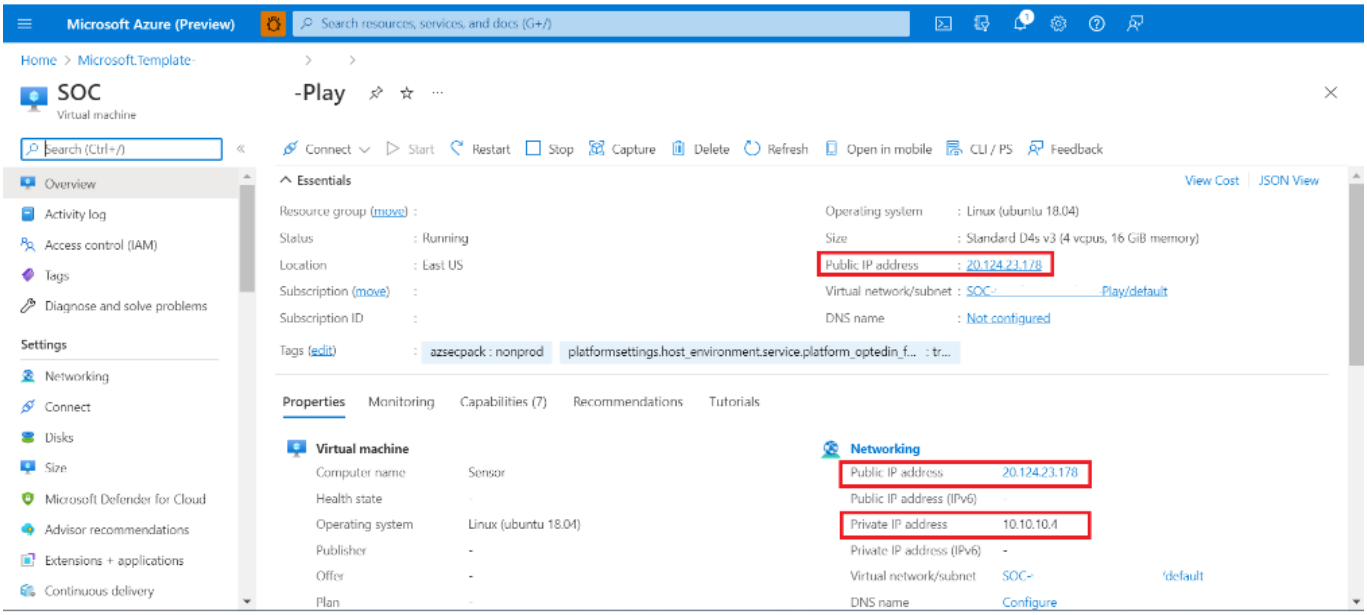
3. Click “go to resource group” from the previous screen.



4. Select the virtual machine from the list of resources in the group.

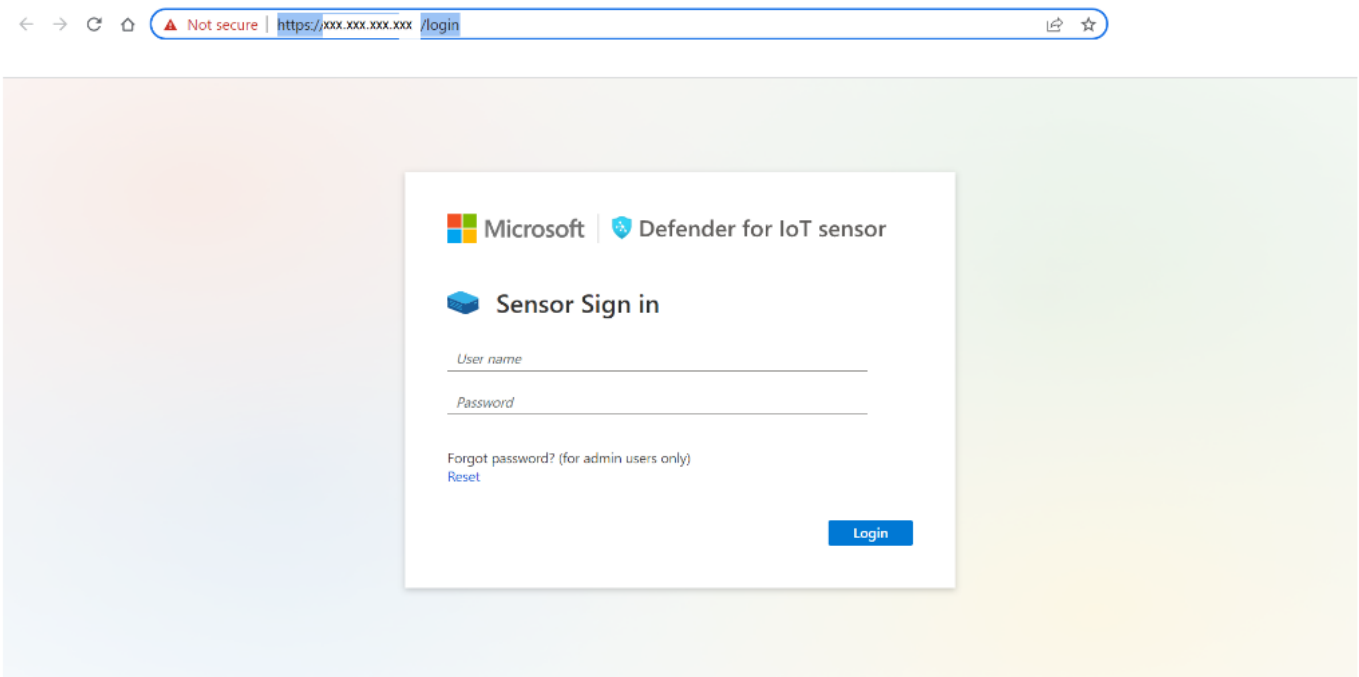


5. Make a note of the Public IP address.

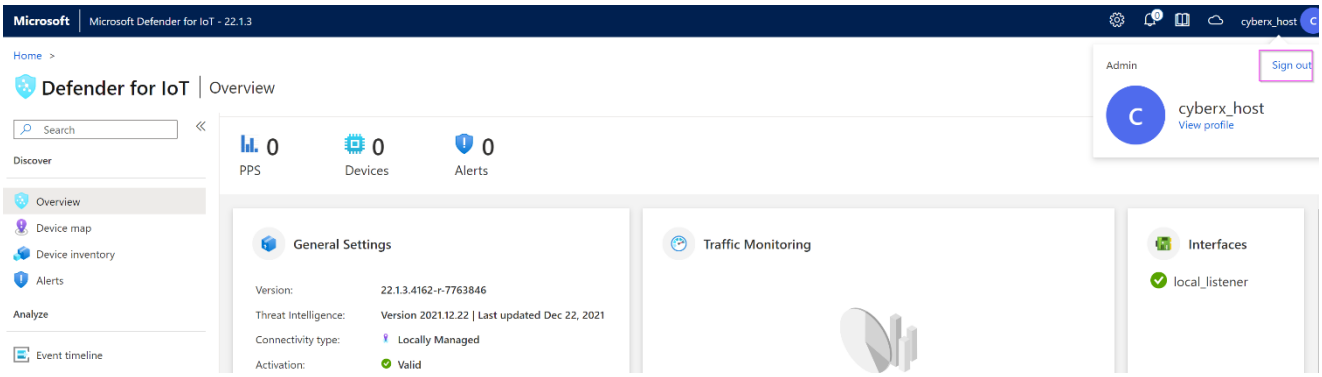


Task 3: Access your sensor via the console

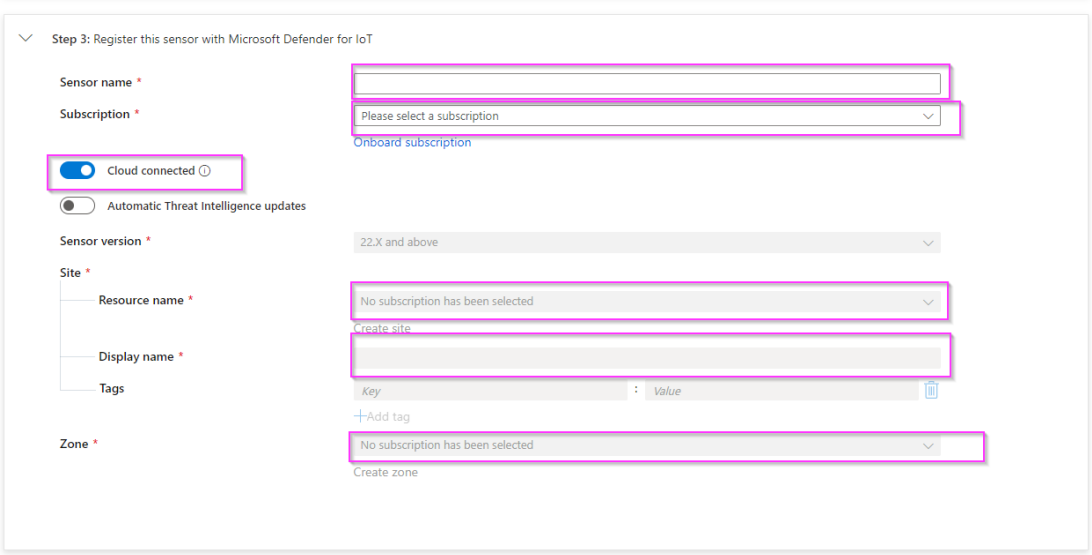
1. Proceed to access the console by using the selected networking method IP (Public or IP) using https:// as shown in the image and sign in with the IP you copied in the previous step. Username is **cyberx_host** and the password is what you copied in step 2.



2. Upon successful login please proceed immediately to change the password by clicking on the username on the top right corner and selecting **Sign out.**

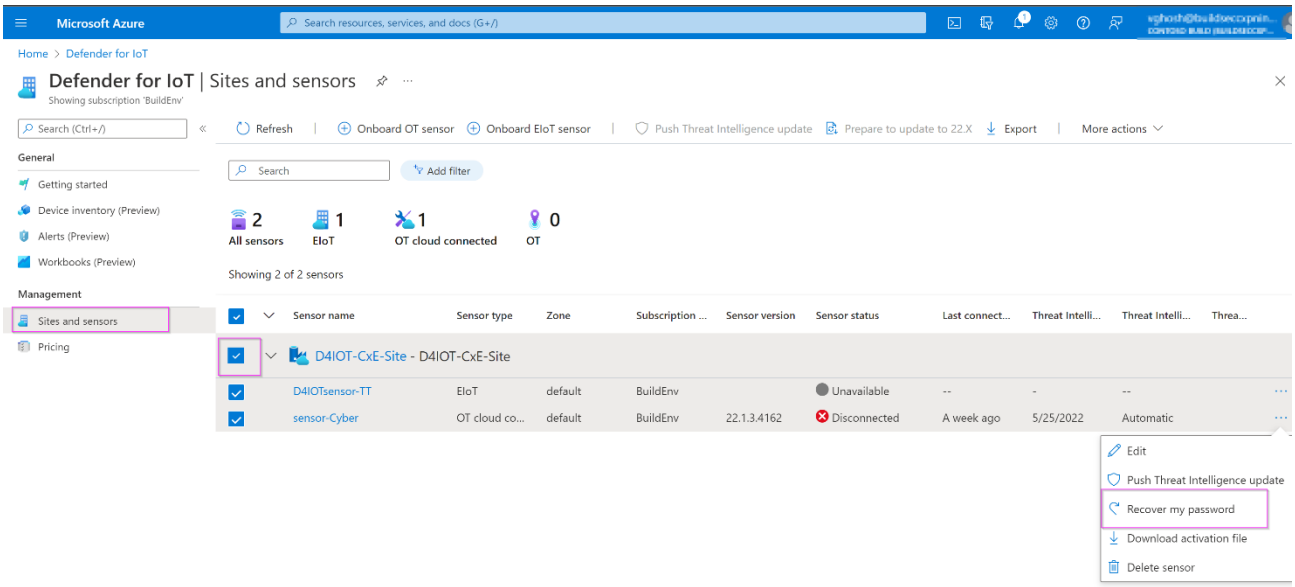


3. After signing out, please return to the Azure portal and navigate to **"Defender for IoT"**. Select **"Sites and sensors"**,
4. Click on "Onboard OT sensor".

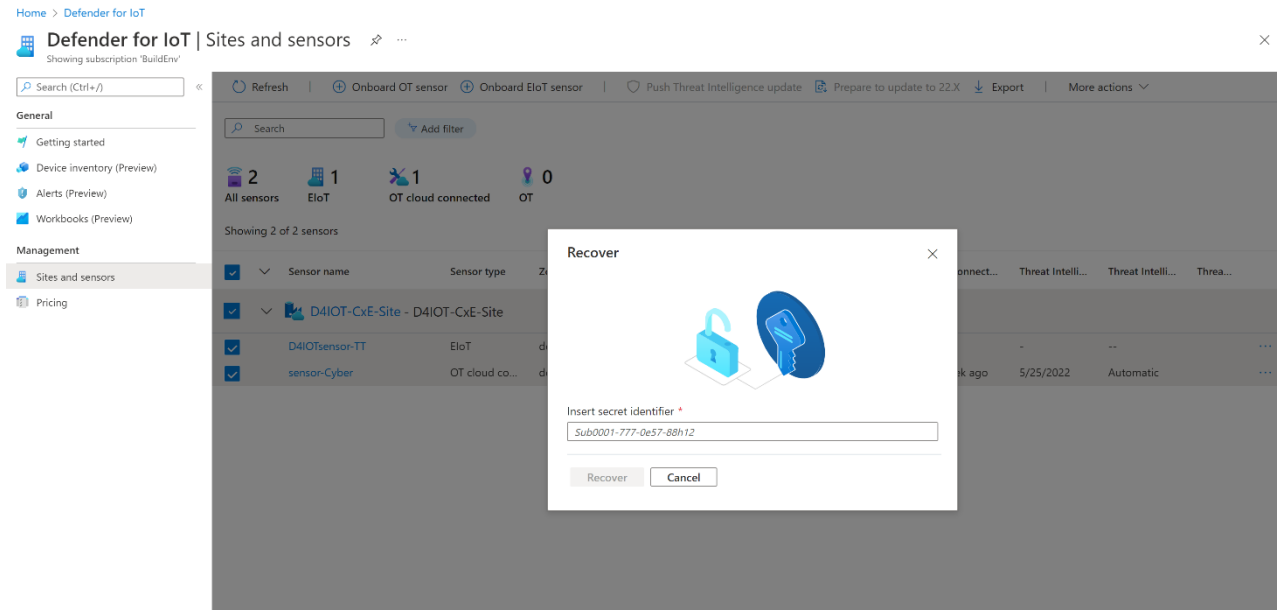


Add in a name for your sensor and pick your subscription from the dropdown. You can choose to cloud connect it. Pick your Resource name from the dropdown, give it a display name and a zone. This automatically initiates the download for the activation file.

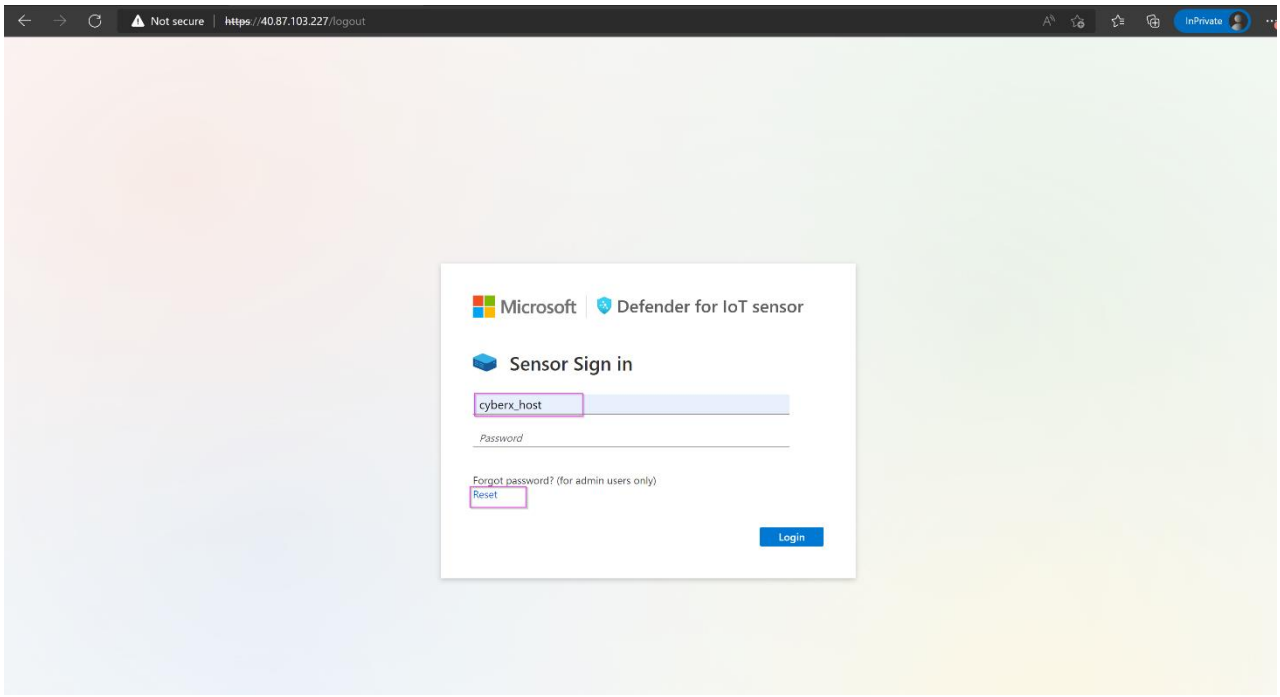
5. Select your sensor from the list and click on **"Recover my password".**



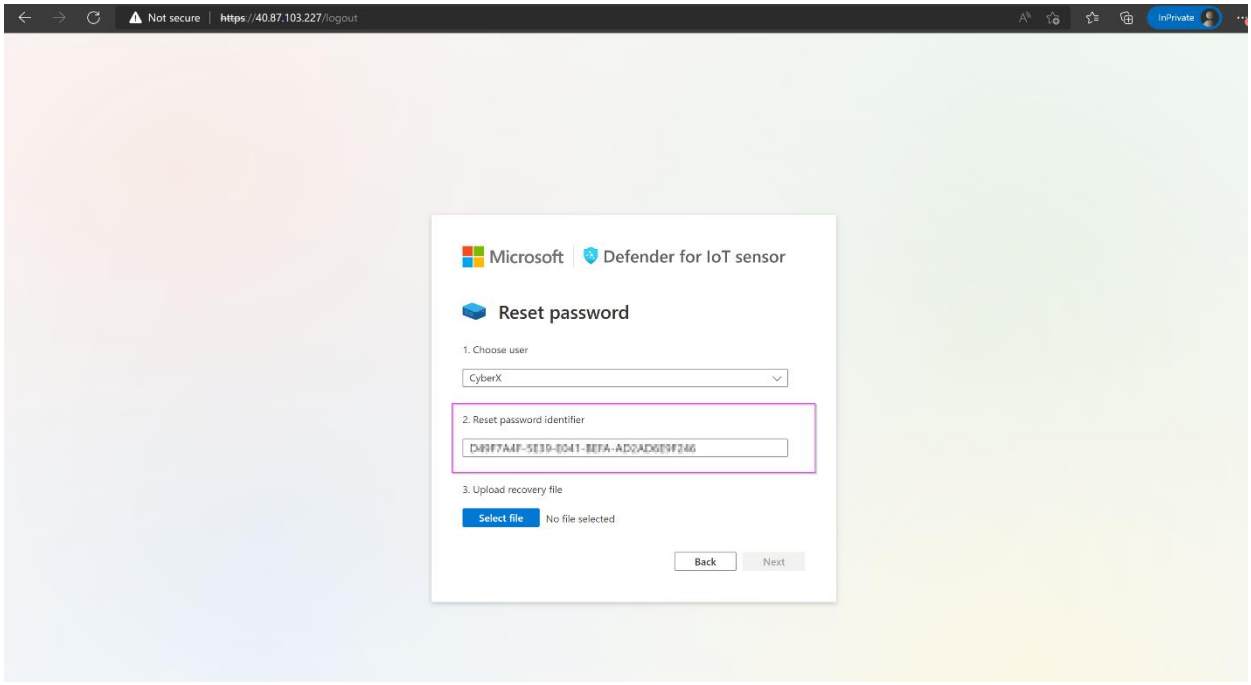
6. You will see this prompt asking for the “secret identifier”.



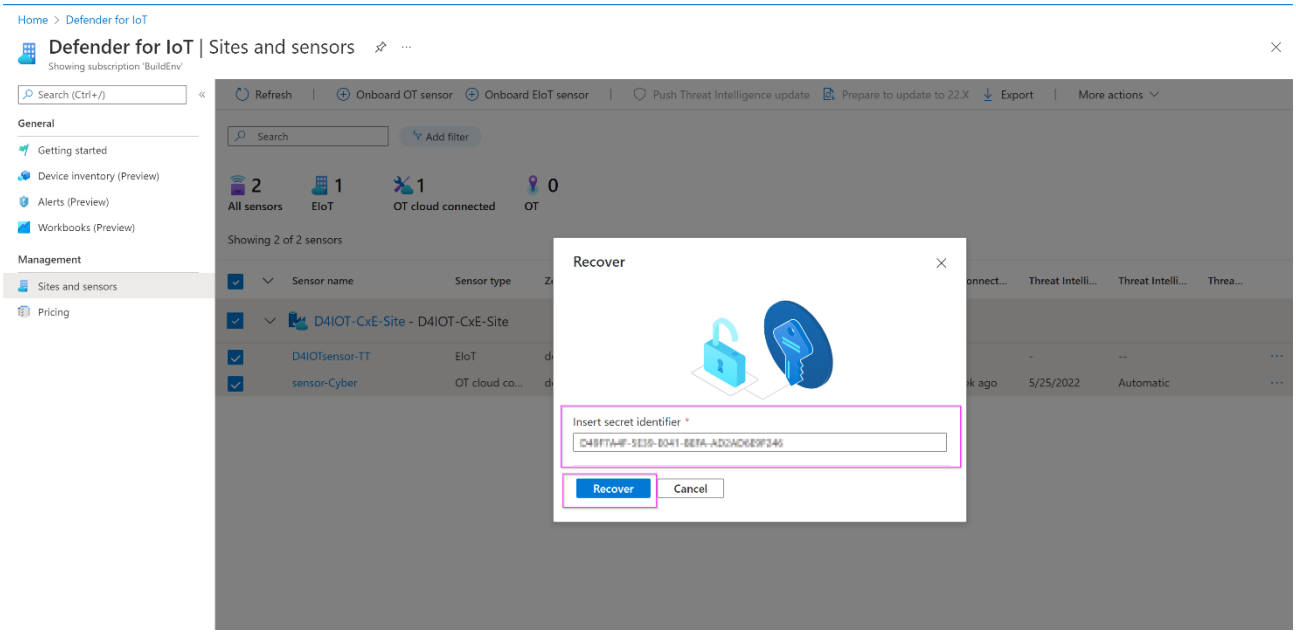
7. Return to the sensor console and type in the username followed by “Reset” as shown.



