

## Summary

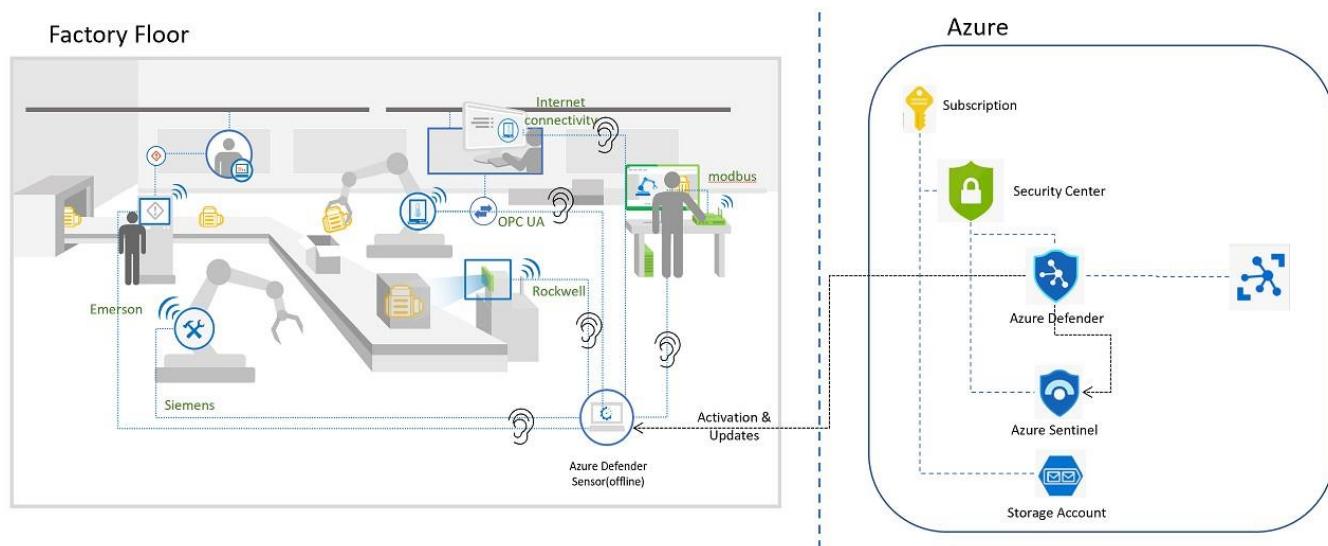
This Hands-on-Lab (HOL) will focus on securing your facilities. We will be simulating traffic by playing some Packet captures, visualizing and analyzing the data on the sensor console. Integrate our sensor with Microsoft Sentinel, to explore alert handling, and for writing queries to help with alert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

# Internet of Things - Microsoft Defender for IoT HOL

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

## Architecture Diagram

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



## Contents

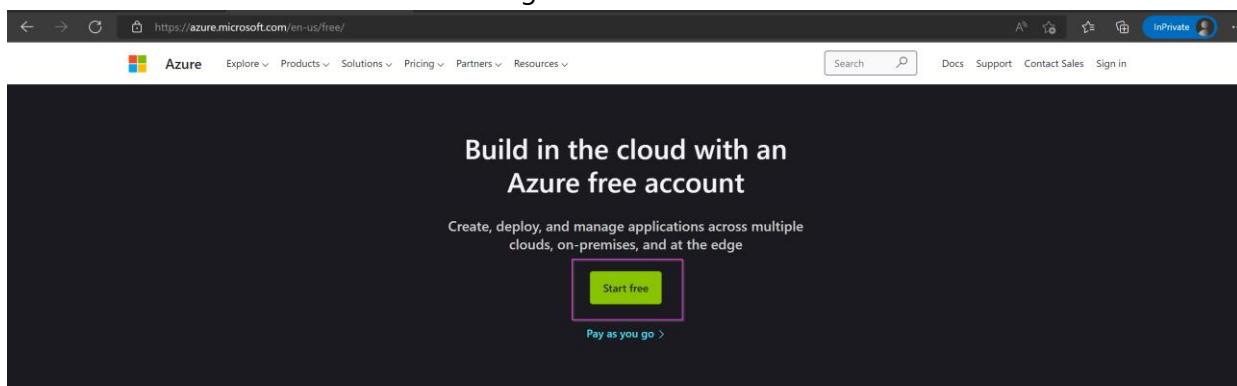
Architecture Diagram.....	1
Exercise #1: Enabling Defender.....	2
Task 1: Create an Azure Subscription .....	2
Task 2: Enabling Microsoft Defender for IoT on the Subscription.....	3
Exercise #2: Deploy the Sensor in Azure .....	5
Task 1: Create a Resource group to automatically deploy your sensor, storage account and network security group to .....	5
Task 2: Access your Virtual Machine. ....	7
Task 3: Access your sensor via the console .....	12

Exercise #3: Simulate Data in your sensor .....	18
Task 1: Enabling the PCAP Player .....	18
Task 2: Play PCAP files.....	20
Exercise 4: Analyzing the Data .....	21
Task 1: Visualize on the Device Map .....	21
Task 2: View the associated Alerts .....	24
Task 3: Device Inventory .....	26
Task 4: View the Event Timeline .....	27
Task 5: Data Mining .....	27
Task 6: Generate a Risk Assessment report.....	29
Exercise 5: Cloud Connect your sensor.....	30
Task 1: Create the cloud connected sensor on the Cloud Management portal .....	30
Task 2: Upload the activation file to cloud connect your sensor.....	30
Task 3: Verify Cloud connection.....	31
Exercise 6: Integrate with Microsoft Sentinel .....	32
Task 1: Connecting Data Connectors.....	32
Task 2: Acknowledge Alerts and Re-run PCAPs.....	37
Task 3: Sentinel interaction with IoT Incidents.....	38
Task 4: Kusto Query Language to Find Alert Details.....	40
Exercise 6: Clean Up .....	41
Task 1: Delete resources.....	43

## Exercise #1: Enabling Defender

### Task 1: Create an Azure Subscription

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



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

The screenshot shows the Microsoft Azure portal homepage. The left sidebar includes 'Create a resource', 'Recent', and a 'Name' dropdown. The main content area has tabs for 'All', 'Services (12)', 'Resources (1)', 'Marketplace (20)', 'Resource Groups (0)', and 'Documentation (0)'. Under 'Services', 'Subscriptions' is highlighted with a pink box. Other listed services include Event Hubs Clusters, Event Grid Subscriptions, Event Hubs, Web PubSub Service, Notification Hubs, Device Update for IoT Hubs, and Azure Synapse Analytics (private link hubs). Below this is a 'Marketplace' section with items like Autonomous Anomaly Detection, Managed Azure Subscription, JewelSuite Subsurface Modeling, SWIFT DR-Subscription, officework | Template Chooser User Subscription, NTT DATA Subscription Management, and Ticketing As A Service (Subscription). At the bottom, there's a 'Give feedback' button and a 'See all' link. The footer features 'Navigate' 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 Azure portal. The top navigation bar includes 'Home >', 'Subscriptions', 'Default Directory', and a search bar. Below the search bar are buttons for '+ Add', 'Manage Policies', and 'View Requests'. The main table lists one subscription: 'Visual Studio Enterprise Subscription' with ID '21311d18-92b6-4c00-b137-937eb90512a', role 'Account admin', cost 'CA\$11.29', secure score '41%', and status 'Active'. The table has columns for 'Subscription name', 'Subscription ID', 'My role', 'Current cost', 'Secure Score', 'Parent management group', and 'Status'.

## 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  
microsoft-defender-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

Partial data is shown because you have limited permissions to some of your subscriptions. Make sure you have Security Reader permissions on the relevant subscriptions to view related data.

General

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

Management

- Sites and sensors
- Pricing**
- 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

Partial data is shown because you have limited permissions to some of your subscriptions. Make sure you have Security Reader permissions on the relevant subscriptions to view related data.

General

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

Management

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

No subscriptions onboarded

Define committed device coverage or work with the trial.

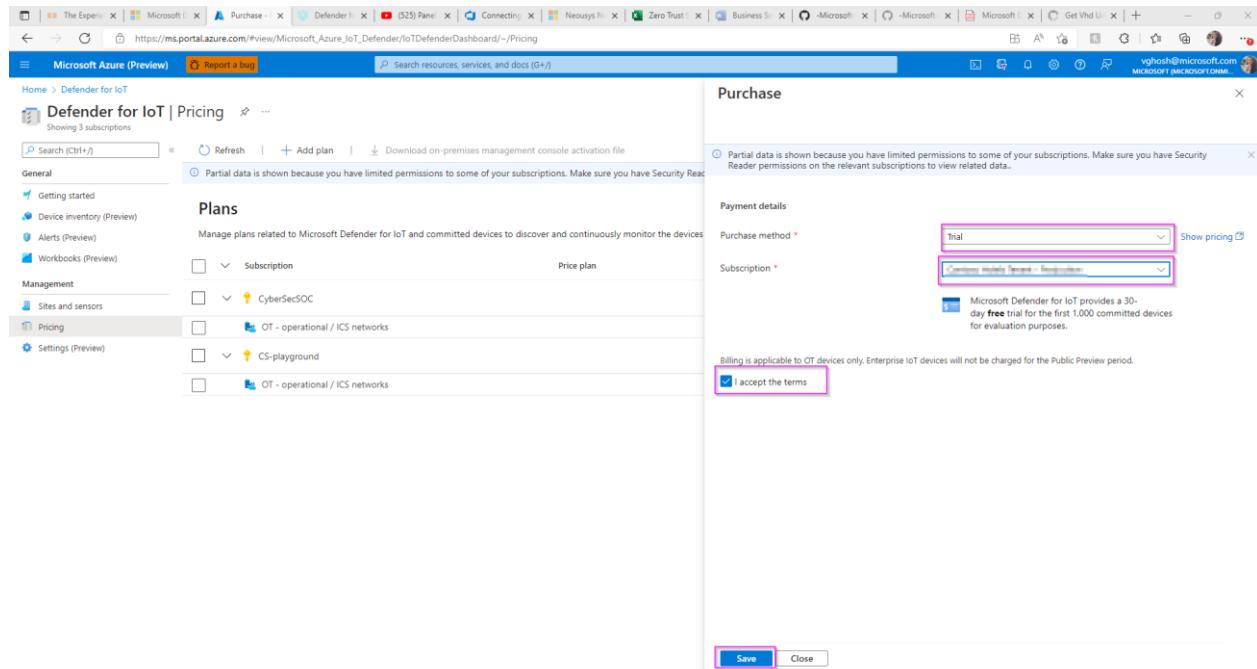
Onboard subscription

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 to [HOL\\_D4IOT@microsoft.com](mailto:HOL_D4IOT@microsoft.com) for a link for the IoT sensor installation. You will receive an email with the link once your request has been received.

