

## 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 to write queries to help with alert investigation.

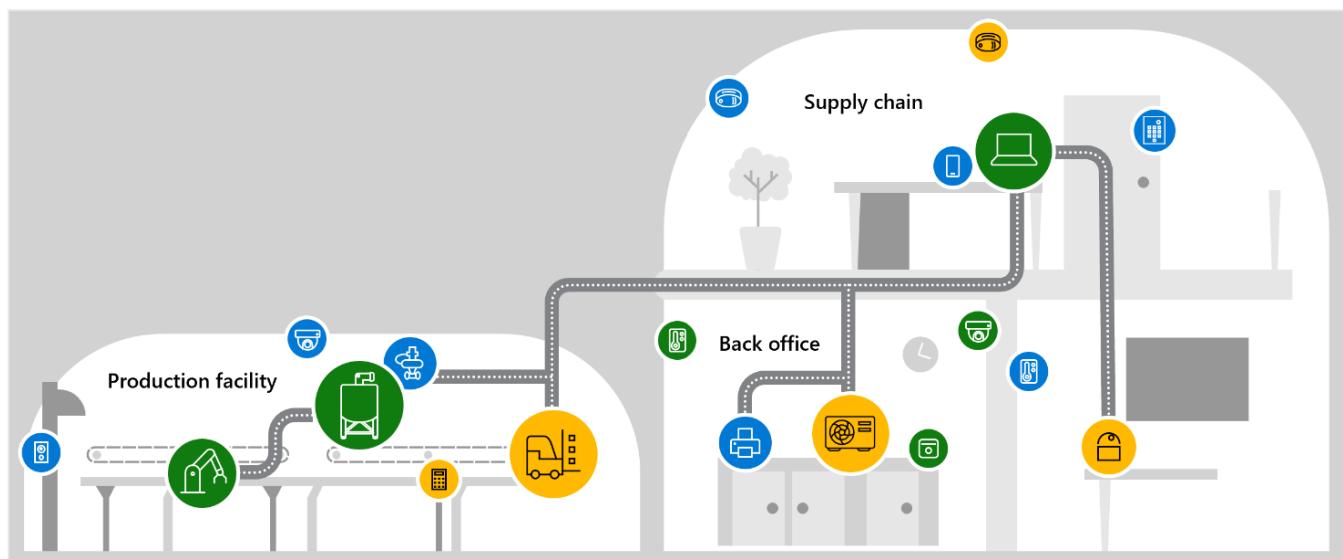
# Microsoft Defender for IoT HOL

---

!! 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 to write 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.



## What is Microsoft Defender for IoT?

Microsoft Defender for IoT is a comprehensive security solution designed to detect IoT and OT devices, vulnerabilities, and threats. This powerful tool can be used to protect your entire IoT/OT environment, including devices that do not have built-in security agents.

One of the key benefits of Defender for IoT is its agentless, network layer monitoring, which ensures that all devices in your environment are secure and protected against potential threats. Additionally, the platform integrates seamlessly with both industrial equipment and security operation center (SOC) tools, allowing you to easily manage your entire security infrastructure from a single, centralized location.

By leveraging the power of Microsoft Defender for IoT, you can rest assured that your IoT and OT devices are protected against known and emerging threats, ensuring the safety and security of your entire organization.

To learn more, watch this video:

<https://youtu.be/G555j-z5Y3I>

## Contents

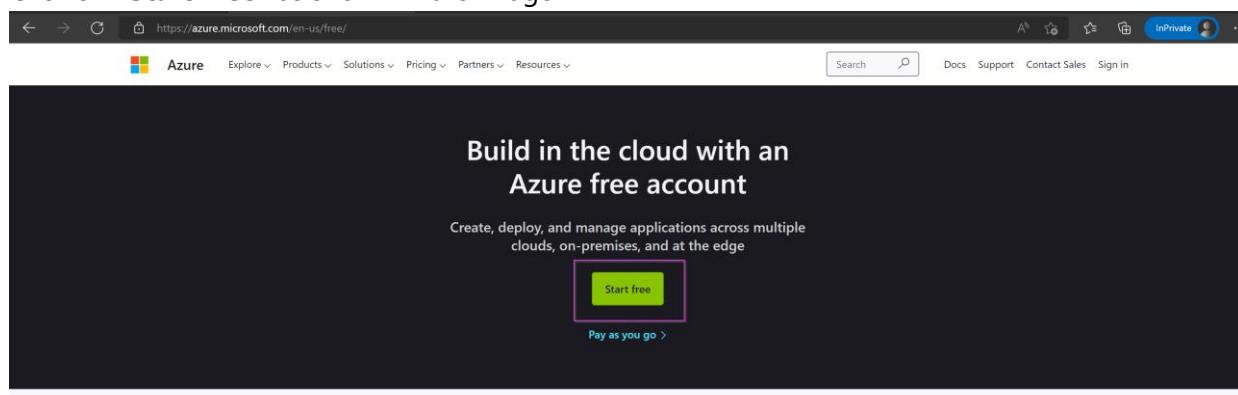
Summary.....	1
!! Since the PDF contains hyperlinks, please download the file before proceeding!!.....	1
Architecture Diagram.....	1
What is Microsoft Defender for IoT? .....	1
Exercise 1: Enabling Defender .....	3
Task 1: Create an Azure Subscription .....	3
Task 2: Enabling Microsoft Defender for IoT on the Subscription.....	4
Exercise 2: Deploy the Sensor in Azure.....	6
Task 1: Create a Resource group to automatically deploy your sensor, storage account and network security group to.....	6
Task 2: Access your Virtual Machine. ....	8
Task 3: Access your sensor via the console.....	14
Exercise 3: Perform an Upgrade .....	20
Task 1: Download the Upgrade ISO file.....	20
Task 2: Upgrade your sensor.....	20
Exercise 4: Simulate Data in your sensor.....	22
Task 1: Enabling the PCAP Player.....	22
Task 2: Play PCAP files.....	23
Exercise 5: Analyzing the Data .....	25
Task 1: Visualize on the Device Map .....	25
Task 2: View the associated Alerts .....	28
Task 3: Device Inventory .....	30
Task 4: View the Event Timeline .....	31
Task 5: Data Mining .....	31
Task 6: Generate a Risk Assessment report.....	33
Exercise 6: Cloud Connect your sensor.....	34
Task 1: Create the cloud connected sensor on the Cloud Management portal .....	34
Task 2: Upload the activation file to cloud connect your sensor. ....	34

Task 3: Verify Cloud connection.....	35
Exercise 7: Manage your sensor via the Cloud Management Portal.....	36
Task 1: Role Based Access Control on your sites and Sensors.....	36
Task 2 : Manage your devices.....	38
Task 3: View your Alerts .....	40
Task 4: View your recommendations .....	42
Task 5: Visualize Data by utilizing Workbooks .....	42
Exercise 8: Integrate with Microsoft Sentinel .....	44
Task 1: Create a Log Analytics Workspace.....	44
Task 2: Install the Defender for IoT package.....	46
Task 3: Create Incidents.....	48
Task 4: Validate Defender for IoT logs are streamed correctly to Sentinel (KQLS on the data) .....	49
Task 5: Investigate Defender for IoT incidents .....	50
Task 6: Investigate further with IoT device entities .....	52
Task 7: Investigate the alert in Defender for IoT .....	53
Task 8: Acknowledge Alerts and Re-run PCAPs.....	54
Exercise 9: Automate response to Defender for IoT alerts.....	55
Exercise 10: Clean Up.....	55
Task 1: Delete resources.....	55
Exercise 11: Submit Feedback .....	55
Appendix:.....	55

## 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-us/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.

The screenshot shows the Microsoft Azure portal interface. The search bar at the top contains the text "Subscriptions". Below the search bar, there is a navigation bar with tabs: All, Services (12), Resources (1), Marketplace (20), Resource Groups (0), and Documentation (0). The "All" tab is selected. The main content area displays a list of resources under the "Services" category. One item, "Subscriptions", is highlighted with a pink box. Other items listed include Event Hubs Clusters, Notification Hubs, Device Update for IoT Hubs, and Azure Synapse Analytics (private link hubs). Below the services section, there is a "Marketplace" section with various subscription options like Autonomous Anomaly Detection, Managed Azure Subscription, and SWIFT DR-Subscription. At the bottom of the list, there is a "See all" button. The left sidebar shows a "Recent" list of resources, and the bottom navigation bar includes links for Subscriptions, Resource groups, All resources, and Dashboard.

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

The screenshot shows the "Subscriptions" page in the Microsoft Azure portal. The title bar says "Subscriptions". There are buttons for "+ Add", "Manage Policies", and "View Requests". Below the title, there is a search bar and filter options: "Search for any field...", "Subscriptions == global filter", "My role == all", "Status == all", and "Add filter". A table lists the subscriptions. The first row, "Visual Studio Enterprise Subscription", is highlighted with a red box. The table columns are: Subscription name, Subscription ID, My role, Current cost, Secure Score, Parent management group, Status, and more. The status for the highlighted subscription is "Active".

## 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.

Microsoft Defender for IoT

All Services (27) Documentation (99+) Azure Active Directory (1) Resources (0) Resource Groups (0)

Marketplace (0)

Services

**Microsoft Defender for IoT**

IoT Hub  
Microsoft Sentinel  
Form recognizers  
Power Platform

See all

Recent resources

Name

- mdfilesmst01
- rg-md4iot-mst01
- vm-md4iot-host
- AIA-Personal-MST01
- firmwaremst
- iot-s1-mst02
- rg-iothubs
- rg-storage
- rg-vms
- rg-eflow-sample-mst01
- rg-cog-services

Documentation

- Microsoft Defender for IoT documentation | Microsoft Docs
- Defender for IoT installation - Azure Defender for IoT ...
- Integrate Microsoft Sentinel and Microsoft Defender for IoT ...
- Manage your IoT devices with the ... - docs.microsoft.com
- Integrate Palo Alto with Microsoft Defender for IoT ...
- Manage subscriptions - Azure Defender for IoT | Microsoft Docs
- Microsoft Defender for IoT trial setup - Azure Defender ...
- What is agentless solution architecture - Azure Defender ...

Azure Active Directory

Microsoft Defender for IoT Micro agent Public Preview  
mst4iot-micro-agent-public@service.microsoft.com

Group

Searching 1 of 34 subscriptions. Change

Give feedback

Resource group      3 weeks ago

Resource group      3 weeks ago

Resource group      3 weeks ago

[https://ms.portal.azure.com/#blade/Microsoft\\_Azure\\_Security/SecurityMenuBlade/Overview](https://ms.portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/Overview)

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

Home > Defender for IoT

Defender for IoT | Pricing

Showing subscription 'Visual Studio Enterprise Subscription'

Search (Ctrl+ /) Refresh Add plan Download on-premises management console activation file

General

Getting started  
Device inventory (Preview)  
Alerts (Preview)  
Workbooks (Preview)

Management

Sites and sensors  
**Pricing** (selected)  
Settings (Preview)

No subscriptions onboarded

Define committed device coverage or work with the trial.

Onboard subscription

For more information on Microsoft Defender for IoT pricing, visit the [Pricing page](#).

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

Home > Defender for IoT

Defender for IoT | Pricing

Showing subscription 'Visual Studio Enterprise Subscription'

Search (Ctrl+ /) Refresh **+ Add plan** Download on-premises management console activation file

General

Getting started  
Device inventory (Preview)  
Alerts (Preview)  
Workbooks (Preview)

Management

Sites and sensors  
**Pricing** (selected)  
Settings (Preview)

No subscriptions onboarded

Define committed device coverage or work with the trial.

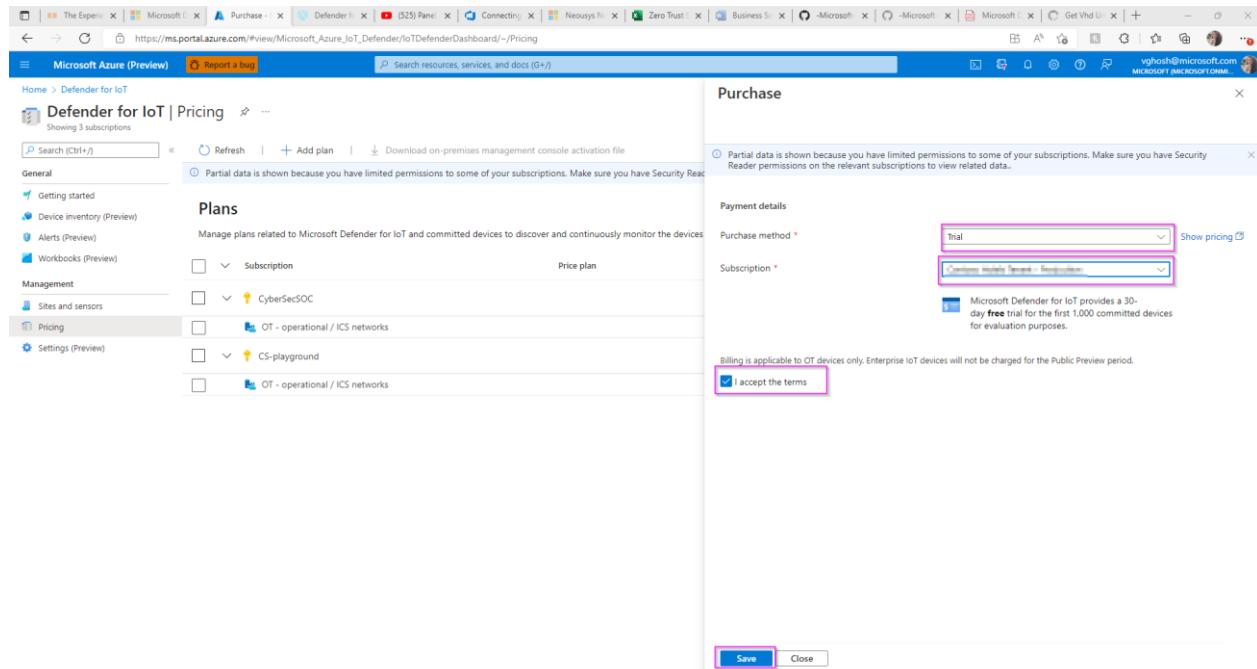
Onboard subscription

For more information on Microsoft Defender for IoT pricing, visit the [Pricing page](#).

4. In the popup screen, select:

- Purchase Method: Trail**

- b. **Subscription:** pick the trial subscription you created
- c. Click “I accept the terms”, followed by “Save”.



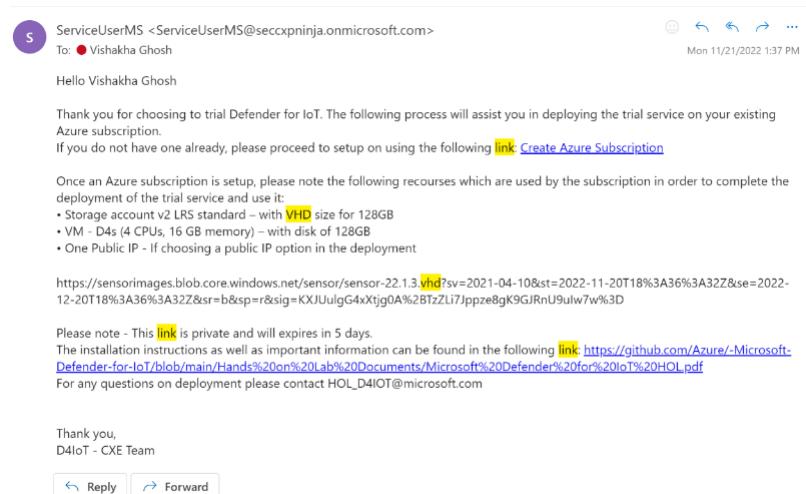
You now have a valid Microsoft Defender for IoT Trial with **1000 committed devices**. These devices represent all those equipment/sensors connected to your network in the facility you are analyzing. This configuration allows you a **30-day trial for free**.

## 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 via [this form](#) for a link for the IoT sensor installation. You will receive an email with the link once your request has been received.

It might go to your Junk/Spam by default. Please search for an email from [ServiceUserMS@secxpnninja.onmicrosoft.com](mailto:ServiceUserMS@secxpnninja.onmicrosoft.com). It should look like this.