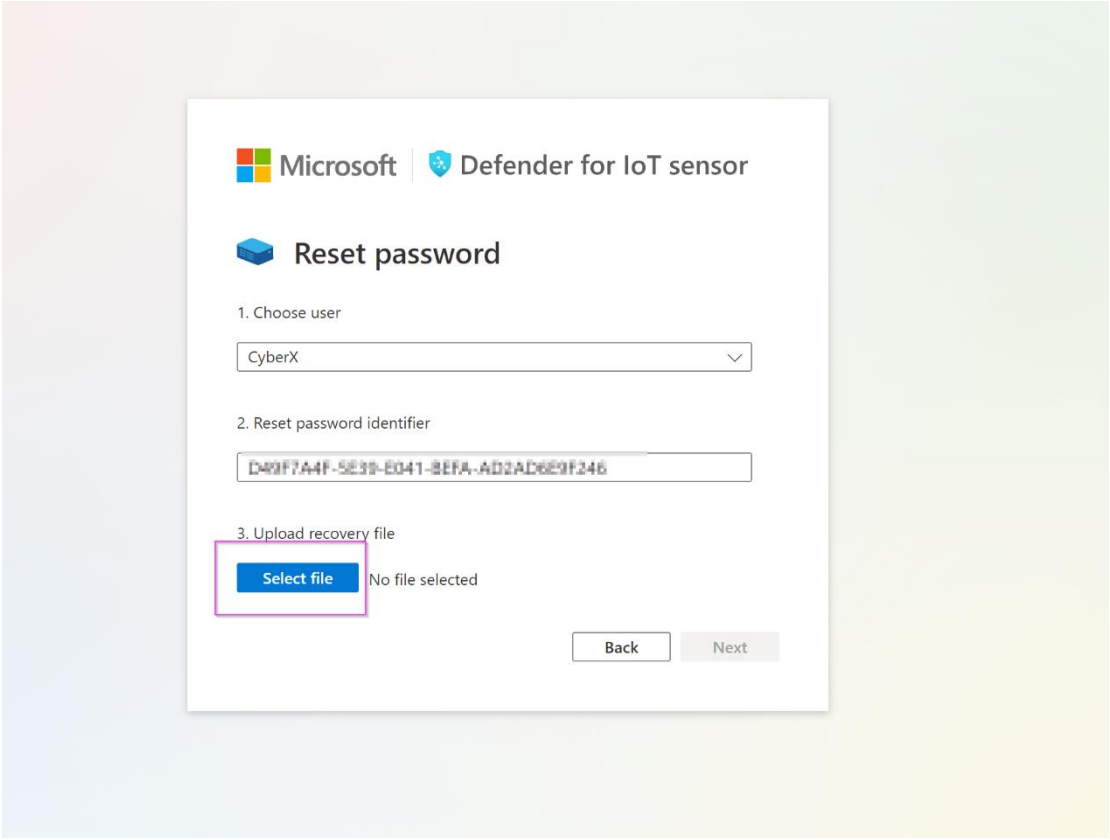
8. Copy the identifier.



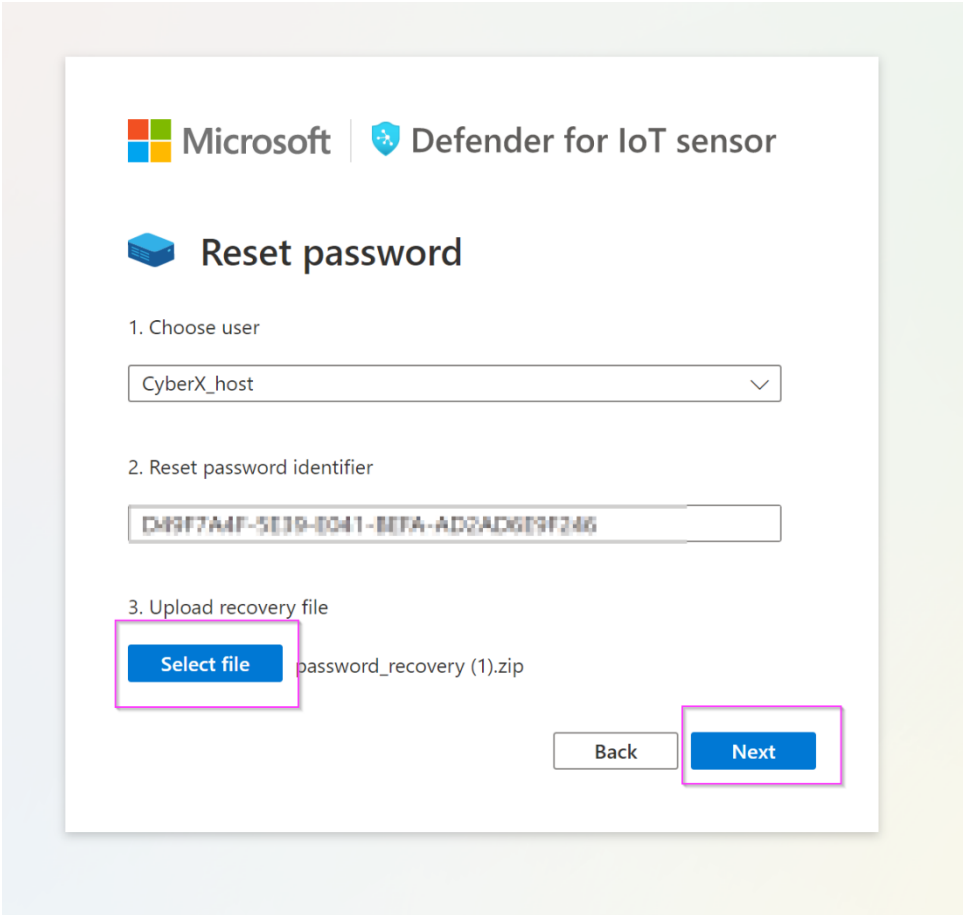
9. Paste in the box on the Defender for IoT Azure window. Click "**Recover".**



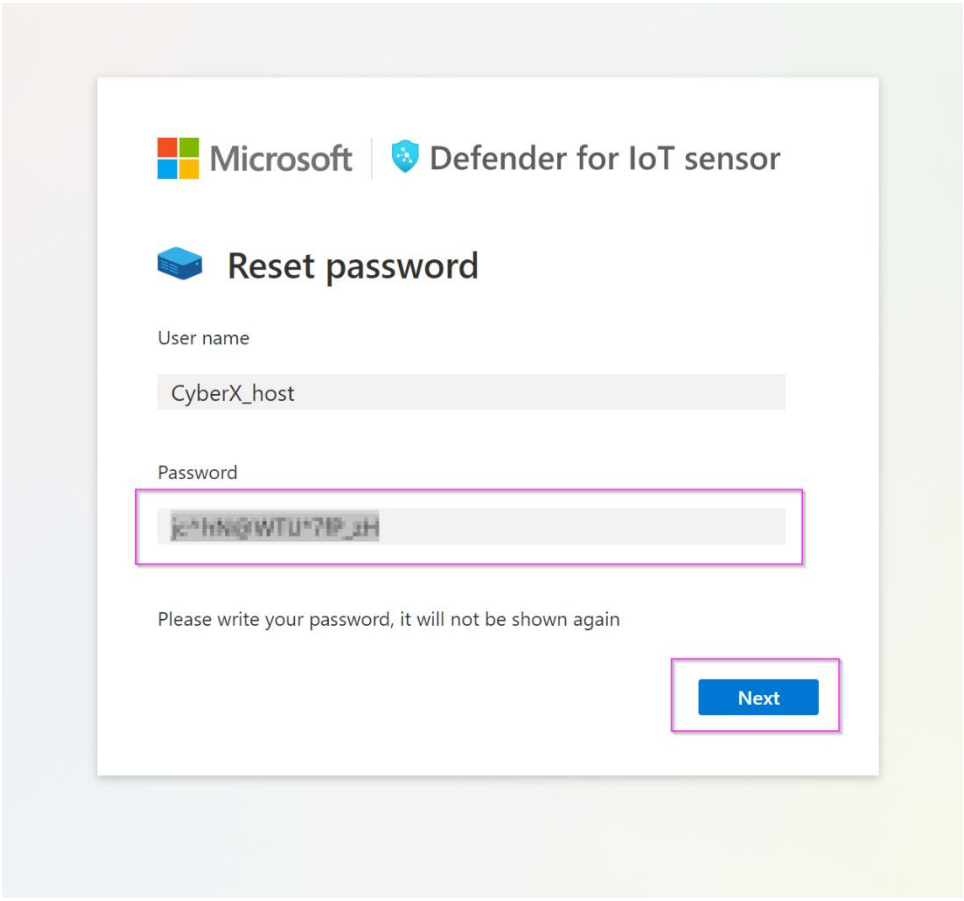
10. The *"password_recovery"* file download starts. Once the download is complete, return to the sensor console and click on **"Upload recovery file". Do not unzip the folder.**



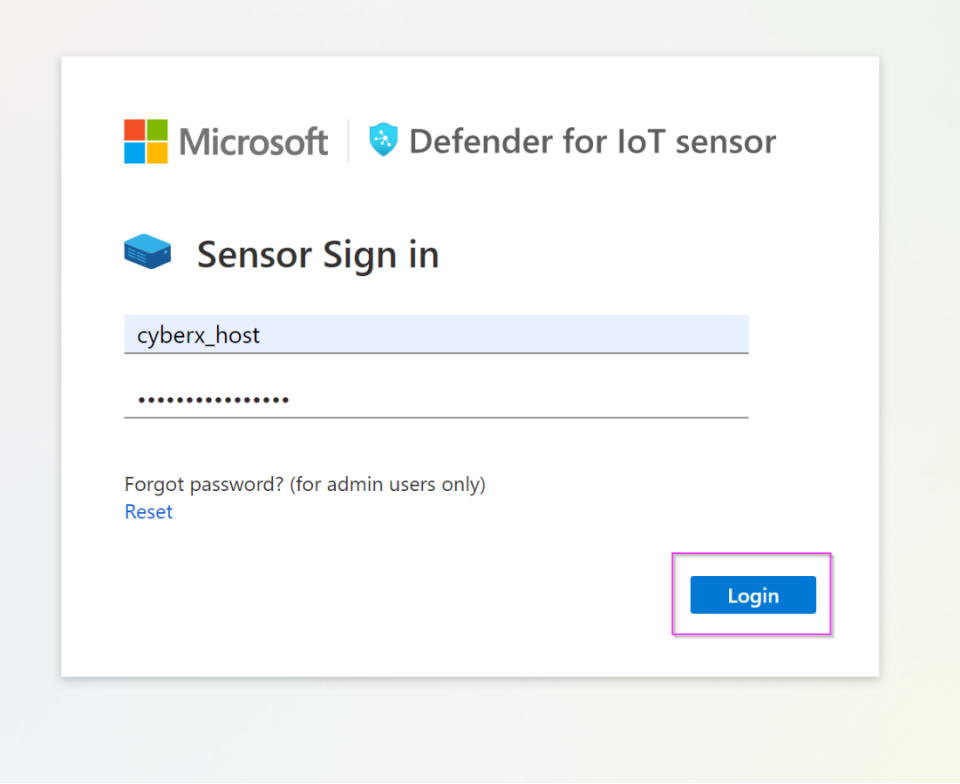
11. Click on **"Next".**



12. After uploading the file, you will be shown a temporary password on the screen. Please note it down.



13. Log in with the new password.

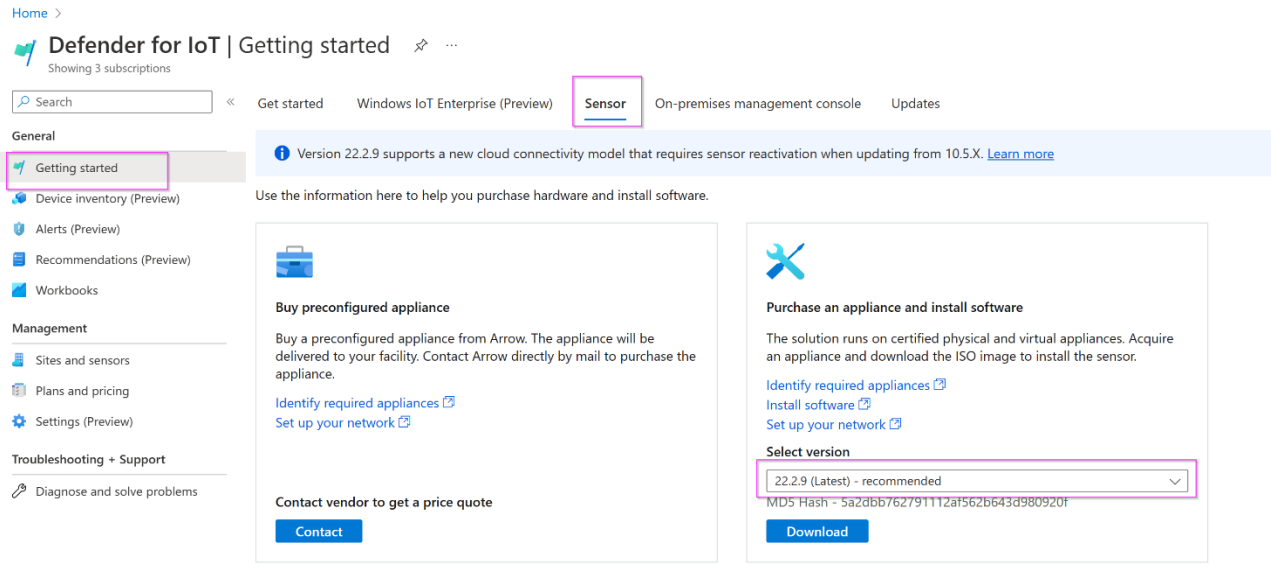


14. Repeat this step for all the usernames.

Exercise 3: Perform an Upgrade

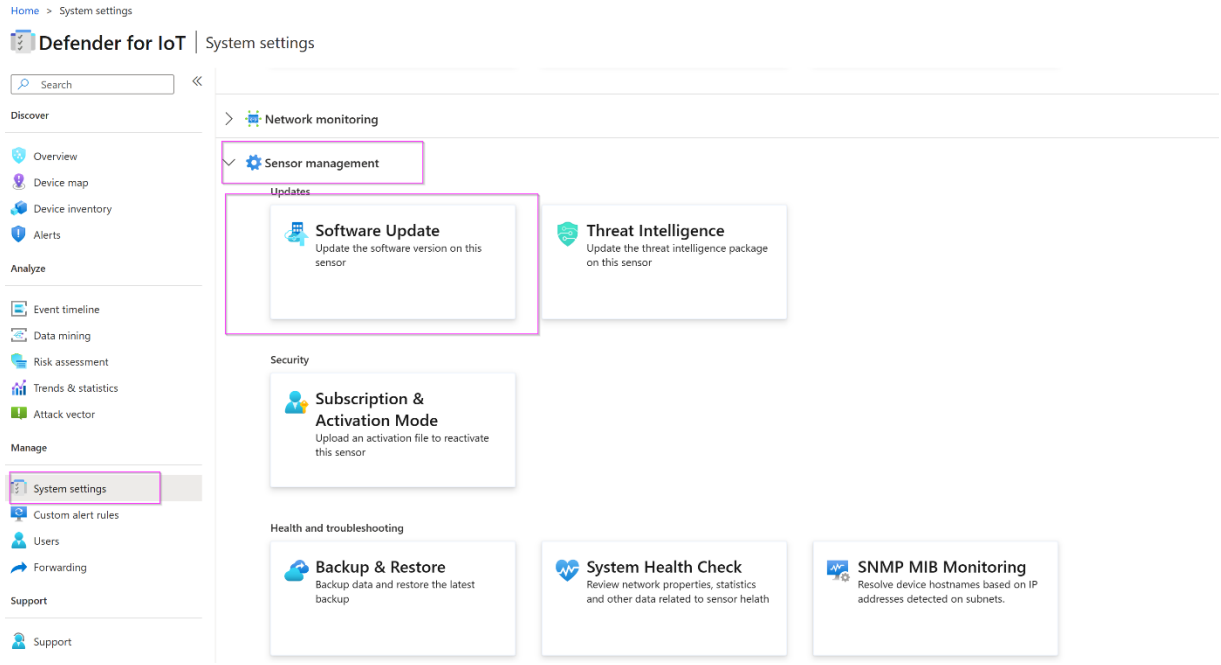
Task 1: Download the Upgrade ISO file

1. Go to the Azure portal and navigate to the Defender for IoT page.
2. Go to “Getting Started” -> “Sensor” -> Download the latest recommended upgrade version.

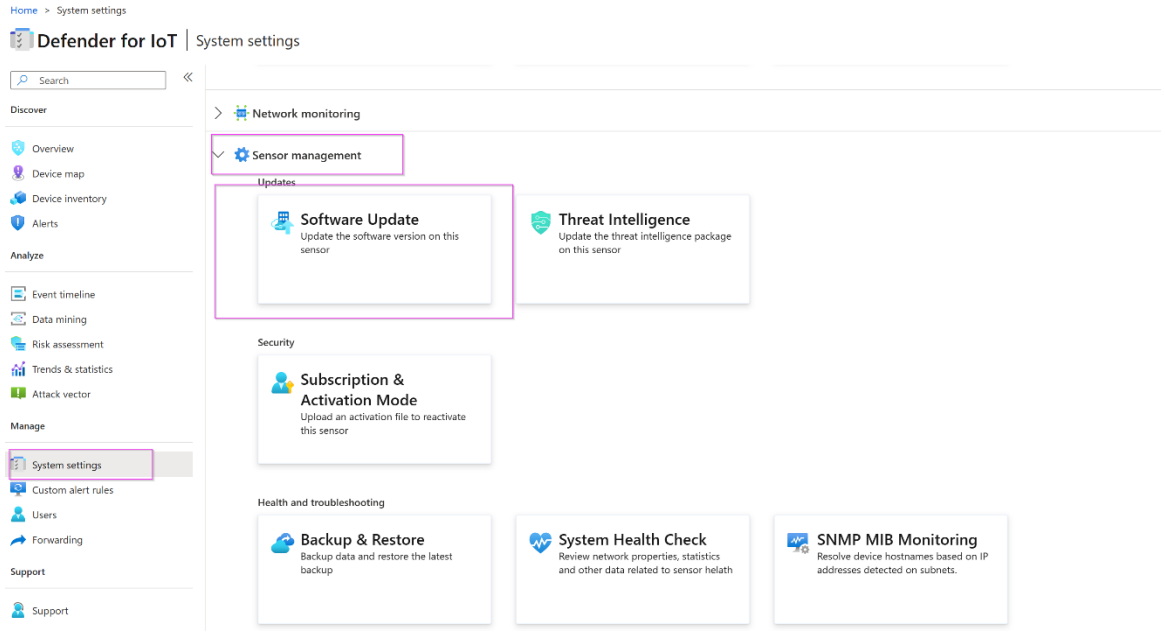


Task 2: Upgrade your sensor

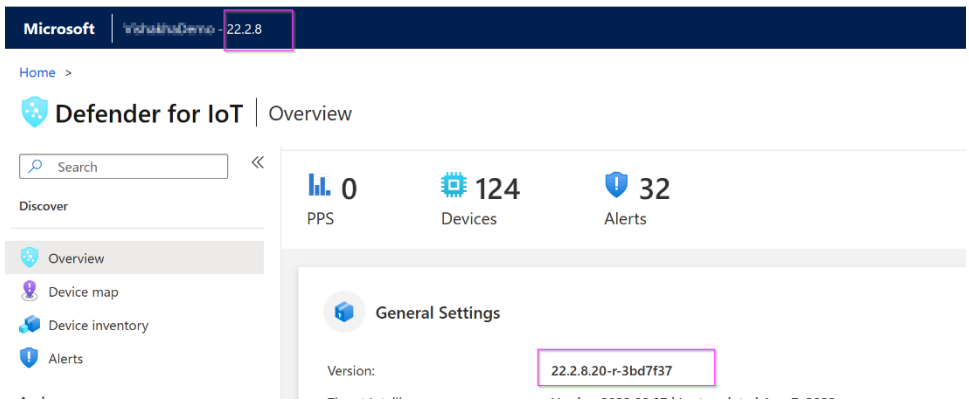
1. On the sensor, go to “System Settings” -> “Sensor Management” -> “Software Update”.



2. Click on “Upload File” and upload the iso file you downloaded.



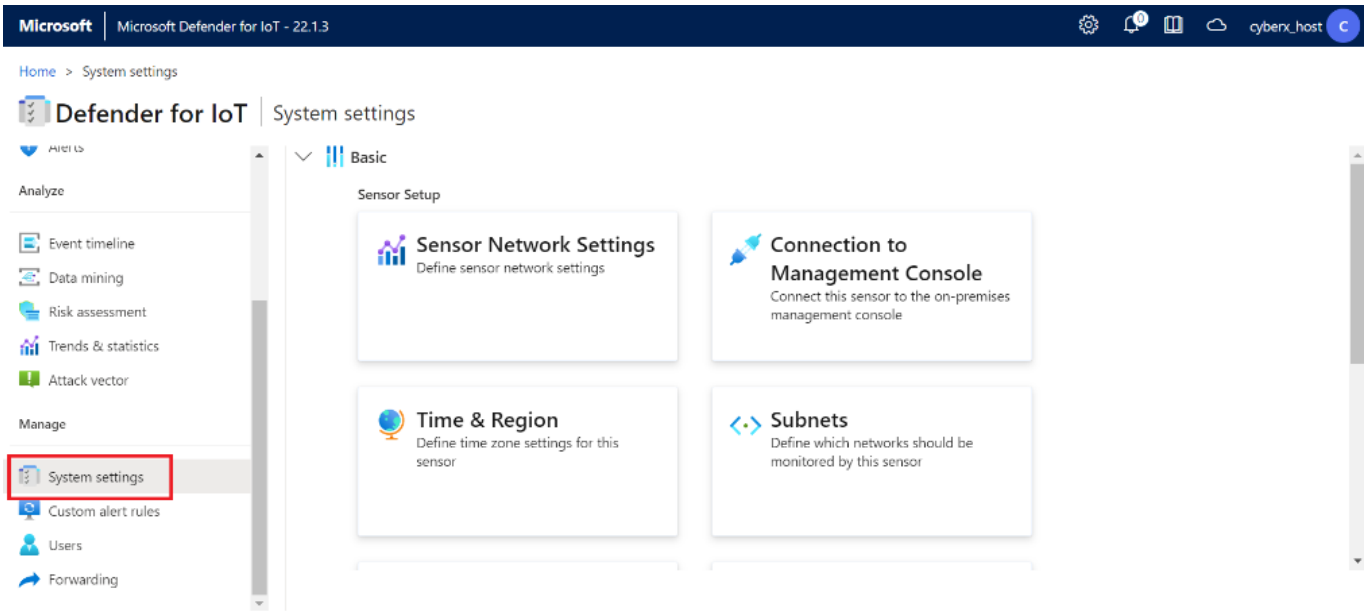
3. Verify the version on the dashboard.