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

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

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

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

**Project details**

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

**Subscription \*** ① BuildEnv

**Resource group \*** ② Create new

**Instance details**

**Region \*** ③ East US

**Location** ④ [resourceGroup().location]

**Deploy Public IP** ⑤ true

**Put Password To Key Vault** ⑥ true

**Source VHDURL \*** ⑦

**Sensor Count** 1

- 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.

**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 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.

**Deployment details (Download)**

Resource	Type	Status	Operation details
Reset-password0	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
Post-Deployment0	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
VMDeployment	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
copyhd	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>

**Next steps**

[Go to resource group](#)

- Go to the keyvault resource from the list.

**Resources**

Name	Type	Location
customx24k5pt7ngp2	Storage account	West US
SOC-KVuq63gjmwvo2do-Play	Key vault	West US
SOC-NSOC4k4kpt7ngp2-Play	Network security group	West US
SOC-vms24k5pt7ngp2-Play	Managed identity	West US
SOC-vms24k5pt7ngp2-Play-image	Image	West US
SOC-vms24k5pt7ngp2-Play-pip0	Regular Network Interface	West US
SOC-vms24k5pt7ngp2-Play-pip0	Public IP address	West US
SOC-vms24k5pt7ngp2-Play20-Play	Virtual machine	West US
SOC-vms24k5pt7ngp2-Play-disk1_16010174160101741601	Disk	West US
SOC-vms24k5pt7ngp2-Play	Virtual network	West US

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

**Access policies**

Access policies enable you to have fine grained control over access to vault items. [Learn more](#)

**APPLICATION**

Name	Email	Key Permissions
SOC-vmsidentityuq63gjmwvo2do-Play		

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

Home > Resource groups > KeyVaultTest > SOC-KVuq63gjmwo2do-Play | Access policies >

Create an access policy ...

SOC-KVuq63gjmwo2do-Play

**① Permissions**   **② Principal**   **③ Application (optional)**   **④ Review + create**

Configure from a template  
Key & Secret Management

Key permissions	Secret permissions	Certificate permissions
Key Management Operations <input checked="" type="checkbox"/> Select all <input checked="" type="checkbox"/> Get <input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Update <input checked="" type="checkbox"/> Create <input checked="" type="checkbox"/> Import <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Recover <input checked="" type="checkbox"/> Backup <input checked="" type="checkbox"/> Restore	Secret Management Operations <input checked="" type="checkbox"/> Select all <input checked="" type="checkbox"/> Get <input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Set <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Recover <input checked="" type="checkbox"/> Backup <input checked="" type="checkbox"/> Restore	Certificate Management Operations <input type="checkbox"/> Select all <input type="checkbox"/> Get <input type="checkbox"/> List <input type="checkbox"/> Update <input type="checkbox"/> Create <input type="checkbox"/> Import <input type="checkbox"/> Delete <input type="checkbox"/> Recover <input type="checkbox"/> Backup <input type="checkbox"/> Restore <input type="checkbox"/> Manage Contacts <input type="checkbox"/> Manage Certificate Authorities <input type="checkbox"/> Get Certificate Authorities <input type="checkbox"/> List Certificate Authorities <input type="checkbox"/> Set Certificate Authorities <input type="checkbox"/> Delete Certificate Authorities
Cryptographic Operations <input type="checkbox"/> Select all <input type="checkbox"/> Decrypt <input type="checkbox"/> Encrypt <input type="checkbox"/> Unwrap Key <input type="checkbox"/> Wrap Key <input type="checkbox"/> Verify <input type="checkbox"/> Sign	Privileged Secret Operations <input type="checkbox"/> Select all <input type="checkbox"/> Purge	Privileged Certificate Operations <input type="checkbox"/> Select all

Previous   **Next**

5. Under "Principle" select a principle

Home > Resource groups > KeyVaultTest > SOC-KVuq63gjmwo2do-Play | Access policies >

Create an access policy ...

SOC-KVuq63gjmwo2do-Play

**① Permissions**   **② Principal**   **③ Application (optional)**   **④ 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](#) [Edit principal](#)
- [Jane Doe](#) [Edit principal](#)
- [Administrators](#) [Edit principal](#)
- [Power Users](#) [Edit principal](#)
- [Guests](#) [Edit principal](#)
- [Everyone](#) [Edit principal](#)

**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)   

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

 5d62bf487ee14fb8884e0582f29be8e1-977f-4fa3-bf83-957308750ffb
 AcmeDnsValidator-ting0113im0 604fb01b-9fe8-4926-b954-b922680cbf40
 aksdemoSP-20200512091755 b59a0f98-632d-403b-987c-c68a88ccf81c0
 amasf 7056827c-0953-418c-9426-f6890b29e79
 ami-94dec3a3-89b7-402c-a6a6-3db32f3b2d40 b179cab-f3fc-4162-a465-eca5e6f54087
 ami-9f876ca0-654b-468b-8d6b-abf6aa26fce9 90534bd9-e88b-46f0-adf8-c7cef00a9954

#### 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	None selected
Object ID	None selected

Previous

Create

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

Subscription (move) : BuildEnv  
Subscription ID : 1c61ccbf-7031-45a3-a1fb-54fc4e46d70a6  
Tags (edit) : createdate : 07/13/2022 owner : vghosh

Deployments : 2 Failed 10 Succeeded  
Location : West US

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

Resource group (move) :  
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		Networking	
Computer name	Sensor	Public IP address	20.124.23.178
Health state	-	Public IP address (IPv6)	-
Operating system	Linux (ubuntu 18.04)	Private IP address	10.10.10.1
Publisher	-	Private IP address (IPv6)	-
Offer	-	Virtual network/subnet	SOC-Play/default
Plan	-	DNS name	Configure

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

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

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

Start time: 6/30/2022, 2:58:25 PM  
Correlation ID: ac55ba5c-e35a-4a36-b3ee-37b01fcdb3f

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
copyvhd	Microsoft.Resources/deployments	OK	Operation details

Next steps  
Go to resource group

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

The screenshot shows the 'Outputs' section of a deployment named 'Reset-password0'. The 'vmObject' output is highlighted with a pink border, showing its JSON value: { "VMName": "SOC-vmw7ne3eaow5oxw0-Play", "Password": "KChR9dMLp3VFkar2Yp8I99PM2V8=", "Status": true }. There is a 'Copied' message next to a clipboard icon.

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

The screenshot shows the 'Overview' page for a deployment named 'Microsoft.Template-20220630145822'. It displays a green checkmark indicating the deployment is complete. Below this, it shows the deployment name, subscription, and resource group. Under 'Deployment details', there is a table with four rows, each showing a successful deployment step. In the 'Next steps' section, there is a blue button labeled 'Go to resource group' which is highlighted with a pink border.

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

The screenshot shows the 'resource group' overview for a group named 'XXX'. It displays basic information like subscription, location, and deployment count. The 'Resources' section lists several resources, including a 'Virtual machine' named 'SOC-vmfici6u5atkwu-Play' which is highlighted with a red border. Other listed resources include 'copyvhd', 'customfici6u5atkwu', and 'SOC NSGfici6u5atkwu-Play'.

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". It features 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

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)

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	...