**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:

The screenshot shows the 'Custom deployment' page in the Azure portal. The 'Basics' tab is active. At the top, there's a 'Template' section with a 'Customized template' card showing 4 resources. Below that is the 'Project details' section with fields for 'Subscription' (set to 'BuildEnv'), 'Resource group' (with a 'Create new' button), 'Region' (set to 'East US'), 'Location' (set to '[resourceGroup().location]'), 'Deploy Public IP' (set to 'true'), 'Put Password To Key Vault' (set to 'true'), 'Source VHDURL \*' (empty), and 'Sensor Count' (set to '1'). Step numbers 1 through 7 are overlaid on the corresponding fields.

- 1) Please select your **Subscription** linked 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.

**Custom deployment**

Deploy from a custom template

Validation Passed

Basics Review + create

Summary

Customized template 3 resources

Terms

Azure Marketplace Terms | Azure Marketplace

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Create < Previous Next >

## Task 2: Access your Virtual Machine.

### Option #1: If you deployed with Keyvault

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

Microsoft.Template-20220713114358 | Overview

Your deployment is complete

Deployment name: Microsoft.Template-20220713114358 Start time: 7/13/2022, 11:44:03 AM

Subscription: Bullshin Correlation ID: #0166659-4ef4-4268-b168-5c8887ada95e

Resource group: KeyVaultTest

Deployment details (Download)

Resource	Type	Status	Operation details
Reset-password0	Microsoft.Resources/deployments	OK	Operation details
Post-Deploy0	Microsoft.Resources/deployments	OK	Operation details
VMDeployment	Microsoft.Resources/deployments	OK	Operation details
copyhd	Microsoft.Resources/deployments	OK	Operation details

Next steps

Go to resource group

- Go to the keyvault resource from the list.

KeyVaultTest

Subscription (move): BuildEnv Deployments: 2 Failed 10 Succeeded

Location: West US

Tags (edit): createdate: 07/13/2022 owner: vghosh

Resources Recommendations

Name	Type	Location
customxx245p7rgp0	Storage account	West US
SOC_Kv245p7rgp2_Pay	Key vault	West US
SOC_NS0d245p7rgp2_Pay	Network security group	West US
SOC_minsteny245p7rgp2_Pay	Managed identity	West US
SOC_mra245p7rgp2_Pay-image	Image	West US
SOC_vmr245p7rgp2_Pay-red10	Regular Network Interface	West US
SOC_wmz245p7rgp2_Pay-pg0	Public IP Address	West US
SOC_wmz245p7rgp2_Pay-pg0	Virtual machine	West US
SOC_wmz245p7rgp2_Pay-disk1	Disk	West US
SOC_vnres245p7rgp2_Pay	Virtual network	West US

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

**(If you have deployed multiple sensors and subsequently have multiple keys, you can use the instructions given in the appendix to export the keys instead of copying them 1 by 1).**

4. Under "Permissions" select "Key & Secret Management" template.

5. Under "Principle" select a principle

Home > Resource groups > KeyVaultTest > SOC-KVuq63gjmwvo2do-Play | Access policies >

## Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

Permissions     Principal     Application (optional)     Review + create

Only 1 principal can be assigned per access policy.

Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Search by object ID, name, or email address

- [John Doe](#)
- [Administrators](#)
- [Jane Smith](#)
- [Power users](#)
- [Alice Johnson](#)
- [Developers](#)

### Selected item

No item selected

## 6. You can skip over "Application".

Home > Resource groups > KeyVaultTest > SOC-KVuq63gjmwvo2do-Play | Access policies >

## Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

Permissions     Principal     Application (optional)     Review + create

Authorizes this application to perform the specified permissions on the User's or Group's behalf.  
Use the new embedded experience to select an application. The previous popup experience can be accessed here. [Select an application](#)

Search by object ID, name, or email address

- 5d62bf487ee14fb8884e9582f29be8e1-977f-4fa3-bf83-957308750ff
- AcmeDnsValidator-ting0113im0604fb01b-9fe8-4926-b954-b922680cbf40
- aksdemoSP-20200512091755b59a0f98-632d-403b-987c-68a88ccf81c0
- amasf7056827c-0953-418c-9426-f6890b2f9e79
- aml-94dec3a3-89b7-402c-a6a6-3db32f3b2d40b179caab-f3fc-4162-a465-ea5e6f54087
- aml-9f876ca0-654b-468b-8d6b-abf6aa26fce90b34bd9-e88b-46f0-adf8-c7ce00a9954

### Selected item

No item selected

Previous

Next

## 7. Click on "Create".

Home > Resource groups > KeyVaultTest > SOC-KVuq63gjmwvo2do-Play | Access policies >

### Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

Permissions     Principal     Application (optional)

**Review + create**

#### Key Permissions

Key Management Operations	All selected
Cryptographic Operations	None selected
Privileged Key Operations	None selected
Rotation Policy Operations	All selected

#### Secret Permissions

Secret Management Operations	All selected
Privileged Secret Operations	None selected

#### Certificate Permissions

Certificate Management Operations	None selected
Privileged Certificate Operations	None selected

#### Principal

Principal name	Vishakha Ghosh
Object ID	4d53f3b7-e555-4354-a330-193b4cd1ef28

#### Application

Authorized application (SAM)	None selected
Object ID	None selected

**Create**

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

Home > Microsoft.Template\_20200713114358 > KeyVaultTest

**KeyVaultTest** Resource group

Search (Ctrl+F) + Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export template Open in mobile

Overview Activity log Access control (IAM) Logs Resource visualizer Events

Deployments Security Policies Properties Locks Cost Management Cost analysis Cost alerts (preview) Budgets Advisor recommendations Monitoring

Essentials Deployment ID : 1c61ccbf-70b1-45a3-a1fb-84fc446d70a6 Tags (edit) createdate : 07/13/2022 owner : vghosh

Deployments : 2 Failed 10 Succeeded Location : West US

Resources Recommendations

Filter for any field... Type equals all Location equals all Add filter

Type	Location	...
Storage account	West US	...
Key vault	West US	...
Network security group	West US	...
Managed identity	West US	...
Image	West US	...
Regular Network Interface	West US	...
Public IP address	West US	...
<b>Virtual machine</b>	West US	...
Disk	West US	...

## 9. Make a note of the Public IP address.

**SOC** Virtual machine

**-Play**

**Essentials**

Resource group (move) : **SOC**  
 Status : Running  
 Location : East US  
 Subscription (move) :  
 Subscription ID :  
 Tags (edit) : azsecpack : nonprod

Operating system : Linux (ubuntu 18.04)  
 Size : Standard D4s v3 (4 vcpus, 16 GiB memory)  
 Public IP address : **20.124.23.178**  
 Virtual network/subnet : **SOC** Play/default  
 DNS name : **Not configured**

**Properties** Monitoring Capabilities (7) Recommendations Tutorials

**Virtual machine**

Computer name	Sensor
Health state	-
Operating system	Linux (ubuntu 18.04)
Publisher	-
Offer	-
Plan	-

**Networking**

Public IP address	<b>20.124.23.178</b>
Public IP address (IPv6)	-
Private IP address	<b>10.10.10.4</b>
Private IP address (IPv6)	-
Virtual network/subnet	<b>SOC</b> default
DNS name	<b>Configure</b>

## Option #2: If you deployed without Keyvault.

- Once the deployment is complete, go to "Reset-password0" by clicking the button.

**Home > Microsoft.Template-20220630145822 | Overview**

**Deployment**

**Your deployment is complete**

Deployment name: Microsoft.Template-20220630145822 Start time: 6/30/2022, 2:58:25 PM  
 Subscription: BuildEnv Correlation ID: ac55ba5c-e35a-4a36-b3ee-37b01fcdb3f

**Deployment details (Download)**

Resource	Type	Status	Operation details
<b>Reset-password0</b>	Microsoft.Resources/deployments	OK	Operation details
Post-Deploy0	Microsoft.Resources/deployments	OK	Operation details
VMdeployment	Microsoft.Resources/deployments	OK	Operation details
copyhd	Microsoft.Resources/deployments	OK	Operation details

**Next steps**

**Go to resource group**

- Copy the system generated random password from the "Password" field and make a note of the VMName.

**Home > Microsoft.Template-20220630145822 > Reset-password0**

**Deployment**

**Reset-password0 | Outputs**

**vmObject**

```
[{"VMName": "SOC-vmw7ne3eaow5oxw0-Play", "Password": "KChR9dMLp3VFkar2Yp8I99PM2V8="}]
```

Copied

**Outputs**

- Click "go to resource group" from the previous screen.

Your deployment is complete

Deployment name: Microsoft.Template-20220630145822  
Subscription: BuildEnv  
Resource group: Vghosh\_IoTSensor

Resource	Type	Status	Operation details
Reset-password	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
Post-Deploy0	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
VMdeployment	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
copyvhdl	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>

Next steps

[Go to resource group](#)

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

Microsoft Azure (Preview)

Home > Microsoft.Template 20220503175515 >

Resource group

Overview

Essentials

Resources

Name	Type	Location
copyvhdl	Deployment Script	East US
customflicwiéuSatkww	Storage account	East US
SOC NSGflicwiéuSatkww Play	Network security group	East US
<b>SOC-vmflicwiéuSatkww-Play</b>	Virtual machine	East US

#### 5. Make a note of the Public IP address.

The screenshot shows the Azure portal interface for a virtual machine named 'SOC'. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Networking, Connect, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, and Continuous delivery. The main pane displays the 'Essentials' and 'Properties' tabs for the virtual machine. Under 'Essentials', the Public IP address is highlighted as 20.124.23.178. Under 'Properties', the Networking section highlights both the Public IP address (20.124.23.178) and the Private IP address (10.10.10.4).

### 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.

The screenshot shows a web browser window with the URL <https://xxx.xxx.xxx.xxx /login>. The page title is "Microsoft | Defender for IoT sensor". The main content is a "Sensor Sign in" form with fields for "User name" and "Password". Below the fields are links for "Forgot password? (for admin users only)" and "Reset". A "Login" button is at the bottom right. The browser status bar indicates "Not secure".

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".

Step 3: Register this sensor with Microsoft Defender for IoT

Sensor name \*

Subscription \*

Cloud connected ⓘ

Automatic Threat Intelligence updates

Sensor version \*

Site \*

Resource name \*

No subscription has been selected  
Create site

Display name \*

Tags

Key	Value
+Add tag	

Zone \*

No subscription has been selected  
Create zone

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**".

Defender for IoT | Sites and sensors

Showing subscription 'BuildEnv'

General

Management

Sites and sensors (highlighted with a pink box)

Pricing

Sensor name	Sensor type	Zone	Subscription ...	Sensor version	Sensor status	Last connect...	Threat Intelli...	Threat Intelli...	Threat...
D4IOTsensor-TT	EIoT	default	BuildEnv	22.1.3.4162	Unavailable	--	--	--	...
sensor-Cyber	OT cloud co...	default	BuildEnv		Disconnected	A week ago	5/25/2022	Automatic	...

Push Threat Intelligence update (highlighted with a pink box)

Recover my password (highlighted with a pink box)

Download activation file

Delete sensor

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

Defender for IoT | Sites and sensors

Showing subscription 'BuildEnv'

General

Management

Sites and sensors (highlighted with a pink box)