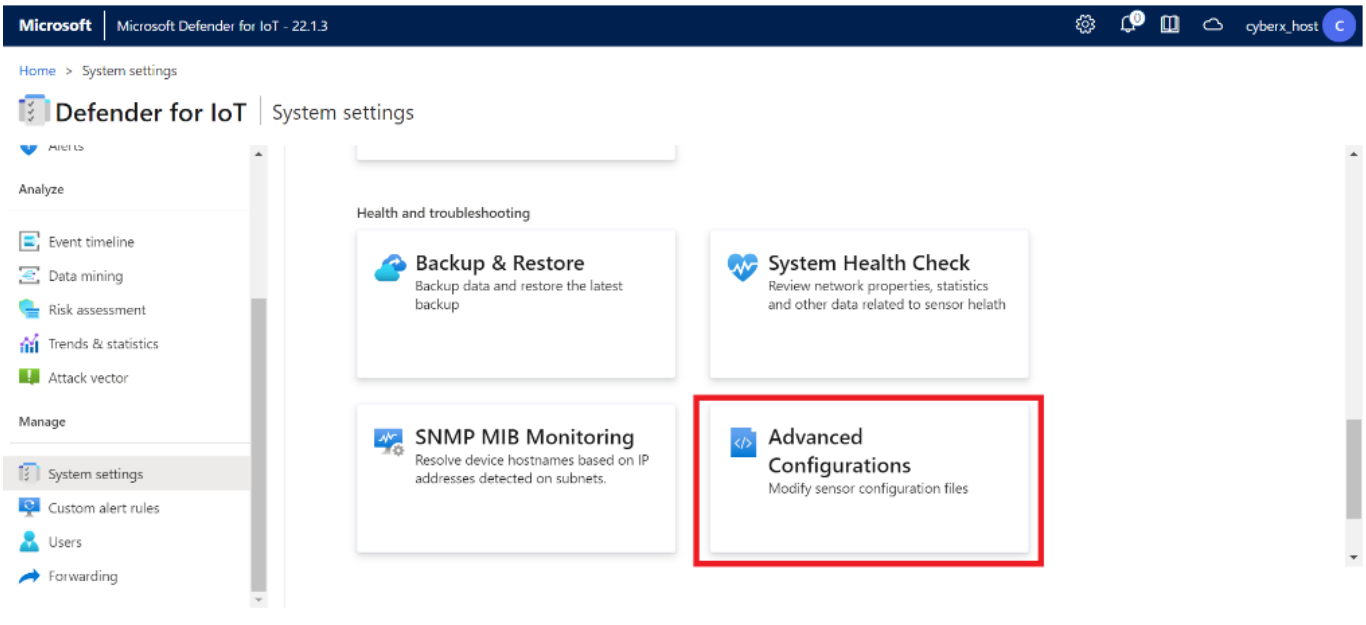
Exercise 4: Simulate Data in your sensor.

Task 1: Enabling the PCAP Player

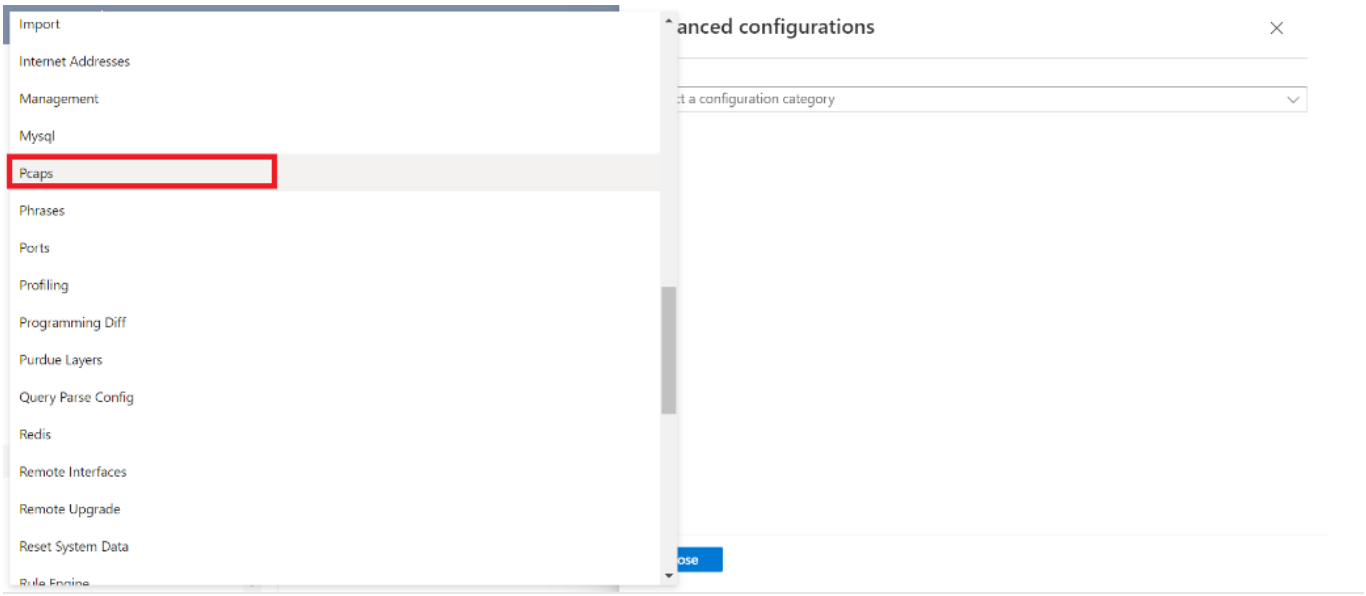
1. The PCAP player needs to be enabled to be visibly available for use in the UI. To do so, please select the "**System settings**" option from the scrolled down left side menu.



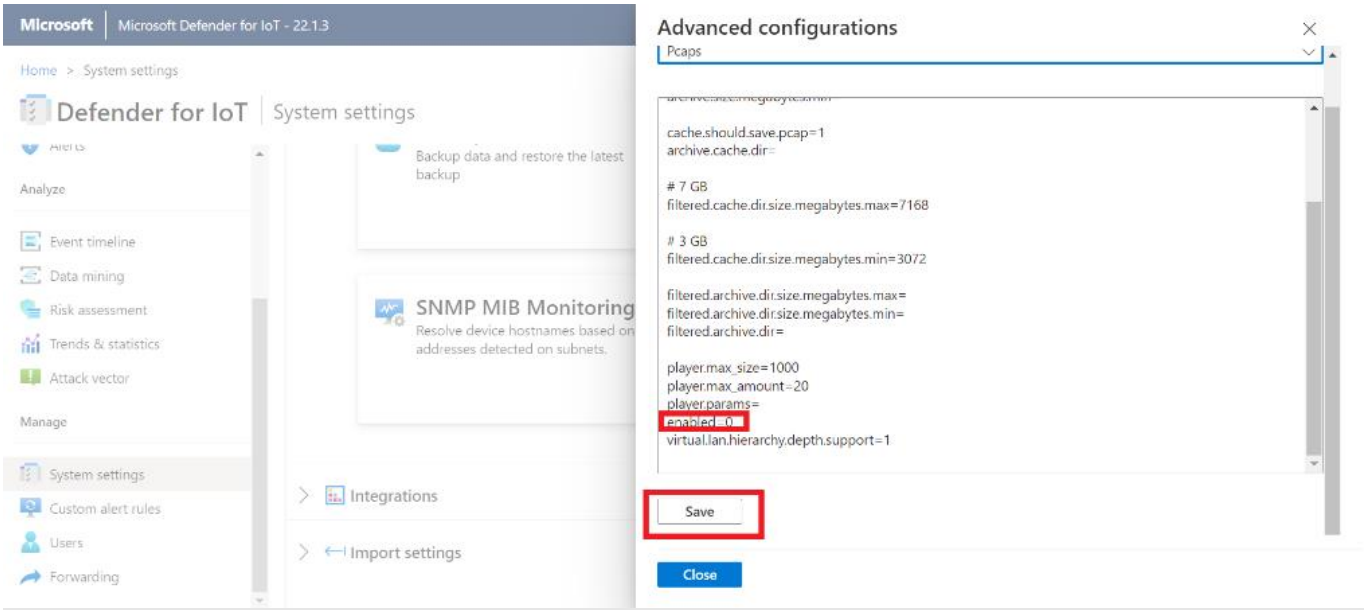
2. Scroll down to locate the **"Advanced Configuration"** option (Shown in the image below in the red square).



3. From “Select a Configuration Category”, select Pcaps.

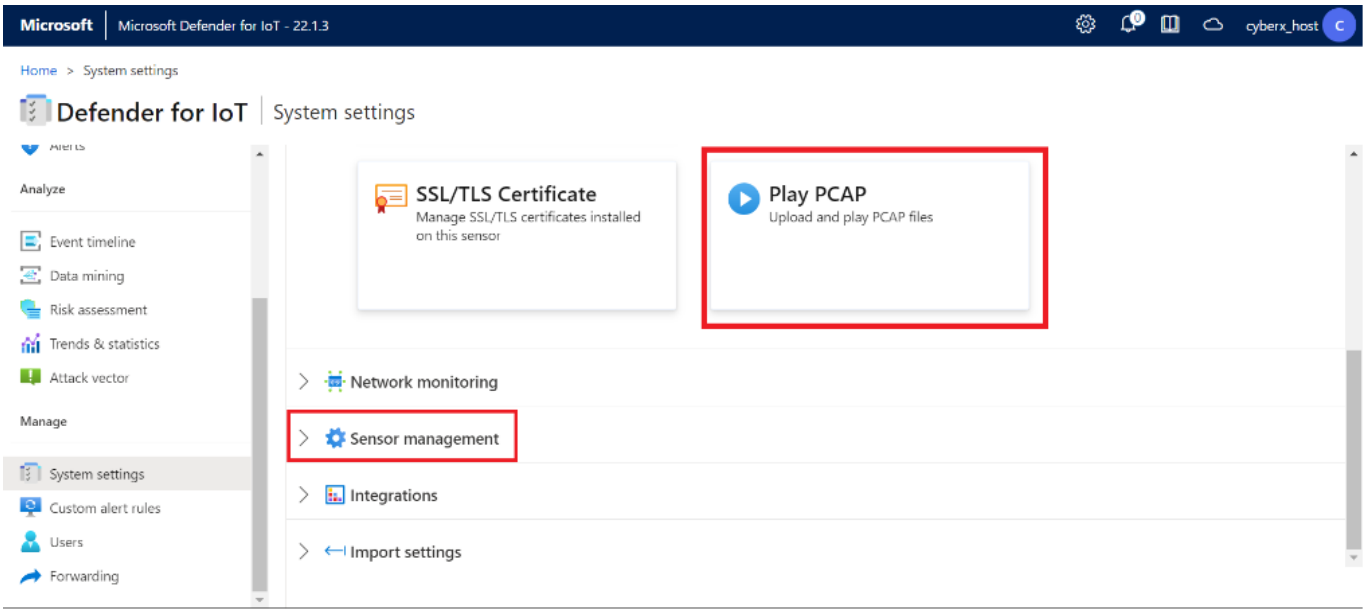


4. Scroll down to locate the "**enabled**" variable and set it to **1**. Click **Save** and approve to commit the change.

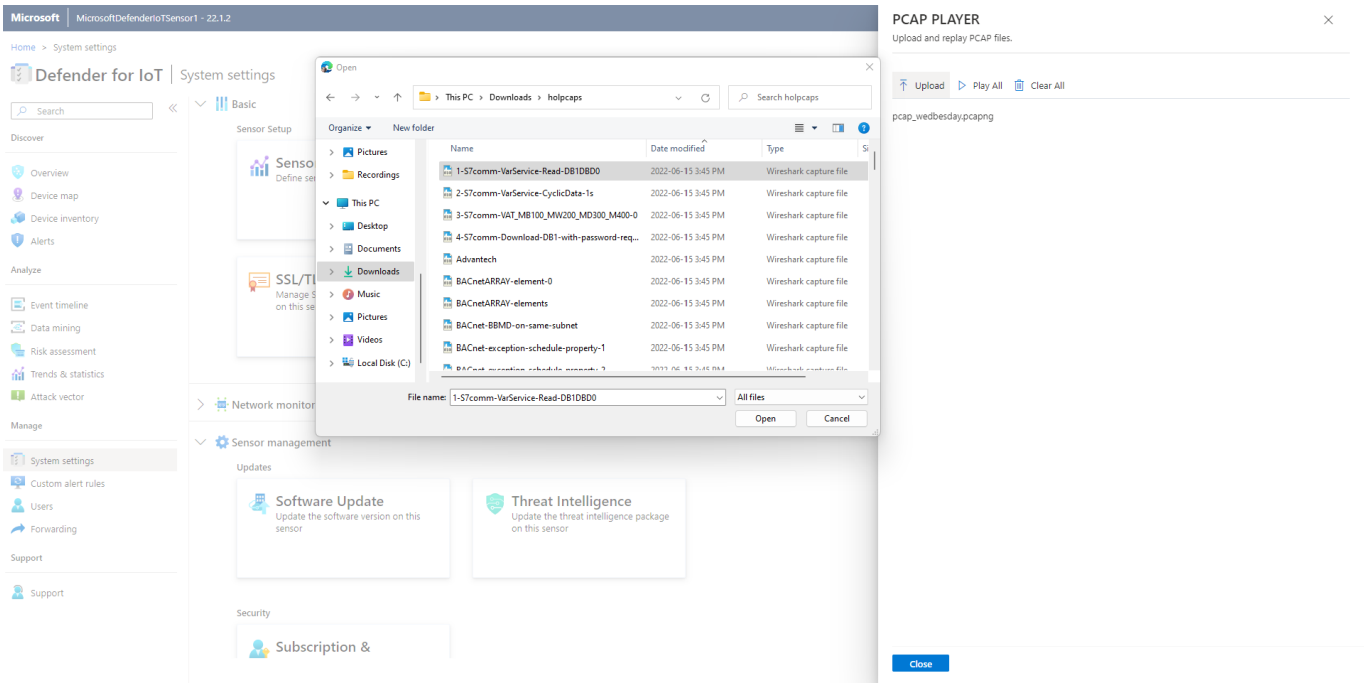


Task 2: Play PCAP files

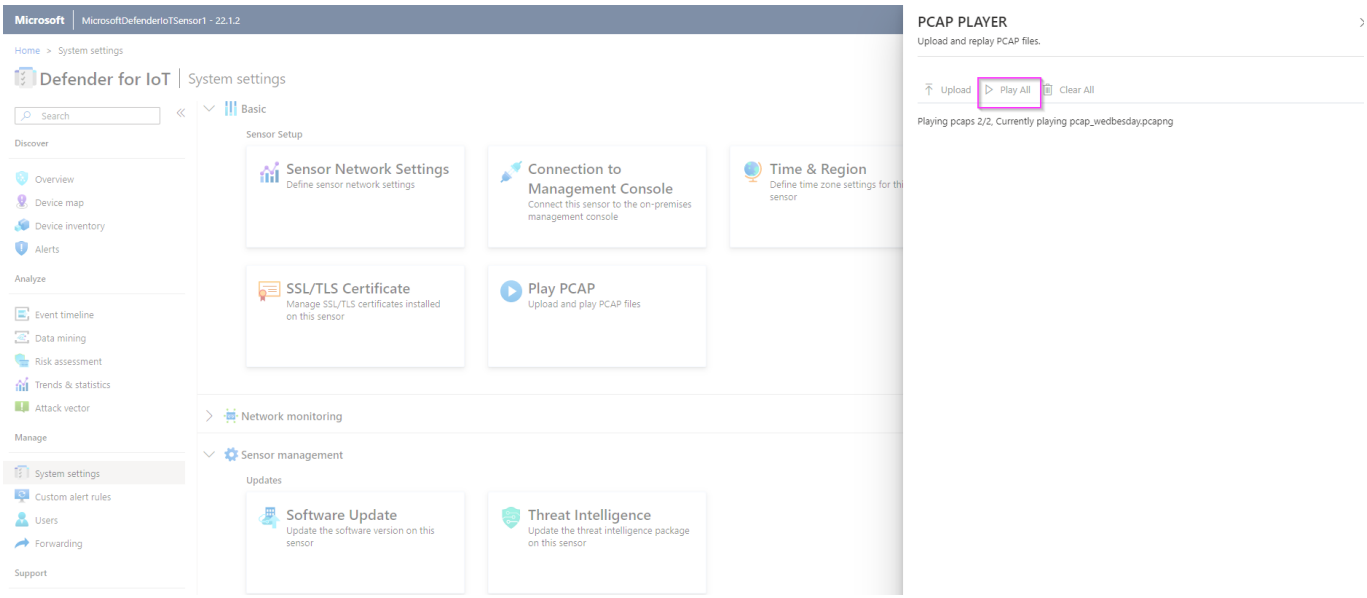
1. Use this link to download the holcaps.zip folder.
2. Unzip the folder.
3. Scroll all the way down to the bottom to locate if the PCAP Player is enabled (Shown in the image below in the red top square) or not. If the PCAP player is not shown, proceed to click on the arrow next to the **Sensor Management** button (Shown in the image below in the red lower square).



4. Click on **"Upload"** and select your Pcap files from the unzipped folder.



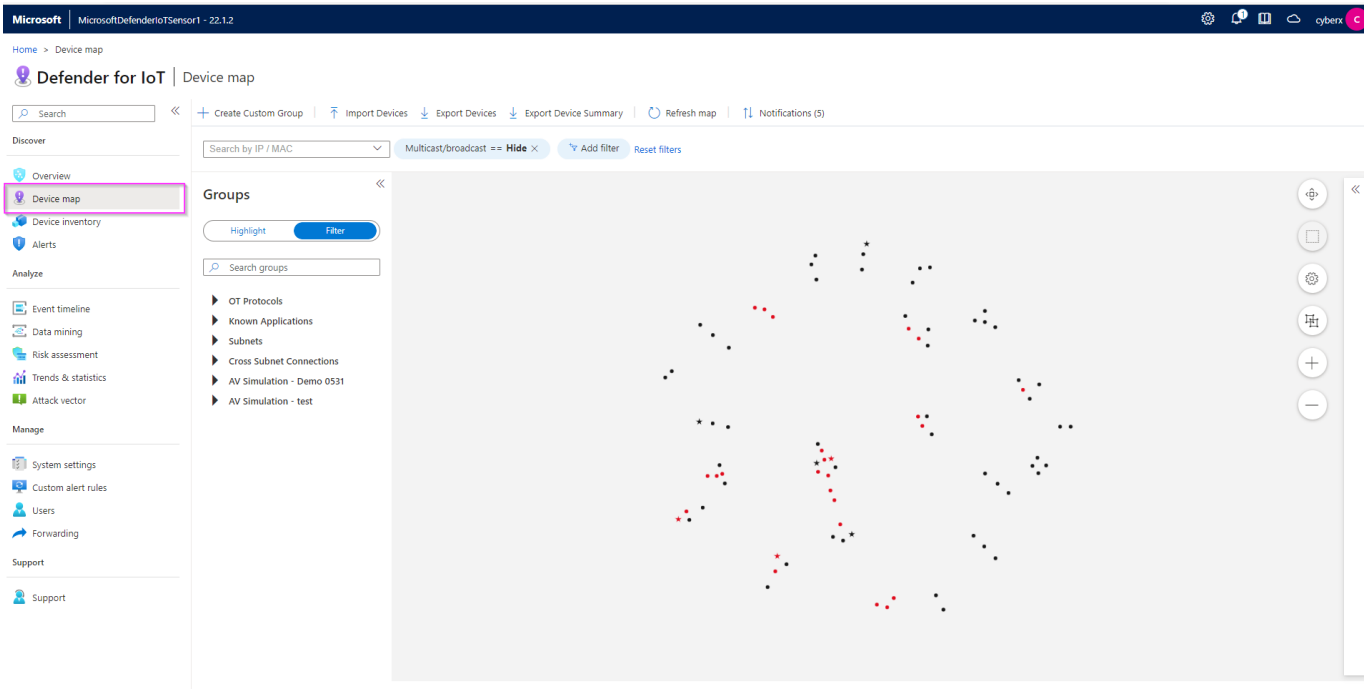
5. Click "Play All" to play the Pcaps.



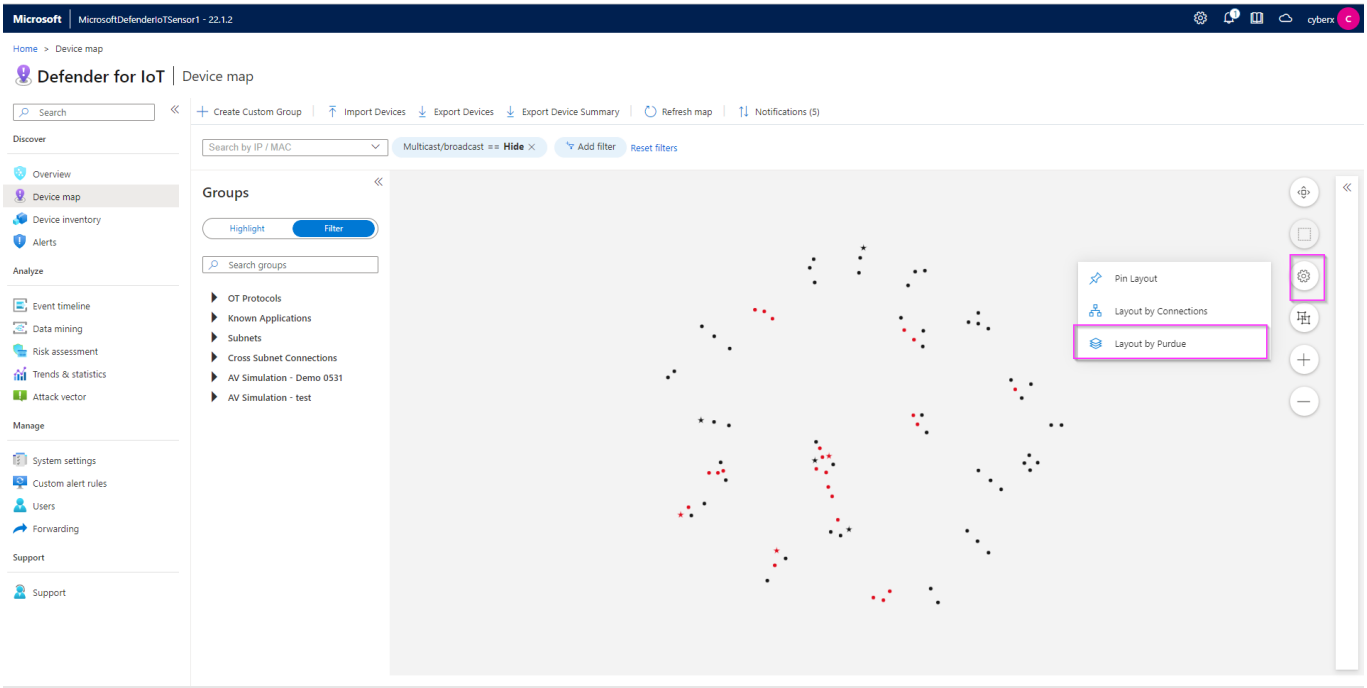
Exercise 5: Analyzing the Data

Task 1: Visualize on the Device Map

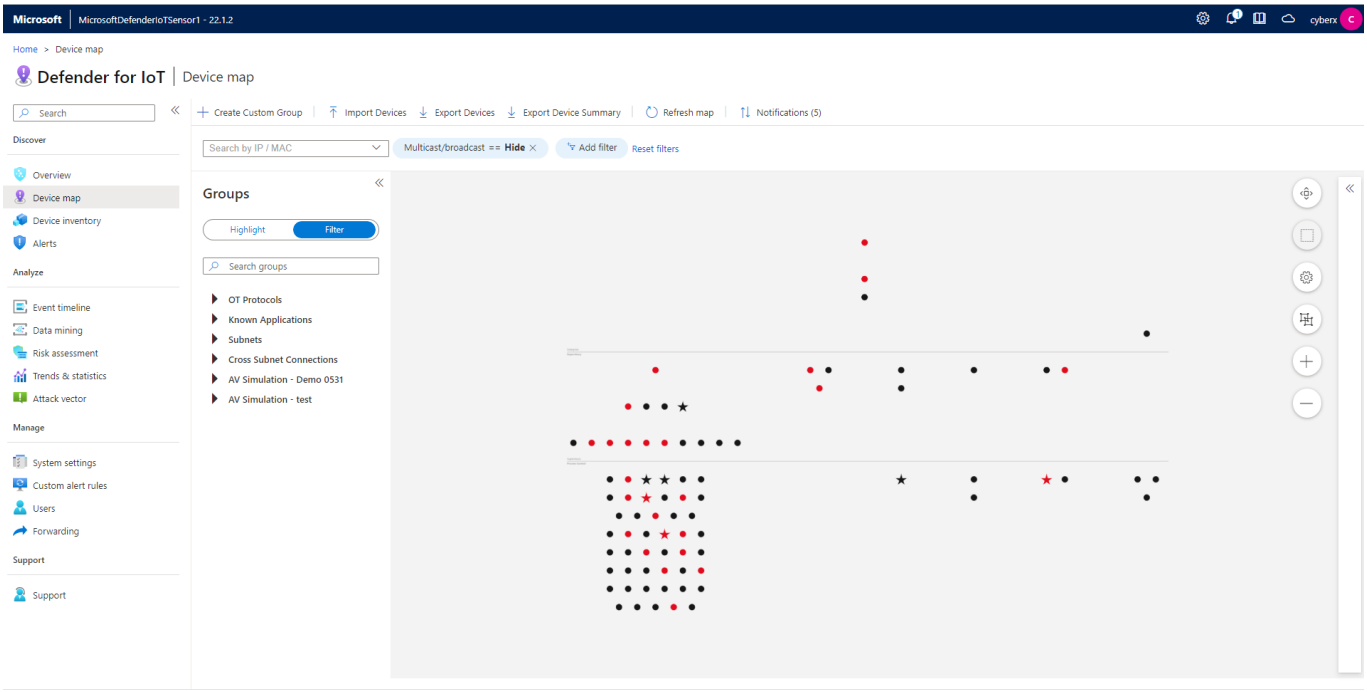
1. Click on **"Device Map"** from the menu on the left side.