Actions (highlighted):

- Edit
- Push Threat Intelligence update
- Recover my password (highlighted)
- 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)

Pricing

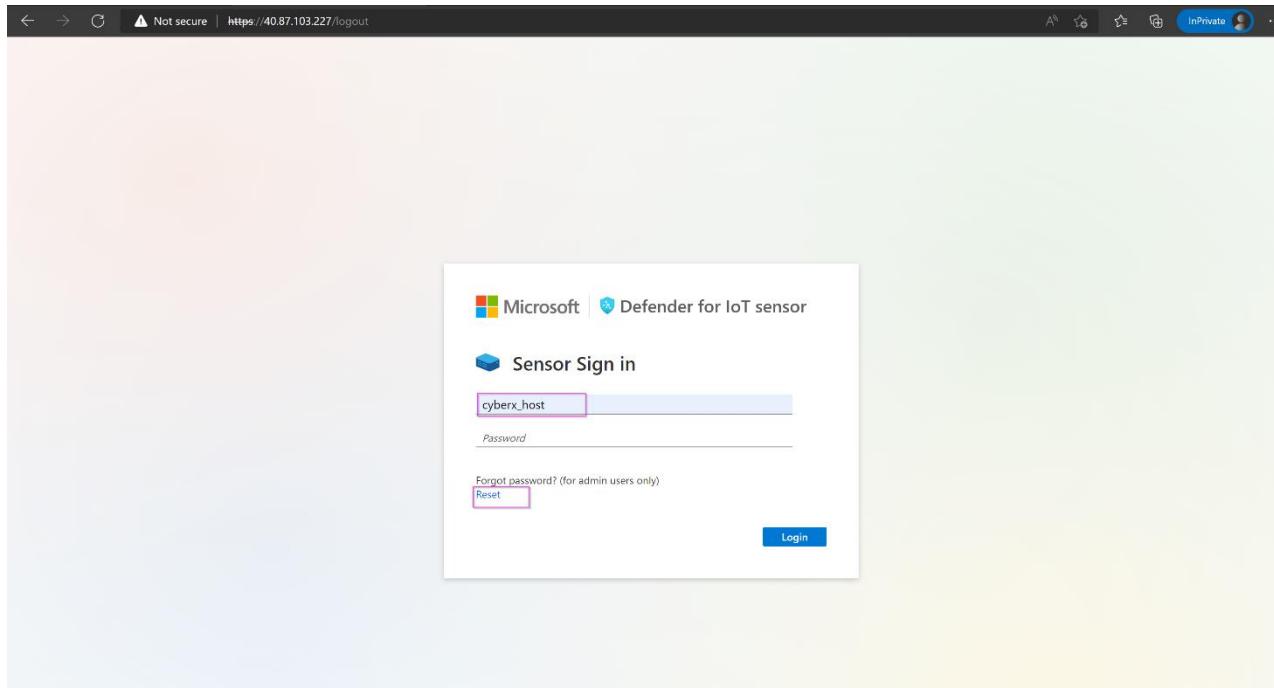
Recover

Insert secret identifier \*

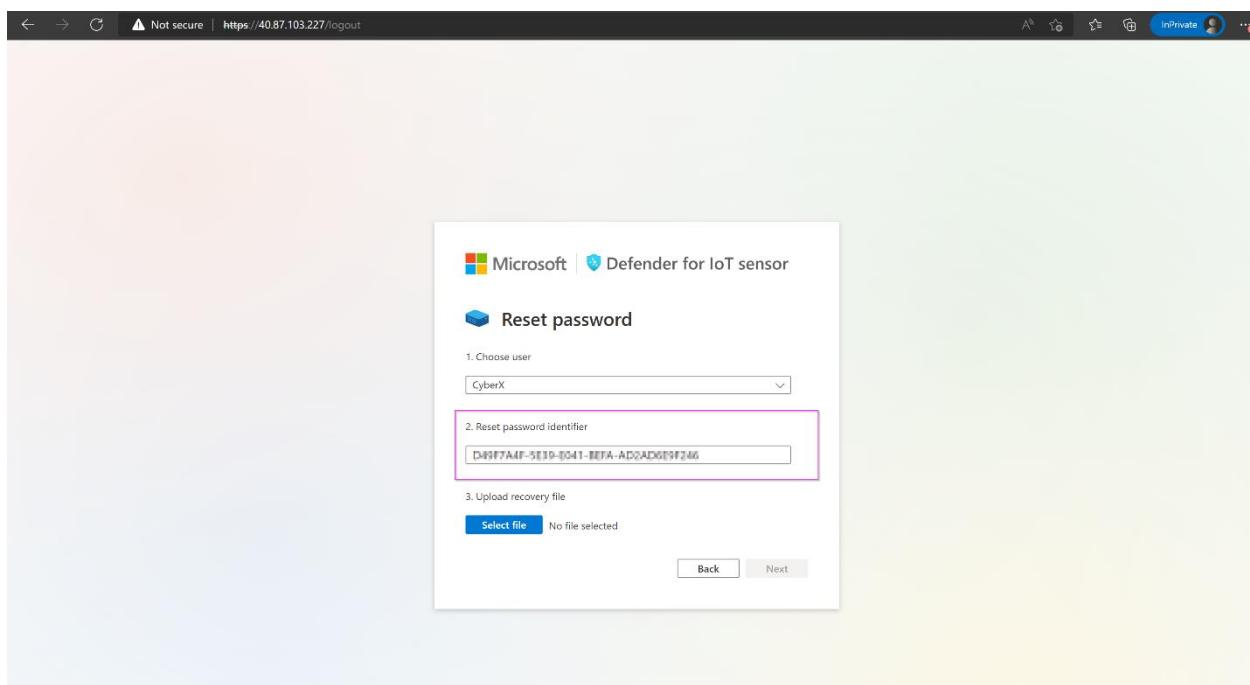
Sub0001-777-0e57-88h12

Recover Cancel

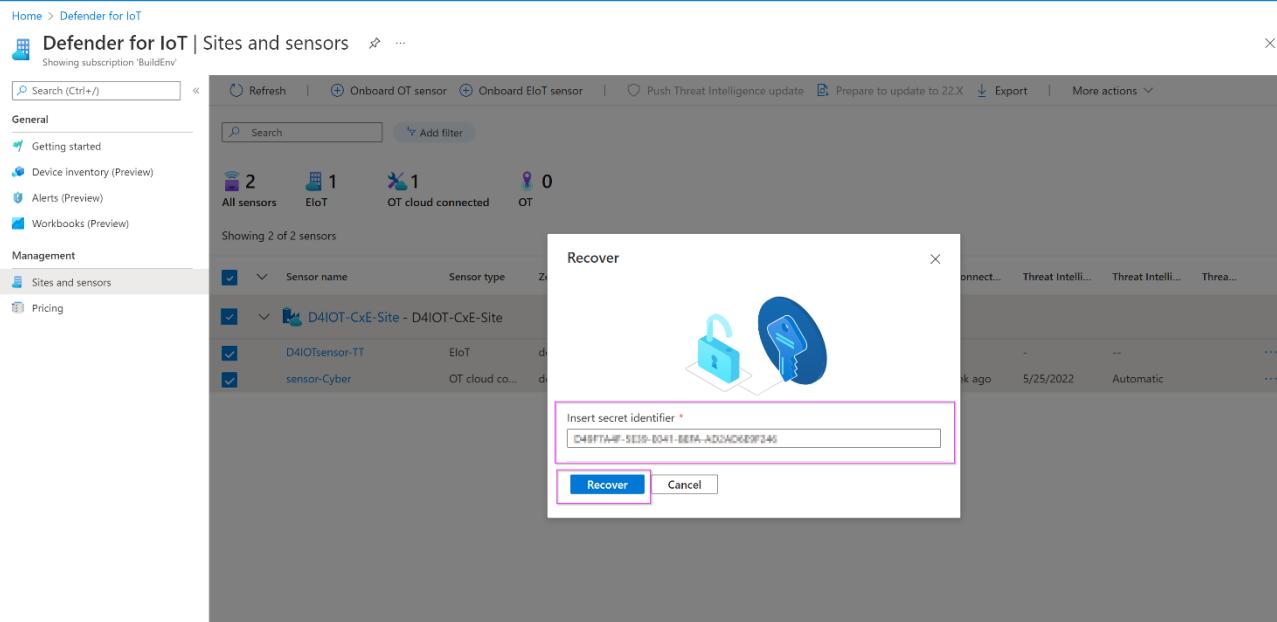
7. Return to the sensor console and type in the username followed by "Reset" as shown.



8. Copy the identifier.

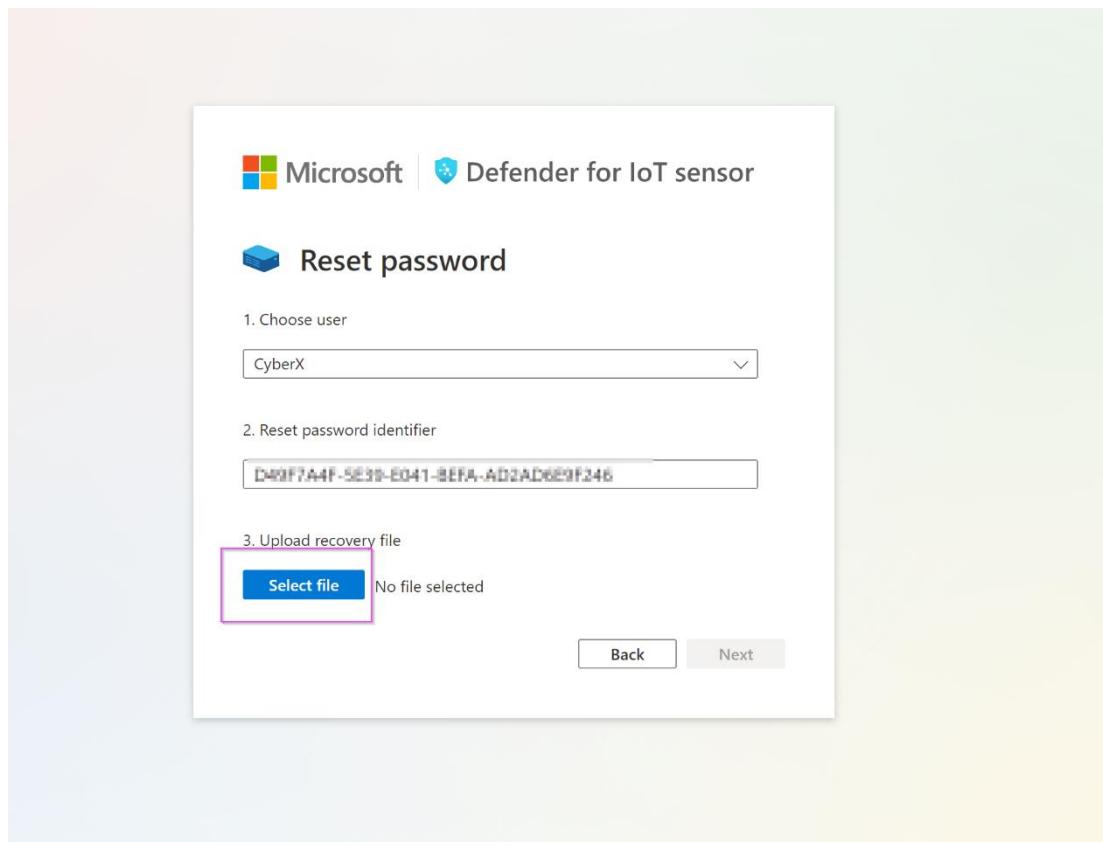


9. Paste in the box on the Defender for IoT Azure window. Click "**Recover**".



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'. A list of sensors is shown, including 'D4IOT-CxE-Site - D4IOT-CxE-Site' (EIoT), 'D4IOTsensor-TT' (EIoT), and 'sensor-Cyber' (OT cloud connected). 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 dropdown set to 'CyberX'. Step 2: Reset password identifier input field containing 'D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246'. Step 3: Upload recovery file section with 'Select file' button highlighted by a pink box. Below it, 'No file selected' is displayed. 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