Pricing

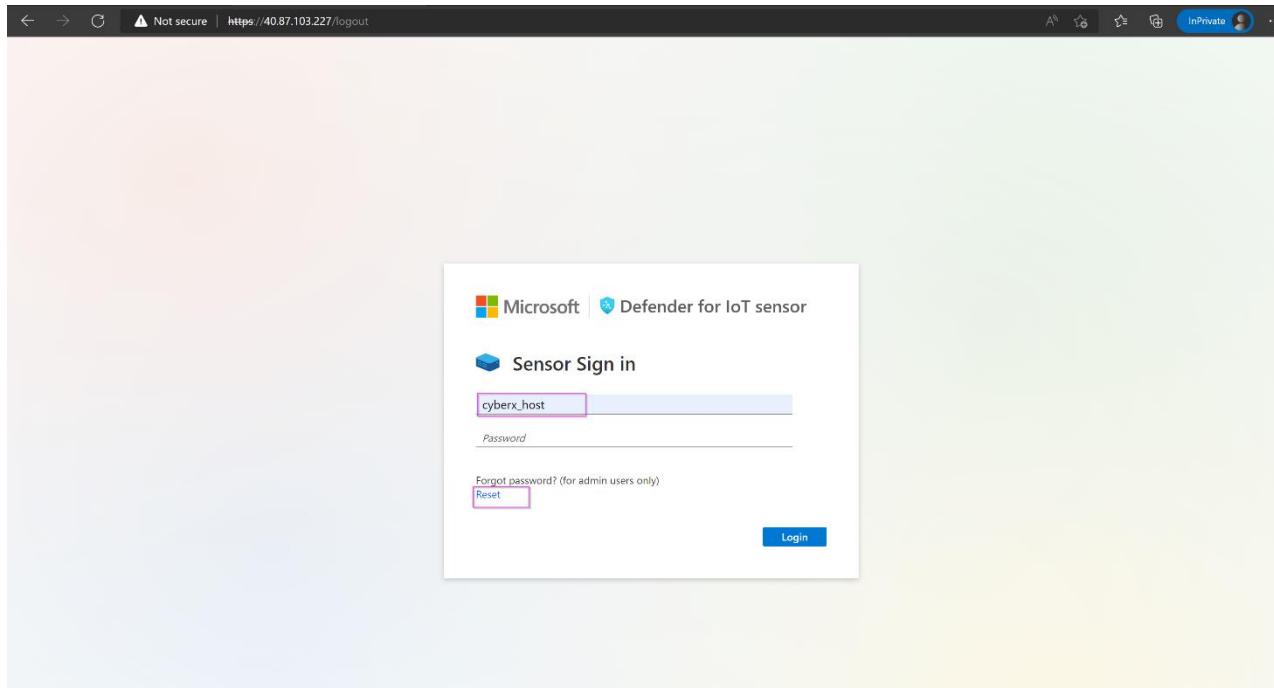
Recover

Insert secret identifier \*

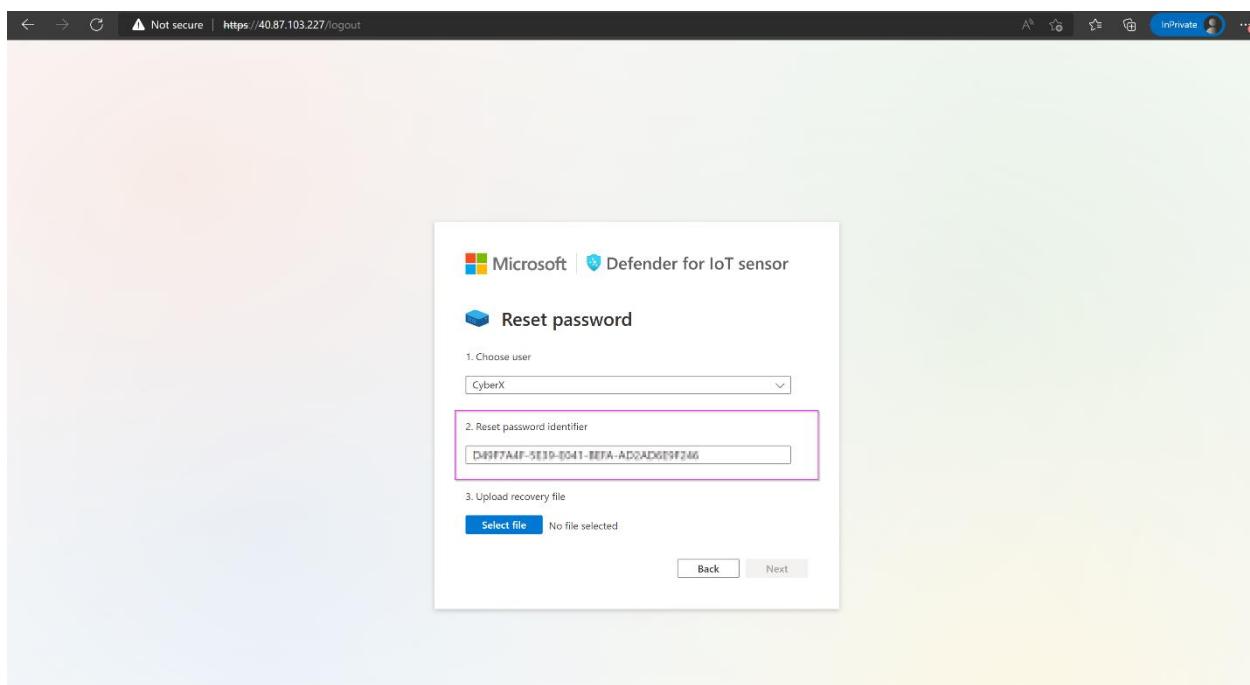
Sub0001-777-0e57-88h12

Recover Cancel

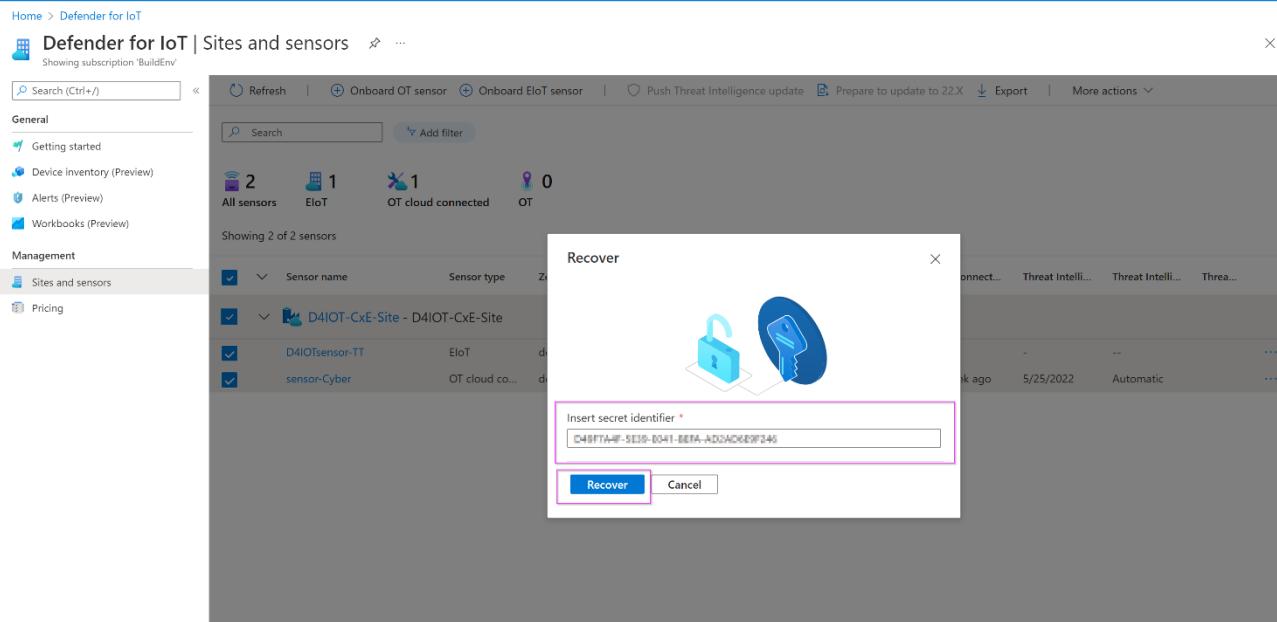
7. Return to the sensor console and type in the username followed by "Reset" as shown.



8. Copy the identifier.

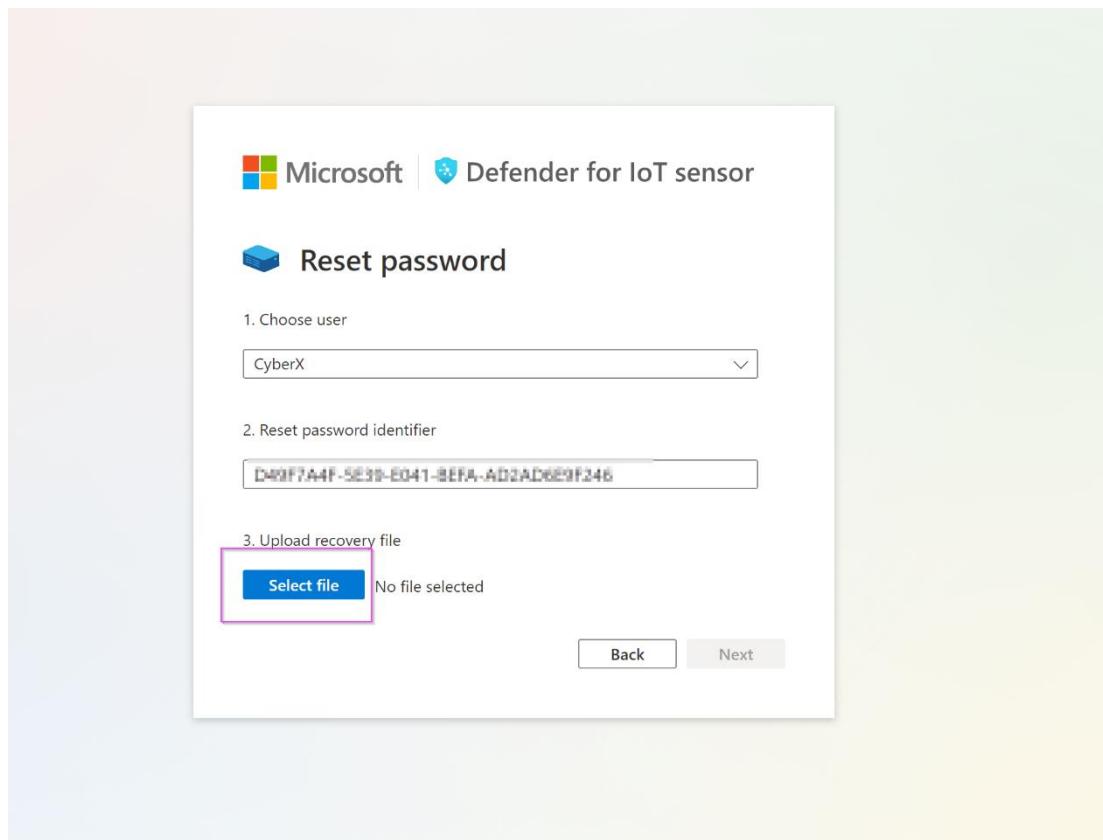


9. Paste in the box on the Defender for IoT Azure window. Click "**Recover**".



The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with 'General' and 'Management' sections. Under 'Management', 'Sites and sensors' is selected. The main area displays sensor statistics: 2 All sensors, 1 EIoT, 1 OT cloud connected, and 0 OT. Below this, it says 'Showing 2 of 2 sensors' and lists two entries: 'D4IOT-CxE-Site - D4IOT-CxE-Site' and 'D4IOTsensor-TT'. A modal window titled 'Recover' is open, prompting for a 'secret identifier' which is a GUID: 'D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246'. It has 'Recover' and 'Cancel' buttons.

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**.



The screenshot shows the 'Reset password' wizard. Step 1: Choose user is set to 'CyberX'. Step 2: Reset password identifier is a GUID: 'D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246'. Step 3: Upload recovery file has a 'Select file' button and a message 'No file selected'. At the bottom are 'Back' and 'Next' buttons.

11. Click on “**Next**”.

The screenshot shows the 'Reset password' process in Microsoft Defender for IoT sensor. Step 3, 'Upload recovery file', is highlighted with a pink box around the 'Select file' button and the uploaded file name 'password\_recovery (1).zip'. The 'Next' button is also highlighted with a pink box.

Microsoft | Defender for IoT sensor

## Reset password

1. Choose user  
CyberX\_host
2. Reset password identifier  
D9F7A4F-5E19-0411-BFA-AD2AD619F246
3. Upload recovery file  
Select file password\_recovery (1).zip

Back Next

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

The screenshot shows the 'Reset password' process in Microsoft Defender for IoT sensor. Step 4 displays the temporary password 'j^>h@WTU\*7IP\_3H' in a highlighted input field. The 'Next' button is highlighted with a pink box.

Microsoft | Defender for IoT sensor

## Reset password

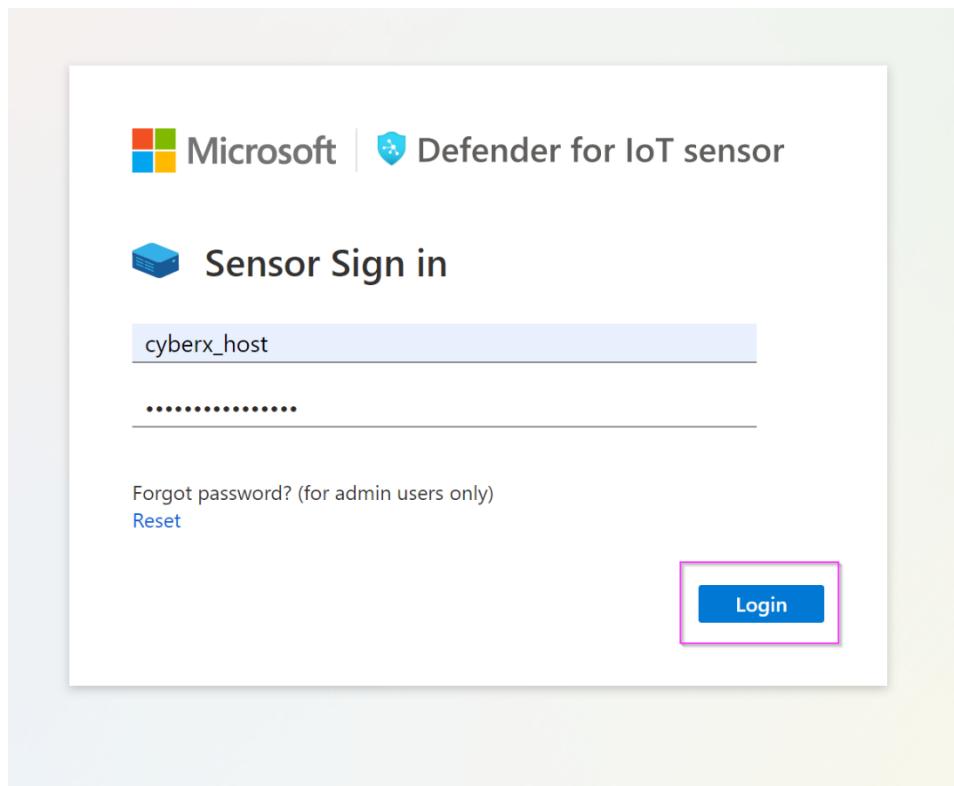
User name  
CyberX\_host

Password  
j^>h@WTU\*7IP\_3H

Please write your password, it will not be shown again

Next

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.

Home >

**Defender for IoT | Getting started** Showing 3 subscriptions

Search Get started Windows IoT Enterprise (Preview) **Sensor** On-premises management console Updates

General

- Getting started**
- Device inventory (Preview)
- Alerts (Preview)
- Recommendations (Preview)
- Workbooks

Management

- Sites and sensors
- Plans and pricing
- Settings (Preview)

Troubleshooting + Support

- Diagnose and solve problems

Version 22.2.9 supports a new cloud connectivity model that requires sensor reactivation when updating from 10.5.X. [Learn more](#)

Use the information here to help you purchase hardware and install software.

**Buy preconfigured appliance**

Buy a preconfigured appliance from Arrow. The appliance will be delivered to your facility. Contact Arrow directly by mail to purchase the appliance.

[Identify required appliances](#) [Install software](#) [Set up your network](#)

**Contact vendor to get a price quote**

[Contact](#)

**Purchase an appliance and install software**

The solution runs on certified physical and virtual appliances. Acquire an appliance and download the ISO image to install the sensor.

[Identify required appliances](#) [Install software](#) [Set up your network](#)

**Select version**

22.2.9 (Latest) - recommended

MDS Hash - 5a2dbb762791112af562b643d980920f

[Download](#)

### Task 2: Upgrade your sensor

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

Home > System settings

## Defender for IoT | System settings

Discover

- Overview
- Device map
- Device inventory
- Alerts

Analyze

- Event timeline
- Data mining
- Risk assessment
- Trends & statistics
- Attack vector

Manage

- System settings**
- Custom alert rules
- Users
- Forwarding
- Support
- Support

< Network monitoring >

Sensor management

Updates

**Software Update** Update the software version on this sensor

**Threat Intelligence** Update the threat intelligence package on this sensor

Security

**Subscription & Activation Mode** Upload an activation file to reactivate this sensor

Health and troubleshooting

**Backup & Restore** Backup data and restore the latest backup

**System Health Check** Review network properties, statistics and other data related to sensor health

**SNMP MIB Monitoring** Resolve device hostnames based on IP addresses detected on subnets.

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

Home > System settings

## Defender for IoT | System settings

Discover

- Overview
- Device map
- Device inventory
- Alerts

Analyze

- Event timeline
- Data mining
- Risk assessment
- Trends & statistics
- Attack vector

Manage

- System settings**
- Custom alert rules
- Users
- Forwarding
- Support
- Support

< Network monitoring >

Sensor management

Updates

**Software Update** Update the software version on this sensor

**Threat Intelligence** Update the threat intelligence package on this sensor

Security

**Subscription & Activation Mode** Upload an activation file to reactivate this sensor

Health and troubleshooting

**Backup & Restore** Backup data and restore the latest backup

**System Health Check** Review network properties, statistics and other data related to sensor health

**SNMP MIB Monitoring** Resolve device hostnames based on IP addresses detected on subnets.

3. Verify the version on the dashboard.

Microsoft | VishalVishal - 22.2.8

Home >

## Defender for IoT | Overview

Discover

- Overview
- Device map
- Device inventory
- Alerts

0 PPS

124 Devices

32 Alerts

General Settings

Version: 22.2.8.20-r-3bd7f37

## Exercise 4: Simulate Data in your sensor.

### Task 1: Enabling the PCAP Player

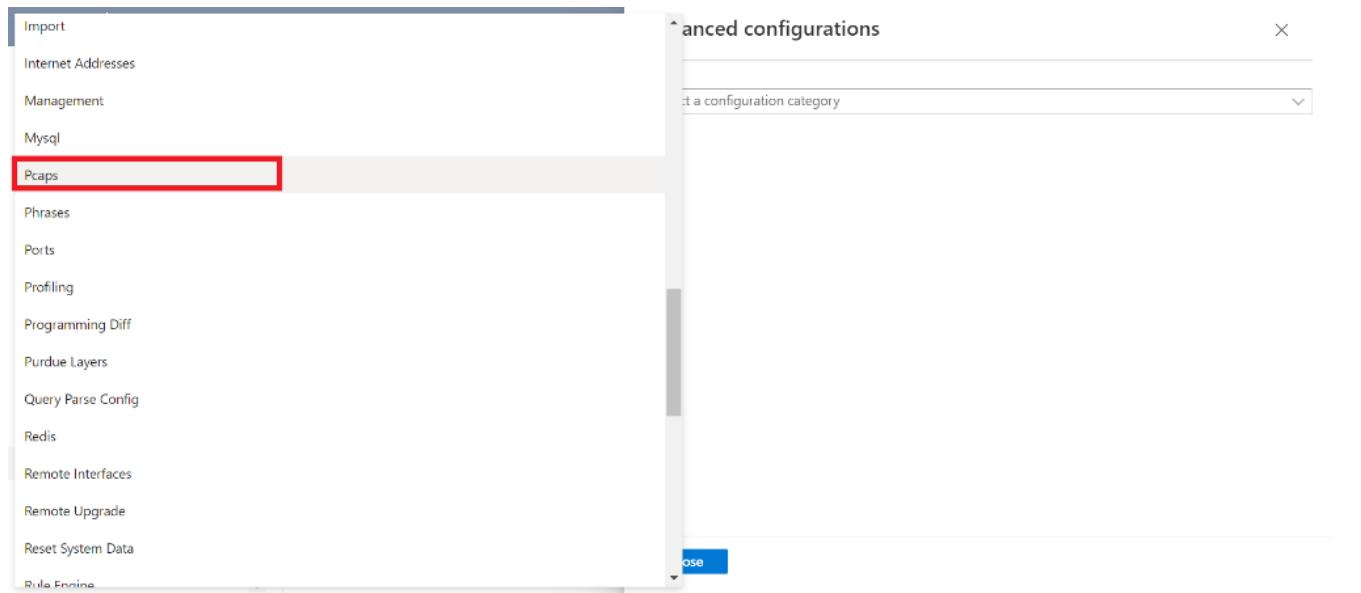
1. The PCAP player needs to be enabled to be visibly available for use in the UI. To do so, please select the "**System settings**" option from the scrolled down left side menu.