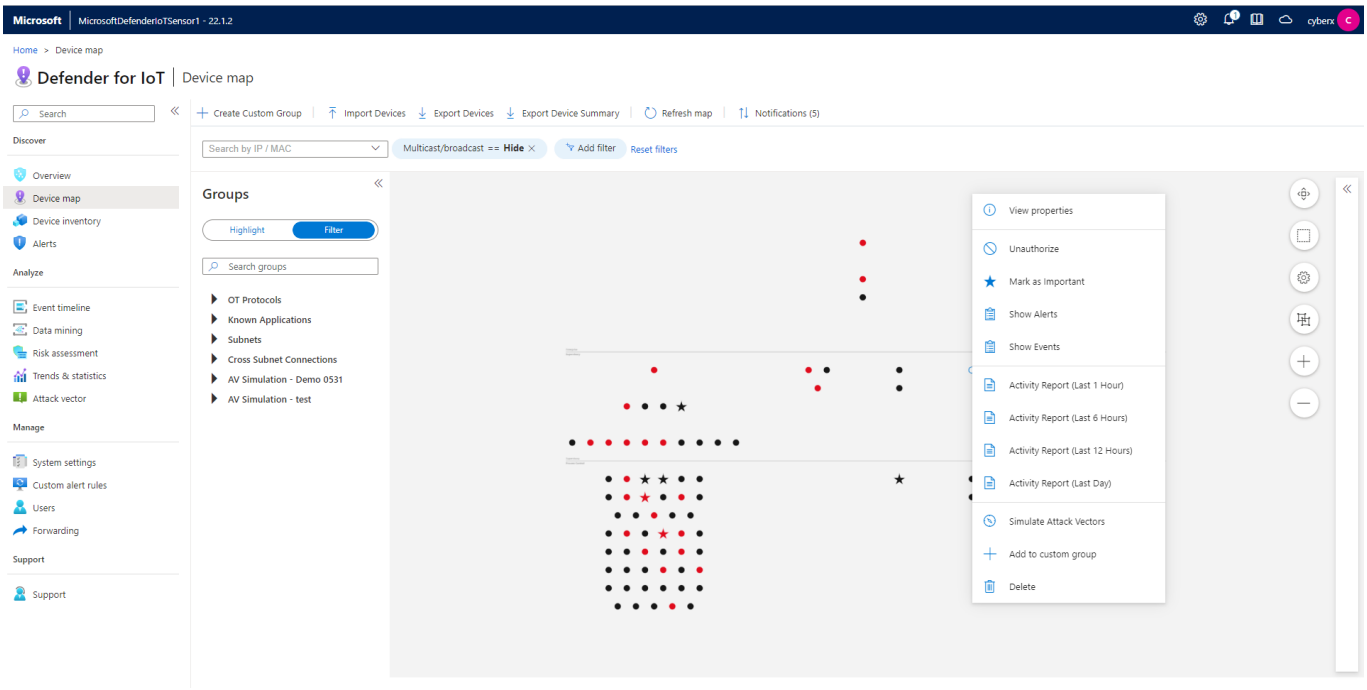
2. Click on the "Settings" option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.



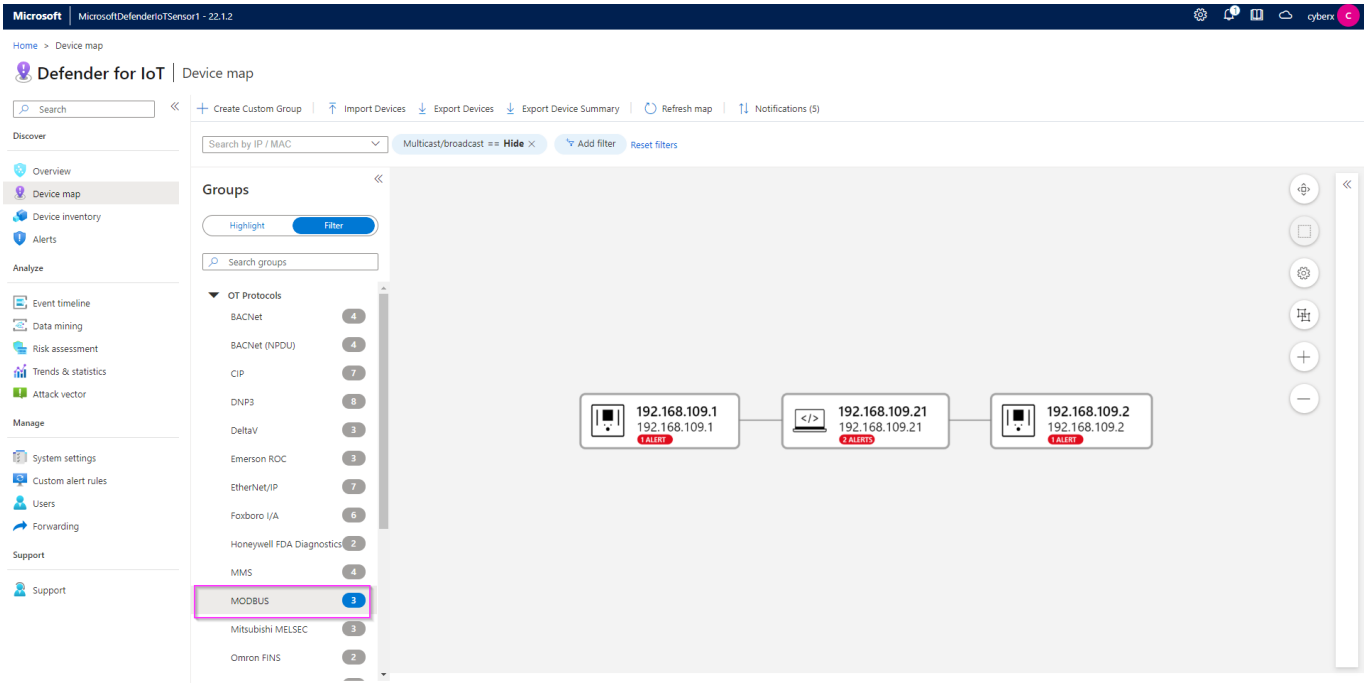
3. Once you confirm the changes, you will see the devices laid out as shown in the image below.



4. Right click on any device (represented by a dot) to view properties, show related events, alerts, reports or simulate attack vectors.

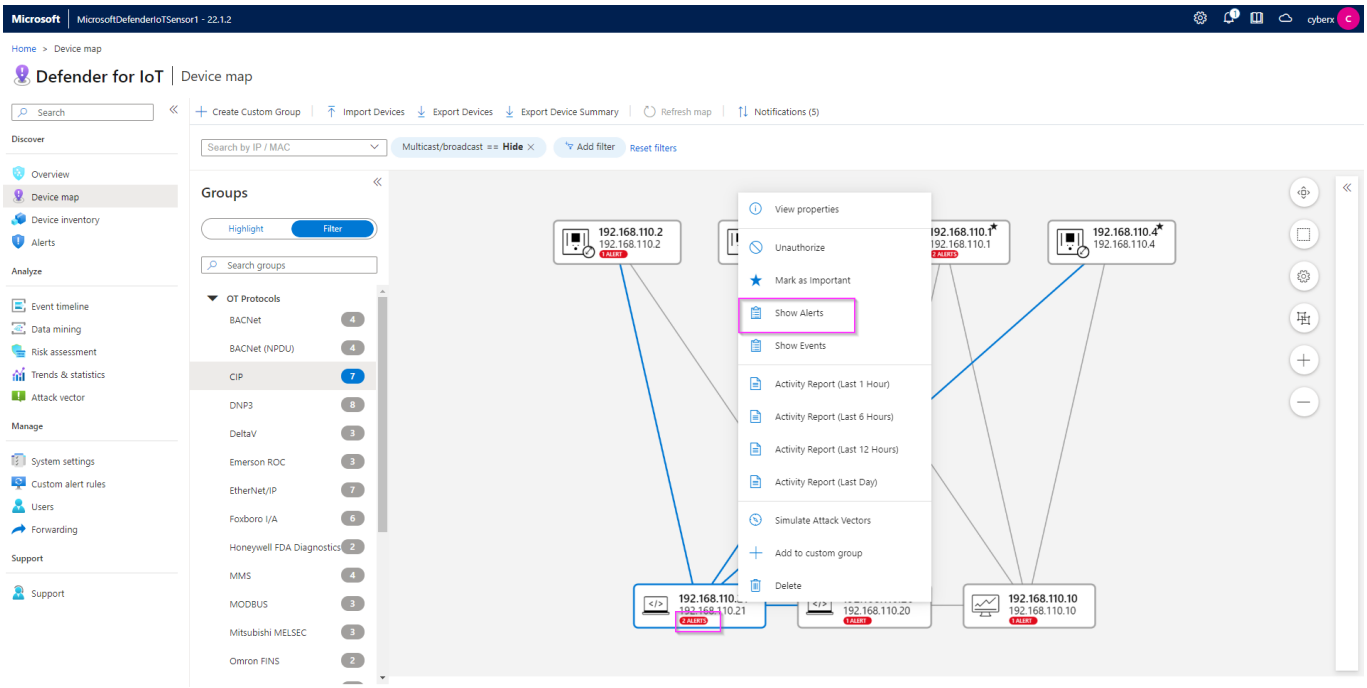


5.To filter by OT Protocols, expand the arrow, and pick the protocol you want to filter by. The console will display the devices that match the filter.

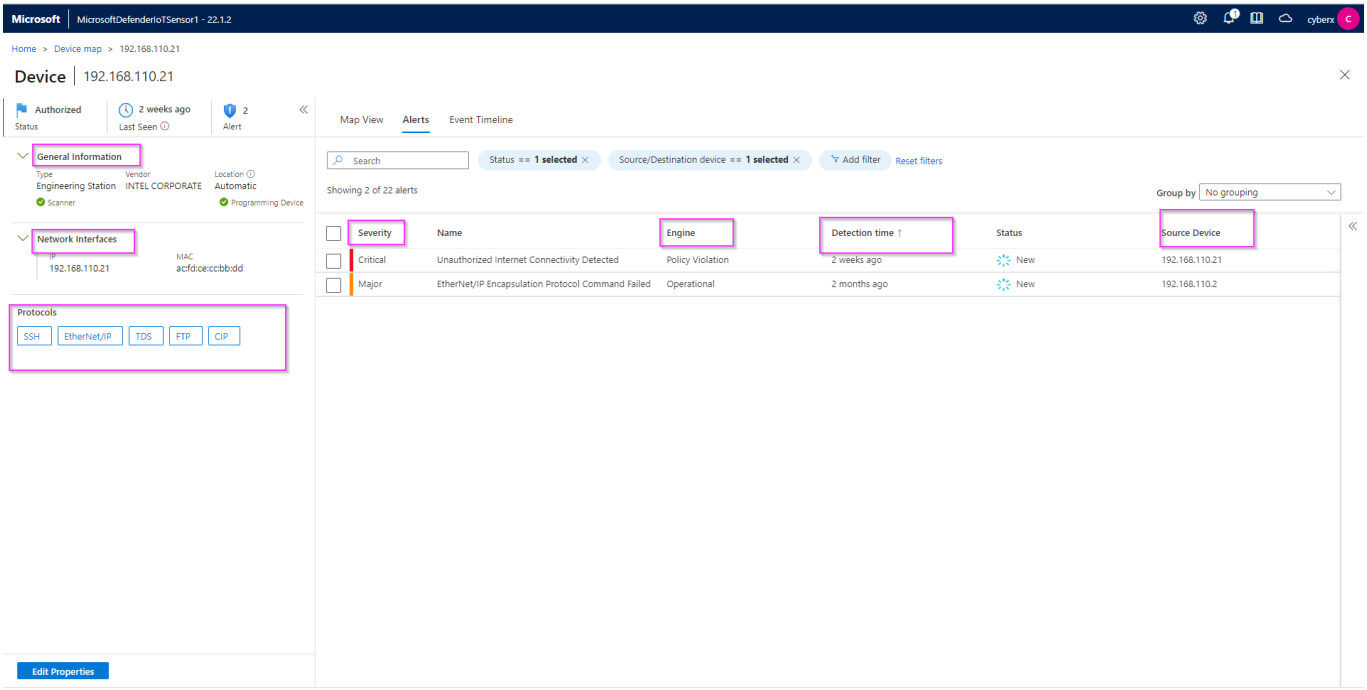


Task 2: View the associated Alerts

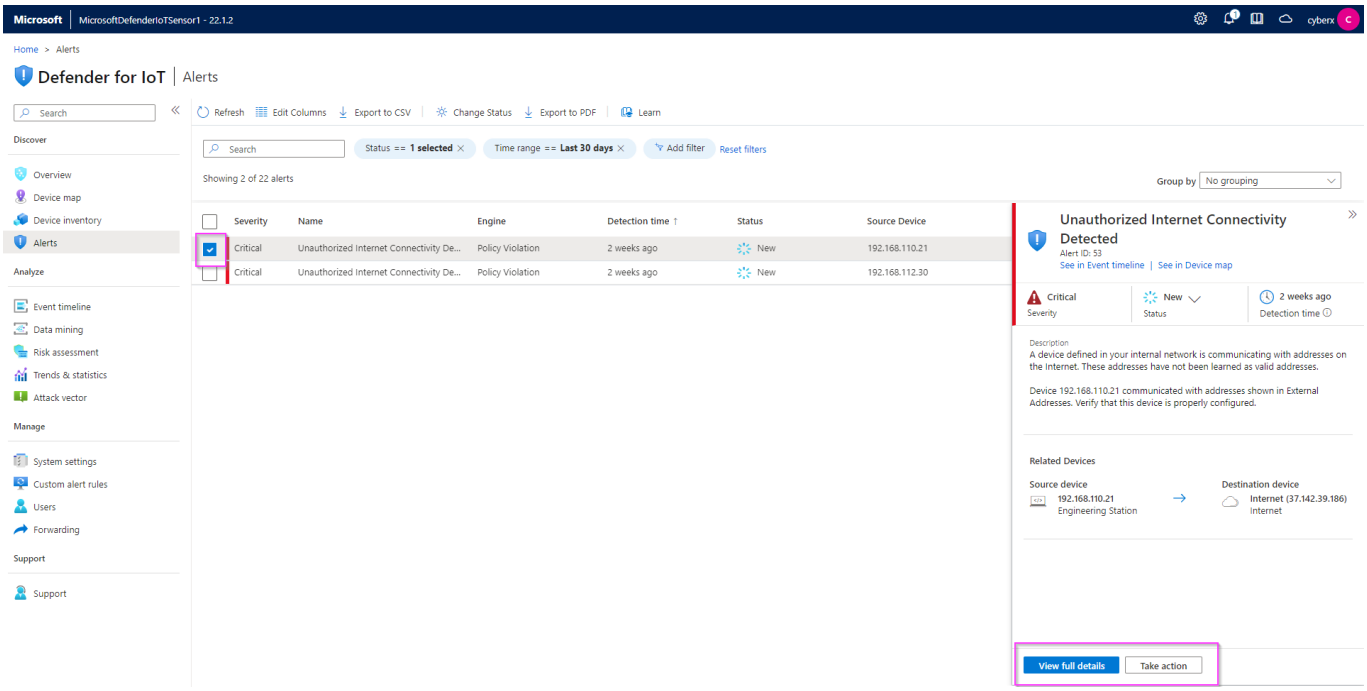
1. Right click on any device that has an Alert associated with it and click on “**Show Alerts”**.



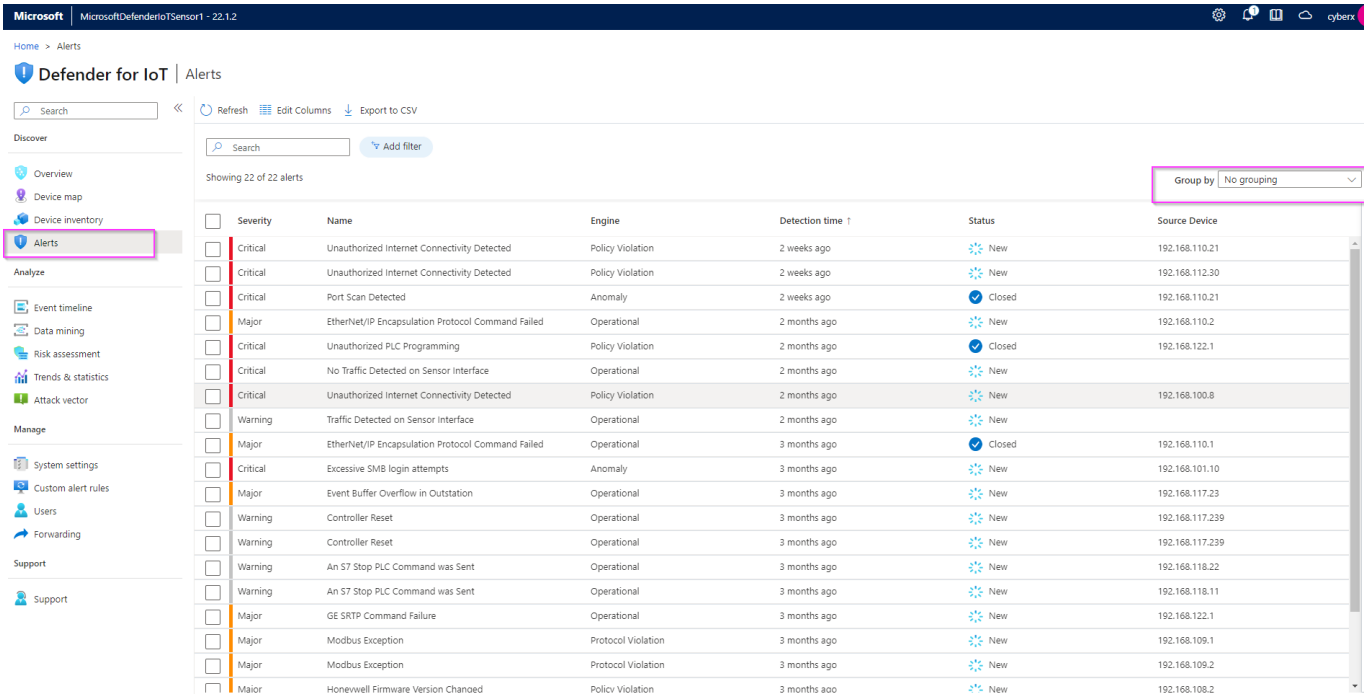
2. The Alerts page helps you identify some important data about the alert, like Alert Severity, Engine, Detection time, as well as the Source Device IPs. It also displays general information about the type of device, network interfaces and protocols.



3.To view more details about the Alert and/or to take remediation actions, select the Alert by checking the box beside it, and picking either **“View Full Details”** or **“Take Action”.**

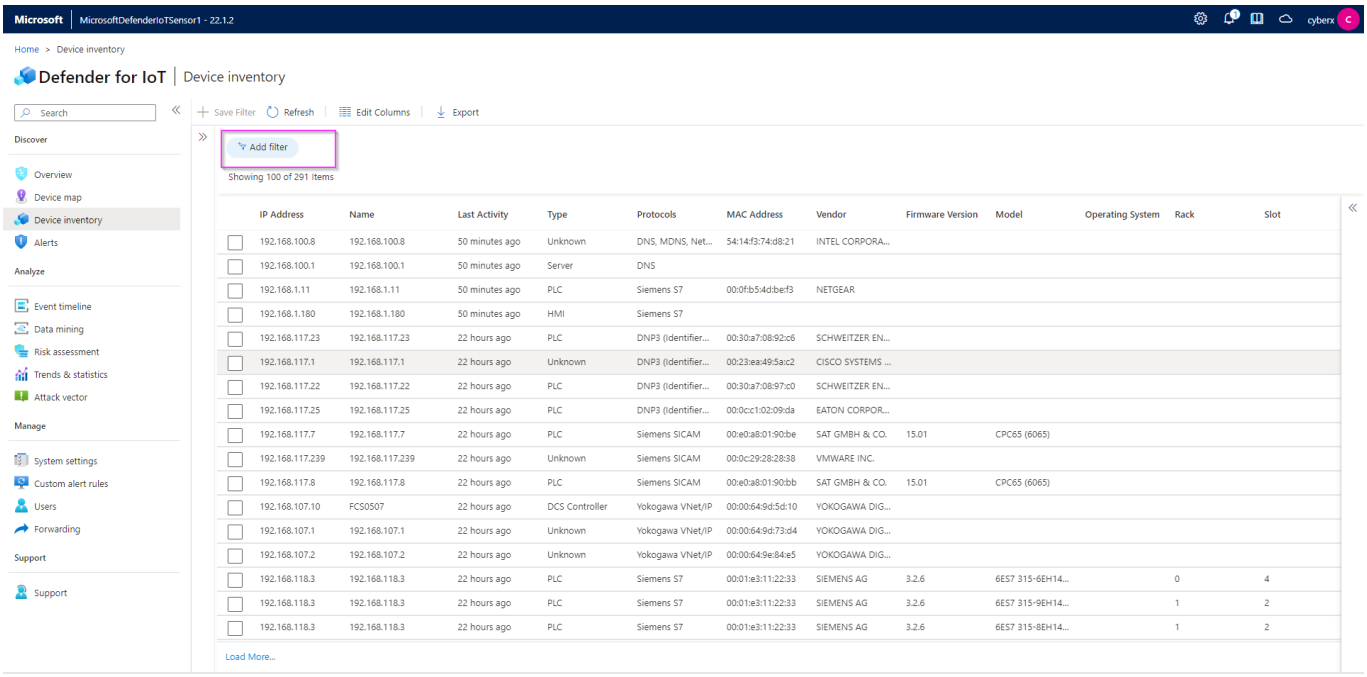


4.You can view all the alerts on your sensor by clicking on the **Alerts** option on the menu on the left. Make sure all the filters are removed. You can group the alerts by picking an option from the **"Group by"** dropdown.