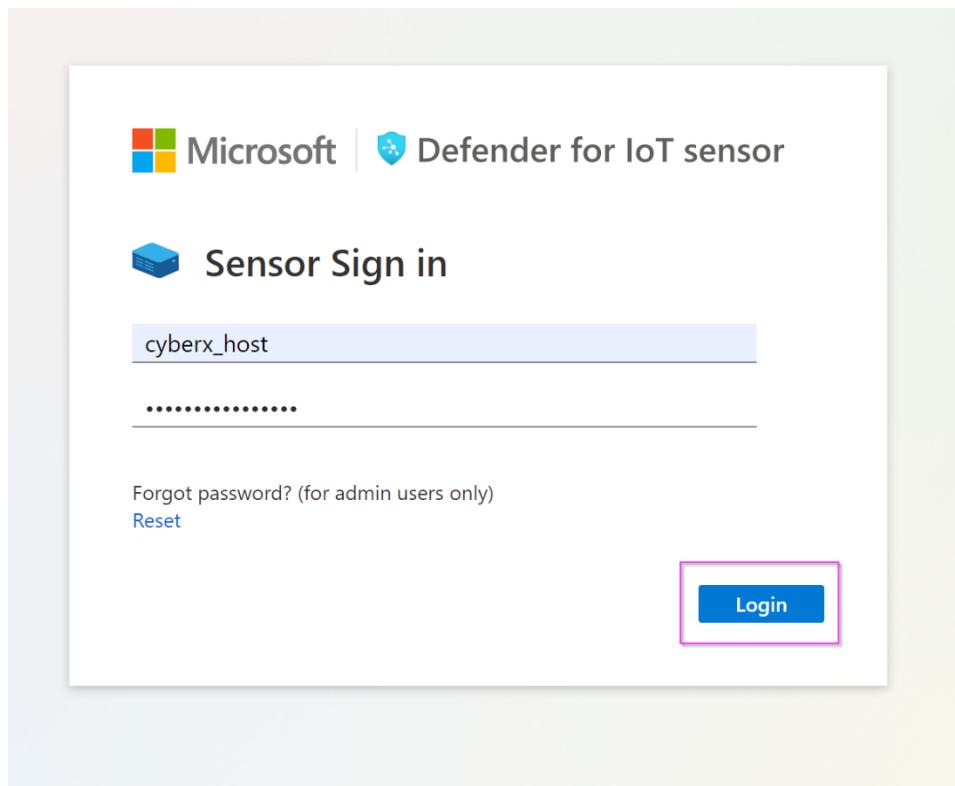
User name  
CyberX\_host

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: 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 - 22.1.3 interface. The left sidebar has a tree view with 'Alerts' expanded, showing 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', and 'Attack vector'. Under 'Manage', 'System settings' is highlighted with a red box. Other options include 'Custom alert rules', 'Users', and 'Forwarding'. The main content area is titled 'System settings' under 'Defender for IoT'. It contains four cards: '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), and 'Subnets' (Define which networks should be monitored by this sensor). The top right corner shows user information for 'cyberx\_host'.

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. On the left, there's a navigation sidebar with sections like Alerts, Analyze, and Manage. Under Manage, 'System settings' is selected. The main area is titled 'Health and troubleshooting' and contains four cards: '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.

The screenshot shows a 'Advanced configurations' dialog box. On the left, a list of categories is shown: Import, Internet Addresses, Management, MySQL, Pcaps (which is highlighted with a red box), Phrases, Ports, Profiling, Programming Diff, Purdue Layers, Query Parse Config, Redis, Remote Interfaces, Remote Upgrade, Reset System Data, and Rule Engine. On the right, there's a search bar labeled 'Select a configuration category' and a 'Close' button at the bottom.

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

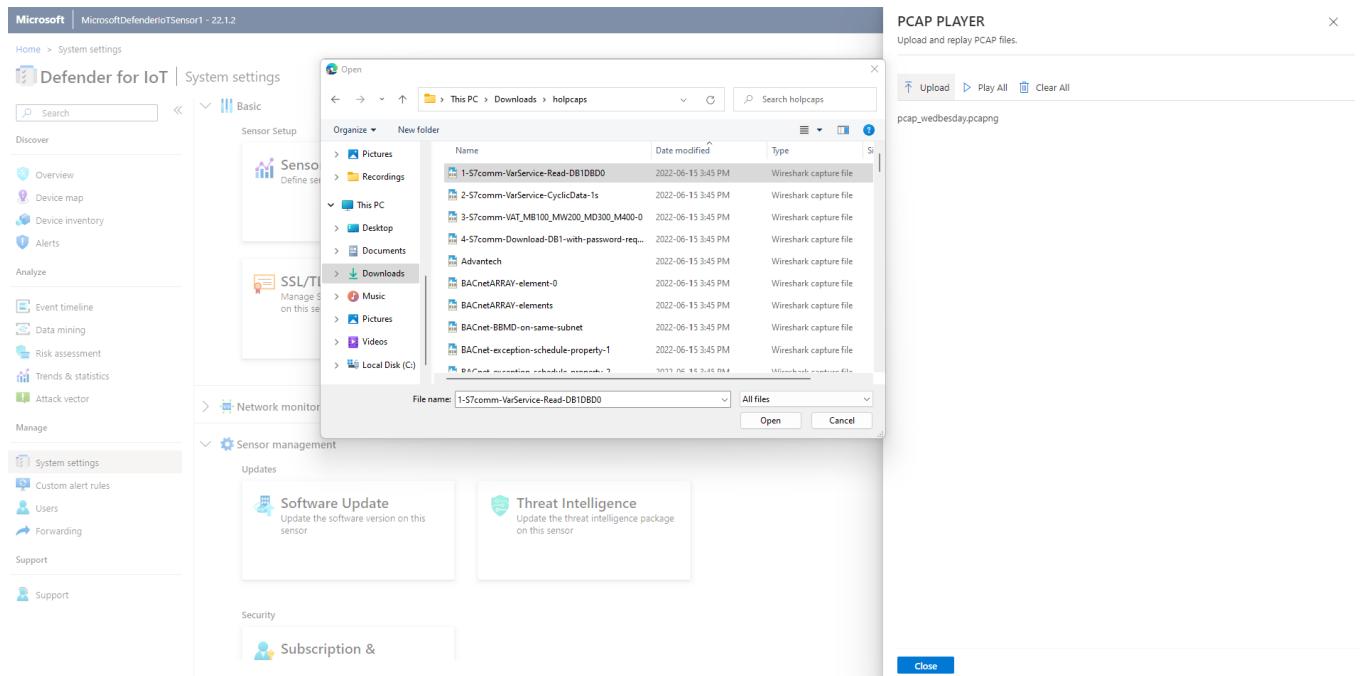
The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with options like 'Analyze', 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', 'Attack vector', 'Manage', 'System settings' (which is selected), 'Custom alert rules', 'Users', and 'Forwarding'. The main content area is titled 'System settings' and contains sections for 'Backup data and restore the latest backup' and 'SNMP MIB Monitoring'. To the right, a 'Advanced configurations' pane is open, showing configuration parameters such as 'cache.should.save.pcap=1', 'archive.cache.dir=' (with a note '# 7 GB'), 'filtered.cache.dir.size.megabytes.max=7168', 'filtered.cache.dir.size.megabytes.min=3072', 'player.max\_size=1000', 'player.max\_amount=20', 'player.params=', and 'enabled\_0'. A red box highlights the 'Save' button at the bottom of this pane. Below the configuration pane, there are 'Integrations' and 'Import settings' buttons.

