

Summary

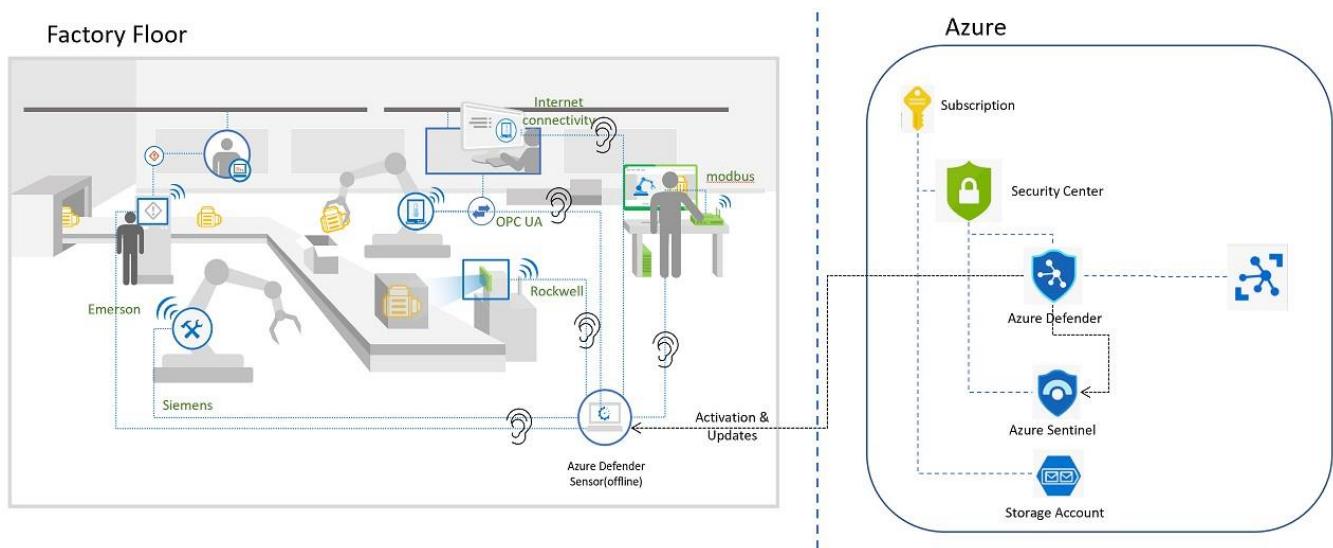
This Hands-on-Lab (HOL) will focus on securing your facilities. We will be simulating traffic by playing some Packet captures, visualizing and analyzing the data on the sensor console. Integrate our sensor with Microsoft Sentinel, to explore alert handling, and for writing queries to help with alert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

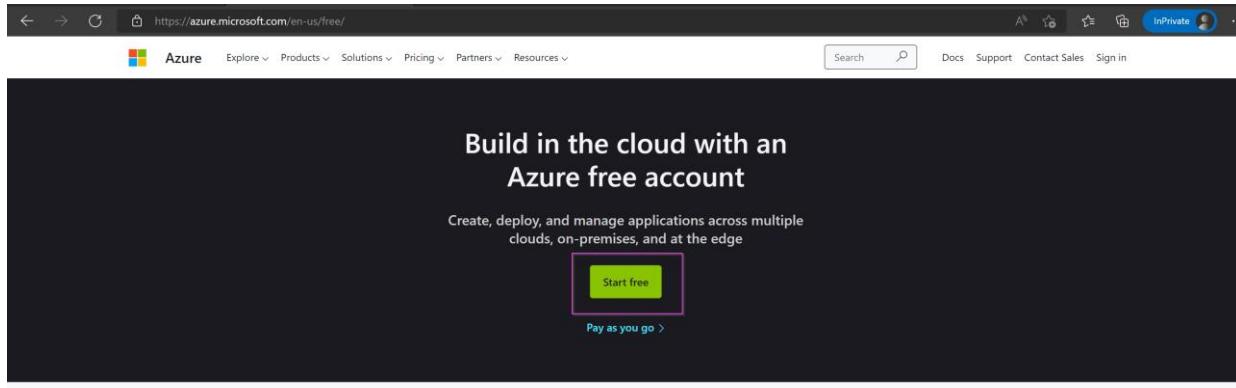
Summary.....	1
!! Since the PDF contains hyperlinks, please download the file before proceeding!!.....	1
Architecture Diagram.....	1
Exercise 1: Enabling Defender	3
Task 1: Create an Azure Subscription	3
Task 2: Enabling Microsoft Defender for IoT on the Subscription.....	4
Exercise 2: Deploy the Sensor in Azure.....	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.....	13
Exercise 3: Perform an Upgrade	19
Task 1: Download the Upgrade ISO file	19
Task 2: Upgrade your sensor.....	19
Exercise 4: Simulate Data in your sensor.....	21
Task 1: Enabling the PCAP Player.....	21
Task 2: Play PCAP files.....	22
Exercise 5: Analyzing the Data	24
Task 1: Visualize on the Device Map.....	24
Task 2: View the associated Alerts	26
Task 3: Device Inventory	28
Task 4: View the Event Timeline	29
Task 5: Data Mining	30
Task 6: Generate a Risk Assessment report.....	31
Exercise 6: Cloud Connect your sensor.....	32
Task 1: Create the cloud connected sensor on the Cloud Management portal	32
Task 2: Upload the activation file to cloud connect your sensor.....	33
Task 3: Verify Cloud connection.....	34
Exercise 7: Integrate with Microsoft Sentinel	35
Task 1: Create a Log Analytics Workspace.....	35
Task 2: Install the Defender for IoT package.....	37
Task 3: Create Incidents.....	39
Task 4: Validate Defender for IoT logs are streamed correctly to Sentinel (KQLS on the data)	40
Task 5: Investigate Defender for IoT incidents	41
Task 6: Investigate further with IoT device entities	43
Task 7: Investigate the alert in Defender for IoT	44
Task 8: Acknowledge Alerts and Re-run PCAPs.....	45
Exercise 8: Automate response to Defender for IoT alerts.....	46
Exercise 9: Clean Up	46
Task 1: Delete resources.....	46