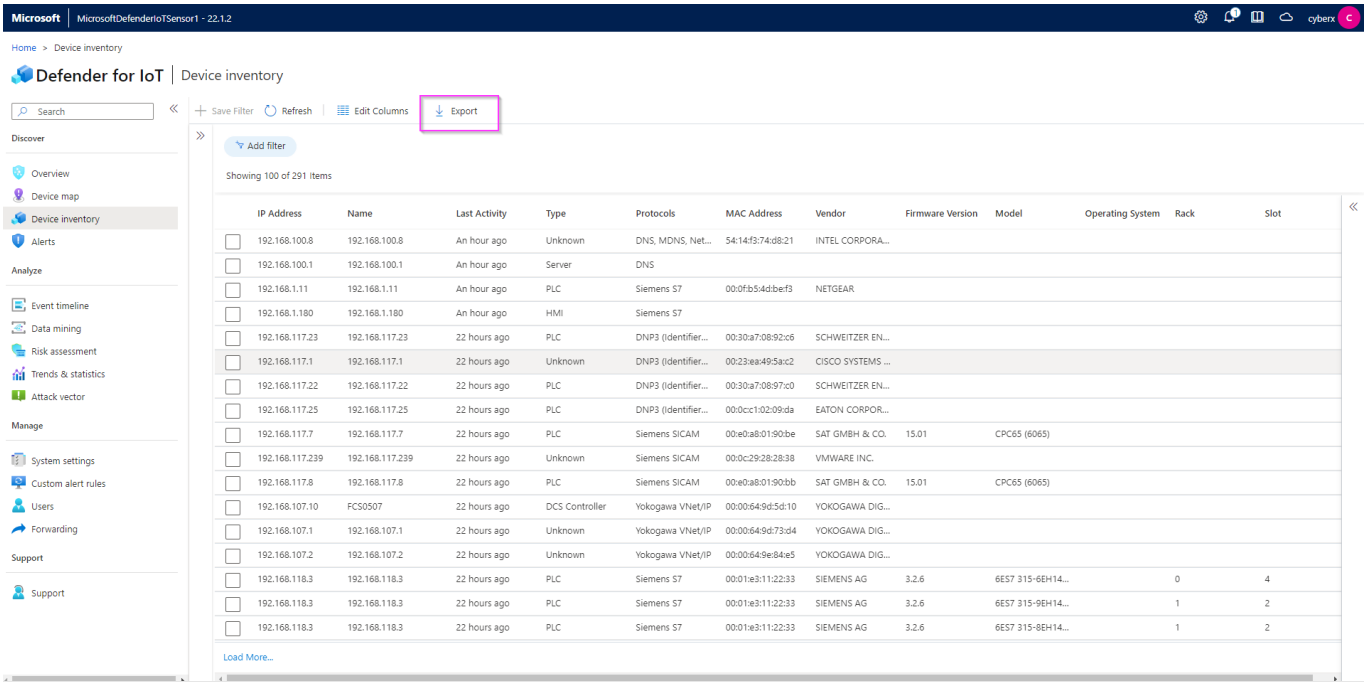


Task 3: Device Inventory

1. This view allows you to see all the devices connected to your sensor as a list. To filter, click on "Add filter" on the top. For example: the "**Is Authorized**" will show you devices that are either authorized or unauthorized depending on value (True or False) you choose.

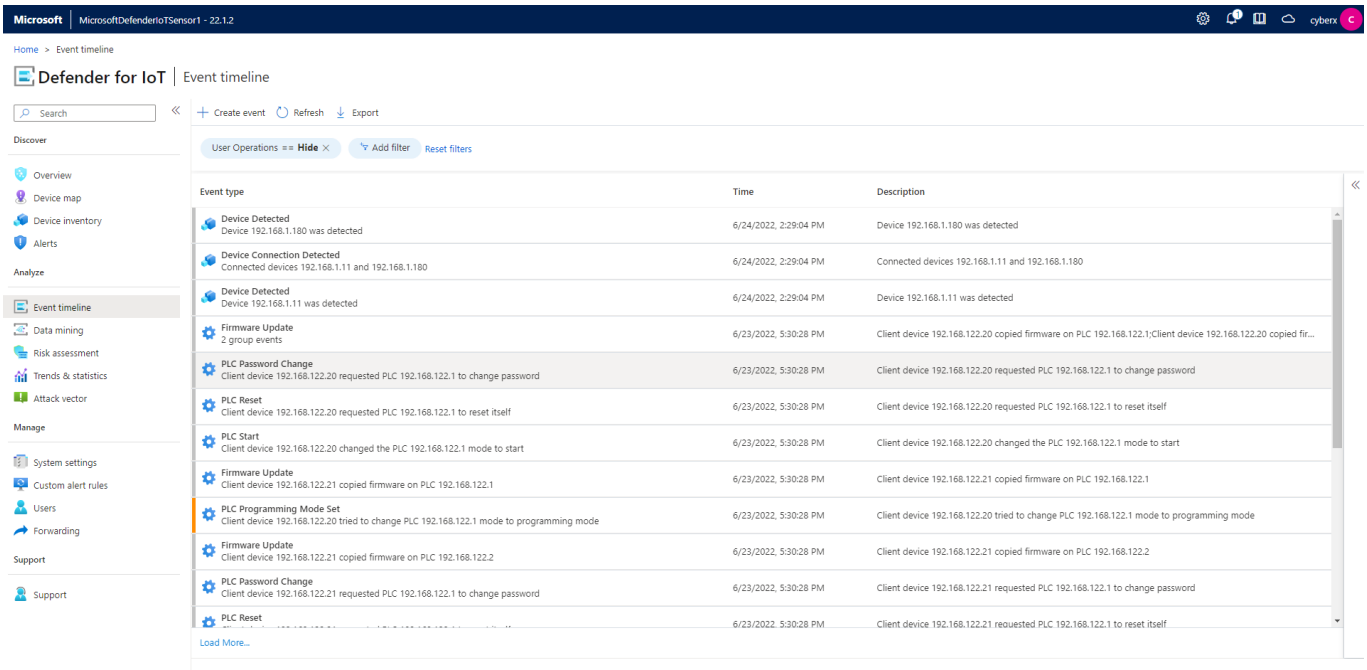


2. You can export the list to a csv file.



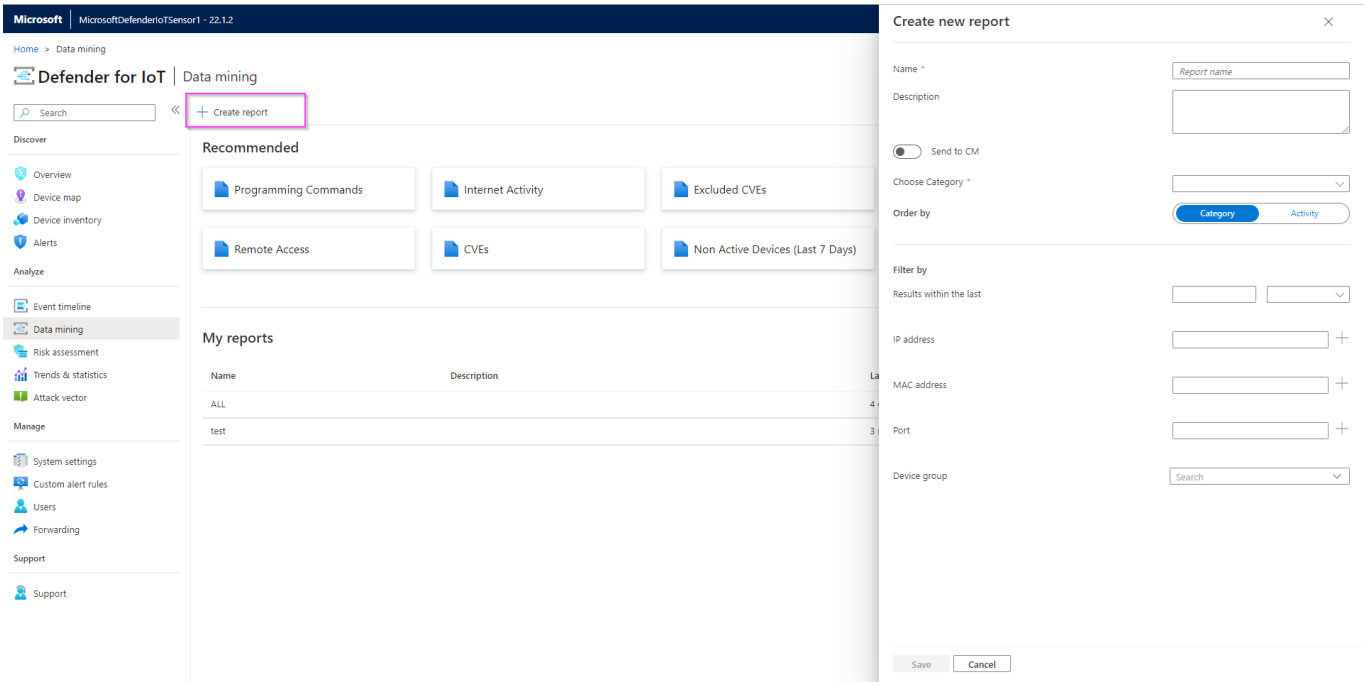
Task 4: View the Event Timeline

1. This view will allow you a Forensic analysis of your alerts. You can choose to Hide or Unhide the User Operations or select more filter types from the “Add filter”.

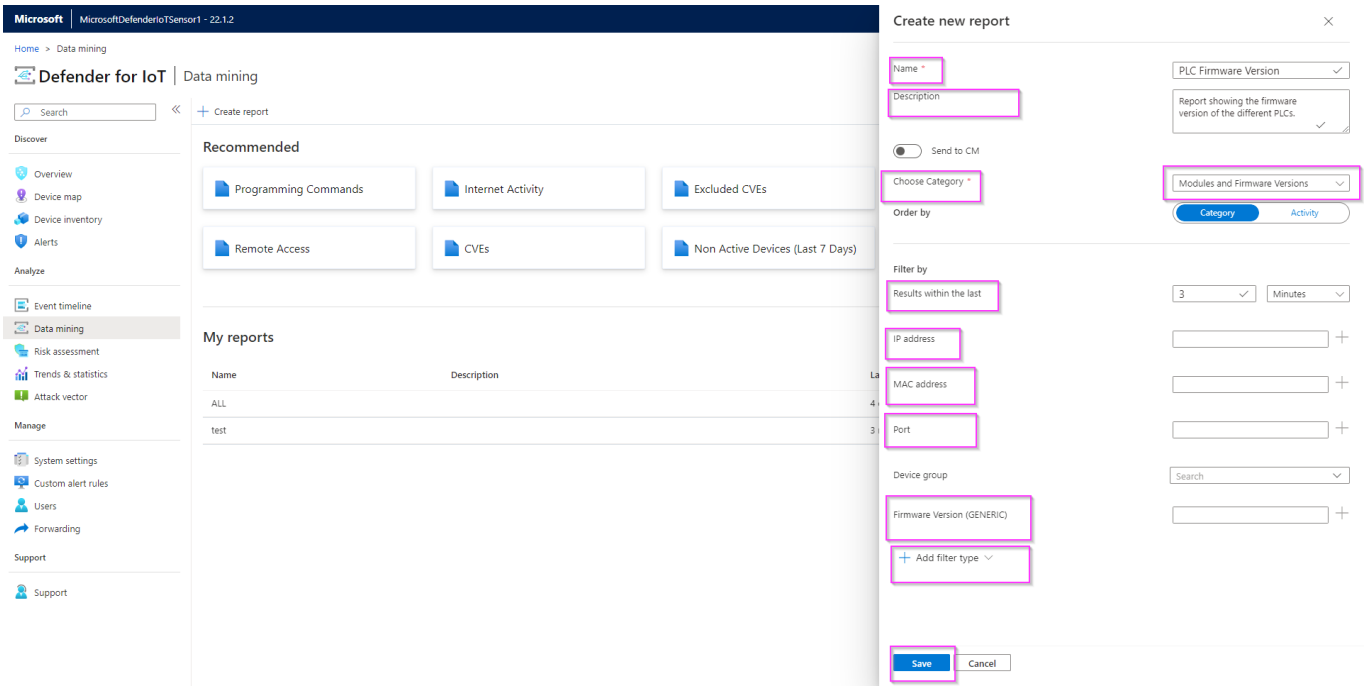


Task 5: Data Mining

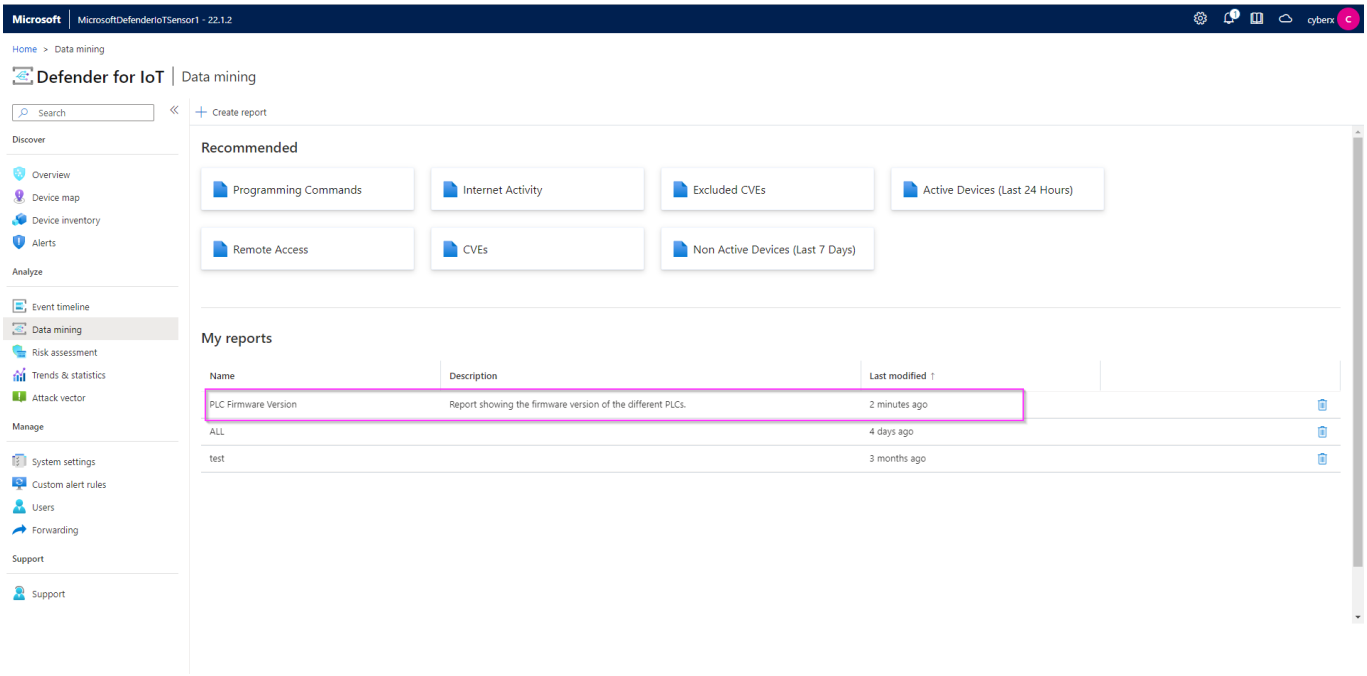
1. In this section you can create multiple custom reports. As an example, we will create a Report based on firmware updates versions. Click on + Create report to open the wizard.



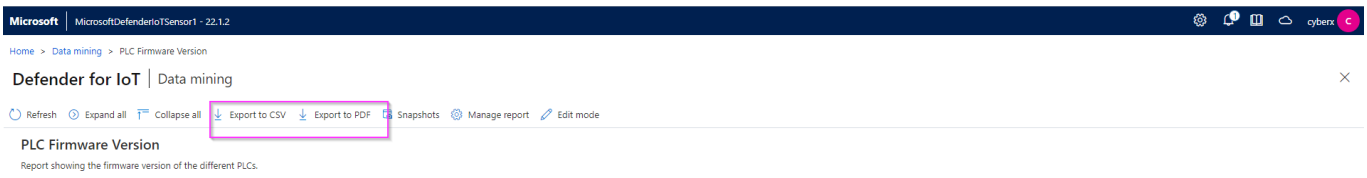
2. Assign a name and a description to your report. Pick **“Modules and Firmware Versions”** for Category, select **“Firmware Version (GENERIC)”** from **“add filter”.**



3. Your report will show up on the list under “My reports”.

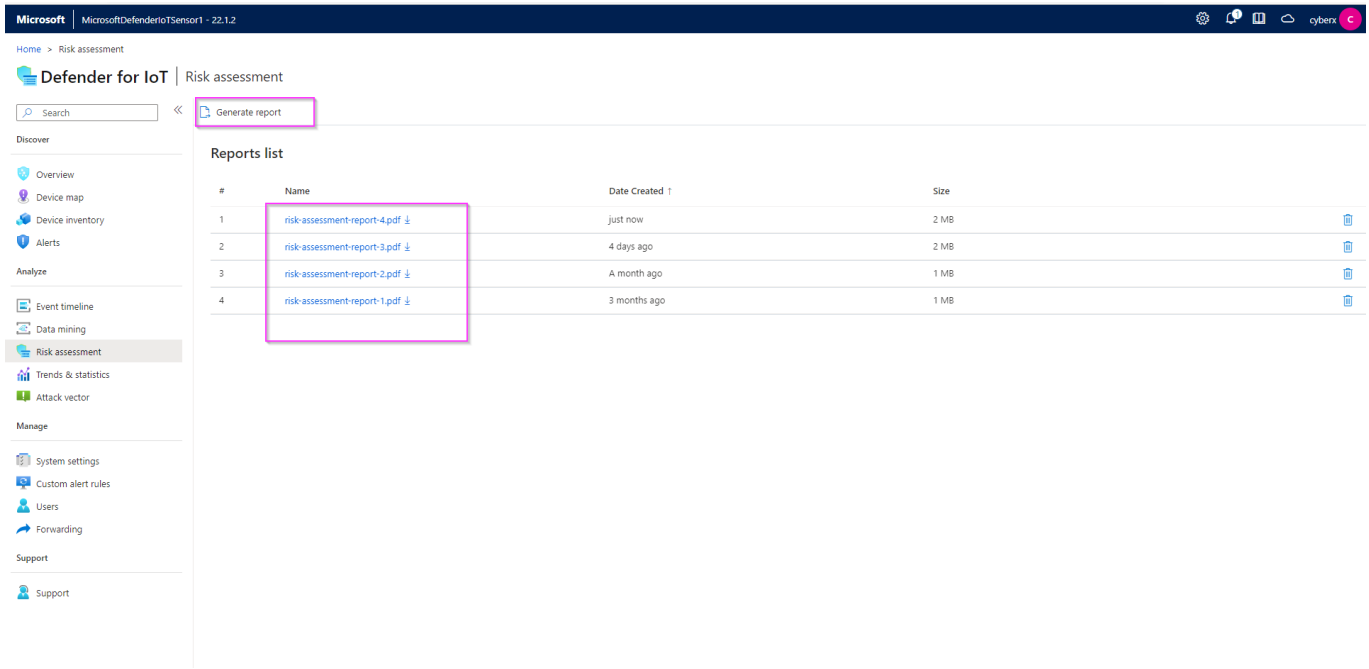


4. You can export the report as pdf or csv.



Task 6: Generate a Risk Assessment report

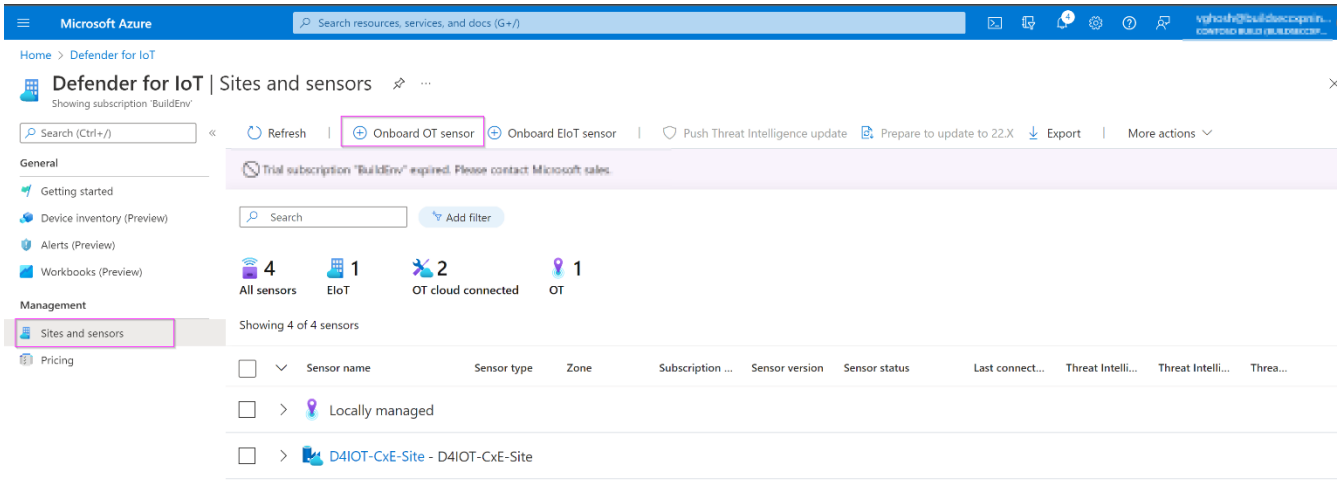
1. On the Risk assessment page, run the assessment by clicking the “Generate report” button. You can download and view the report as pdf.



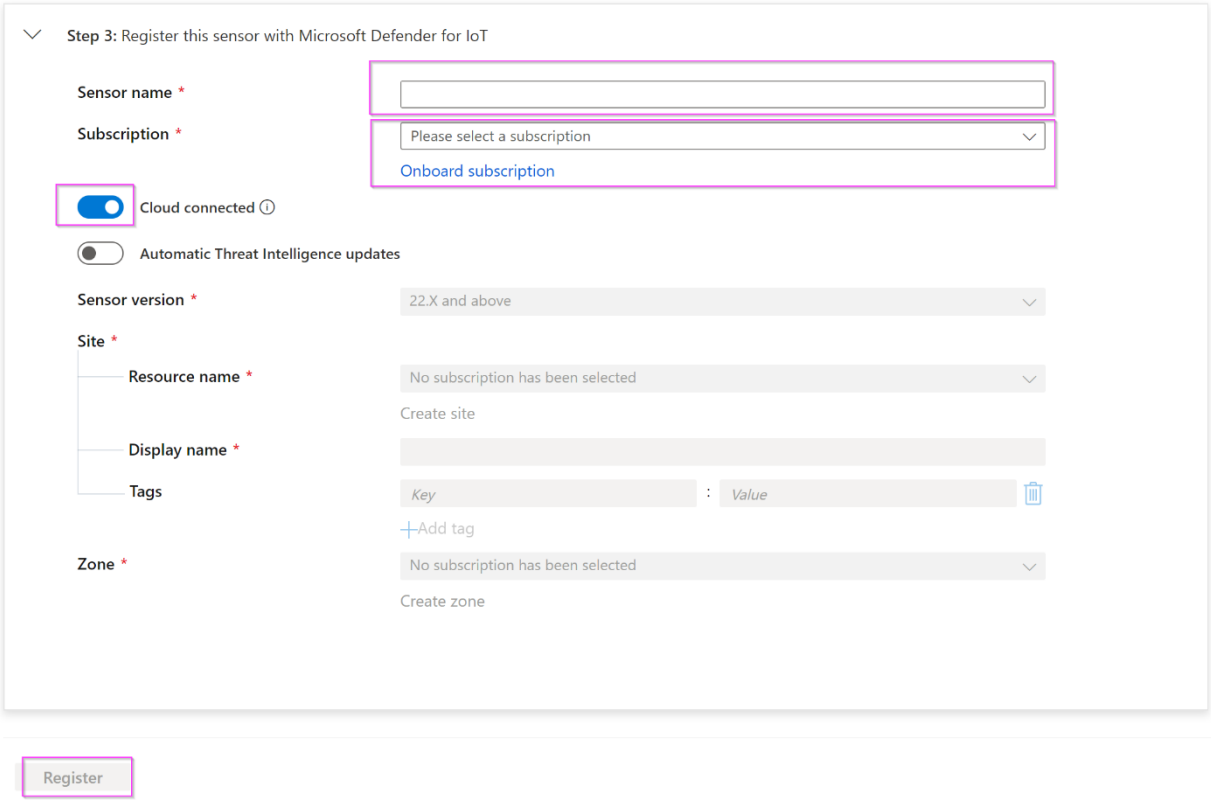
Exercise 6: Cloud Connect your sensor.