## Task 2: Play PCAP files

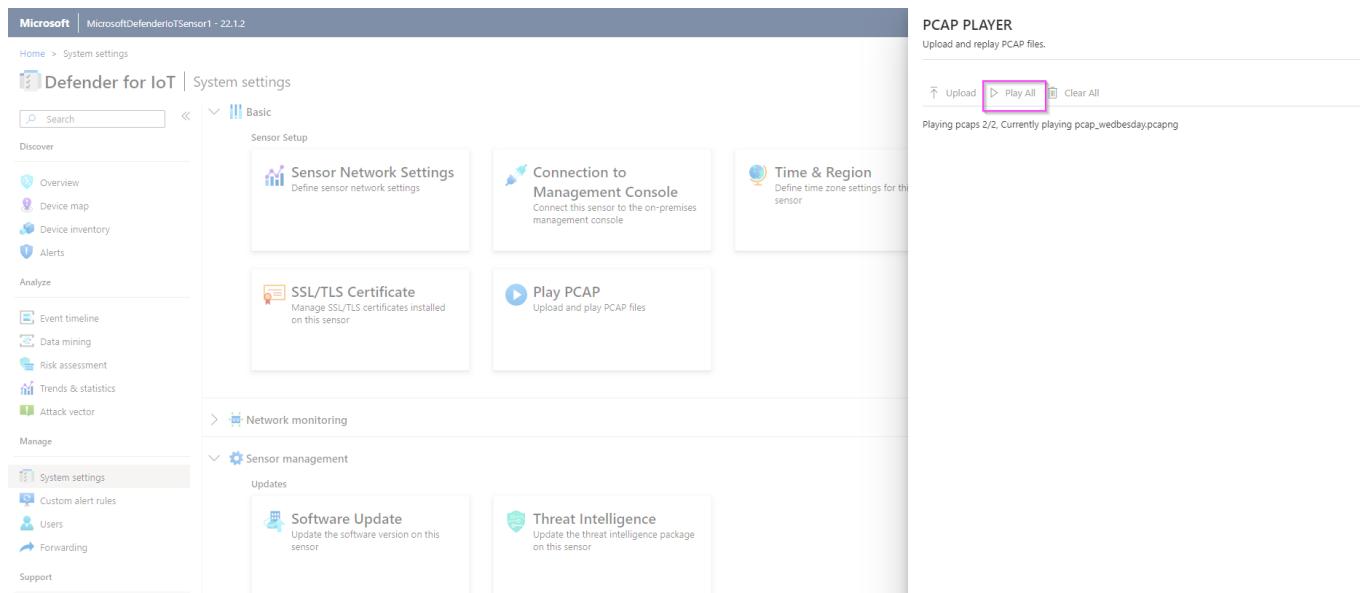
1. Use [this](#) link to download the holcaps.zip folder.
2. Unzip the folder.
3. Scroll all the way down to the bottom to locate if the PCAP Player is enabled (Shown in the image below in the red top square) or not. If the PCAP player is not shown, proceed to click on the arrow next to the **Sensor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

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar includes 'Analyze', 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', 'Attack vector', 'Manage', 'System settings' (selected), 'Custom alert rules', 'Users', and 'Forwarding'. The main area has sections for 'SSL/TLS Certificate' and 'Play PCAP' (which is highlighted with a red box). Under 'Manage', there's a 'Sensor management' button (also highlighted with a red box). Below these are 'Network monitoring', 'Integrations', and 'Import settings'.

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



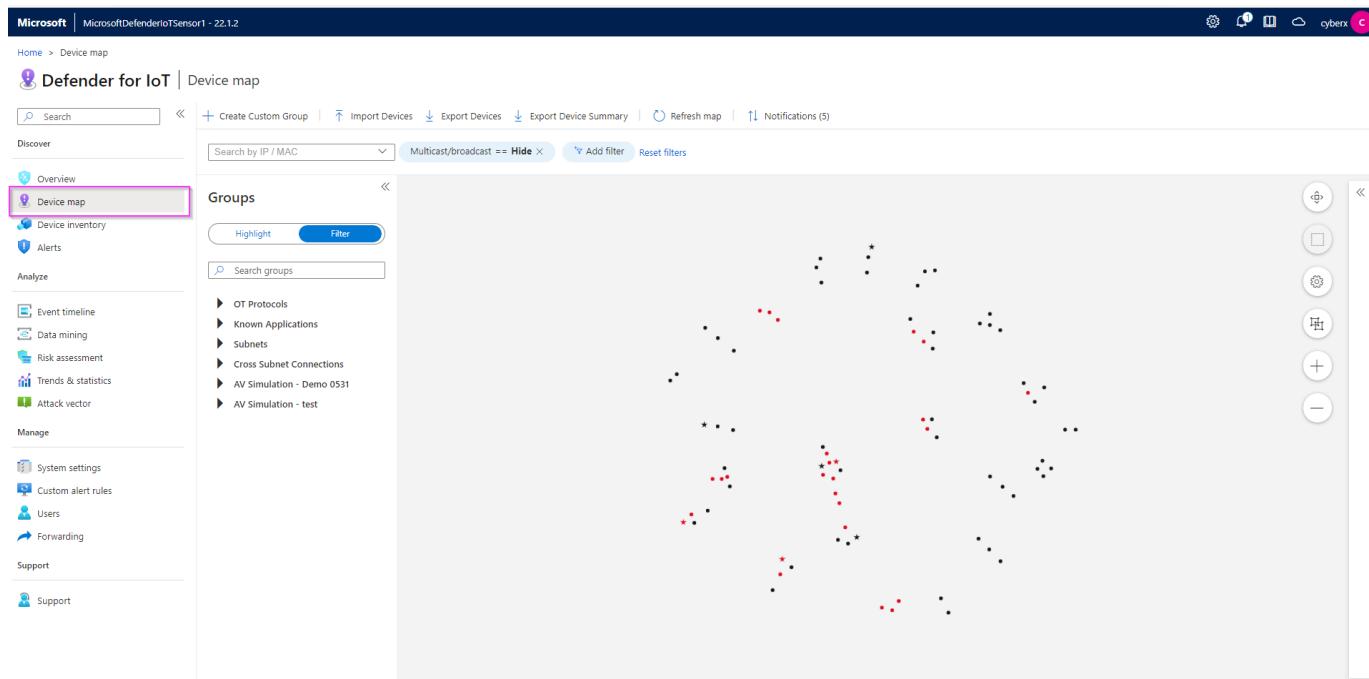
## 5. Click "Play All" to play the Pcaps.