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.

A screenshot of the Microsoft Azure portal. The search bar at the top has "Subs" typed into it. Below the search bar, the "Services" tab is selected in a navigation bar. Under the "Services" section, the "Subscriptions" item is highlighted with a pink rectangle. The main area shows a list of subscriptions and resource groups. At the bottom, there are navigation links for "Subscriptions", "Resource groups", "All resources", and "Dashboard".

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

The screenshot shows the Microsoft Azure Subscriptions page. At the top, there are filter options: 'Subscriptions == global filter', 'My role == all', 'Status == all', and '+ Add filter'. Below the filters, a table lists one subscription: 'Visual Studio Enterprise Subscription' with Subscription ID '21311d18-92b6-4c80-b327-917e1b90517a', My role 'Account admin', Current cost 'CA\$11.29', Secure Score '41%', Parent management group 'None', and Status 'Active'. The 'Visual Studio Enterprise Subscription' row is highlighted with a red box.

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.

The screenshot shows the Microsoft Azure search results for 'Microsoft Defender for IoT'. The search bar at the top contains 'Microsoft Defender for IoT'. Below the search bar, there are tabs for 'All', 'Services (27)', 'Documentation (99+)', 'Azure Active Directory (1)', 'Resources (0)', and 'Resource Groups (0)'. The 'Services' section contains cards for 'Microsoft Defender for IoT' (highlighted with a red box), 'IoT Hub', 'Microsoft Sentinel', 'Form recognizers', and 'Power Platform'. The 'Recent resources' sidebar on the left lists various Azure resources like 'mdfilesmst01', 'rg-md4iot-mst01', etc. The bottom of the screen shows the URL 'https://ms.portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/'.

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

The screenshot shows the 'Defender for IoT | Pricing' page. The top navigation bar includes 'Home > Defender for IoT' and a search bar. Below the navigation, there are sections for 'General' (with 'Getting started', 'Device inventory (Preview)', 'Alerts (Preview)', and 'Workbooks (Preview)'), 'Management' (with 'Sites and sensors', 'Pricing' highlighted with a purple box, and 'Settings (Preview)'), and 'Onboard subscription' (with a button). A message states 'No subscriptions onboarded' and 'Define committed device coverage or work with the trial.' A link to the 'Pricing page' is also present.

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

The screenshot shows the Microsoft Defender for IoT Pricing page. At the top, there's a search bar, refresh button, and a '+ Add plan' button. Below the header, there are sections for General (Getting started, Device inventory (Preview), Alerts (Preview), Workbooks (Preview)) and Management (Sites and sensors). The 'Pricing' section is currently selected. A large central area displays a magnifying glass icon over a document, with the text 'No subscriptions onboarded'. Below this, it says 'Define committed device coverage or work with the trial.' and features a blue 'Onboard subscription' button. A note at the bottom states: 'For more information on Microsoft Defender for IoT pricing, visit the [Pricing page](#)'.