Task 1: Create the cloud connected sensor on the Cloud Management portal

1. On the cloud management (Azure) portal, navigate to “Sites and sensors” and click on “Onboard OT sensor”.



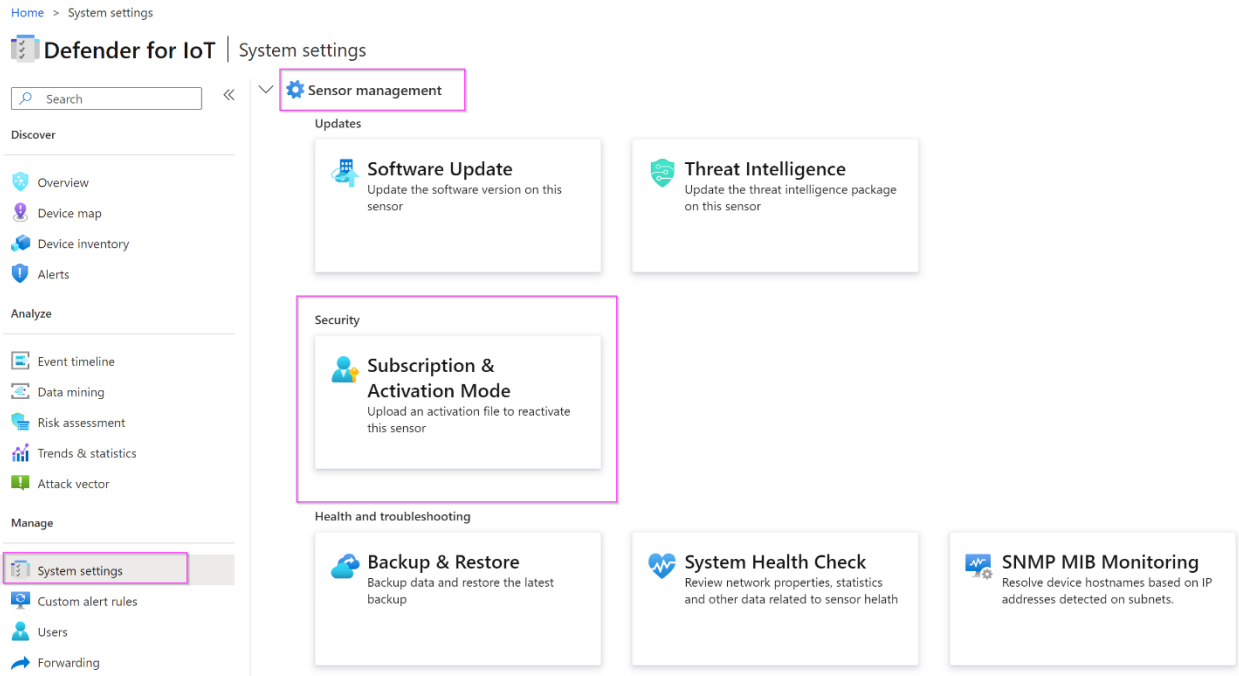
2. Give the sensor a meaningful name, pick the subscription from the dropdown menu, and ensure that “cloud connected” is checked. Click on “Register”.



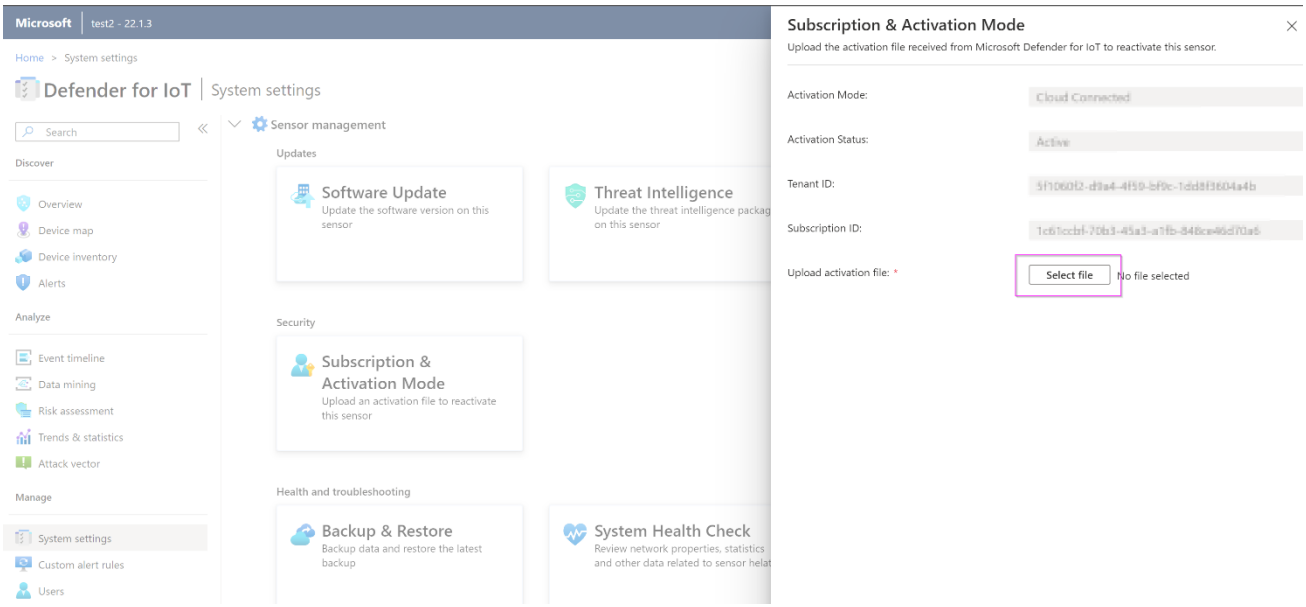
3. The download for the activation starts immediately. Please check your downloads.

Task 2: Upload the activation file to cloud connect your sensor.

1. Navigate back to your sensor and click on “System settings” -> “Sensor management” -> “Subscription and Activation Mode”.

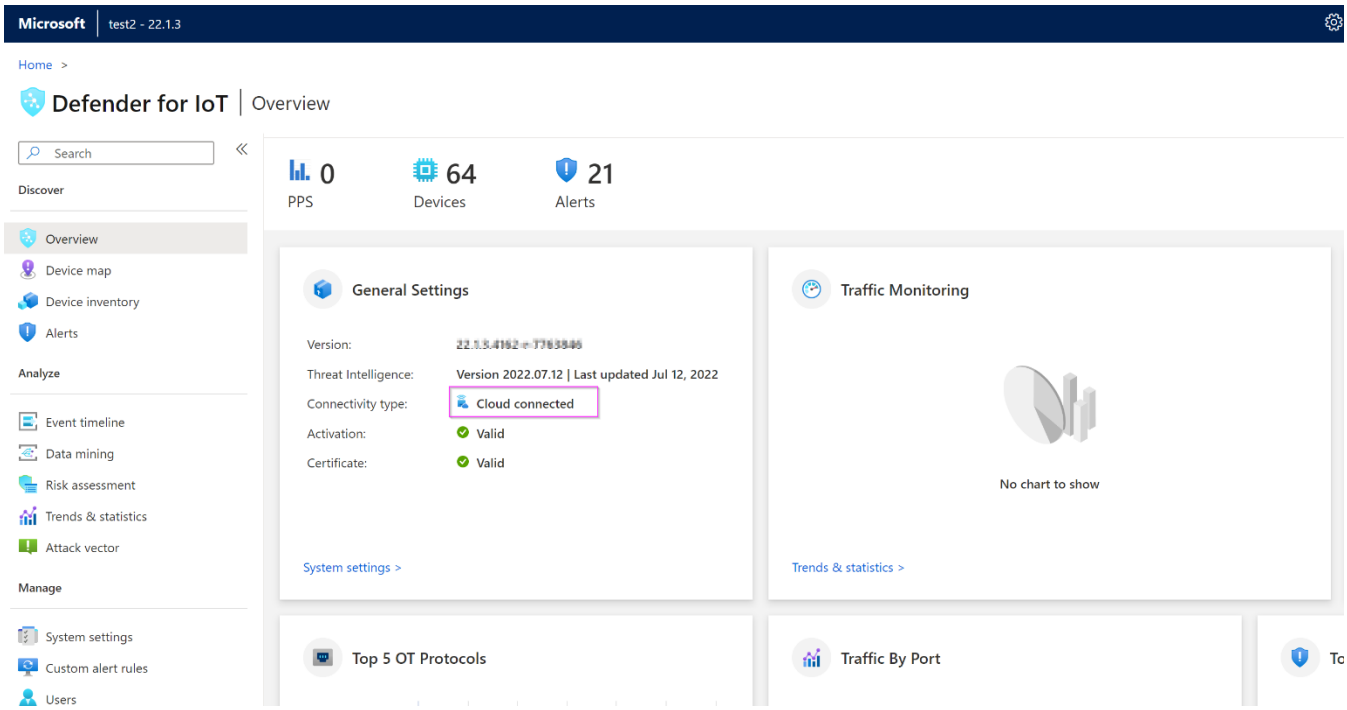


2. Upload the activation file you downloaded in the previous step. Click on “Activate”.

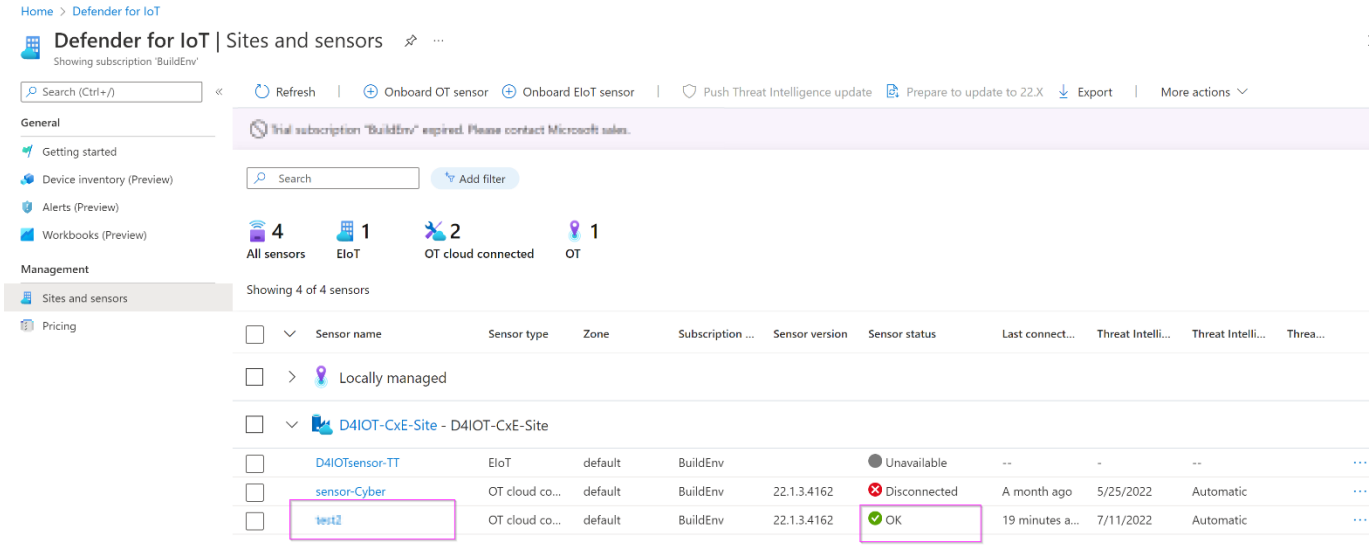


Task 3: Verify Cloud connection

1. On the sensor console.



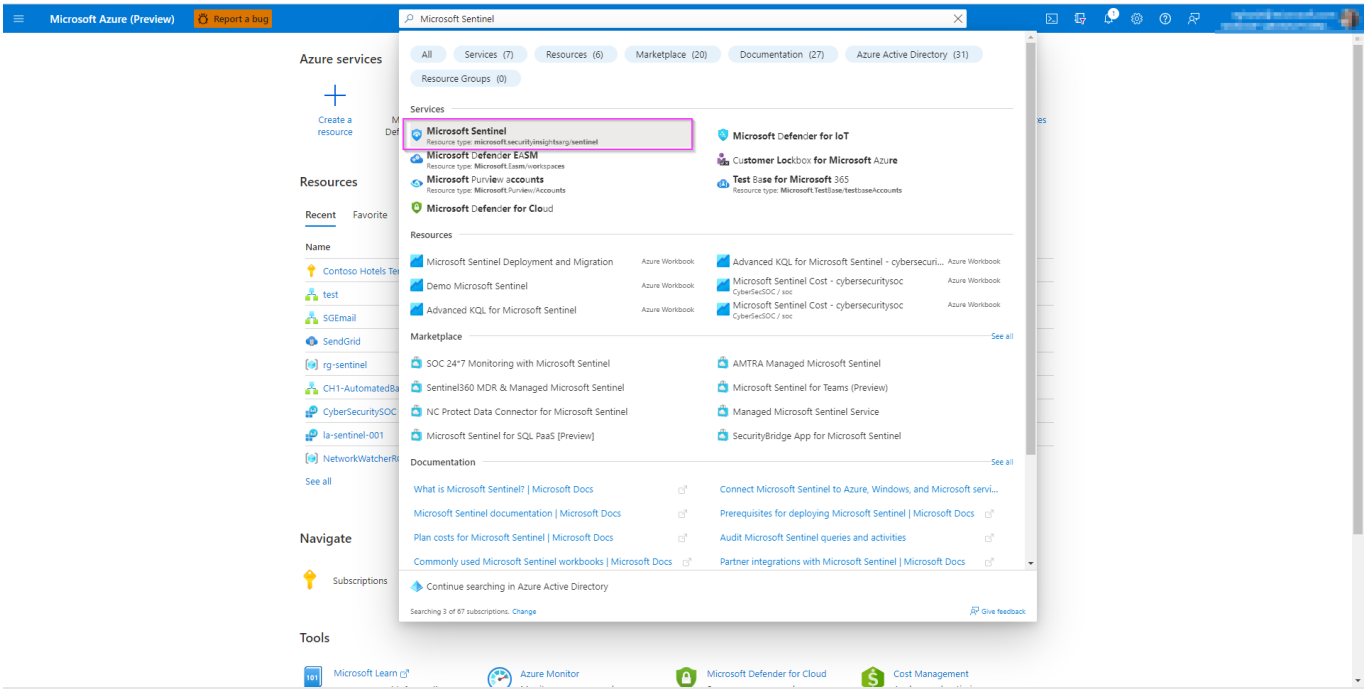
2. On the Cloud management console.



Exercise 7: Integrate with Microsoft Sentinel

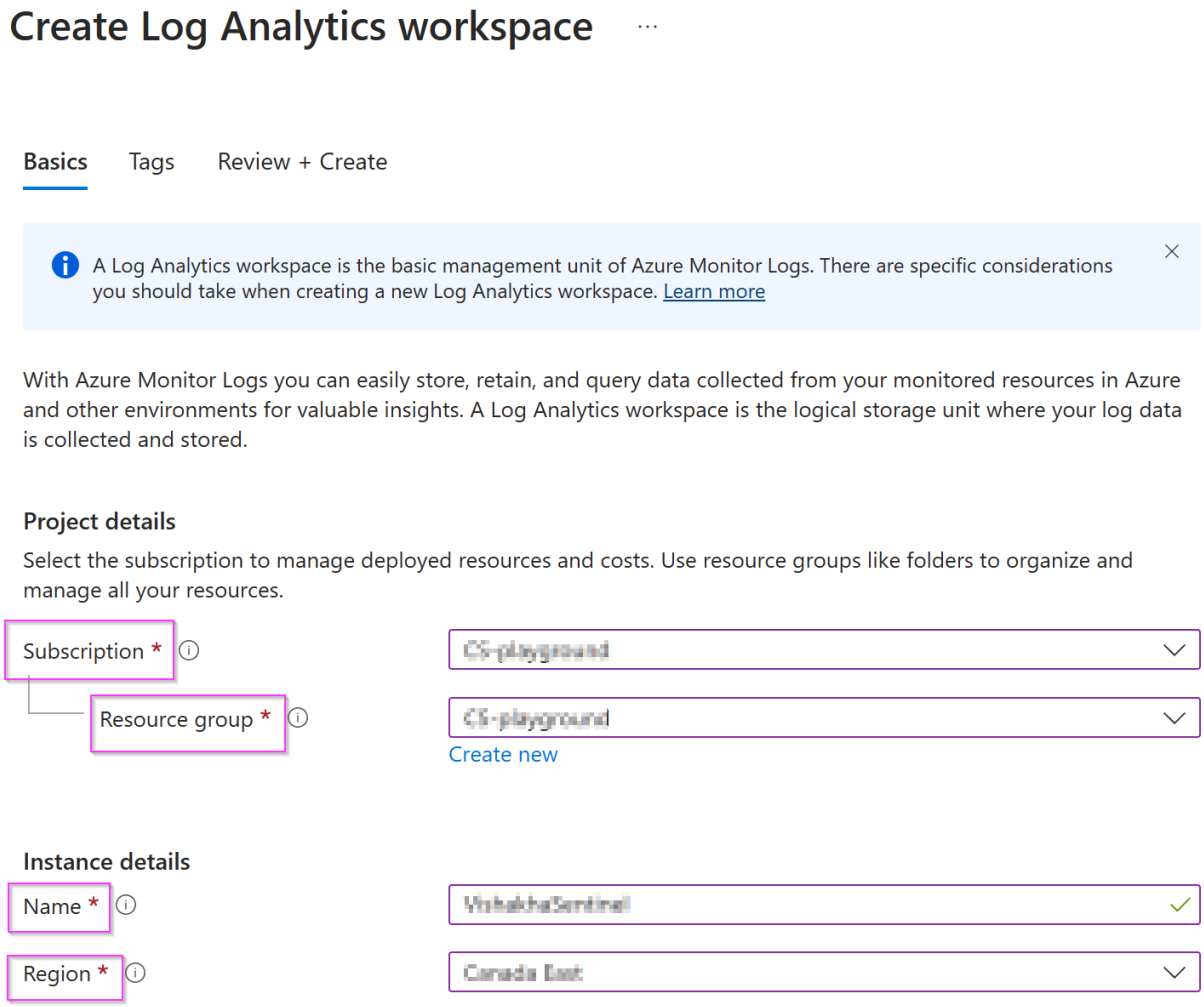
Task 1: Create a Log Analytics Workspace

1. On the Azure portal, search for **Microsoft Sentinel.**

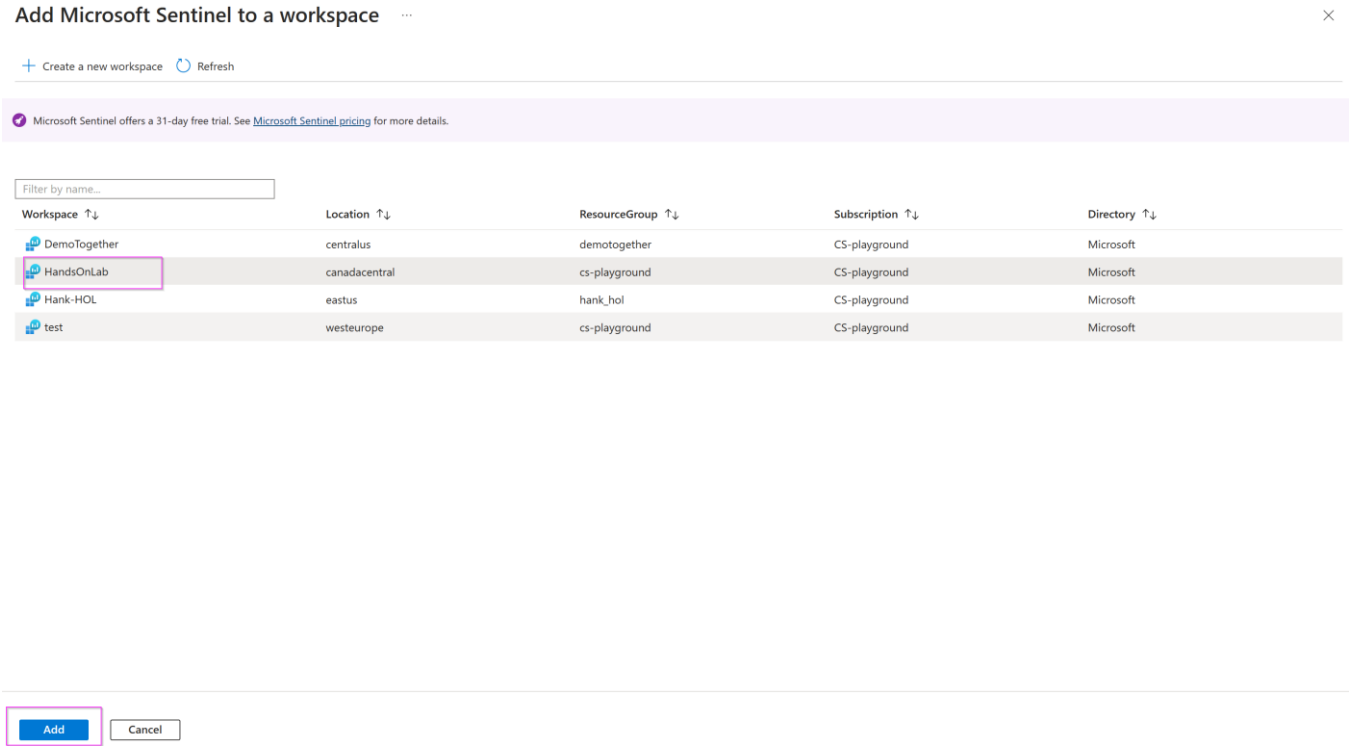


2. Click on “+Create” -> “+Create a new workspace”.

3. Pick your subscription, Resource Group, Name and Region

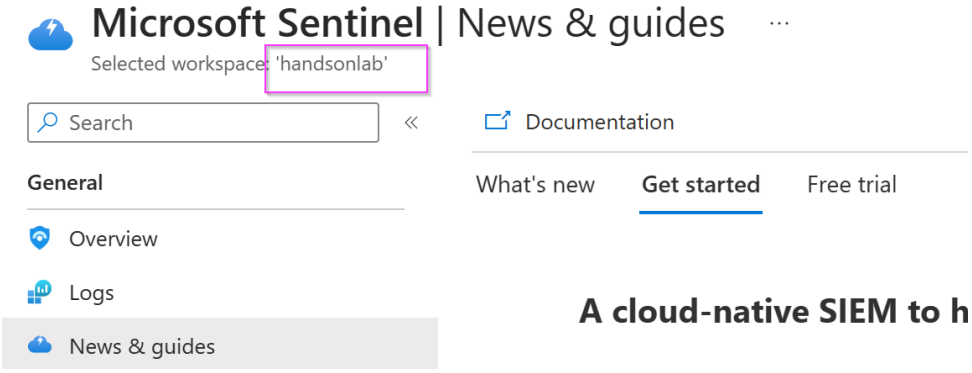


4. Click on “Review +Create” -> “Create”.
5. Go to Sentinel -> find the workspace you just created -> Click “Add” to add the workspace to Sentinel.