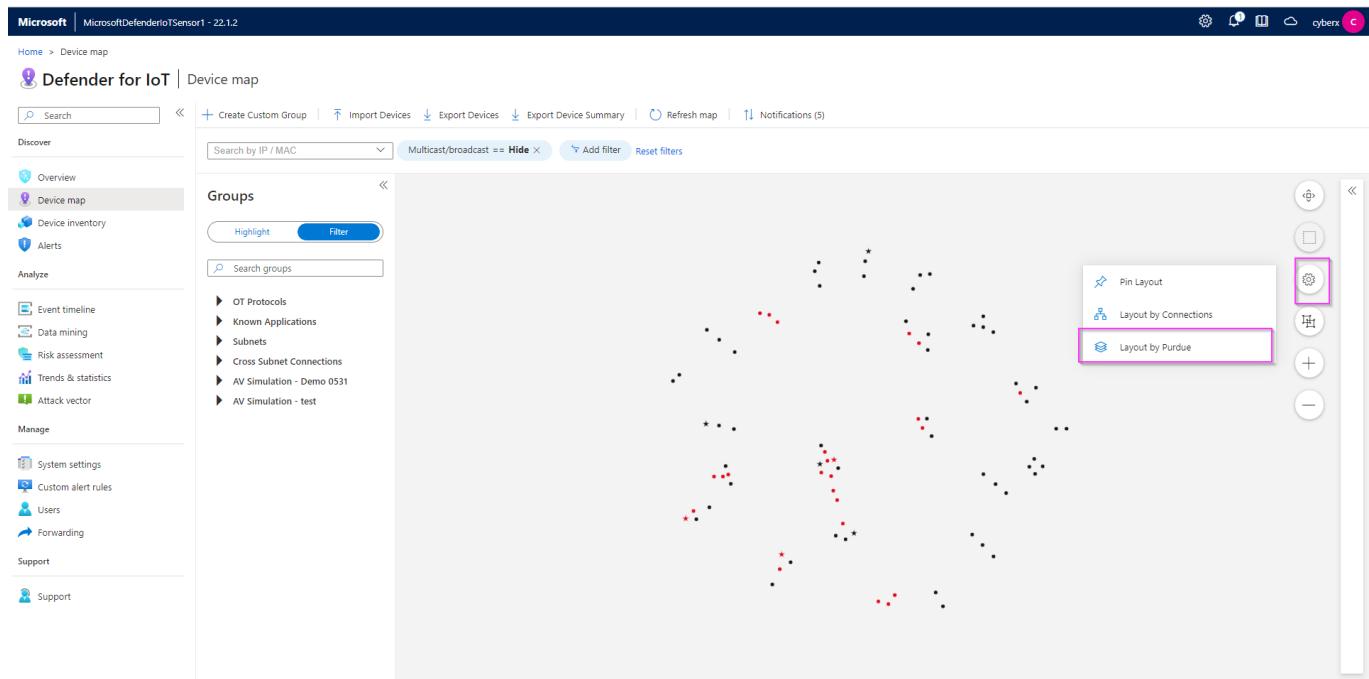
## Exercise 4: Analyzing the Data

### Task 1: Visualize on the Device Map

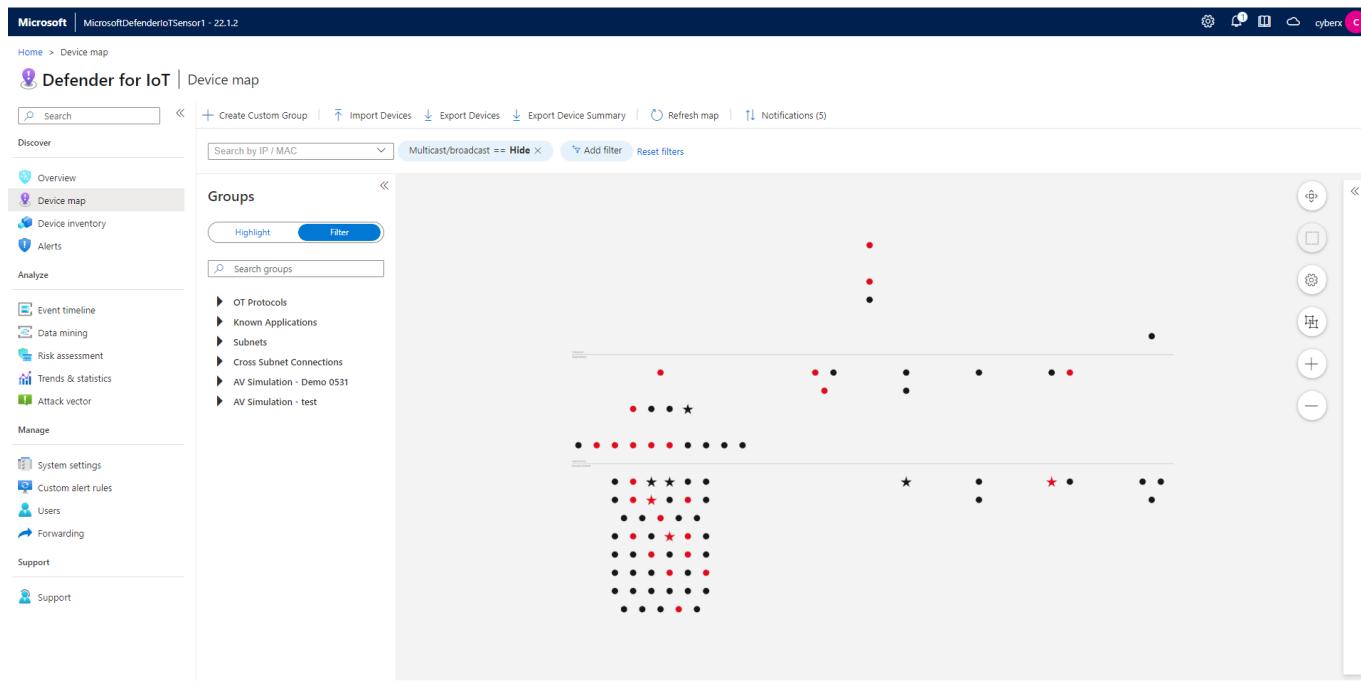
1. Click on “Device Map” from the menu on the left side.



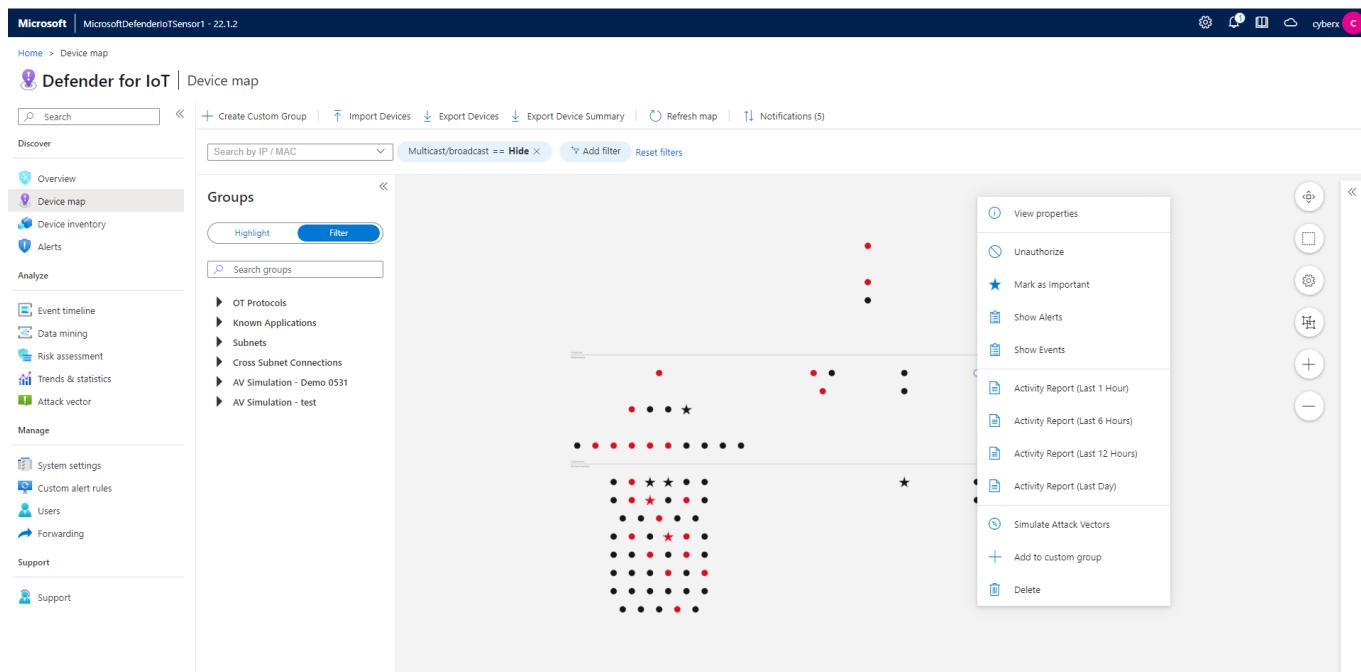
2. Click on the "Settings" option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.



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 lists various categories like Overview, Device map, Device inventory, Alerts, Analyze, Manage, and Support. Under the 'Device map' section, there's a 'Groups' dropdown menu where 'MODBUS' is highlighted with a red box. In the main pane, a network diagram shows three nodes: 192.168.109.1, 192.168.109.21, and 192.168.109.2. The node 192.168.109.1 has a red alert icon. The entire interface has a dark blue header and sidebar.

## Task 2: View the associated Alerts

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

This screenshot shows the Microsoft Defender for IoT Device map interface again. The sidebar and network diagram are similar to the previous one, but the network diagram now includes 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 a red alert icon. A context menu is open over this device, with the 'Show Alerts' option highlighted with a red box. The menu also includes other options like 'View properties', 'Unauthorized', 'Mark as Important', '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'.

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 navigation pane with 'Device' selected. The main area displays a device card for '192.168.110.21'. The card includes sections for 'General Information' (Type: Engineering Station, Vendor: INTEL CORPORATE, Location: Automatic), 'Network Interfaces' (MAC: acfdce:ccbbdd, IP: 192.168.110.21), 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 ('Status == 1 selected', 'Source/Destination device == 1 selected') are at the top. The alert list shows two entries: 'Unauthorized Internet Connectivity Detected' (Critical, Policy Violation, 2 weeks ago, New) and 'EtherNet/IP Encapsulation Protocol Command Failed' (Major, Operational, 2 months ago, New). The alert table has columns for Severity, Name, Engine, Detection time, Status, and Source Device.

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 '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), and 'Support' sections. The 'Alerts' section is selected. The main area shows a list of alerts with a search bar and filter options ('Status == 1 selected', 'Time range == Last 30 days'). Two alerts are listed: 'Unauthorized Internet Connectivity Detected' (Critical, Policy Violation, 2 weeks ago, New) and another identical entry. The second alert is selected, indicated by a checked checkbox. To the right, a detailed view of the selected alert is shown. It includes a summary box with 'Unauthorized Internet Connectivity Detected', 'Alert ID: 53', 'See in Event timeline | See in Device map', and 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.' Below this is a 'Related Devices' section showing a connection between 'Source device' (192.168.110.21, Engineering Station) and 'Destination device' (Internet (37.142.39.186), Internet). At the bottom are 'View full details' and 'Take action' buttons.

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:f9:74: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:c1:02:09: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 navigation sidebar with various 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 (e.g., 'Report name'), Description, and Category (e.g., 'Category'). It also includes filters for IP address, MAC address, Port, and Device group, along with a 'Send to CM' toggle. Buttons for 'Save' and 'Cancel' are at the bottom.

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 with pink boxes. In the 'Create new report' dialog, the 'Name' field (containing 'PLC Firmware Version') and the 'Description' field (containing 'Report showing the firmware version of the different PLCs') are highlighted. The 'Choose Category' dropdown is also highlighted, showing 'Modules and Firmware Versions'. A 'Filter by' section has three fields highlighted: 'Results within the last' (set to '3 Minutes'), 'IP address', and 'MAC address'. Another 'Filter by' section has 'Port' highlighted. At the bottom, the 'Save' button is highlighted. The rest of the interface is identical to the first screenshot.

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

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with sections like Discover, Analyze, Manage, and Support. Under Analyze, 'Data mining' is selected. In the main area, there's 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 that is a 'My reports' section with a table. One row in the table, 'PLC Firmware Version', has a pink box around it. The table columns are Name, Description, and Last modified.

Name	Description	Last modified
PLC Firmware Version	Report showing the firmware version of the different PLCs.	2 minutes ago
ALL		4 days ago
test		3 months ago

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

This screenshot shows a detailed view of a report titled 'PLC Firmware Version'. At the top, there are buttons for Refresh, Expand all, Collapse all, Export to CSV, Export to PDF, Snapshots, Manage report, and Edit mode. The 'Export to CSV' and 'Export to PDF' buttons are highlighted with a pink box. Below the buttons, the report content is displayed with the heading 'PLC Firmware Version' and a brief description: 'Report showing the firmware version of the different PLCs.'

## 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.

This screenshot shows the 'Risk assessment' page. On the left is a navigation sidebar with 'Discover', 'Analyze', 'Manage', and 'Support' sections. 'Risk assessment' is selected under 'Analyze'. In the main area, there's a 'Generate report' button highlighted with a pink box. Below it is a 'Reports list' table. The table has columns for #, Name, Date Created, and Size. Four reports are listed, each with a pink box around its row.