4. In the popup screen, select:

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

The screenshot shows a Microsoft Azure Purchase dialog. On the left, the main interface shows the 'Defender for IoT | Pricing' page with a list of plans. On the right, the 'Purchase' dialog is open. It has sections for 'Payment details' (with a dropdown set to 'Trial') and 'Subscription' (with a dropdown set to 'Customer Intent Terms - Registration'). Below these, a note states: 'Microsoft Defender for IoT provides a 30-day free trial for the first 1,000 committed devices for evaluation purposes.' At the bottom of the dialog, there's a checkbox labeled 'I accept the terms' which is checked. At the very bottom are 'Save' and 'Close' buttons.

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

Exercise 2: Deploy the Sensor in Azure

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

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

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

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

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

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

The screenshot shows the 'Custom deployment' page in the Azure portal. The 'Basics' tab is selected. The 'Template' section shows a 'Customized template' with 4 resources. Below it, the 'Project details' section includes fields for 'Subscription' (BuildEnv), 'Resource group' (Create new), 'Region' (East US), 'Location' ([resourceGroup().location]), 'Deploy Public IP' (true), 'Put Password To Key Vault' (true), 'Source VHDURL' (empty), and 'Sensor Count' (1). Step numbers 1 through 7 are overlaid on the fields: 1 on the Subscription dropdown, 2 on the Resource group dropdown, 3 on the Region dropdown, 4 on the Location field, 5 on the Deploy Public IP dropdown, 6 on the Put Password To Key Vault dropdown, and 7 on the Source VHDURL field.

- 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-b168-5c8887ada956

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:vgrosh

Resources Recommendations

Name	Type	Location
customxx245p7rgp02	Storage account	West US
SOC_Kv245p7rgp2_Pay	Key vault	West US
SOC_NS0d24kpt7ngp2_Pay	Network security group	West US
SOC_minsteny24kpt7ngp2_Pay	Managed identity	West US
SOC_m24kpt7ngp2_Pay-image	Image	West US
SOC_vmr24kpt7ngp2_Pay-red10	Regular Network Interface	West US
SOC_wmz24kpt7ngp2_Pay-pg0	Public IP Address	West US
SOC_wmz24kpt7ngp2_Pay-pg02	Virtual machine	West US
SOC_wmz24kpt7ngp2_Pay-disk1	Disk	West US
SOC_vnres24kpt7ngp2_Pay	Virtual network	West US

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

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

SOC-KVuq63gjmwvo2do-Play | Access policies

Key vault | Directory: Microsoft

+ Create Refresh Delete Edit

Search Permissions : All Type : All

Showing 1 to 1 of 1 records.

Name Email Key Permissions

APPLICATION

SOC-vmsidentityuq63gjmwvo2do-Play

Events

Objects

Keys

Secrets

Certificates

Settings

Access configuration

Networking

Microsoft Defender for Cloud

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

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

Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

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

Configure from a template

Key & Secret Management

Key permissions

Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore

Cryptographic Operations

Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign

Secret permissions

Select all
Get
List
Set
Delete
Recover
Backup
Restore

Privileged Secret Operations

Select all
Purge

Certificate permissions

Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities

Privileged Certificate Operations

Select all

Previous Next

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-abf6aa26fceeb0b34bd9-e88b-46f0-adf8-c7ce00a9954

Selected item

No item selected

Previous

Next

7. Click on "Create".

Home > Resource groups > KeyVaultTest > SOC-KVuq63gjmwv02do-Play | Access policies >

Create an access policy ...

SOC-KVuq63gjmwv02do-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

Overview + Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export template Open in mobile

Essentials

Subscription (main) : BuildEnv Deployment : 2 Failed 10 Succeeded

Subscription ID : 1c61ccbf-70b1-45a3-a1fb-84fc446d70a6 Location : West US

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

Resources Recommendations

Showing 1 to 10 of 10 records. Show hidden types Add filter

Type	Location	Actions
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	...
Virtual machine	West US	...
Disk	West US	...

9. Make a note of the Public IP address.

SOC Virtual machine

-Play

Essentials

- 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

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

Networking

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

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

Overview

We'd love your feedback! →

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
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

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

Home > Microsoft.Template-20220630145822 > Reset-password0

Reset-password0 | Outputs

Deployment

Outputs

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

Copied

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

The screenshot shows the 'Overview' tab for a deployment named 'Microsoft.Template-20220630145822'. The status is 'Your deployment is complete'. Deployment details include a start time of 6/30/2022, 2:58:25 PM, and a correlation ID of ac55ba5c-e35a-4a36-b3ee-37b01fcdb2f. The table lists four resources: 'Reset-password', 'Post-Deploy0', 'VMdeployment', and 'copyvhd', all in 'OK' status. A 'Next steps' section contains a 'Go to resource group' button.