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar has a 'Manage' section with 'System settings' highlighted by a red box. The main area is titled 'System settings' and contains four cards under 'Sensor Setup': 'Sensor Network Settings', 'Connection to Management Console', 'Time & Region', and 'Subnets'.

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

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar has a 'Manage' section with 'System settings' highlighted by a red box. The main area is titled 'System settings' and contains four cards under 'Health and troubleshooting': 'Backup & Restore', 'System Health Check', 'SNMP MIB Monitoring', and 'Advanced Configurations'. The 'Advanced Configurations' card is highlighted with a red box.

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.

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar includes sections like Home, System settings, Defender for IoT (selected), Analyze, Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector, Manage, System settings (selected), Custom alert rules, Users, and Forwarding. The main area shows 'Backup data and restore the latest backup' and 'SNMP MIB Monitoring'. A 'System settings' dialog box is open, titled 'Advanced configurations' with 'Pcaps' selected. The configuration pane contains code-like settings: cache.should.save.pcap=1, archive.cache.dir=, # 7 GB, filtered.cache.dir.size.megabytes.max=7168, # 3 GB, filtered.cache.dir.size.megabytes.min=3072, filtered.archive.dir.size.megabytes.max=, filtered.archive.dir.size.megabytes.min=, filtered.archive.dir=, player.max\_size=1000, player.max\_amount=20, player.params=, enabled\_0, virtual.lan.hierarchy.depth.support=1. A red box highlights the 'Save' button at the bottom of the configuration pane.

## 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).

Microsoft | Microsoft Defender for IoT - 22.1.3

Home > System settings

Defender for IoT | System settings

Analyze

- Event timeline
- Data mining
- Risk assessment
- Trends & statistics
- Attack vector

Manage

- System settings (highlighted)
- Custom alert rules
- Users
- Forwarding

SSL/TLS Certificate

Manage SSL/TLS certificates installed on this sensor

Play PCAP

Upload and play PCAP files

Sensor management (highlighted)

Network monitoring

Integrations

Import settings

4. Click on “Upload” and select your Pcap files from the unzipped folder.

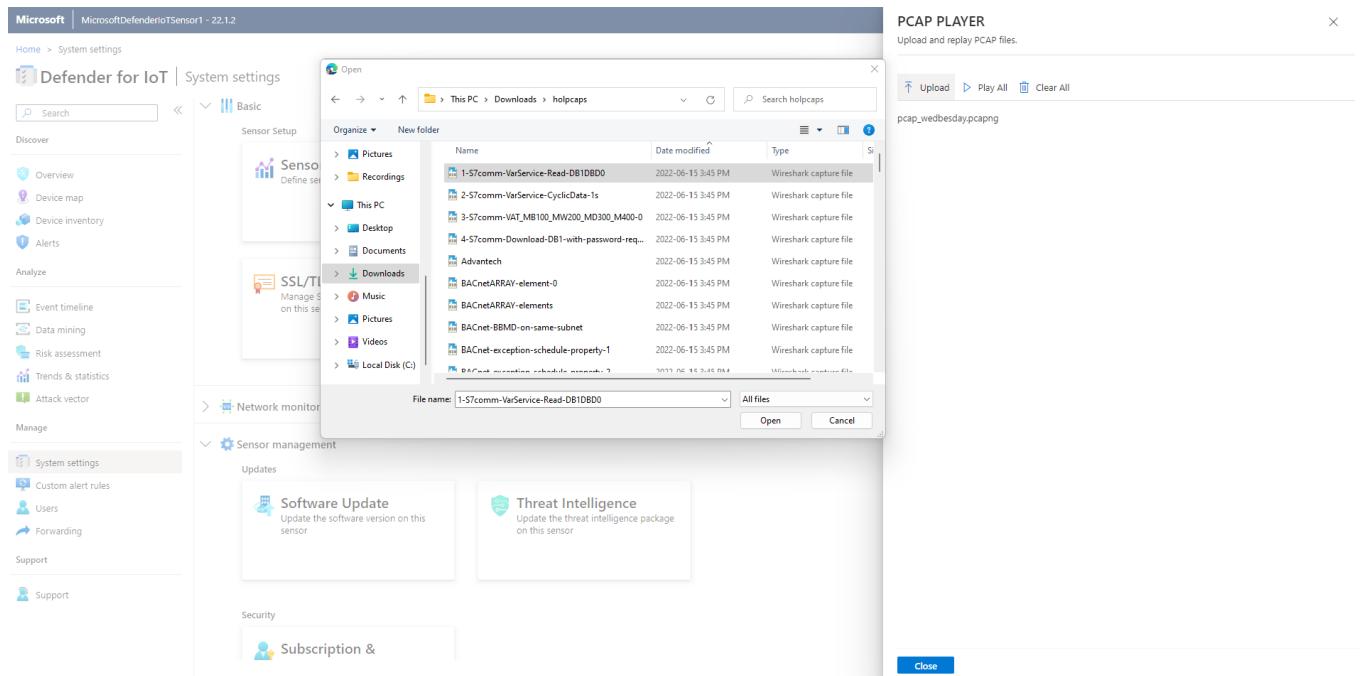
Advanced configurations

Pcaps

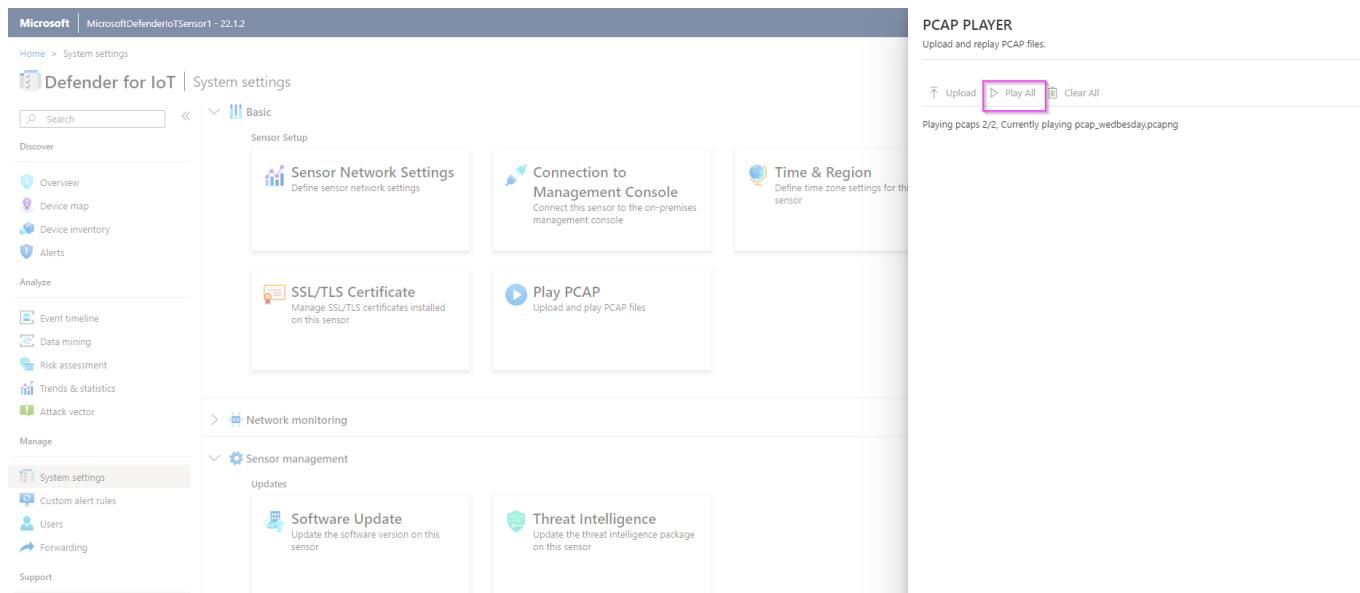
```
size.megabytes.max=44032  
archive.size.megabytes.max=  
size.megabytes.min=17408  
archive.size.megabytes.min=  
cache.should.save.pcap=1  
archive.cache.dir=  
filtered.cache.dir.size.megabytes.max=7168  
filtered.cache.dir.size.megabytes.min=3072  
filtered.archive.dir.size.megabytes.max=  
filtered.archive.dir.size.megabytes.min=  
filtered.archive.dir=  
player.max_size=10000  
player.max_amount=200  
player.params=-M 20 #runs the pcaps faster in the UI  
player.enabled=1  
virtual.lan.hierarchy.depth.support=1  
filtered.timeout.seconds=10
```

Save

Close



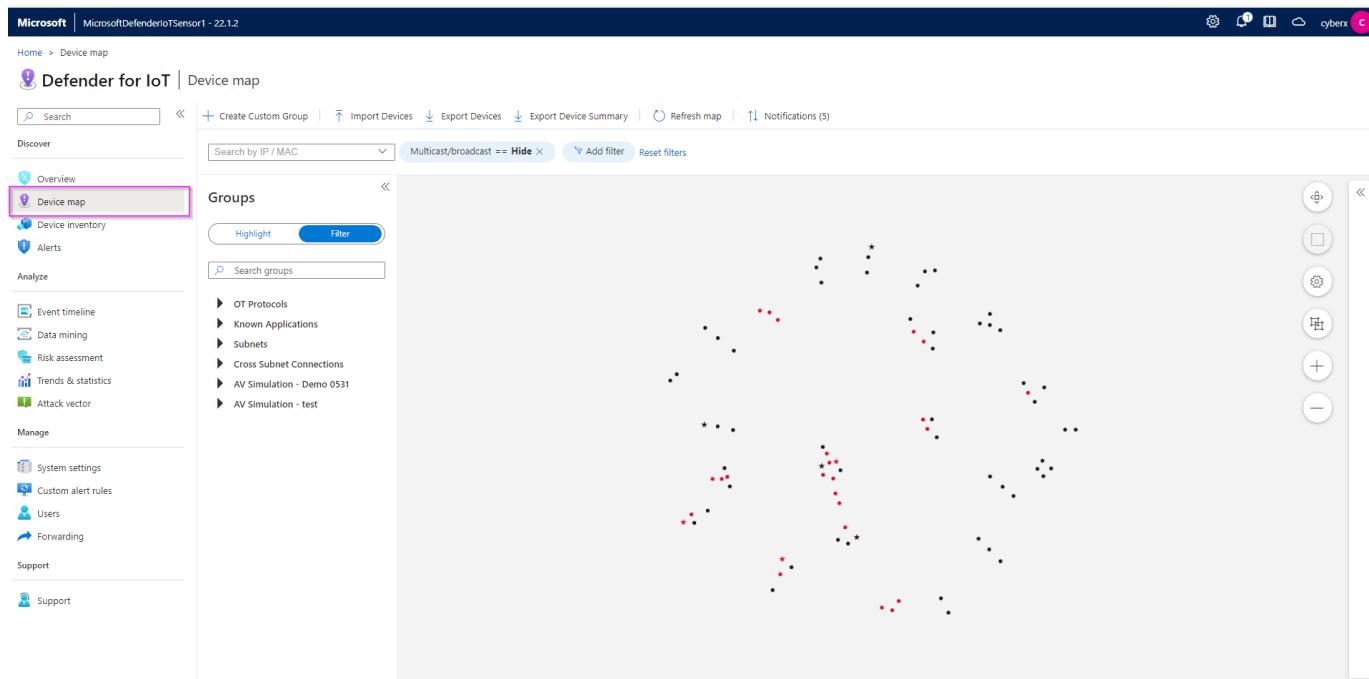
## 5. Click "Play All" to play the Pcaps.



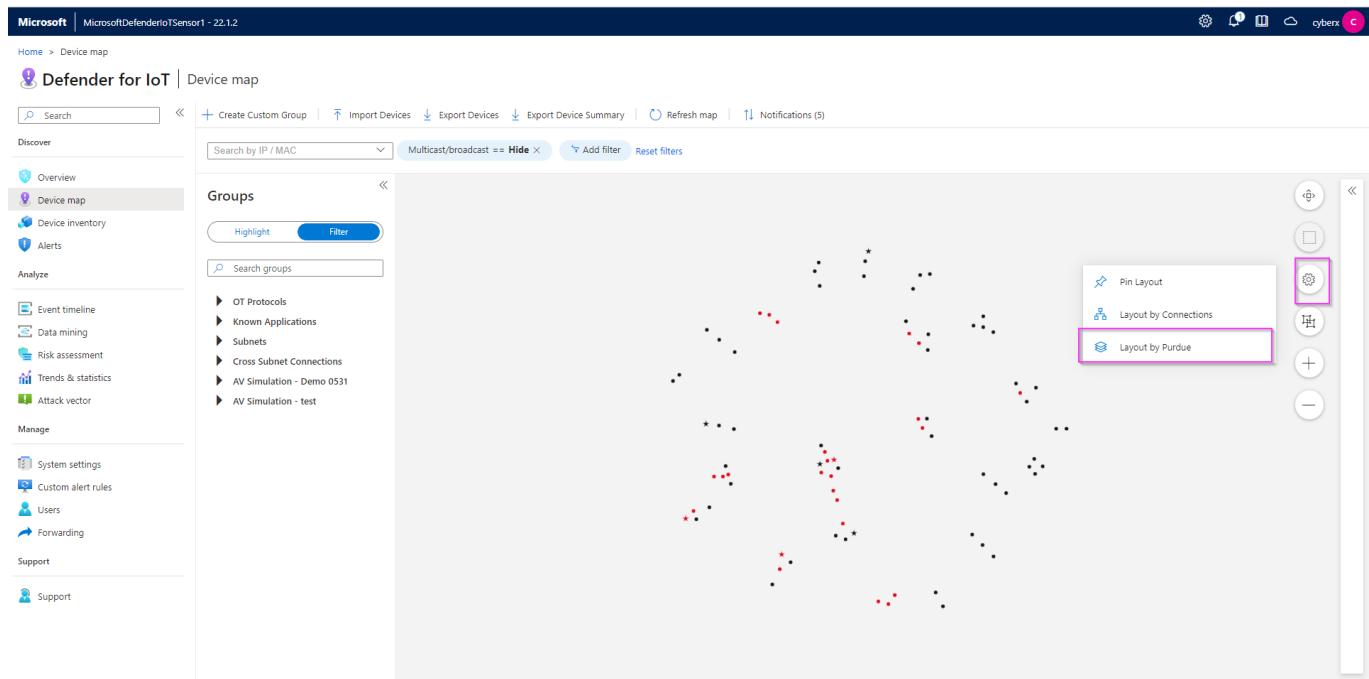
## Exercise 5: Analyzing the Data

### Task 1: Visualize on the Device Map

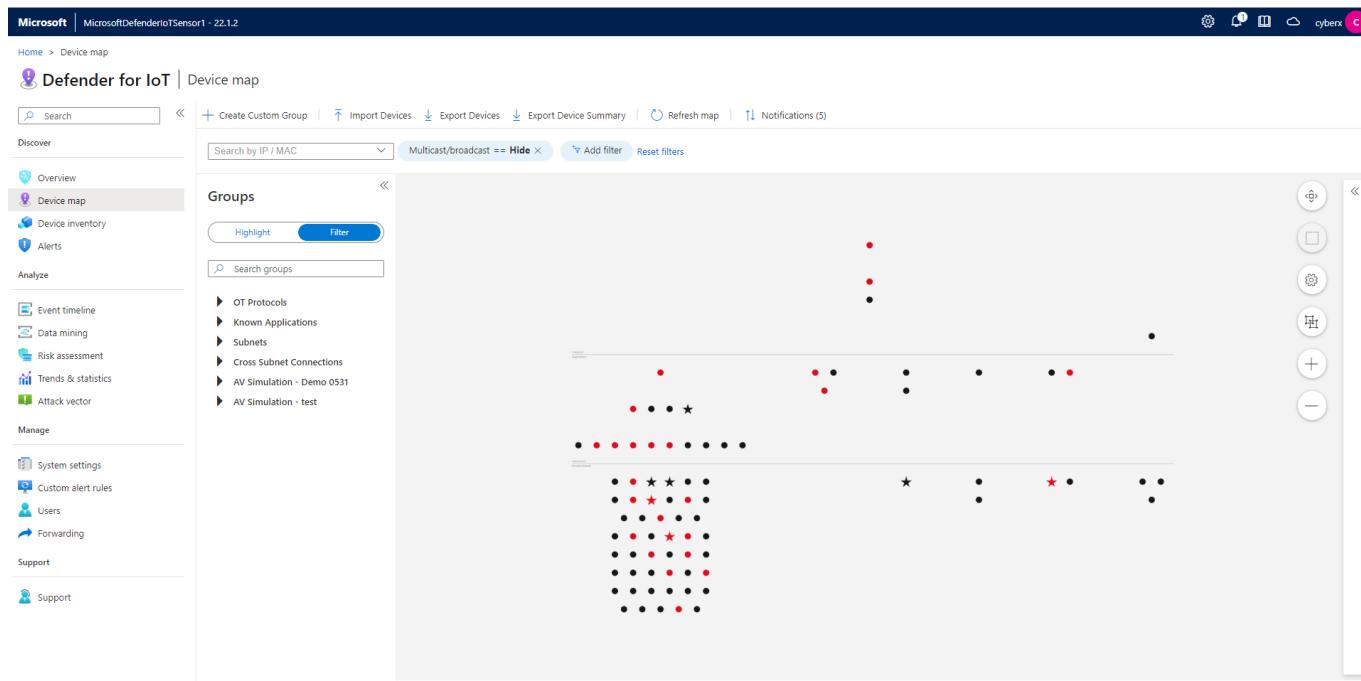
1. Click on “Device Map” from the menu on the left side.