#	Name	Date Created	Size
1	risk-assessment-report-4.pdf	just now	2 MB
2	risk-assessment-report-3.pdf	4 days ago	2 MB
3	risk-assessment-report-2.pdf	A month ago	1 MB
4	risk-assessment-report-1.pdf	3 months ago	1 MB

## Exercise 5: 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 with the 'Defender for IoT | Sites and sensors' page selected. At the top, there's a search bar and several navigation icons. Below the header, there are sections for 'General' (Getting started, Device inventory (Preview), Alerts (Preview), Workbooks (Preview)) and 'Management' (Sites and sensors). The 'Sites and sensors' section is currently active and shows 4 All sensors, 1 IoT, 2 OT cloud connected, and 1 OT. A message at the top says 'Trial subscription "BuildEnv" expired. Please contact Microsoft sales.' Below this, a table lists four sensors, with the first one ('D4IOT-CxE-Site - D4IOT-CxE-Site') being expanded to show it's locally managed.

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 (set to 'Onboard subscription'), Cloud connected (checked), Automatic Threat Intelligence updates, Sensor version (22.X and above), Site (Resource name and Display name both set to 'No subscription has been selected'), Tags (Key: Value pairs), and Zone (No subscription has been selected). The 'Register' button is located at the bottom left of the form.

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 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.

## 2. On the Cloud management console.

Sensor name	Sensor type	Zone	Subscription ...	Sensor version	Sensor status	Last connect...	Threat Intelli...	Threat Intelli...	Threa...
D4IOTsensor-TT	EloT	default	BuildEnv		Unavailable	--	-	--	...
sensor-Cyber	OT cloud co...	default	BuildEnv	22.1.3.4162	Disconnected	A month ago	5/25/2022	Automatic	...
test1	OT cloud co...	default	BuildEnv	22.1.3.4162	OK	19 minutes a...	7/11/2022	Automatic	...

## Exercise 6: Integrate with Microsoft Sentinel

### Task 1: Connecting Data Connectors

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

## 2. Create a new workspace.

## 3. Go to Configuration > Data Connectors > Search **Microsoft Defender for IoT** to connect Microsoft Defender for IoT to Microsoft Sentinel.

## 4. Click the Open Connector Page.

The screenshot shows the Microsoft Sentinel Data connectors page. On the left, there's a sidebar with various workspace names listed. The main area shows a summary of 133 Connectors and 35 Connected ones. A search bar at the top right allows filtering by provider, data type, and status. Below the summary, a table lists connectors, with 'Microsoft Defender for IoT' by Microsoft being highlighted. To the right, a detailed card for 'Microsoft Defender for IoT' provides metrics like 'Connected' (1), 'Provider' (Microsoft), 'Last Log Received' (6 days ago), and a chart showing data received over time. A button at the bottom right says 'Open connector page'.

5. Review the instructions and click the “**Connect**” button to connect Microsoft Defender for IoT to Sentinel. If the connection continues to fail, this will most likely be due to the user not having the **“Contributor”** permissions and you may have missed the access step in the prerequisites.

The screenshot shows the Microsoft Defender for IoT (Preview) configuration page. It has sections for 'Instructions' and 'Next steps'. Under 'Prerequisites', it lists 'Workspace' and 'Subscription' requirements. The 'Configuration' section starts with 'Connect Microsoft Defender for IoT to Microsoft Sentinel'. It includes a note about selecting subscriptions to connect and links to 'Microsoft Defender for IoT pricing model' and 'Select the relevant Subscriptions to connect'. At the bottom, there are buttons for 'Connect All' and 'Disconnect All', and a search bar. A table lists 'Subscription' names (e.g., 'Azure Pass - Sponsorship') and their 'Status'. The 'Connect' button for the first subscription is highlighted with a red box.

6. If connected correctly you should expect to see the Status change to “**Connected**” and the link light up green.

The screenshot shows the Microsoft Azure Microsoft Defender for IoT (Preview) configuration page. The top navigation bar includes the Microsoft Azure logo, a search bar, and various navigation icons. The main content area has a breadcrumb trail: Home > Microsoft Sentinel > Microsoft Sentinel > Microsoft Defender for IoT (Preview). The left sidebar has two tabs: "Instructions" (selected) and "Next steps". The main content starts with a "Prerequisites" section, which lists requirements for integration: "Workspace" (read and write permissions) and "Subscription" (Contributor permissions to the subscription of your IoT Hub). Below this is a "Configuration" section. It contains a sub-section titled "Connect Microsoft Defender for IoT to Microsoft Sentinel" with the instruction "Select Connect next to each Subscription whose IoT Hub's alerts you want to stream to Microsoft Sentinel." A "Search" input field is provided. A table lists a single subscription: "Azure Pass - Sponsorship". The "Status" column for this subscription shows a green "Connected" link, which is highlighted with a red box. There are also "Connect" and "Disconnect" buttons in the table row. At the bottom of the configuration section, there is a note about the "Microsoft Defender for IoT pricing model".

7.Click on “Next steps” tab to enable Out of the Box alerts and Workbooks

7. Fill in the “Name” and click **Review and Create**, followed by **Create**. This is enabling incidents to be created based on the Azure Defender IoT alerts that are ingested into Sentinel.

8. Additionally, you can create the rule not only on the data connectors page but also on Microsoft Sentinel “**Analytics**” blade. Go to the “**Rule Templates**” tab and filter data sources by “Microsoft Defender for IoT” to see all the alerts from the IoT connector.

The screenshot shows the Microsoft Sentinel Analytics blade. On the left, there's a navigation sidebar with sections like General, Threat management, Content management, and Configuration. Under Configuration, the 'Data connectors' section is expanded, and the 'Analytics' item is highlighted with a pink rectangle. In the main content area, the 'Rule templates' tab is selected. A search bar at the top has 'Data Sources : Microsoft Defender for IoT' typed into it and is highlighted with a pink rectangle. Below the search bar, there's a table with columns for Severity, Name, Rule type, Data sources, Tactics, Techniques, and Source name. The table shows several rows of rules, with one row specifically for 'Microsoft Security' under 'Data sources'. At the bottom of the blade, there are pagination controls.

## Task 2: 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 so we can re-run the alerts to show how they are sent and analyzed by Sentinel.

The screenshot shows the Microsoft Defender for IoT Sensor1 console. On the left, there's a navigation sidebar with sections like Discover, Analyze, Manage, and Support. The 'Alerts' item is selected and highlighted with a pink rectangle. In the main content area, the 'Alerts' blade is displayed, showing a list of 22 alerts. The alert table has columns for Severity, Name, Engine, Detection time, Status, and Source Device. Each alert row has a checkbox in the first column. The 'Learn' button at the top right of the alert table is highlighted with a pink rectangle. The alert list includes various types of detections such as Policy Violation, Anomaly, and Operational.

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

The screenshot shows the Microsoft Defender for IoT Sensor Settings page. On the left, there's a navigation sidebar with sections for Discover, Analyze, Manage, and Support. Under Manage, 'System settings' is selected. The main area has several cards: 'Sensor Network Settings', 'Connection to Management Console', 'Time & Region', 'SSL/TLS Certificate', and 'Play PCAP'. To the right, a 'PCAP PLAYER' window is open, displaying a file named 'pcap\_wednesday.pcapng' with a 'Play All' button highlighted.

## Task 3: Sentinel interaction with IoT Incidents

1. Go back to the Sentinel console and under the **Threat Management** section, select the **Incidents** tab. Filter by Product Name **Azure Defender for IoT**.

The screenshot shows the Microsoft Sentinel Incidents page. The 'Incidents' tab is selected. The interface includes a search bar, refresh button, and filters for 'Last 24 hours', 'Actions', 'Security efficiency workbook', 'Columns', 'Guides & Feedback', 'Severity: All', 'Status: 2 selected', 'Product name: Microsoft Defender for IoT' (which is highlighted with a red box), and 'Owner: All'. The main table lists 16 open incidents, 16 new incidents, and 0 active incidents. Each incident row contains columns for Severity, Incident ID, Title, Alerts, Product names, Created time, Last update time, and Owner. One specific incident is highlighted in yellow.

Severity	Incident ID	Title	Alerts	Product names	Created time	Last update time	Owner
High	16	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:42 PM	01/25/22, 04:42 PM	Unas...
High	15	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Low	14	Outstation Restarted	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	13	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	12	Firmware Change Detected	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Low	11	Controller Stop	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
High	10	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	9	EtherNet/IP CIP Service Requ...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	8	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
High	7	Unauthorized Internet Conne...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	6	Unknown Object Sent to Out...	1	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	5	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	4	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	3	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	2	BACNet Operation Failed	1	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...

2. Select one of the alerts and click **View full details**

Microsoft Sentinel | Incidents

Selected workspace: mylogoworkspace-msiot2

General

- Overview
- Logs
- News & guides
- Threat management
- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- Content management
- Content hub (Preview)
- Repositories (Preview)
- Community
- Configuration
- Data connectors
- Analytics
- Watchlist
- Automation
- Settings

16 Open incidents 16 New incidents 0 Active incidents

Open incidents by severity

Severity	Count
High (4)	4
Medium (10)	10
Low (2)	2
Informational (0)	0

Search by ID, title, tags, owner or product Severity: All Status: 2 selected Product name: Microsoft Defender for IoT Owner: All

Severity	Incident ID	Title	Product names	Created time	Last update time	Owner
High	16	Unauthorized internet Conn...	Microsoft Defender ...	01/25/22, 04:42 PM	01/25/22, 04:42 PM	Unas...
High	15	Unauthorized internet Conn...	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Low	14	Outstation Restarted	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	13	BACNet Operation Failed	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	12	Firmware Change Detected	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Low	11	Controller Stop	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
High	10	Unauthorized Internet Conn...	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	9	EtherNet/IP CIP Service Requ...	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	8	BACNet Operation Failed	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
High	7	Unauthorized Internet Conn...	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	6	Unknown Object Sent to Out...	Microsoft Defender ...	01/25/22, 04:41 PM	01/25/22, 04:41 PM	Unas...
Medium	5	BACNet Operation Failed	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	4	BACNet Operation Failed	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	3	BACNet Operation Failed	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...
Medium	2	BACNet Operation Failed	Microsoft Defender ...	01/25/22, 04:40 PM	01/25/22, 04:40 PM	Unas...