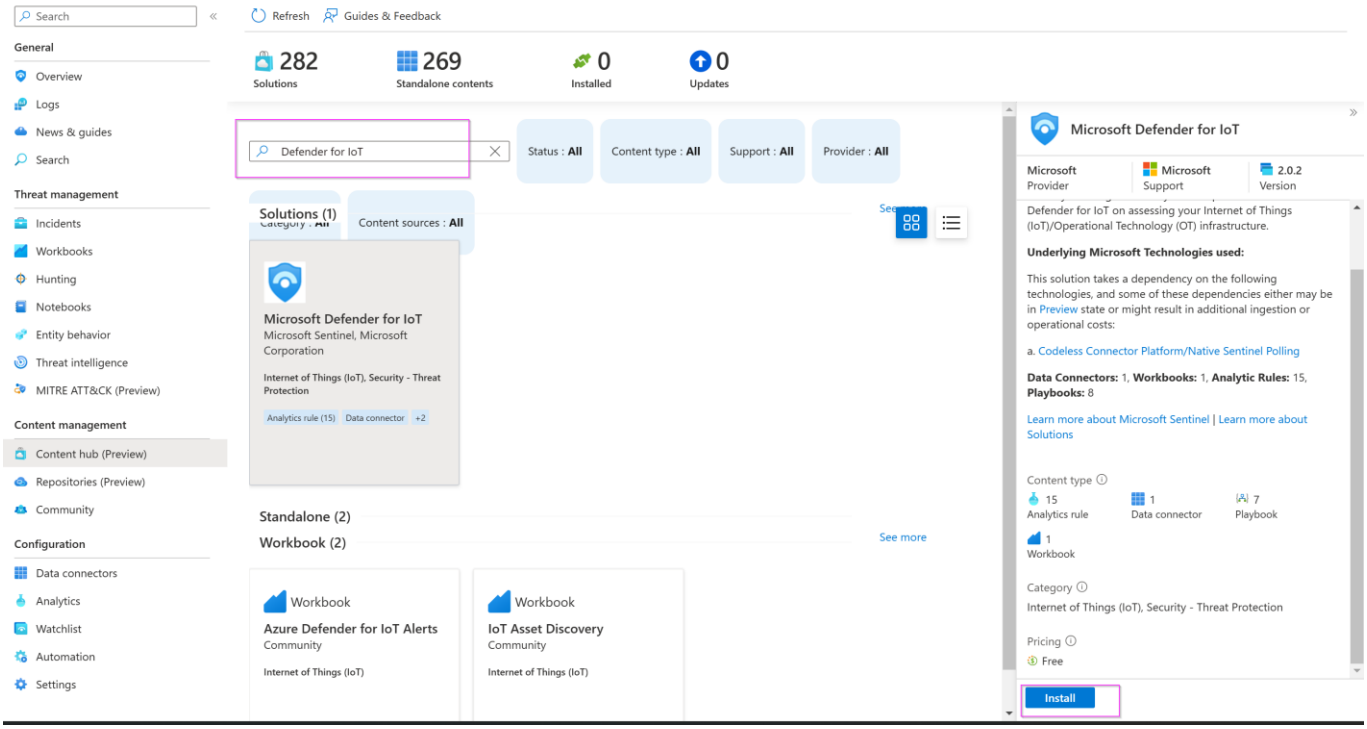


Task 2: Install the Defender for IoT package

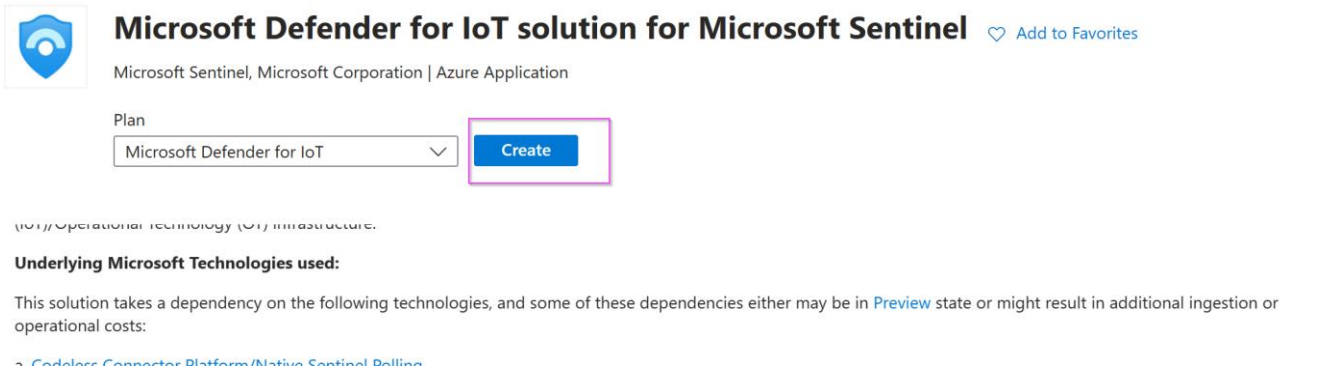
1.Go to Sentinel, make sure your workspace is selected.



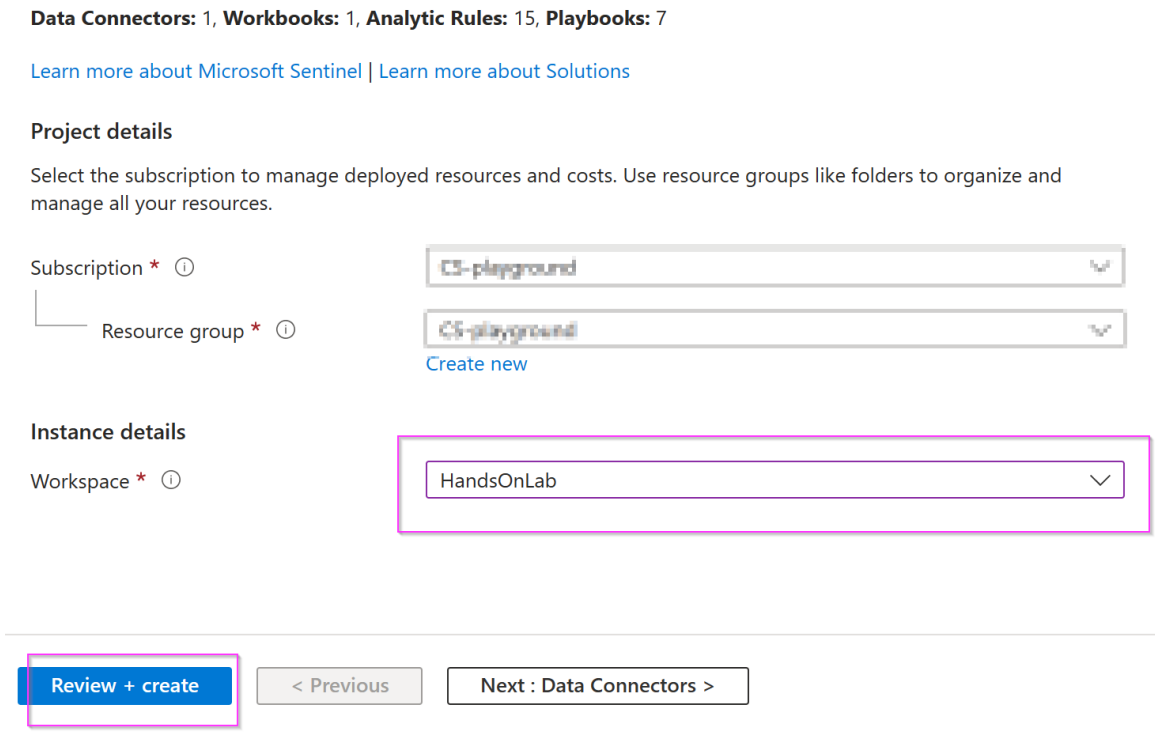
2.Go to “Content Hub” -> Type “Defender for IoT” and click on “Install”. The package includes Analytic Rukles, Data Connector, Playbooks and Workbooks.



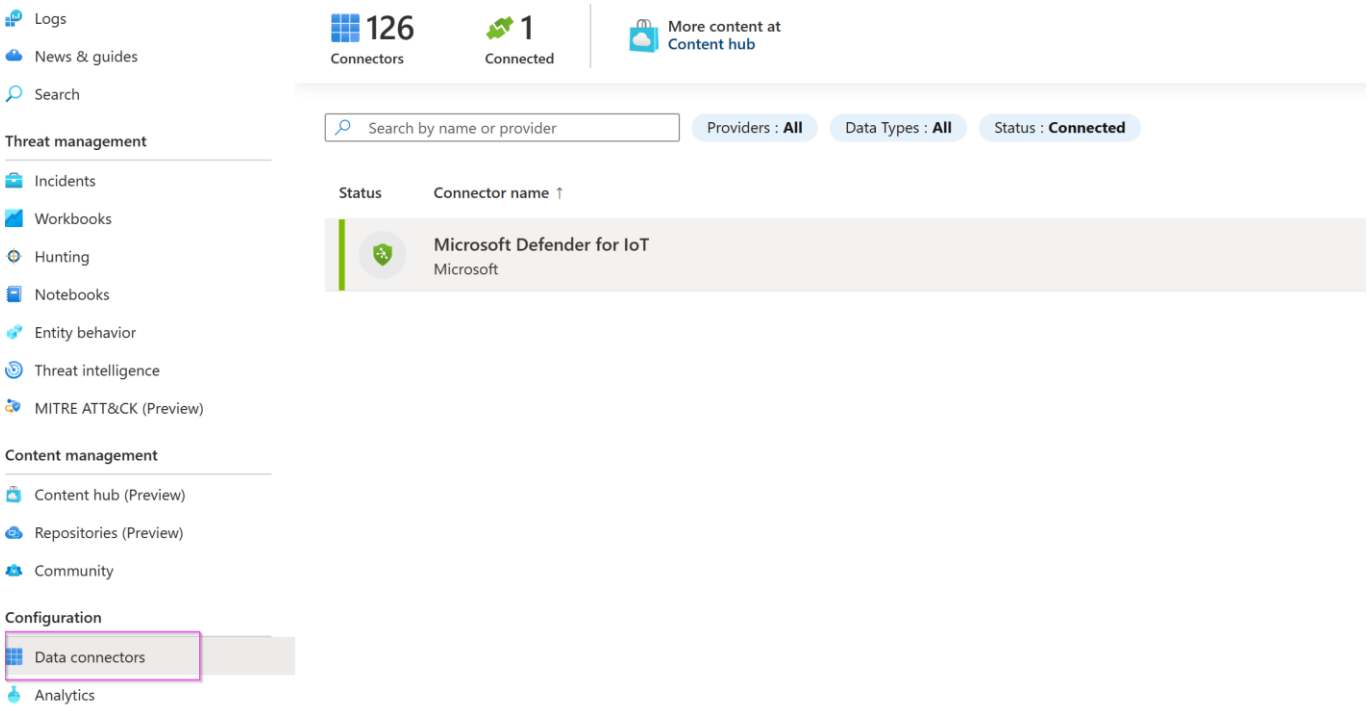
3.Click on “Create”.



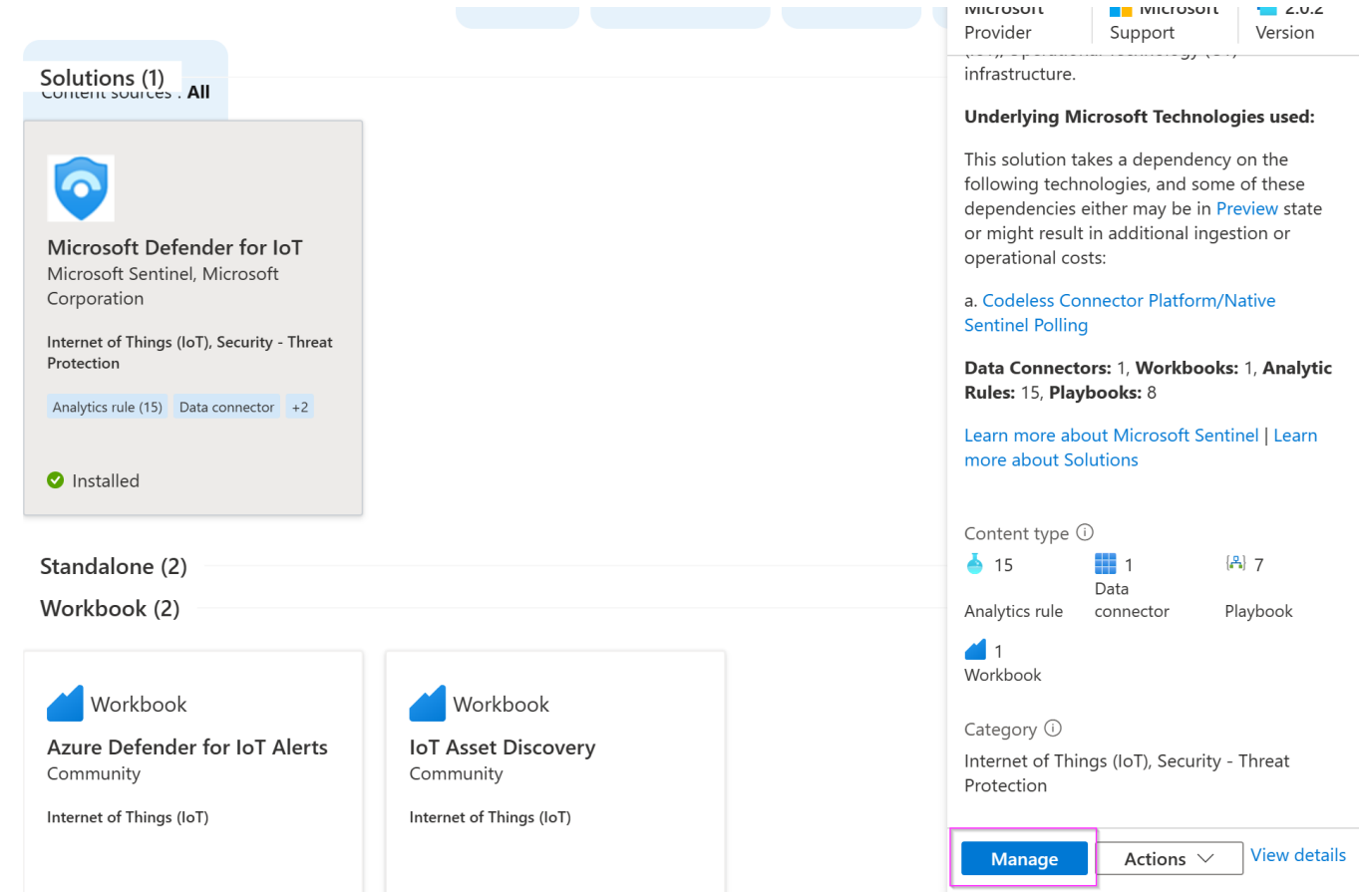
4.Select the workspace and click on “Review and Create”.

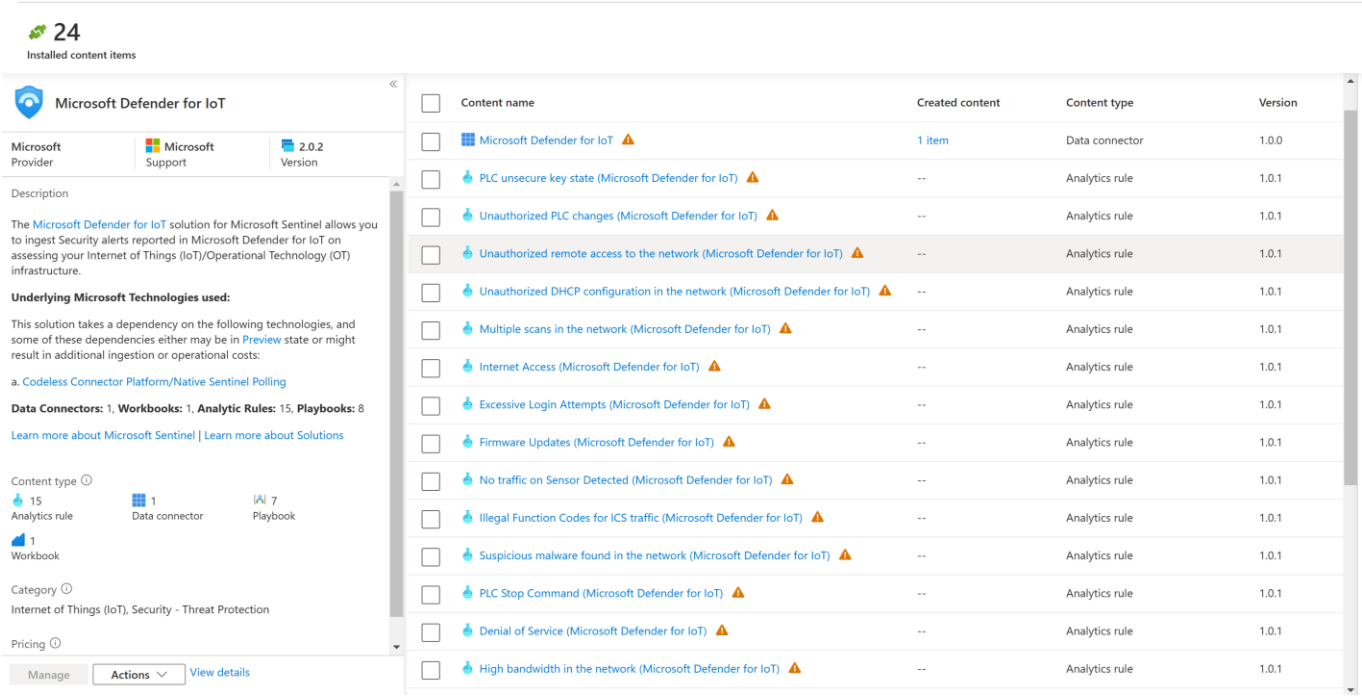


5.Go to “Data Connectors” and verify that the Defender for IoT Connector is connected.



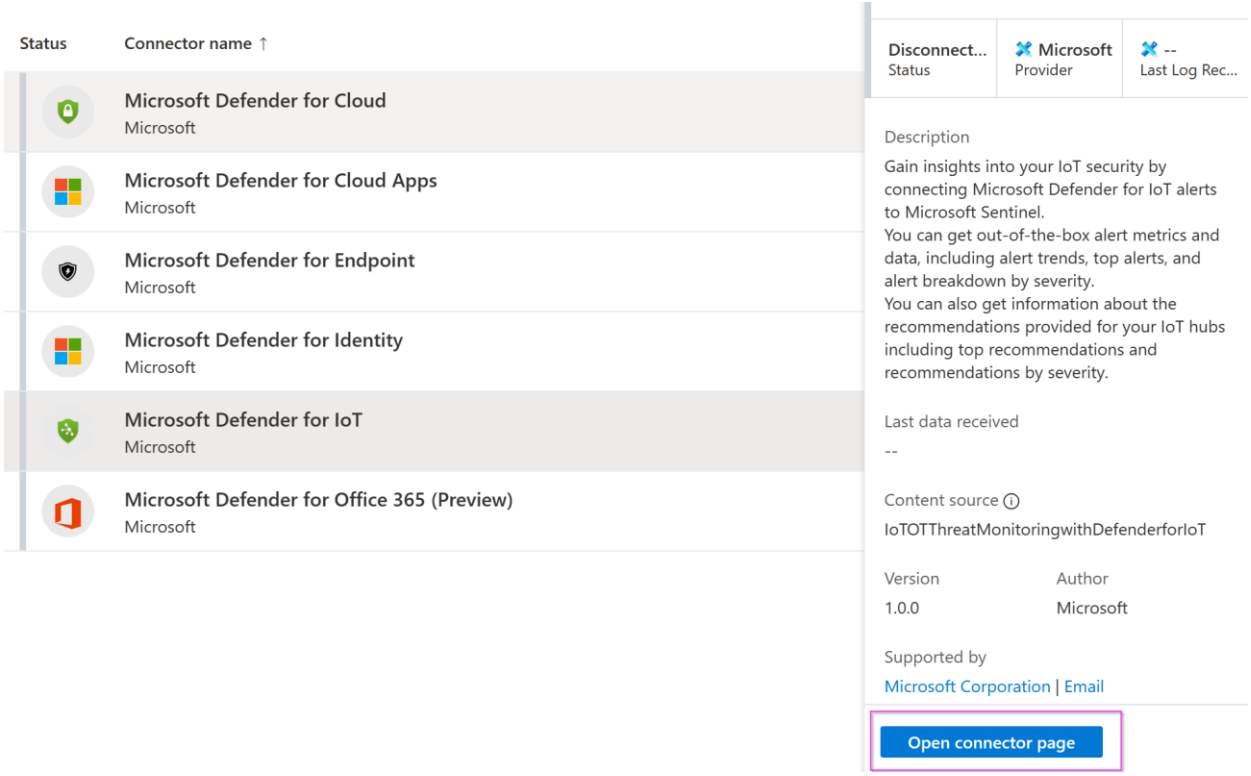
6.Go to the package and click on “Manage” to see a list of resources installed as a part of the package.



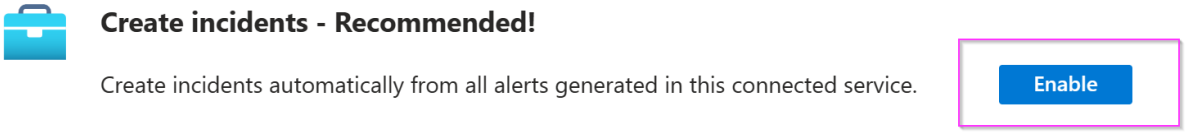


Task 3: Create Incidents

1.Go to the Defender for IoT connector and click on “Open Connector Page”.



2.Click on “Create Incidents” to automatically create alerts from the connector.



Task 4: Validate Defender for IoT logs are streamed correctly to Sentinel (KQLS on the data)

1.In Microsoft Sentinel, select Logs > AzureSecurityOfThings > SecurityAlert, or search for SecurityAlert.