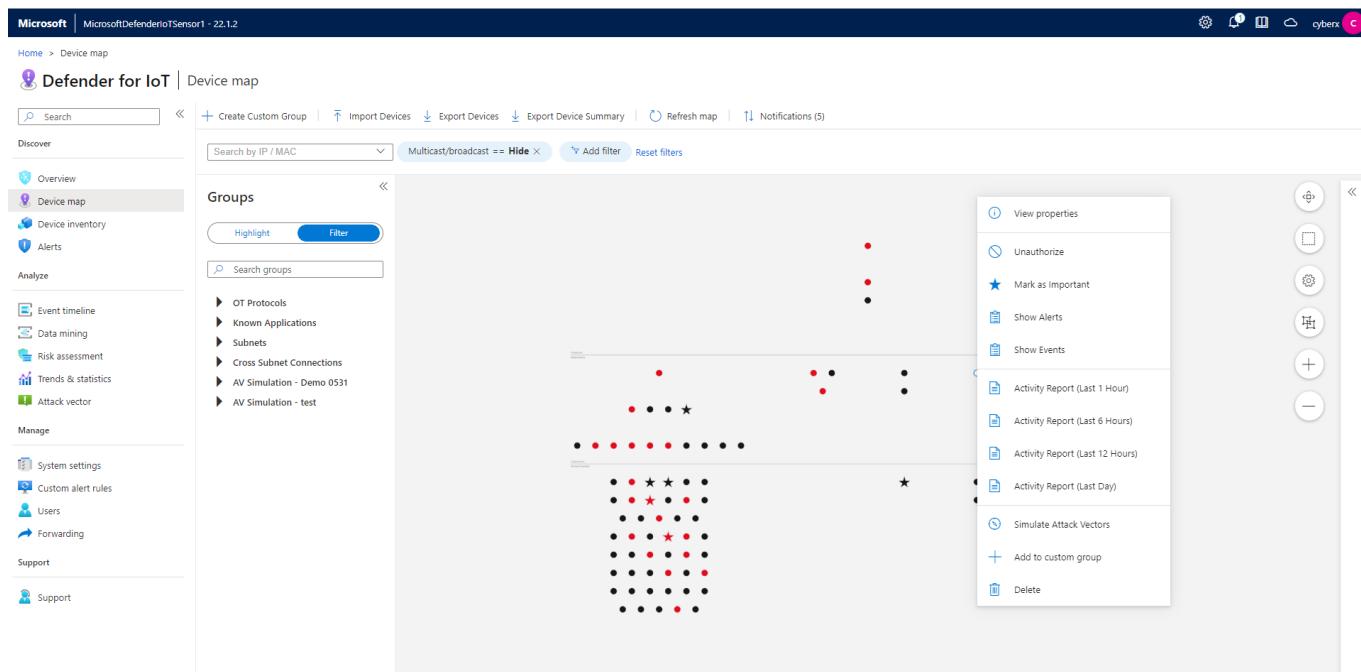
2. Click on the "Settings" option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.



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.

The screenshot shows the Microsoft Defender for IoT Device map interface. On the left, a sidebar menu includes sections for Discover, Overview, Device map (which is selected and highlighted in grey), Device inventory, Alerts, Analyze, Manage, and Support. The 'Device map' section contains a search bar, a 'Groups' dropdown with 'Highlight' and 'Filter' buttons, and a 'Search groups' input field. Below this is a list of OT Protocols: BACNet (4), BACNet (NPDU) (4), CIP (7), DNP3 (8), DeltaV (3), Emerson ROC (3), EtherNet/IP (7), Foxboro I/A (6), Honeywell FDA Diagnostics (2), MMS (4), MODBUS (3) [highlighted with a red box], Mitsubishi MELSEC (3), and Omron FINS (2). In the center, a network diagram shows three nodes connected in a line: 192.168.109.1 (with an alert icon), 192.168.109.21, and 192.168.109.2. Each node has an alert icon.

## Task 2: View the associated Alerts

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

The screenshot shows the Microsoft Defender for IoT Device map interface. The sidebar menu is identical to the previous screenshot. The 'Device map' section shows a network diagram with four nodes: 192.168.110.2, 192.168.110.1, 192.168.110.4, and 192.168.110.10. The node 192.168.110.10 has an alert icon. A context menu is open over this device, listing options: View properties, Unauthorized, Mark as Important, Show Alerts [highlighted with a red box], Show Events, Activity Report (Last 1 Hour), Activity Report (Last 6 Hours), Activity Report (Last 12 Hours), Activity Report (Last Day), Simulate Attack Vectors, Add to custom group, and Delete. The 'Show Alerts' option is specifically highlighted with a red box.

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.

This screenshot shows the Microsoft Defender for IoT Device map interface. On the left, there's a sidebar with navigation links like Home, Device map, and Alerts. The main area displays a device card for 'Device | 192.168.110.21'. The card includes sections for General Information (Type: Engineering Station, Vendor: INTEL CORPORATE, Location: Automatic), Network Interfaces (IP: 192.168.110.21, MAC: acfdce:ccbbdd), and Protocols (SSH, EtherNet/IP, TDS, FTP, CIP). Below the card is an 'Edit Properties' button. At the top right, there are tabs for Map View, Alerts (which is selected), and Event Timeline. A search bar and filter options are also present. The main content area shows a table of alerts with columns for Severity, Name, Engine, Detection time, Status, and Source Device. Two alerts are listed: 'Unauthorized Internet Connectivity Detected' (Critical, Policy Violation, 2 weeks ago, New, 192.168.110.21) and 'EtherNet/IP Encapsulation Protocol Command Failed' (Major, Operational, 2 months ago, New, 192.168.110.2). A 'Group by' dropdown menu is visible at the top right of the alert table.

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**”.

This screenshot shows the Microsoft Defender for IoT Alerts page. The left sidebar has links for Discover, Device inventory, Alerts (which is selected), Analyze, Manage, and Support. The main area shows a table of alerts with columns for Severity, Name, Engine, Detection time, Status, and Source Device. Two alerts are listed: 'Unauthorized Internet Connectivity Detected' (Critical, Policy Violation, 2 weeks ago, New, 192.168.110.21) and another identical entry. To the right of the table, a detailed view of the first alert is shown. It includes a summary box with the alert ID (53), status (New), and detection time (2 weeks ago). Below this is a 'Description' section stating: 'A device defined in your internal network is communicating with addresses on the internet. These addresses have not been learned as valid addresses.' It also notes that 'Device 192.168.110.21 communicated with addresses shown in External Addresses. Verify that this device is properly configured.' Further down are sections for 'Related Devices' (Source device: 192.168.110.21, Destination device: Internet (37.142.39.186)) and two buttons at the bottom: 'View full details' and '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.

Showing 22 of 22 alerts

Severity	Name	Engine	Detection time	Status	Source Device
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 weeks ago	New	192.168.110.21
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 weeks ago	New	192.168.110.23
Critical	Port Scan Detected	Anomaly	2 weeks ago	Closed	192.168.110.21
Major	EtherNet/IP Encapsulation Protocol Command Failed	Operational	2 months ago	New	192.168.110.2
Critical	Unauthorized PLC Programming	Policy Violation	2 months ago	Closed	192.168.122.1
Critical	No Traffic Detected on Sensor Interface	Operational	2 months ago	New	192.168.100.8
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 months ago	New	192.168.110.8
Warning	Traffic Detected on Sensor Interface	Operational	2 months ago	New	192.168.110.1
Major	EtherNet/IP Encapsulation Protocol Command Failed	Operational	3 months ago	Closed	192.168.117.23
Critical	Excessive SMB login attempts	Anomaly	3 months ago	New	192.168.117.23
Major	Event Buffer Overflow in Outstation	Operational	3 months ago	New	192.168.117.23
Warning	Controller Reset	Operational	3 months ago	New	192.168.117.23
Warning	Controller Reset	Operational	3 months ago	New	192.168.117.23
Warning	An S7 Stop PLC Command was Sent	Operational	3 months ago	New	192.168.118.22
Warning	An S7 Stop PLC Command was Sent	Operational	3 months ago	New	192.168.118.11
Major	GE SRTP Command Failure	Operational	3 months ago	New	192.168.109.1
Major	Modbus Exception	Protocol Violation	3 months ago	New	192.168.109.2
Major	Modbus Exception	Protocol Violation	3 months ago	New	192.168.108.2
Major	Honeywell Firmware Version Changed	Policy Violation	3 months ago	New	192.168.108.2

## 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.

Showing 100 of 291 items

IP Address	Name	Last Activity	Type	Protocols	MAC Address	Vendor	Firmware Version	Model	Operating System	Rack	Slot
192.168.100.8	192.168.100.8	50 minutes ago	Unknown	DNS, MDNS, Net...	54:14:f8:74:d8:21	INTEL CORPORA...					
192.168.100.1	192.168.100.1	50 minutes ago	Server	DNS							
192.168.1.11	192.168.1.11	50 minutes ago	PLC	Siemens S7	00:fb:54:db:ef:9	NETGEAR					
192.168.1.180	192.168.1.180	50 minutes ago	HMI	Siemens S7							
192.168.117.23	192.168.117.23	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:92:c6	SCHWEITZER EN...					
192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	00:23:ea:49:5a:c2	CISCO SYSTEMS ...					
192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:97:0	SCHWEITZER EN...					
192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	00:cc:1c:02:09:da	EATON CORPOR...					
192.168.117.7	192.168.117.7	22 hours ago	PLC	Siemens SICAM	00:e0:a8:01:90:be	SAT GMBH & CO.	15.01	CPC65 (6065)			
192.168.117.239	192.168.117.239	22 hours ago	Unknown	Siemens SICAM	00:0c:29:28:28:38	VMWARE INC.					
192.168.117.8	192.168.117.8	22 hours ago	PLC	Siemens SICAM	00:e0:a8:01:90:bb	SAT GMBH & CO.	15.01	CPC65 (6065)			
192.168.107.10	FC50507	22 hours ago	DCS Controller	Yokogawa VNet/IP	00:00:64:9d:5d:10	YOKOGAWA DIG...					
192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9d:73:d4	YOKOGAWA DIG...					
192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9e:84:e5	YOKOGAWA DIG...					
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-6EH14...	0	4	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-9EH14...	1	2	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-8EH14...	1	2	

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

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Device inventory

**Defender for IoT | Device inventory**

Search | Save Filter | Refresh | Edit Columns | Export

Discover

- Overview
- Device map
- Device inventory**
- Alerts
- Analyze
- Event timeline
- Data mining
- Risk assessment
- Trends & statistics
- Attack vector
- Manage
- System settings
- Custom alert rules
- Users
- Forwarding
- Support
- Support

Showing 100 of 291 items

	IP Address	Name	Last Activity	Type	Protocols	MAC Address	Vendor	Firmware Version	Model	Operating System	Rack	Slot
<input type="checkbox"/>	192.168.100.8	192.168.100.8	An hour ago	Unknown	DNS, MDNS, Net...	5:14:f3:7d:8:21	INTEL CORPORA...					
<input type="checkbox"/>	192.168.100.1	192.168.100.1	An hour ago	Server	DNS							
<input type="checkbox"/>	192.168.1.11	192.168.1.11	An hour ago	PLC	Siemens S7	0:0:fb:5:4:be:f3	NETGEAR					
<input type="checkbox"/>	192.168.1.180	192.168.1.180	An hour ago	HMI	Siemens S7							
<input type="checkbox"/>	192.168.117.23	192.168.117.23	22 hours ago	PLC	DNP3 (Identifier...)	0:30:a7:08:92:c6	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	0:23:ea:49:5a:c2	CISCO SYSTEMS ...					
<input type="checkbox"/>	192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	0:30:a7:08:97:c0	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	0:0cc1:02:09:da	EATON CORPOR...					
<input type="checkbox"/>	192.168.117.7	192.168.117.7	22 hours ago	PLC	Siemens SICAM	0:e0:a8:01:90:be	SAT GMBH & CO.	15.01	CPC65 (6065)			
<input type="checkbox"/>	192.168.117.239	192.168.117.239	22 hours ago	Unknown	Siemens SICAM	0:0:c2:92:28:38	VMWWARE INC.					
<input type="checkbox"/>	192.168.117.8	192.168.117.8	22 hours ago	PLC	Siemens SICAM	0:e0:a8:01:90:bb	SAT GMBH & CO.	15.01	CPC65 (6065)			
<input type="checkbox"/>	192.168.107.10	FC50507	22 hours ago	DCS Controller	Yokogawa VNet/IP	0:0:0:64:9d:5:d:10	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	0:0:0:64:9d:7:3:d	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	0:0:0:64:9e:84:e5	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	0:0:1:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-6EH14...	0	4	
<input type="checkbox"/>	192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	0:0:1:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-9EH14...	1	2	
<input type="checkbox"/>	192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	0:0:1:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-8EH14...	1	2	

Load More...

## Task 4: View the Event Timeline

- 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".

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Event timeline

**Defender for IoT | Event timeline**

Search | Create event | Refresh | Export

User Operations == Hide | Add filter | Reset filters

Discover

- Overview
- Device map
- Device inventory
- Alerts
- Analyze
- Event timeline**
- Data mining
- Risk assessment
- Trends & statistics
- Attack vector
- Manage
- System settings
- Custom alert rules
- Users
- Forwarding
- Support
- Support

Event type

Event type	Time	Description
Device Detected	6/24/2022, 2:29:04 PM	Device 192.168.1.180 was detected
Device Connection Detected	6/24/2022, 2:29:04 PM	Connected devices 192.168.1.11 and 192.168.1.180
Device Detected	6/24/2022, 2:29:04 PM	Device 192.168.1.11 was detected
Firmware Update	6/23/2022, 5:30:28 PM	Client device 192.168.122.20 copied firmware on PLC 192.168.122.1:Client device 192.168.122.20 copied fir...
PLC Password Change	6/23/2022, 5:30:28 PM	Client device 192.168.122.20 requested PLC 192.168.122.1 to change password
PLC Reset	6/23/2022, 5:30:28 PM	Client device 192.168.122.20 requested PLC 192.168.122.1 to reset itself
PLC Start	6/23/2022, 5:30:28 PM	Client device 192.168.122.20 changed the PLC 192.168.122.1 mode to start
Firmware Update	6/23/2022, 5:30:28 PM	Client device 192.168.122.21 copied firmware on PLC 192.168.122.1
PLC Programming Mode Set	6/23/2022, 5:30:28 PM	Client device 192.168.122.20 tried to change PLC 192.168.122.1 mode to programming mode
Firmware Update	6/23/2022, 5:30:28 PM	Client device 192.168.122.21 copied firmware on PLC 192.168.122.2
PLC Password Change	6/23/2022, 5:30:28 PM	Client device 192.168.122.21 requested PLC 192.168.122.1 to change password
PLC Reset	6/23/2022, 5:30:28 PM	Client device 192.168.122.21 requested PLC 192.168.122.1 to reset itself

Load More...