Description: Unauthorized Internet Connectivity Detected  
Incident ID: 16  
Investigate in Microsoft Defender for IoT

Owner: Unassigned Status: New Severity: High

Events: N/A Alerts: 1 Bookmarks: 0

Entities (4): 141.81.0.130, 10.200.1.124, HUB-MD4IOT-MST..., 10.200.1.124  
Tactics (1): Initial Access

Last update time: 01/25/22, 04:42 PM Creation time: 01/25/22, 04:42 PM

Entities (4): 141.81.0.130, 10.200.1.124, HUB-MD4IOT-MST..., 10.200.1.124  
Tactics (1): Initial Access

View full details Actions

3. It will take you to this screen to get all the information relative to the incident. This allows analyst to get more details on the entity including what other alerts made up the incident, playbooks to enrich the context of the alert, and comments section to leave details on what the analyst discovered during review or how they came to the determination to dismiss the incident.

Microsoft Azure

Home > Microsoft Sentinel >

Incident

Incident ID 16

Refresh

Unauthorized Internet Connectivity Detected

Incident ID: 16  
Investigate in Microsoft Defender for IoT

Owner: Unassigned Status: New Severity: High

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

Events: N/A Alerts: 1 Bookmarks: 0

Last update time: 01/25/22, 04:42 PM Creation time: 01/25/22, 04:42 PM

Entities (4): 141.81.0.130, 10.200.1.124, HUB-MD4IOT-MST..., 10.200.1.124  
Tactics (1): Initial Access

Timeline content: All Severity: All Tactics: All

Jan 25 4:41 PM Unauthorized Internet Connectivity Detected High | Detected by Microsoft Defender for IoT | Tactics: Initial Access

View playbooks

Unauthorized Internet Connectivity Detected

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

Severity: High Status: New

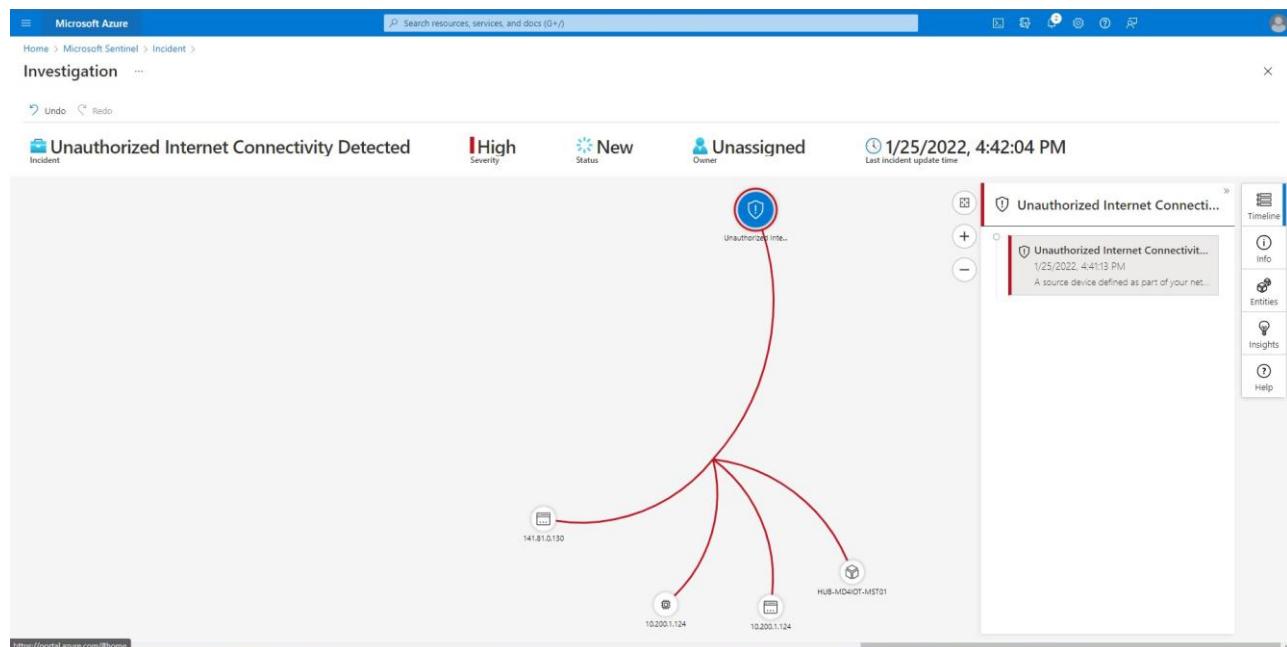
Events: N/A Product name: Microsoft Defender for IoT

Entities (4): 141.81.0.130, 10.200.1.124, HUB-MD4IOT-MST..., 10.200.1.124  
Tactics (1): Initial Access

System alert ID: 741e1606-64de-5f93-8336--  
Last update time: 01/25/22, 04:41 PM Updates: 0  
Start time: 01/25/22, 04:41 PM End time: 01/25/22, 04:41 PM  
Alert link: https://portal.azure.com/#blade/Microsoft\_Azure\_IoT\_Defender/Alert...  
Remediation steps:

Investigate Actions

4. By clicking the **Investigate** button, you can dig deeper in the cause of the incident and the relation to other incidents.



## Task 4: Kusto Query Language to Find Alert Details

1. Navigate to the “Logs” tab and run the queries provided below, and view the results.

The screenshot shows the Microsoft Azure Microsoft Sentinel Logs view. The left sidebar includes 'General' (Overview, Logs selected), 'Threat management' (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence), 'Content management' (Content hub (Preview), Repositories (Preview), Community), and 'Configuration' (Data connectors, Analytics, Watchlist, Automation, Settings). The main area shows a query editor with the following Kusto query:

```
SecurityAlert | where ProviderName contains "IoTSecurity"
```

The 'Run' button is highlighted with a red box. The results table shows 51 records from the last 24 hours. The columns are: TimeGenerated (UTC), DisplayName, AlertName, AlertSeverity, and Description. The results include various events such as 'Unknown Object Sent to Outstation', 'Outstation Restarts Frequently', 'Firmware Change Detected', 'Port Scan Detected', 'Unauthorized Internet Connectivity Detected', 'BACNet Operation Failed', 'Outstation Restarted', 'Controller Stop', and 'EtherNet/IP CIP Service Request Failed'. The 'Description' column provides a brief explanation for each event.

The screenshot shows the Microsoft Defender for IoT Query Editor interface. At the top, there is a search bar with the query: `SecurityAlert | where CompromisedEntity == "hub-md4iot-mst01"`. Below the search bar are various navigation and action buttons: Run, Time range: Last 7 days, Save, Share, New alert rule, Export, Pin to dashboard, and Format query. The main area displays the results of the query, which are listed in a table. The table has columns: TimeGenerated [UTC], DisplayName, AlertName, AlertSeverity, and Description. The results show several alerts from October 1, 2021, including Unauthorized Internet Connectivity Det., BACNet Operation Failed, Controller Stop, and Port Scan Detected, all categorized as High severity.

TimeGenerated [UTC]	DisplayName	AlertName	AlertSeverity	Description
10/1/2021, 4:00:04.420 PM	Unauthorized Internet Connectivity Det...	Unauthorized Internet Connectivity Det...	High	A source devi
10/1/2021, 4:00:04.087 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server retur
10/1/2021, 4:00:07.358 PM	Controller Stop	Controller Stop	Low	The source de
10/1/2021, 4:00:07.445 PM	Port Scan Detected	Port Scan Detected	High	A source devi

## Exercise 6: 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.

The screenshot shows the Microsoft Defender for IoT Getting started page for Sensors. On the left, there is a sidebar with links: General (Getting started, Device inventory (Preview), Alerts (Preview), Recommendations (Preview), Workbooks), Management (Sites and sensors, Plans and pricing, Settings (Preview)), and Troubleshooting + Support (Diagnose and solve problems). The main content area is titled "Sensor" and shows two options: "Buy preconfigured appliance" and "Purchase an appliance and install software". The "Purchase an appliance and install software" section includes a note about version 22.2.9 supporting a new cloud connectivity model. It also provides links for identifying required appliances, installing software, and setting up the network. A dropdown menu for selecting the version is set to "22.2.9 (Latest) - recommended".

### Task 2: Upgrade your sensor

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

The screenshot shows the Microsoft Defender for IoT dashboard. The left sidebar has 'System settings' selected. The main area shows 'Network monitoring' with a 'Sensor management' section. Under 'Updates', there are two options: 'Software Update' and 'Threat Intelligence'. The 'Software Update' box is highlighted with a pink rectangle. Other sections include 'Subscription & Activation Mode', 'Backup & Restore', 'System Health Check', and 'SNMP MIB Monitoring'.

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

This screenshot is identical to the one above, showing the Microsoft Defender for IoT dashboard with the 'System settings' sidebar selected. The 'Software Update' option under 'Updates' is highlighted with a pink rectangle, indicating where to click to upload the ISO file.

3. Verify the version on the dashboard.

The screenshot shows the Microsoft Defender for IoT dashboard with the 'Overview' sidebar selected. At the top, it displays 'Microsoft | VishalnaDema - 22.2.8'. Below this, the 'Discover' section shows 0 PPS, 124 Devices, and 32 Alerts. In the 'General Settings' section, the 'Version:' field is shown as '22.2.8.20-r-3bd7f37', which is highlighted with a pink rectangle.

## Exercise 7: 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.