2.Use the following sample queries to filter the logs and view alerts generated by Defender for IoT:

To see all alerts generated by Defender for IoT:

SecurityAlert | where ProductName == "Azure Security Center for IoT"

To see specific sensor alerts generated by Defender for IoT:

SecurityAlert

| where ProductName == "Azure Security Center for IoT"

| where tostring(parse_json(ExtendedProperties).SensorId) == “<sensor_name>”

To see specific OT engine alerts generated by Defender for IoT:

```
SecurityAlert
| where ProductName == "Azure Security Center for IoT"
| where ProductComponentName == "MALWARE"

SecurityAlert
| where ProductName == "Azure Security Center for IoT"
| where ProductComponentName == "ANOMALY"

SecurityAlert
| where ProductName == "Azure Security Center for IoT"
| where ProductComponentName == "PROTOCOL_VIOLATION"

SecurityAlert
| where ProductName == "Azure Security Center for IoT"
| where ProductComponentName == "POLICY_VIOLATION"

SecurityAlert
| where ProductName == "Azure Security Center for IoT"
| where ProductComponentName == "OPERATIONAL"
```

To see high severity alerts generated by Defender for IoT:

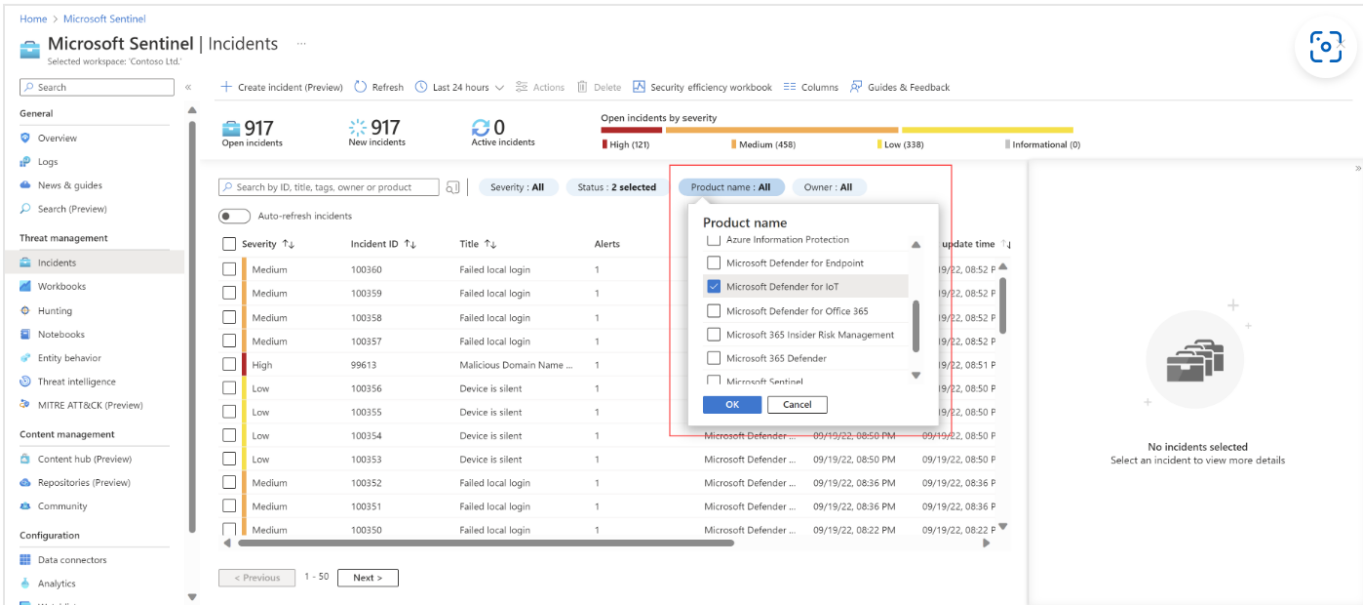
```
SecurityAlert
| where ProductName == "Azure Security Center for IoT"
| where AlertSeverity == "High"
```

To see specific protocol alerts generated by Defender for IoT:

```
SecurityAlert
| where ProductName == "Azure Security Center for IoT"
| where tostring(parse_json(ExtendedProperties).Protocol) == "<protocol_name>"
```

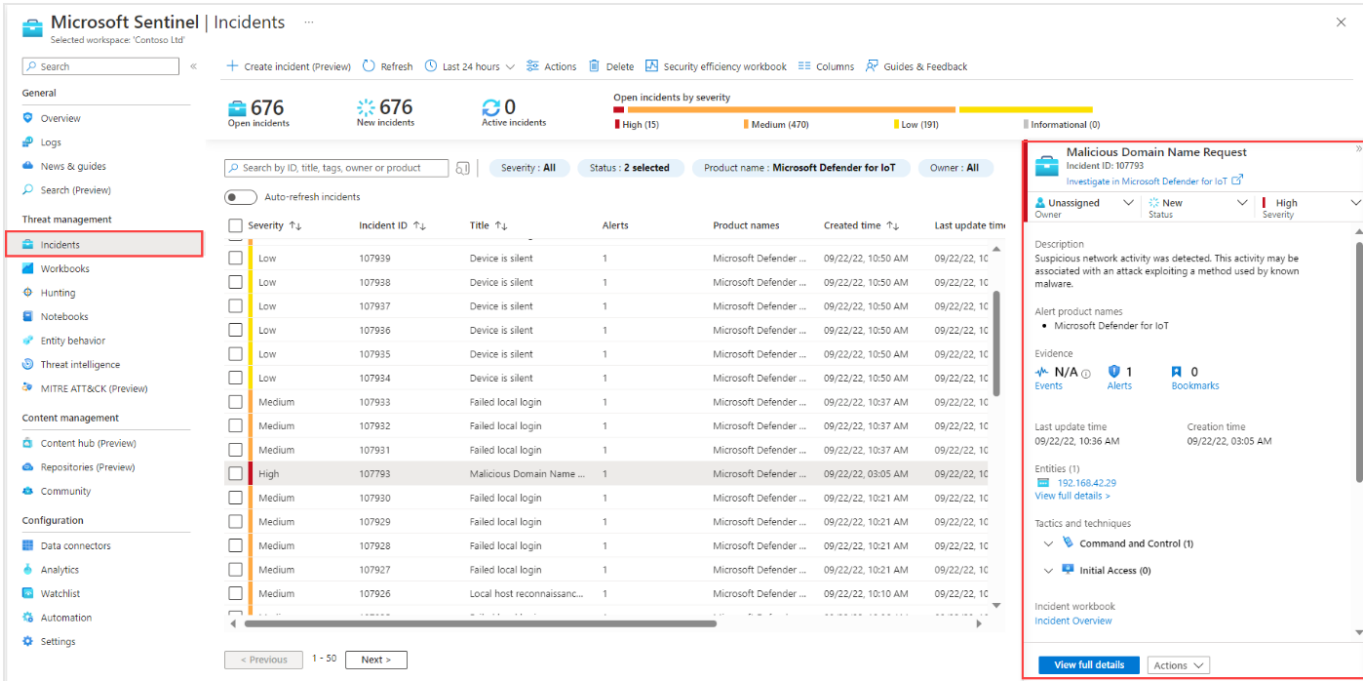
Task 5: Investigate Defender for IoT incidents

1. In Microsoft Sentinel, go to the **Incidents** page.
2. Above the incident grid, select the **Product name** filter and clear the **Select all** option. Then, select **Microsoft Defender for IoT** to view only incidents triggered by Defender for IoT alerts. For example:



3. Select a specific incident to begin your investigation.

   In the incident details pane on the right, view details such as incident severity, a summary of the entities involved, any mapped MITRE ATT&CK tactics or techniques, and more.

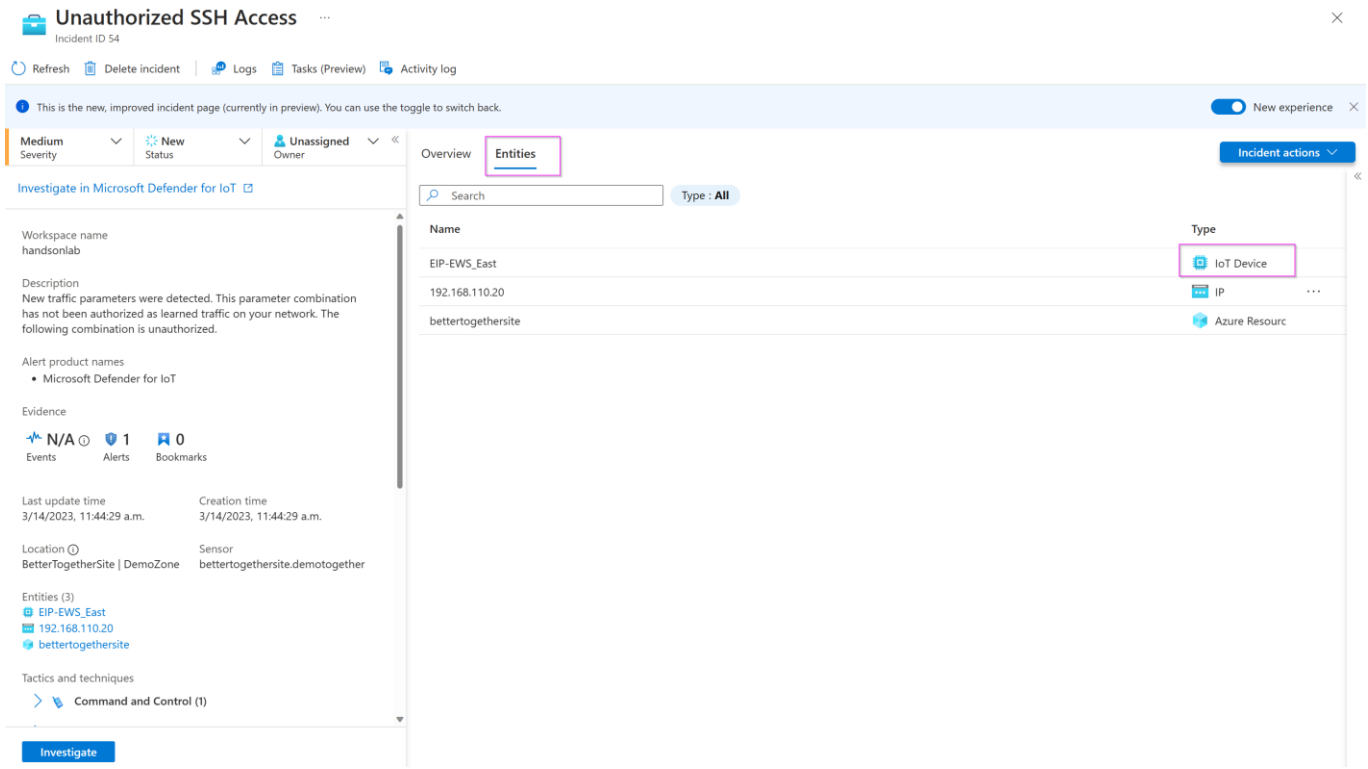


Task 6: Investigate further with IoT device entities

The IoT device entity page provides contextual device information, with basic device details and device owner contact information. The device entity page can help prioritize remediation based on device importance and business impact, as per each alert's site, zone, and sensor.

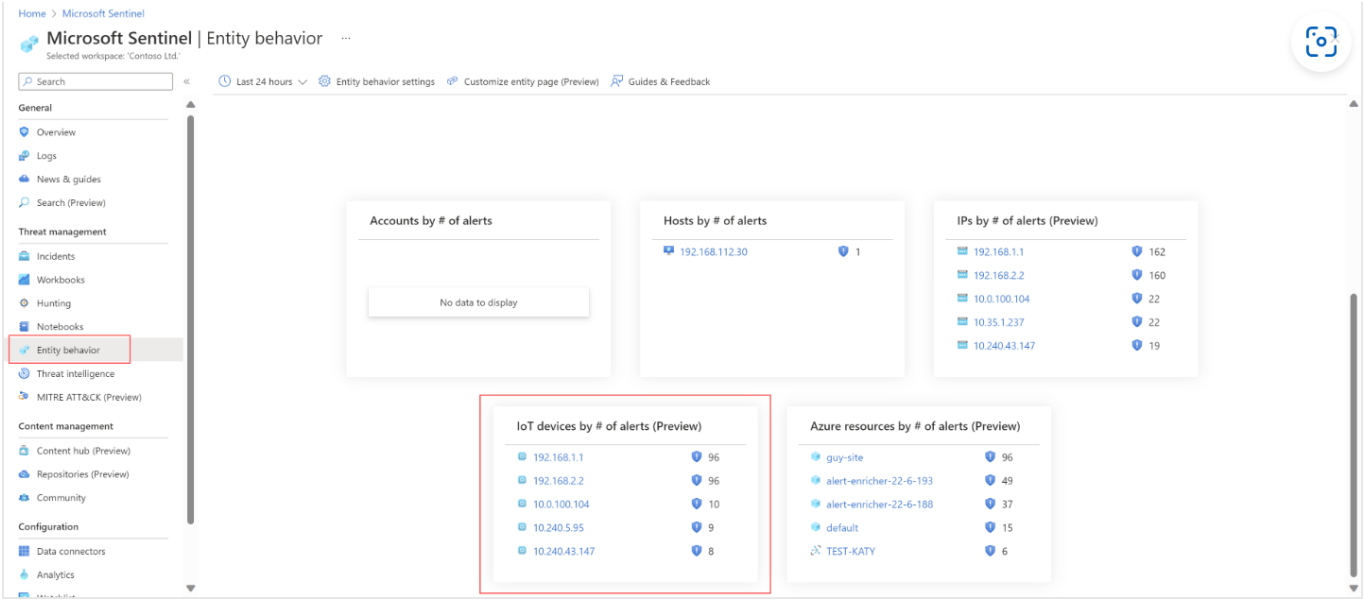
1. When you are at the incident details page, click on “Entities”.

2.Find the IoT identity categorized by this device icon:



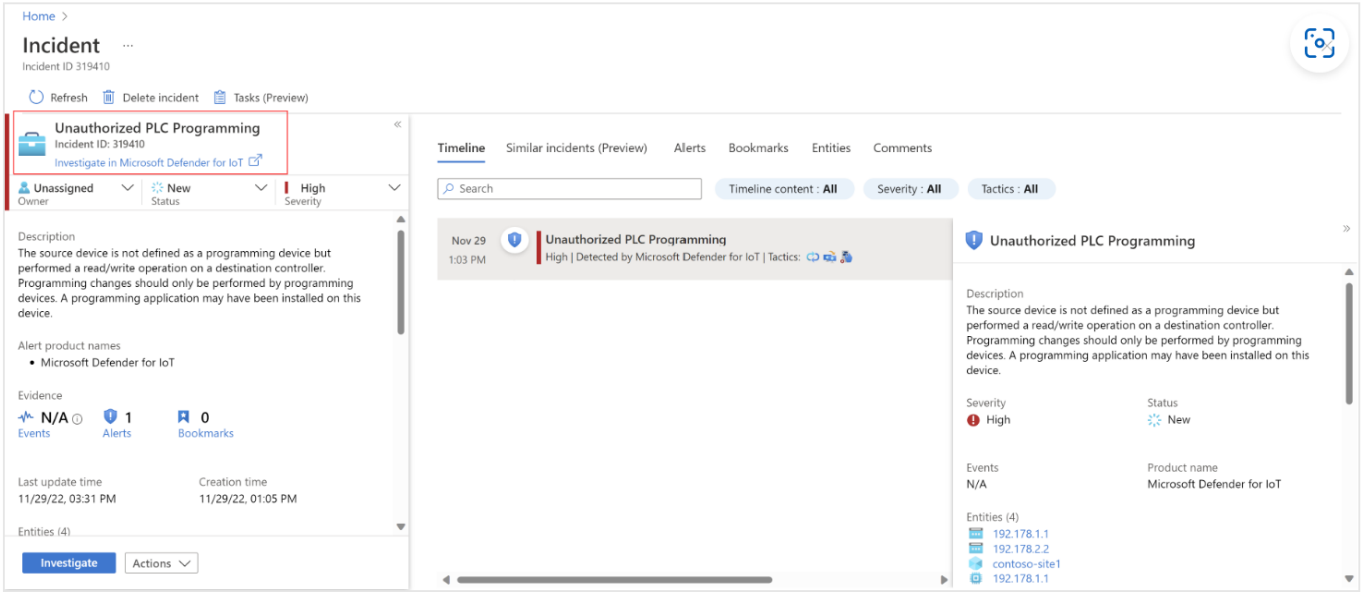
3.To drill down even further, select the IoT device entity link and open the device entity details page.

4. Alternatively, you can hunt for vulnerable devices on the Microsoft Sentinel Entity behavior page. For example, view the top five IoT devices with the highest number of alerts, or search for a device by IP address or device name:



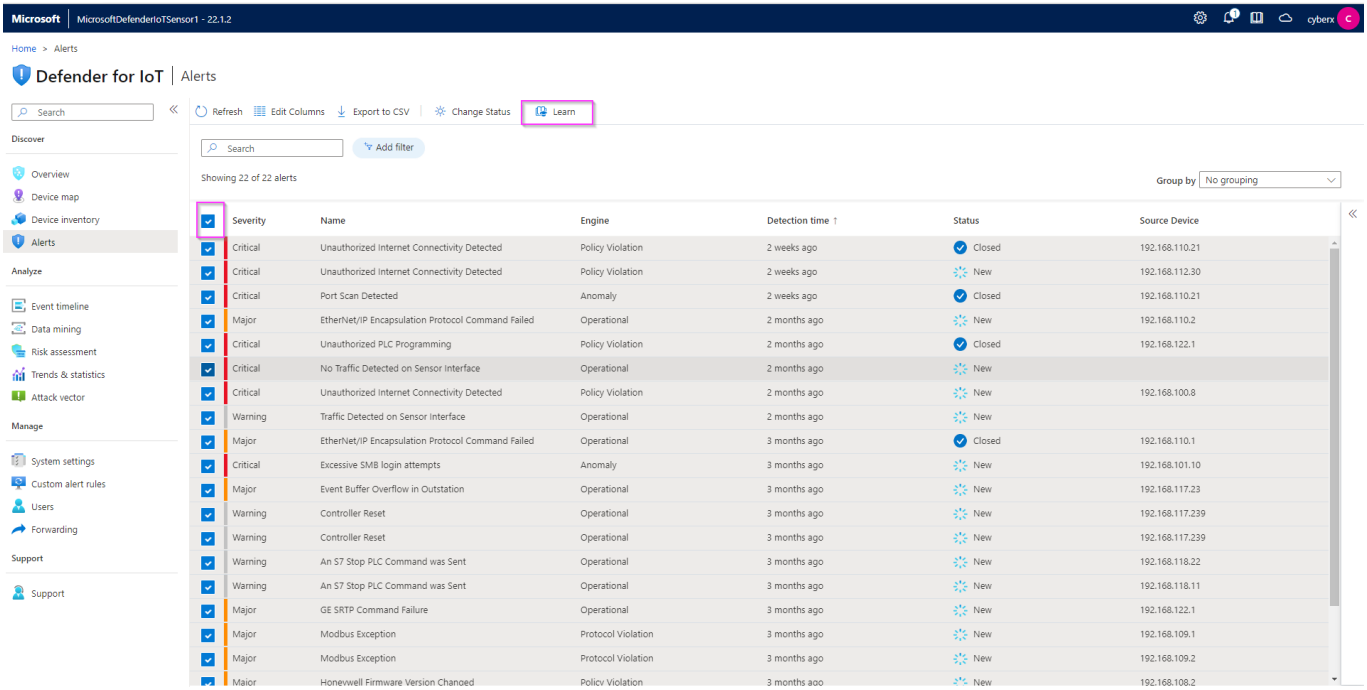
Task 7: Investigate the alert in Defender for IoT

1. Go to your incident details page and view the alerts listed under “Timeline”.

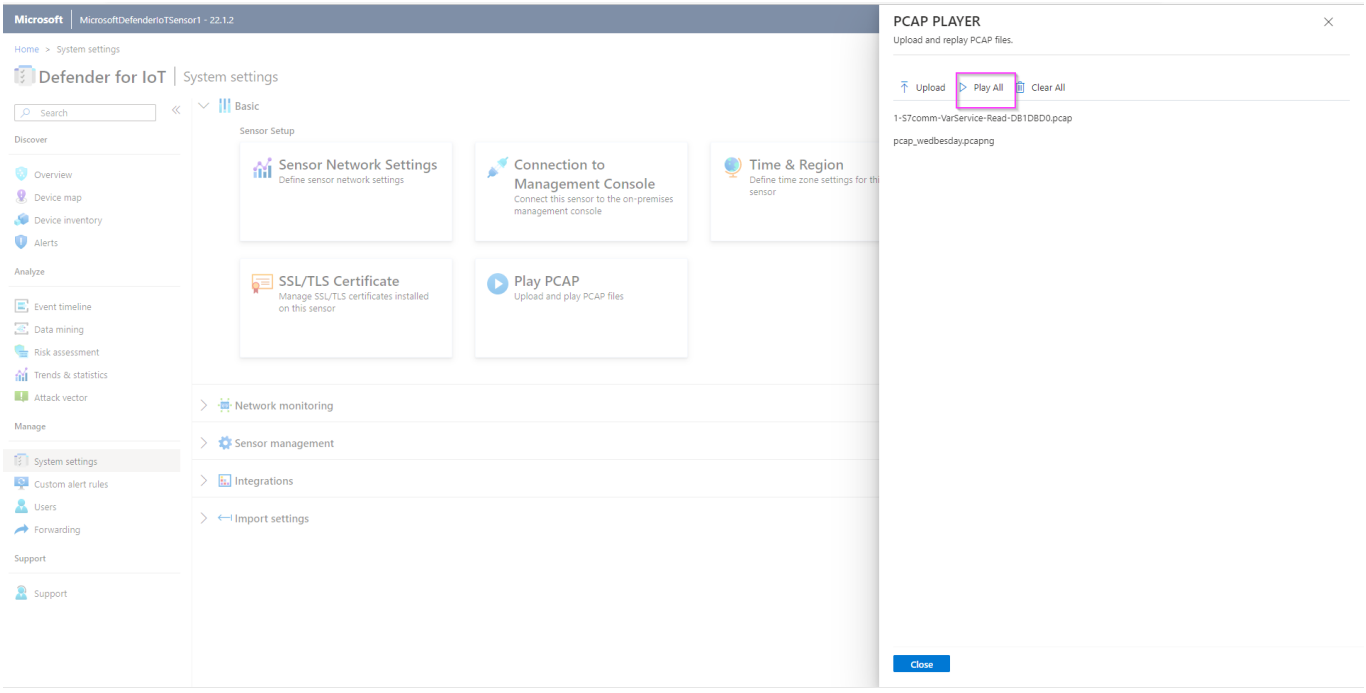


Task 8: Acknowledge Alerts and Re-run PCAPs

1. Go back to your sensor console, select all the alerts, and click on **"Learn".** The reason we are doing this is that we can re-run the alerts to show how they are sent and analyzed by Sentinel.



2. From the System Settings tab, Click the "Play All" on the PCAP Files to replay simulating the alerts.



Exercise 8: Automate response to Defender for IoT alerts.

Playbooks are collections of automated remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually or set to run automatically in response to specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.

Before using the out-of-the-box playbooks, make sure you perform the following prerequisites, as needed for each playbook:

- Ensure valid playbook connections
- Add a required role to your subscription
- Connect your incidents, relevant analytics rules, and the playbook

For a full list of DIoT Playbooks, refer to this document.

Exercise 9: Clean Up

Task 1: Delete resources

It is best practice to delete all your resources after the training.

Search for the Resource Group created for this training.

Select Delete resource group on the top right side.

Enter your-resource-group-name for **TYPE THE RESOURCE GROUP NAME** and select Delete. This operation will take a few minutes.

After that is done go to Microsoft Defender for IoT and deactivate the subscription.