## Task 5: Data Mining

- 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.

The screenshot shows the Microsoft Defender for IoT interface with the 'Data mining' tab selected. On the left, there's a sidebar with various navigation options like Overview, Device map, Device inventory, Alerts, Analyze, Manage, and Support. The main area displays a 'Recommended' section with cards for Programming Commands, Internet Activity, Excluded CVEs, Remote Access, CVEs, and Non Active Devices (Last 7 Days). Below this is a 'My reports' section showing a single entry named 'test'. To the right, a 'Create new report' dialog box is open, prompting for a 'Name' (Report name), 'Description', and 'Choose Category' (Category). It also includes filters for 'Results within the last' time period, IP address, MAC address, Port, and Device group. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

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

This screenshot is similar to the previous one but with several fields highlighted by pink boxes. The 'Name' field (Report name) and 'Description' field are highlighted. The 'Choose Category' dropdown is set to 'Modules and Firmware Versions'. Under the 'Filter by' section, the 'Firmware Version (GENERIC)' filter is also highlighted. The 'Save' button at the bottom is also highlighted with a pink box.

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

The screenshot shows the Microsoft Defender for IoT Data mining interface. On the left, there's a navigation sidebar with options like Overview, Device map, Device inventory, Alerts, Event timeline, Data mining (which is selected and highlighted in grey), Risk assessment, Trends & statistics, and Attack vector. The main area is titled 'Defender for IoT | Data mining'. It features a 'Recommended' section with cards for Programming Commands, Internet Activity, Excluded CVEs, Active Devices (Last 24 Hours), Remote Access, CVEs, and Non Active Devices (Last 7 Days). Below this is a 'My reports' section with a table. The first row in the table, 'PLC Firmware Version', has a pink box around it. The table columns are Name, Description, and Last modified. The 'PLC Firmware Version' row contains 'Report showing the firmware version of the different PLCs.', '2 minutes ago', and a file icon. Other rows include 'ALL' (4 days ago) and 'test' (3 months ago).

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

This screenshot shows the 'PLC Firmware Version' report page. At the top, there's a toolbar with Refresh, Expand all, Collapse all, Export to CSV, Export to PDF (which is highlighted with a pink box), Snapshots, Manage report, and Edit mode. The main content area is titled 'PLC Firmware Version' and contains the text 'Report showing the firmware version of the different PLCs.'. There are also some small icons for device status and alert levels.

## 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.

The screenshot shows the Microsoft Defender for IoT Risk assessment page. The left sidebar is identical to the previous screenshots, with 'Data mining' selected. The main area is titled 'Defender for IoT | Risk assessment'. A 'Generate report' button is highlighted with a pink box. Below it is a 'Reports list' table. The table has columns for #, Name, Date Created, and Size. It lists four reports: 'risk-assessment-report-4.pdf' (just now, 2 MB), 'risk-assessment-report-3.pdf' (4 days ago, 2 MB), 'risk-assessment-report-2.pdf' (A month ago, 1 MB), and 'risk-assessment-report-1.pdf' (3 months ago, 1 MB). Each report entry has a pink box around it.

## 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".

The screenshot shows the Microsoft Azure Cloud Management portal. In the top navigation bar, there's a search bar and several icons. Below it, the main title is 'Defender for IoT | Sites and sensors'. A message says 'Trial subscription "BuildEnv" expired. Please contact Microsoft sales.' There are four categories: 'All sensors' (4), 'EIoT' (1), 'OT cloud connected' (2), and 'OT' (1). Under 'Management', the 'Sites and sensors' tab is selected and highlighted with a pink box. It shows 4 of 4 sensors. The first sensor listed is 'D4IOT-CxE-Site - D4IOT-CxE-Site', which is locally managed. The 'Onboard OT sensor' button at the top right of the main area is also highlighted with a pink box.

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

This screenshot shows the 'Step 3: Register this sensor with Microsoft Defender for IoT' configuration page. It includes fields for Sensor name, Subscription (with a dropdown menu showing 'Please select a subscription' and 'Onboard subscription'), and a 'Cloud connected' checkbox (which is checked and highlighted with a pink box). Other fields include Sensor version (set to '22.X and above'), Site (with Resource name and Display name fields), Tags, and Zone. At the bottom left is a 'Register' button.

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".

The screenshot shows the Microsoft Defender for IoT Sensor management interface. On the left, there's a navigation sidebar with sections like Discover, Analyze, and Manage. Under Manage, 'System settings' is selected and highlighted with a pink box. In the main content area, there are several cards: 'Software Update', 'Threat Intelligence', 'Subscription & Activation Mode' (which is also highlighted with a pink box), 'Backup & Restore', 'System Health Check', and 'SNMP MIB Monitoring'. The 'Subscription & Activation Mode' card has a sub-instruction: 'Upload an activation file to reactivate this sensor'.

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

This screenshot shows the 'Subscription & Activation Mode' dialog box open on the right side of the screen. It contains fields for Activation Mode (set to 'Cloud Connected'), Activation Status (set to 'Active'), Tenant ID (a long GUID), Subscription ID (another long GUID), and a file upload input field labeled 'Upload activation file:' which is currently empty and highlighted with a pink box. The background shows the same interface as the first screenshot, with the 'System settings' section still highlighted.

## Task 3: Verify Cloud connection

1. On the sensor console.

**Defender for IoT | Overview**

Discover

- Overview (selected)
- Device map
- Device inventory
- Alerts

Analyze

- Event timeline
- Data mining
- Risk assessment
- Trends & statistics
- Attack vector

Manage

- System settings
- Custom alert rules
- Users

0 PPS    64 Devices    21 Alerts

**General Settings**

Version: 22.1.3.4162 (7763846)  
Threat Intelligence: Version 2022.07.12 | Last updated Jul 12, 2022  
Connectivity type: Cloud connected (highlighted)  
Activation: Valid  
Certificate: Valid

**Traffic Monitoring**

No chart to show

**Top 5 OT Protocols**

**Traffic By Port**

## 2. On the Cloud management console.

**Defender for IoT | Sites and sensors**

Showing subscription 'BuildEnv'

General

- Getting started
- Device inventory (Preview)
- Alerts (Preview)
- Workbooks (Preview)

Management

- Sites and sensors (selected)
- Pricing

4 All sensors    1 EloT    2 OT cloud connected    1 OT

Sensor name	Sensor type	Zone	Subscription ...	Sensor version	Sensor status	Last connect...	Threat Intelli...	Threat Intelli...	Threat ...
D4IOT-CxE-Site - D4IOT-CxE-Site	EloT	default	BuildEnv	Unavailable	--	-	--	--	...
sensor-Cyber	OT cloud co...	default	BuildEnv	Disconnected	A month ago	5/25/2022	Automatic	...	...
test1	OT cloud co...	default	BuildEnv	OK	19 minutes a...	7/11/2022	Automatic	...	...

## Exercise 7: Manage your sensor via the Cloud Management Portal

The cloud management portal serves as a central management tool when you deploy multiple sensors, and gives you a consolidated view of all the devices, alerts and incidents across different sites and zones.

### Task 1: Role Based Access Control on your sites and Sensors

1. Click on the site you just created. When the "Edit Site" panel on the side opens up, click on "Manage Site Access Control".

The screenshot shows the Microsoft Defender for IoT - Sites and sensors interface. On the left, there's a navigation sidebar with sections like General, Incidents (Preview), Recommendations (Preview), Workbooks, Firmware analysis (Preview), Management, Troubleshooting + Support, Diagnose and solve problems, and New support request (Preview). The main area displays a summary of devices: 41 All sensors, 4 IoT, 15 OT - Cloud connected, 22 OT - Locally managed, 11 Unhealthy, and 0 Unsupported. Below this, a list of sites is shown, including 'Ah2225', 'BetterTogetherSite', 'cs-playground', 'cybersecurityIoThub', 'Enterprise-network', 'Muli - Muli', 'testsitename', 'trestesttest', and 'Locally managed'. A modal window titled 'Edit site' is open for 'cs-playground', showing fields for Site resource name, Display name (VishakhaSensor), Owners (example@mail.com), and Tags (Key and Value). A button 'Manage site access control (Preview)' is also visible.

2.Click on "Add role assignment".

The screenshot shows the 'Access Control' page. At the top, there are buttons for '+ Add', 'Download role assignments', 'Edit columns', 'Refresh', 'Remove', and 'Feedback'. Below these, a purple box highlights the 'Add role assignment' button. Other buttons include 'Add co-administrator', 'My access' (with a 'View my access' button), 'Check access' (with a 'Check access' button), 'Grant access to this resource' (with a 'Learn more' link and 'Add role assignment' button), 'View access to this resource' (with a 'Learn more' link and 'View' button), and 'View deny assignments' (with a 'Learn more' link and 'View' button).

3.Type the security role you would like to grant and select it from the list. For example: "Security Reader".

The screenshot shows the 'Add role assignment' dialog. At the top, tabs include 'Role' (selected), 'Members' (highlighted with a red border), and 'Review + assign'. A note says 'A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles.' Below this, 'Assignment type' dropdowns show 'Job function roles' and 'Privileged administrator roles'. A note says 'Grant access to Azure resources based on job function, such as the ability to create virtual machines.' A search bar shows 'security'. A table lists security roles: 'D4IoT Security Analyst2' (CustomRole, None, View), 'Security Admin' (BuiltInRole, Security, View), and 'Security Reader' (BuiltInRole, Security, View). A note at the bottom says 'Showing 1 - 3 of 3 results.'

4.Click on "Members" -> "+Select Members". Type the name of the user you want to assign the role to.

**Add role assignment**

**Role** Members Review + assign

**Selected role** Security Reader

**Assign access to** User, group, or service principal

**Members** + Select members

Name	Object ID	Type
No members selected		

**Description** Optional

Review + assign Previous Next Select Close

5. Click on review and assign after reviewing the permission level and the user.

**Add role assignment**

**Role** Members Review + assign

**Selected role** Security Reader

**Assign access to** User, group, or service principal

**Members** + Select members

Name	Object ID	Type
Vishakha Ghosh	4d53f3b7-e555-4354-a330-193b4cd1ef28	User

**Description** Optional

Review + assign Previous Next

6. To review permissions, go to "Role Assignments", and change "Scope = This Resource". This allows you to audit who has what level of permissions.

**Access Control**

+ Add Download role assignments Edit columns Refresh Remove Feedback

Check access Role assignments Roles Deny assignments Classic administrators

**Number of role assignments for this subscription** 116 4000

Search by name or email Assignment type : All Type : All Role : All Scope : This resource Group by : Role

8 items (8 Users)

Name	Type	Role	Scope	Condition
Contributor				
D4IoT Security Analyst2				
Security Admin				
Vishakha Ghosh	User	Security Admin	This resource	None
Security Reader				
Vishakha Ghosh	User	Security Reader	This resource	None

## Task 2 : Manage your devices

1. Click on "Device Inventory", and see your total number of devices, new devices, and classification of devices.

Device inventory

**447 Total devices**

**78 New devices**

Last active time == 03/02/2023 - 03/16/2023 Network location (Preview) == All Add filter

Showing 447 of 447 devices

Group by (Preview) No grouping

Site	IPv4 address	Name	Type	Subtype	Vendor	Model	MAC address	VLAN
cs-playground	192.168.111.1	192.168.111.1	Industrial	DCS controller	FISHER CONTROLS	DeltaV MD/MD Plus	00:80:74:02:0F:42	--
cs-playground	192.168.111.20	192.168.111.20	Industrial	Engineering station	DELL INC.	--	18:66:DA:FA:4B:0C	--
cs-playground	192.168.111.2	192.168.111.2	Industrial	DCS controller	FISHER CONTROLS	DeltaV MD/MD Plus	00:80:74:02:0F:44	--
cs-playground	192.168.109.1	PLC_B	Industrial	PLC	INTEL CORPORATE	BME P58 1020	00:1C:C0:5F:49:0C	--
cs-playground	192.168.118.4	PLC_A	Industrial	PLC	SIEMENS AG	6ES7 315-2EH14-0A	00:01:E3:11:22:34	--
cs-playground	192.168.114.2	192.168.114.2	Industrial	Engineering station	MITSUBISHI ELECTR	QJ71GF11-T2	58:52:8A:B4:B1:4D	--
cs-playground	192.168.122.21	192.168.122.21	Industrial	Engineering station	--	--	--	--
b25eioltlab	192.168.0.17	192.168.0.17	Industrial	PLC	Acuity Brands Lighti	255F T2550 PAC	00:11:00:4E:51:62	--
b25eioltlab	192.168.0.3	192.168.0.3	Industrial	PLC	KNX LTD.	BACnet Server	00:C0:72:3F:FF:A3	--

2.Click on any device to open details about that device.

**10.140.32.30** Unclassified

Status: Authorized | Last Seen: 7 days ago | Alerts: 0

PROCURVE NETWORKING BY HP | cs-playground | EMEA | Supervisory

Network interfaces:

- IP: 10.140.32.30 | MAC: 00:16:B9:8C:AB:00

Protocols: SNMP

Tags: 10.140.32.0/24, 10.9.14.0/24, 10.140.32.0/24

3.Click on “View Full Details” to open the full device page.

**10.140.32.30**

Attributes: Vulnerabilities, Alerts, Recommendations

Name	Value
Authorization	Authorized
Class	Unclassified
Data source	OT sensor
First seen	3/8/2023, 11:54:19 a.m.
Importance	Normal
Last activity	3/9/2023, 4:56:05 a.m.
Network location	Local
Parent slot	0
Programming device	No
Protocols	SNMP
Purdue level	Supervisory
Rack	0
Scanner device	No
Sensor	css-eee-1722024942
Site	cs-playground
Subtype	Unclassified

General information:

- Type: Unclassified | Subtype: Unclassified
- Vendor: PROCURVE NETWORKING BY HP | Location: cs-playground | EMEA | Supervisory

Network interfaces:

- IP: 10.140.32.30 | MAC: 00:16:B9:8C:AB:00

Protocols: SNMP

Tags: 10.140.32.0/24, 10.9.14.0/24, 10.140.32.0/24

4.Click on the “Group by” dropdown, and pick any of the other options, for example: Zone or Vendor, to see the different views.

Device inventory

**Total devices** 447    **New devices** 76

Devices by class

- OT (105)
- Endpoint (86)
- Network (20)
- IoT (6)

Last active time == 03/02/2023 - 03/16/2023    Network location (Preview) == All    Add filter

Showing 52 groups by vendor

Group by (Preview) Vendor

	Site	IPv4 address	Name	Type	Subtype	Vendor	Model	MAC address	VLAN
<input type="checkbox"/>	>	AAEON TECHNOLOGY INC.	(24)						
<input type="checkbox"/>	>	ACT'L	(1)						
<input type="checkbox"/>	>	Acuity Brands Lighting, Inc.	(1)						
<input type="checkbox"/>	>	AMERICAN POWER CONVERSION CORP	(1)						
<input type="checkbox"/>	>	AUTOMATEDLOGIC CORPORATION	(1)						
<input type="checkbox"/>	>	B&R INDUSTRIAL AUTOMATION GMBH	(1)						
<input type="checkbox"/>	>	BROCADE COMMUNICATIONS SYSTEMS LLC	(1)						

## Task 3: View your Alerts

1. Click on the "Alerts" tab and view your Open Alerts, New Alerts and Alert count by severity.

Getting started

**Alerts**

Device inventory

Incidents (Preview)

Recommendations (Preview)

Workbooks

Firmware inventory (Preview)

Management

Sites and sensors

Plans and pricing

Settings (Preview)

Troubleshooting + Support

Diagnose and solve problems

New support request (Preview)

**Open alerts** 584    **New alerts** 584    **Active alerts** 0

Open alerts by severity

High (228)    Medium (196)    Low (160)

Last detection == Last month    Status == 2 selected    Add filter

Showing 278 of 278 alerts

Group by No grouping

	Severity	Name	Site	Engine	First detection	Status	Source device	Tactics	
<input type="checkbox"/>	High	Unauthorized Internet Connectivity	D	b25eiotlab	POLICY_VIOLATION	21 hours ago	<span style="color: green;">New</span>	Internet	<span style="color: blue;">Initial access</span>
<input type="checkbox"/>	High	Port Scan Detected		b25eiotlab	ANOMALY	21 hours ago	<span style="color: green;">New</span>	10.0.100.20	<span style="color: blue;">Discovery</span>
<input type="checkbox"/>	Low	An S7 Stop PLC Command was Sent		b25eiotlab	OPERATIONAL	21 hours ago	<span style="color: green;">New</span>	192.168.119.22	<span style="color: blue;">Malware</span>
<input type="checkbox"/>	High	Unauthorized PLC Programming		b25eiotlab	POLICY_VIOLATION	21 hours ago	<span style="color: green;">New</span>	ahi2225	<span style="color: blue;">Malware</span>
<input type="checkbox"/>	Medium	Unauthorized PLC Configuration Writ		b25eiotlab	POLICY_VIOLATION	21 hours ago	<span style="color: green;">New</span>	192.168.118.22	<span style="color: blue;">Malware</span>
<input type="checkbox"/>	Medium	Unauthorized PLC Configuration Writ		b25eiotlab	POLICY_VIOLATION	21 hours ago	<span style="color: green;">New</span>	192.168.119.22	<span style="color: blue;">Malware</span>
<input type="checkbox"/>	High	Unauthorized PLC Programming		b25eiotlab	POLICY_VIOLATION	21 hours ago	<span style="color: green;">New</span>	192.168.119.22	<span style="color: blue;">Malware</span>
<input type="checkbox"/>	High	Unauthorized PLC Programming		b25eiotlab	POLICY_VIOLATION	21 hours ago	<span style="color: green;">New</span>	ahi2225	<span style="color: blue;">Malware</span>
<input type="checkbox"/>	High	Unauthorized PLC Programming		b25eiotlab	POLICY_VIOLATION	21 hours ago	<span style="color: green;">New</span>	192.168.118.22	<span style="color: blue;">Malware</span>
<input type="checkbox"/>	Medium	Unauthorized PLC Program Upload		b25eiotlab	POLICY_VIOLATION	21 hours ago	<span style="color: green;">New</span>	10.0.101.15	<span style="color: blue;">Malware</span>

2. Click on any alert to see the details.

Showing 278 of 278 alerts

Severity	Name	Site	Engine	First detection	Status
High	Unauthorized Internet Connectivity D	b25eioltab	POLICY_VIOLATION	21 hours ago	
High	Port Scan Detected	b25eioltab	ANOMALY	21 hours ago	
Low	An S7 Stop PLC Command was Sent	b25eioltab	OPERATIONAL	21 hours ago	
High	Unauthorized PLC Programming	b25eioltab	POLICY_VIOLATION	21 hours ago	
Medium	Unauthorized PLC Configuration Writ	b25eioltab	POLICY_VIOLATION	21 hours ago	
Medium	Unauthorized PLC Configuration Writ	b25eioltab	POLICY_VIOLATION	21 hours ago	
High	Unauthorized PLC Programming	b25eioltab	POLICY_VIOLATION	21 hours ago	
High	Unauthorized PLC Programming	b25eioltab	POLICY_VIOLATION	21 hours ago	
High	Unauthorized PLC Programming	b25eioltab	POLICY_VIOLATION	21 hours ago	
Medium	Unauthorized PLC Program Upload	b25eioltab	POLICY_VIOLATION	21 hours ago	
Low	Unauthorized PLC Configuration Rec	b25eioltab	POLICY_VIOLATION	21 hours ago	
Low	Unauthorized PLC Configuration Rec	b25eioltab	POLICY_VIOLATION	21 hours ago	
Low	PLC Operating Mode Changed	b25eioltab	OPERATIONAL	21 hours ago	
Low	PLC Operating Mode Changed	b25eioltab	OPERATIONAL	21 hours ago	

**Unauthorized Internet Connectivity Detected** Alert ID: 95a746d9-021a-4223-819c-a8a73e9346de

Severity: High | Status: New | Last detection: 21 hours ago

Description: A device defined as part of your network is communicating with Internet addresses. The device is not authorized to communicate with Internet addresses.

Source device: Internet (137.220.100.146) Unknown → Destination device: 192.168.0.110 Unclassified

MITRE ATT&CK®

[View full details](#)

3.Click on "View full details" to view the alert page.

Alerts | Unauthorized Internet Connectivity Detected ...

Refresh | Download PCAP

**Unauthorized Internet Connectivity Detected** Alert ID: 95a746d9-021a-4223-819c-a8a73e9346de

Severity: High | Status: New | Last detection: 21 hours ago

Description: A device defined as part of your network is communicating with Internet addresses. The device is not authorized to communicate with Internet addresses.

Source device: Internet (137.220.100.146) Unknown → Destination device: 192.168.0.110 Unclassified

MITRE ATT&CK®

Tactics: Initial access: The adversary is trying to get into your network. [read more on attack.mitre.org](#)

Techniques: Internet accessible device: T0883

**Alert details**

Source device	Site	Device IP type
Internet	b25eioltab	Internal
Source device address	Zone	First detection (in the network)
137.220.100.146	default	3/15/2023, 6:08:42 p.m.
Destination device	Sensor	Last detection (in the network)
192.168.0.110	ah1225	3/15/2023, 6:08:42 p.m.
Destination device address	Category	Last activity (manual or automated changes)
192.168.0.110	Internet Access	3/15/2023, 10:18:00 p.m.
	Protocol	
	GENERIC	

**Take action**

**Entities**

- Devices (1)**

ID	Name	Subtype	Protocols	Vendor
4d09a3fc-8818-42c7-a339-a5	192.168.0.110	Unclassified	FTP, MDNS, Netbios Name Se	INTEL CORPORATE
- IP (1)**

Address
137.220.100.146

4.Click on the "Group by" dropdown to view the alerts by severity, site, engine, etc.

Device inventory Alerts 584 Open alerts 584 New alerts 0 Active alerts

Open alerts by severity:

High (228) | Medium (196) | Low (160)

Search: Last detection == Last month | Status == 2 selected | Add filter

Showing 278 of 278 alerts

Group by: Severity

Severity	Name	Site	Engine	First detection	Status	Source device	Tactics
> High (88)							
> Low (96)							
> Medium (94)							

Troubleshooting + Support

Diagnose and solve problems New support request (Preview)

## Task 4: View your recommendations

- Click on the "Recommendations" tab, to view the list of recommended fixes/remediation steps for alerts or misconfigurations on the sensors.

The screenshot shows the 'Recommendations (Preview)' tab selected in the left sidebar. The main area displays 'Active recommendations' with a count of 2. A search bar and filter button are present. Below, it says 'Showing 2 of 2 recommendations'. A table lists the recommendations:

Severity	Name	Unhealthy devices	Healthy devices	Last update time
Medium	Review PLC operating mode	16 devices	0 devices	3/20/2023
Low	Review unauthorized devices	31 devices	616 devices	3/20/2023

- Click on any recommendation to view full details.

The screenshot shows the details for the 'Review PLC operating mode' recommendation. It includes a summary section with severity (Medium), number of unhealthy devices (16), and last update (3/20/2023). Below is a table of 16 unhealthy devices:

Name	IP	Site	Last update time
EIP-Line1	192.168.110.1	bettertogethersite	3/20/2023
10.0.100.105	10.0.100.105	b25eiotlab	3/16/2023
192.168.0.17	192.168.0.17	b25eiotlab	3/15/2023
10.0.101.105	10.0.101.105	b25eiotlab	3/15/2023
10.0.101.110	10.0.101.110	b25eiotlab	3/15/2023
10.0.100.104	10.0.100.104	b25eiotlab	3/15/2023
10.0.100.110	10.0.100.110	b25eiotlab	3/15/2023
EIP-Line4	192.168.110.4	bettertogethersite	3/14/2023
192.168.90.122	192.168.90.122	cs-playground	3/12/2023
EIP-Line1	192.168.110.1	muli	3/1/2023
EIP-Line3	192.168.110.3	muli	3/1/2023
EIP-Line2	192.168.110.2	muli	3/1/2023
EIP-Line4	192.168.110.4	muli	3/1/2023

## Task 5: Visualize Data by utilizing Workbooks

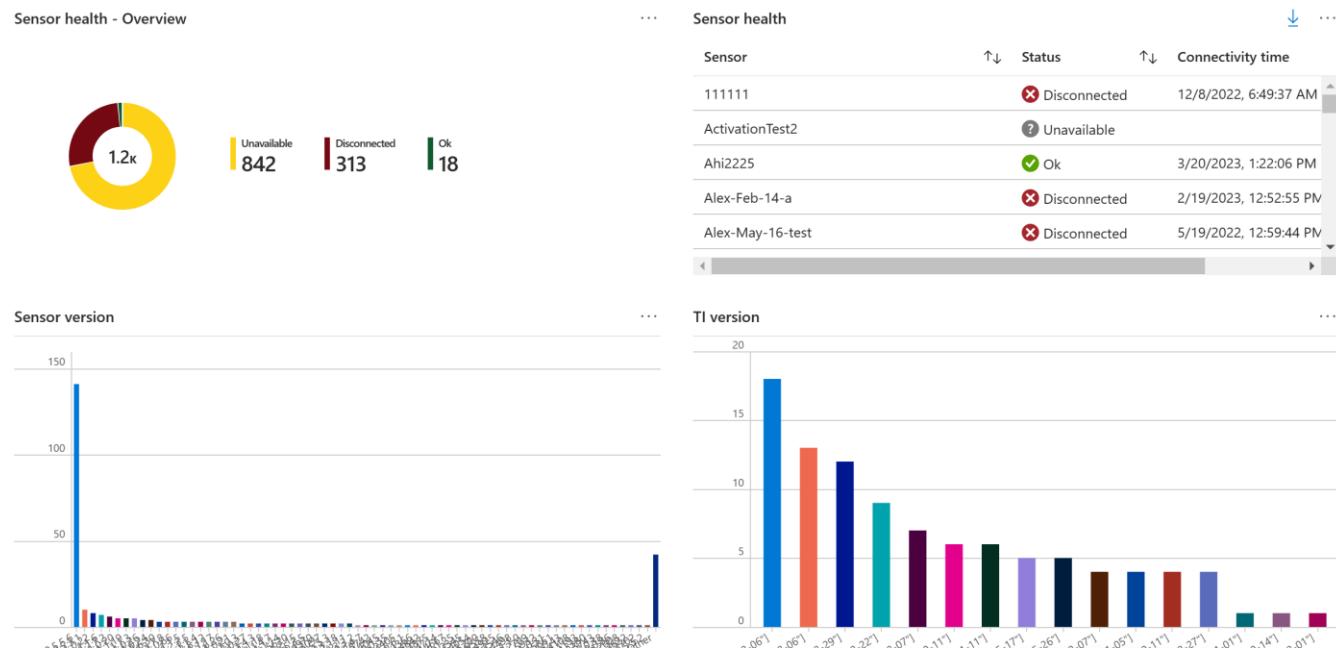
- Click on the "Workbooks" tab, to view the list of Defender for IoT workbooks.

The screenshot shows the Microsoft Defender for IoT Workbooks Gallery. On the left, there's a sidebar with categories: General (Getting started, Device inventory, Alerts, Recommendations (Preview), Workbooks), Management (Sites and sensors, Plans and pricing, Settings (Preview)), and Troubleshooting + Support (Diagnose and solve problems). The 'Workbooks' section is highlighted with a pink box. At the top, there's a search bar, a 'New' button, a 'Refresh' button, a 'Feedback' button, a 'Help' button, a 'Community Git repo' dropdown, and a 'Browse across galleries' button. Below the search bar, there are tabs for All, Workbooks, Public Templates, and My Templates. A filter bar shows 'Subscription : CS-playground', 'Resource Group : All', and 'Reset filters'. The main area displays several workbooks: 'Empty' (a completely empty workbook), 'Recently modified workbooks (8)' including 'Alerts Specific', 'Sensors Data', 'Detected MAC', 'Devices by Protocols', 'ByOS type', 'Workbook 3', 'DeviceInvestigation', and 'Workbook 2'; and 'Defender for IoT (4)' including 'Sensor health', 'Alerts', 'Devices', and 'Vulnerabilities'.

2. Click on any workbook, for example: "Sensor Health" , to view the preconfigured widgets on the workbook

### Sensors

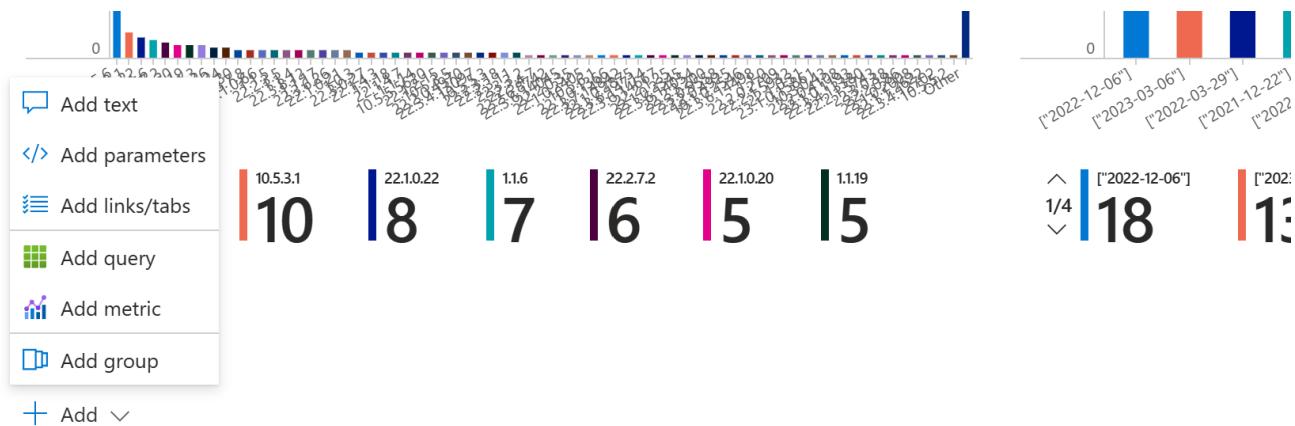
This report consolidates data regarding your sensors' health.



3. Click on the "Edit" option on the top ribbon to edit the existing widgets.



4. Click on "+Add" at the bottom of the workbook to add a widget to the workbook.



- Click on "Save" to view your added widget.

## Exercise 8: Integrate with Microsoft Sentinel

### Task 1: Create a Log Analytics Workspace

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

The screenshot shows the Azure portal search results for 'Microsoft Sentinel'. The search bar at the top contains the query 'Microsoft Sentinel'. The results page has a sidebar on the left with sections for 'Azure services', 'Recent', 'Favorite', 'Name', 'Resources', 'Navigate', 'Tools', and 'Subscriptions'. The main content area shows a list of resources under 'Services' and 'Marketplace'. The 'Services' section includes 'Microsoft Sentinel' (selected), 'Microsoft Defender EASM', 'Microsoft Purview accounts', and 'Microsoft Defender for Cloud'. The 'Marketplace' section includes 'Advanced KQL for Microsoft Sentinel', 'Demo Microsoft Sentinel', 'Advanced KQL for Microsoft Sentinel', 'SOC 24x7 Monitoring with Microsoft Sentinel', 'Sentinel360 MDR & Managed Microsoft Sentinel', 'NC Protect Data Connector for Microsoft Sentinel', 'Microsoft Sentinel for SQL PaaS', 'AMTRA Managed Microsoft Sentinel', 'Microsoft Sentinel for Teams (Preview)', 'Managed Microsoft Sentinel Service', and 'SecurityBridge App for Microsoft Sentinel'. The 'Documentation' section includes links to 'What is Microsoft Sentinel?', 'Microsoft Sentinel documentation', 'Plan costs for Microsoft Sentinel', 'Commonly used Microsoft Sentinel workbooks', and 'Continue searching in Azure Active Directory'.

- Click on "+Create" -> "+Create a new workspace".

- Pick your subscription, Resource Group, Name and Region

# Create Log Analytics workspace

Basics Tags Review + Create

**i** A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

## Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	CS-playground
Resource group *	CS-playground
	<a href="#">Create new</a>

## Instance details

Name *	VishakhaSentinel
Region *	Canada East

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

## Add Microsoft Sentinel to a workspace

+ Create a new workspace    ⏪ Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...				
Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
DemoTogether	centralus	demotogether	CS-playground	Microsoft
HandsOnLab	canadacentral	cs-playground	CS-playground	Microsoft
Hank-HOL	eastus	hank_hol	CS-playground	Microsoft
test	westeurope	cs-playground	CS-playground	Microsoft

[Add](#)   [Cancel](#)

## Task 2: Install the Defender for IoT package

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

The screenshot shows the Microsoft Sentinel News & guides interface. At the top, it says "Selected workspace: 'handsonlab'". Below that is a search bar and a documentation link. The navigation menu includes "General", "Overview", "Logs", and "News & guides", with "News & guides" being the active tab. The main content area features the heading "A cloud-native SIEM to h".

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

The screenshot shows the Microsoft Sentinel Content Hub. On the left is a sidebar with "General", "Threat management", "Content management", and "Configuration" sections. The "Content hub (Preview)" option under "Content management" is selected. In the center, there's a search bar with "Defender for IoT" typed in. A detailed view of the "Microsoft Defender for IoT" solution is shown on the right, including its provider (Microsoft), support (Microsoft Support), version (2.0.2), and a brief description. The "Install" button is highlighted with a pink box.

3.Click on “Create”.

The screenshot shows the "Microsoft Defender for IoT solution for Microsoft Sentinel" creation page. It has a "Plan" dropdown set to "Microsoft Defender for IoT" and a "Create" button highlighted with a pink box. The page also includes a "Microsoft Sentinel, Microsoft Corporation | Azure Application" section and a "Underlying Microsoft Technologies used:" section.

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

**Data Connectors: 1, Workbooks: 1, Analytic Rules: 15, Playbooks: 7**

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

C3-playground

Resource group \* ⓘ

C3-playground

Create new

### Instance details

Workspace \* ⓘ

HandsOnLab

**Review + create**

< Previous

Next : Data Connectors >

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

The screenshot shows the Microsoft Sentinel interface. On the left, there's a sidebar with links like Logs, News & guides, Search, Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview)), Content management (Content hub (Preview), Repositories (Preview), Community), and Configuration (Data connectors, Analytics). The 'Data connectors' link is highlighted with a pink box. In the main area, there's a summary bar with 126 Connectors (1 Connected) and a 'More content at Content hub' link. Below it, a table lists the connected connector: Microsoft Defender for IoT, Microsoft, with a status of 'Connected'. There are also filters for Status (All), Data Types (All), and Providers (All).

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

**Solutions (1)** Content sources . All

**Microsoft Defender for IoT**  
Microsoft Sentinel, Microsoft Corporation  
Internet of Things (IoT), Security - Threat Protection  
Analytics rule (15) Data connector +2  
Installed

**Standalone (2)**

**Workbook (2)**

Content name	Created content	Content type	Version
Microsoft Defender for IoT	1 item	Data connector	1.0.0
PLC unsecure key state (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Unauthorized PLC changes (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Unauthorized remote access to the network (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Unauthorized DHCP configuration in the network (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Multiple scans in the network (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Internet Access (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Excessive Login Attempts (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Firmware Updates (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
No traffic on Sensor Detected (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Illegal Function Codes for ICS traffic (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Suspicious malware found in the network (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
PLC Stop Command (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
Denial of Service (Microsoft Defender for IoT)	--	Analytics rule	1.0.1
High bandwidth in the network (Microsoft Defender for IoT)	--	Analytics rule	1.0.1

**Content type** i 15 Data connector 7 Playbook 1 Workbook

**Category** i Internet of Things (IoT), Security - Threat Protection

**Manage** Actions View details

**24** Installed content items

**Microsoft Defender for IoT**

**Provider** Microsoft Provider **Support** Microsoft Support **Version** 2.0.2

**Description**

The Microsoft Defender for IoT solution for Microsoft Sentinel allows you to ingest Security alerts reported in Microsoft Defender for IoT on assessing your Internet of Things (IoT)/Operational Technology (OT) infrastructure.

**Underlying Microsoft Technologies used:**

This solution takes a dependency on the following technologies, and some of these dependencies either may be in [Preview](#) state or might result in additional ingestion or operational costs:

a. [Codeless Connector Platform/Native Sentinel Polling](#)

**Data Connectors:** 1, **Workbooks:** 1, **Analytic Rules:** 15, **Playbooks:** 8

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

**Content type** i 15 Data connector 7 Playbook 1 Workbook

**Category** i Internet of Things (IoT), Security - Threat Protection

**Manage** Actions View details

**Content type** i 15 Data connector 7 Playbook 1 Workbook

**Category** i Internet of Things (IoT), Security - Threat Protection

**Pricing** i

**Manage** Actions View details

## Task 3: Create Incidents

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

Status	Connector name ↑	Disconnect... Status	Microsoft Provider	Last Log Rec...
	Microsoft Defender for Cloud Microsoft			
	Microsoft Defender for Cloud Apps Microsoft			
	Microsoft Defender for Endpoint Microsoft			
	Microsoft Defender for Identity Microsoft			
	Microsoft Defender for IoT Microsoft			
	Microsoft Defender for Office 365 (Preview) Microsoft	Last data received --	Content source ⓘ IoTOTThreatMonitoringwithDefenderforIoT	Version 1.0.0 Author Microsoft
				Supported by <a href="#">Microsoft Corporation</a>   <a href="#">Email</a>
				<a href="#">Open connector page</a>

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



### Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service.

[Enable](#)

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:

The screenshot shows the Microsoft Sentinel Incidents page. On the left, there's a navigation sidebar with sections like General, Threat management, Content management, and Configuration. The Threat management section has 'Incidents' selected, which is highlighted with a red box. The main area shows a grid of incidents with columns for Severity, Incident ID, Title, Alerts, and Last update time. Above the grid, there are filters for 'Severity: All' and 'Status: 2 selected'. A modal dialog is open over the grid, titled 'Product name', with a list of products. The 'Microsoft Defender for IoT' checkbox is checked and highlighted with a red box. Other products listed include Azure Information Protection, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft 365 Insider Risk Management, Microsoft 365 Defender, and Microsoft Sentinel. At the bottom of the dialog are 'OK' and 'Cancel' buttons. To the right of the grid, there's a large circular icon with three boxes and a plus sign, with the text 'No incidents selected' and 'Select an incident to view more details'.

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.

The screenshot shows the Microsoft Sentinel Incidents page with the 'Incidents' section selected in the sidebar. The main area displays a grid of incidents. A specific incident is selected and shown in a detailed pane on the right. The incident details pane includes the following sections: 
 

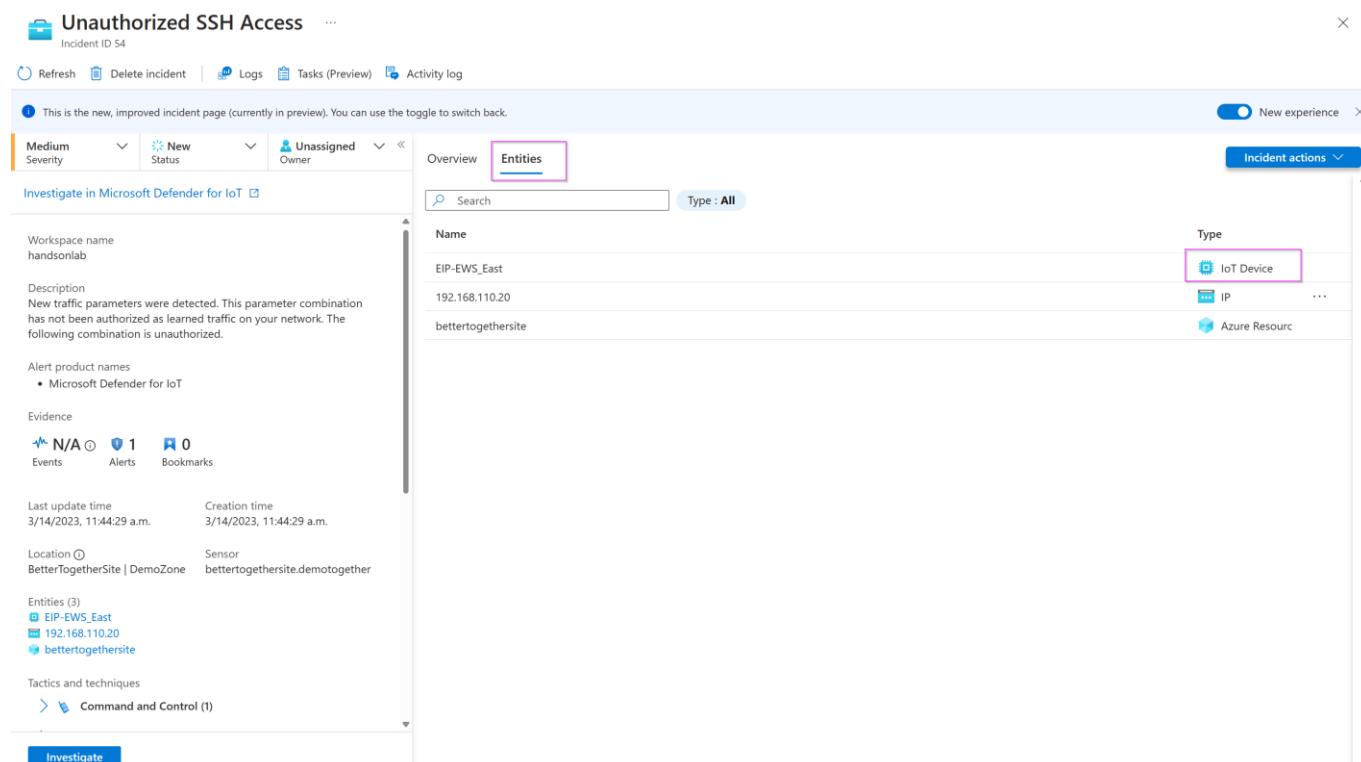
- Malicious Domain Name Request**: Incident ID: 107793, Status: New, Severity: High. It includes a link to 'Investigate in Microsoft Defender for IoT'.
- Description**: 'Suspicious network activity was detected. This activity may be associated with an attack exploiting a method used by known malware.'
- Alert product names**: Microsoft Defender for IoT.
- Evidence**: 1 Event, 0 Alerts, 0 Bookmarks.
- Last update time**: 09/22/22, 10:36 AM. **Creation time**: 09/22/22, 03:05 AM.
- Entities**: 1 (192.168.42.23), with a link to 'View full details >'.
- Tactics and techniques**: Command and Control (1) and Initial Access (0).
- Incident workbook** and **Incident Overview** buttons at the bottom.

## 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: 



The screenshot shows the Microsoft Defender for IoT incident details page for an 'Unauthorized SSH Access' incident (Incident ID 54). The 'Entities' tab is selected. A table lists three entities:

Name	Type
EIP-EWS_East	IoT Device
192.168.110.20	IP
bettertogethersite	Azure Resource

The 'IoT Device' row is highlighted with a pink box. Other tabs include Overview, Logs, Tasks (Preview), Activity log, and Incident actions. The page also displays workspace name, description, alert product names, evidence (Events: N/A, Alerts: 1, Bookmarks: 0), and location information.

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:

The screenshot shows the Microsoft Sentinel Entity behavior page. On the left, a sidebar navigation includes General, Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior - highlighted with a red box), Content management (Content hub, Repositories, Community), and Configuration (Data connectors, Analytics). The main area displays several cards: 'Accounts by # of alerts' (No data to display), 'Hosts by # of alerts' (1 host, 1 alert), 'IPs by # of alerts (Preview)' (list of IP addresses and alert counts), 'IoT devices by # of alerts (Preview)' (list of IoT devices and alert counts, highlighted with a red box), and 'Azure resources by # of alerts (Preview)' (list of Azure resources and alert counts).

## Task 7: Investigate the alert in Defender for IoT

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

The screenshot shows the Microsoft Sentinel Incident details page for Incident ID 319410. The left sidebar shows the incident summary: 'Unauthorized PLC Programming' (Incident ID: 319410, Investigate in Microsoft Defender for IoT). The main area has tabs for Timeline, Similar incidents (Preview), Alerts, Bookmarks, Entities, and Comments. The Timeline tab is selected, showing a single entry: 'Nov 29 1:03 PM | Unauthorized PLC Programming | High | Detected by Microsoft Defender for IoT | Tactics: [redacted]'. The right side of the screen shows detailed information for this incident, including Description, Severity (High), Status (New), Product name (Microsoft Defender for IoT), and a list of Entities (4) with their respective IP addresses.

## 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.

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Alerts

**Defender for IoT | Alerts**

Search Refresh Edit Columns Export to CSV Change Status Learn

Discover Overview Device map Device inventory Alerts Analyze Event timeline Data mining Risk assessment Trends & statistics Attack vector Manage System settings Custom alert rules Users Forwarding Support Support

Showing 22 of 22 alerts Group by No grouping

Severity	Name	Engine	Detection time	Status	Source Device
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 weeks ago	Closed	192.168.110.21
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 weeks ago	New	192.168.112.30
Critical	Port Scan Detected	Anomaly	2 weeks ago	Closed	192.168.110.21
Major	EtherNet/IP Encapsulation Protocol Command Failed	Operational	2 months ago	New	192.168.110.2
Critical	Unauthorized PLC Programming	Policy Violation	2 months ago	Closed	192.168.122.1
Critical	No Traffic Detected on Sensor interface	Operational	2 months ago	New	192.168.100.8
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 months ago	New	192.168.100.1
Warning	Traffic Detected on Sensor interface	Operational	2 months ago	New	192.168.101.10
Major	EtherNet/IP Encapsulation Protocol Command Failed	Operational	3 months ago	Closed	192.168.117.23
Critical	Excessive SMB login attempts	Anomaly	3 months ago	New	192.168.117.239
Major	Event Buffer Overflow in Outstation	Operational	3 months ago	New	192.168.117.239
Warning	Controller Reset	Operational	3 months ago	New	192.168.118.22
Warning	Controller Reset	Operational	3 months ago	New	192.168.118.11
Warning	An S7 Stop PLC Command was Sent	Operational	3 months ago	New	192.168.12.1
Warning	An S7 Stop PLC Command was Sent	Operational	3 months ago	New	192.168.109.1
Major	GE SRTP Command Failure	Operational	3 months ago	New	192.168.109.2
Major	Modbus Exception	Protocol Violation	3 months ago	New	192.168.108.2
Major	Modbus Exception	Protocol Violation	3 months ago	New	192.168.108.2
Major	Honeywell Firmware Version Chanoed	Policy Violation	3 months ago	New	192.168.108.2

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

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > System settings

**Defender for IoT | System settings**

Search Basic Sensor Setup

Discover Overview Device map Device inventory Alerts Analyze Event timeline Data mining Risk assessment Trends & statistics Attack vector Manage System settings Custom alert rules Users Forwarding Support Support

PCAP PLAYER Upload and replay PCAP files.

Upload Play All Clear All

1-S7comm-VaService-Read-D61DBD0.pcap  
pcap\_wednesdaypcapng

Sensor Network Settings Define sensor network settings

Connection to Management Console Connect this sensor to the on-premises management console

Time & Region Define time zone settings for this sensor

SSL/TLS Certificate Manage SSL/TLS certificates installed on this sensor

Play PCAP Upload and play PCAP files

Network monitoring Sensor management Integrations Import settings

Close

## Exercise 9: 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 10: 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.

## Exercise 11: Submit Feedback

It is through your feedback and suggestions that we can continue to improve the experience. Please share how your experience was via [this form](#).

## Appendix:

### Export Keys and VMs from Keyvault

Download and run this script hosted on Github [-Microsoft-Defender-for-IoT/Hands on Lab Documents/vmsexporter at main · Azure/-Microsoft-Defender-for-IoT \(github.com\)](#), to export a list of your passwords and VM names.

Ensure that you have:

1. Fill in your subscription id on line 8, resource group name on line 9, and key vault name on line 19.

2. Install all the modules mentioned in line 1 to line 5 mentioned in the code.

3. Install Azure CLI using this document - [Install the Azure CLI for Windows | Microsoft Learn](#)