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

The screenshot shows the 'Overview' page for a resource group named 'XXX'. It displays deployment statistics (13 succeeded) and a list of resources. The 'Resources' section shows a table with columns: Name, Type, and Location. One row for a 'Virtual machine' named 'SOC-vmficiwieu5atkwu-Play' is highlighted with a red border.

Name	Type	Location
SOC-vmficiwieu5atkwu-Play	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 has sections like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main content area shows the 'Essentials' tab with details such as Resource group, Status (Running), Location (East US), Subscription, Subscription ID, and Tags. The 'Properties' tab is selected, showing the Virtual machine section with Computer name (Sensor), Operating system (Linux (ubuntu 18.04)), Publisher, Offer, and Plan. The Networking section is also visible, highlighting the Public IP address (20.124.23.178) and Private IP address (10.10.10.4). Buttons for Connect, Start, Stop, Capture, Delete, Refresh, Open in mobile, CLI / PS, and Feedback are at the top.

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 address bar displaying 'Not secure | https://xxx.xxx.xxx.xxx /login'. The main content is a login form titled 'Sensor Sign in' for 'Microsoft | Defender for IoT sensor'. It has fields for 'User name' and 'Password', and links for 'Forgot password? (for admin users only)' and 'Reset'. A 'Login' button is at the bottom. The background of the browser window is light grey.

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 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

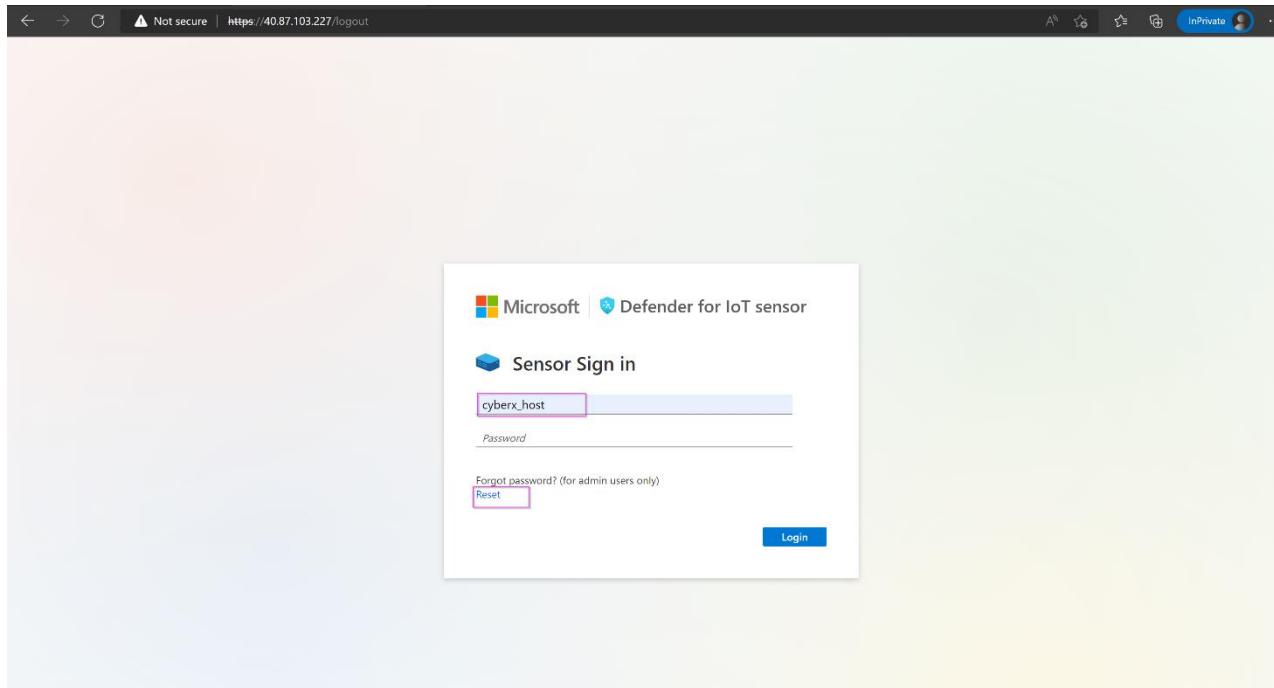
Recover

Insert secret identifier *

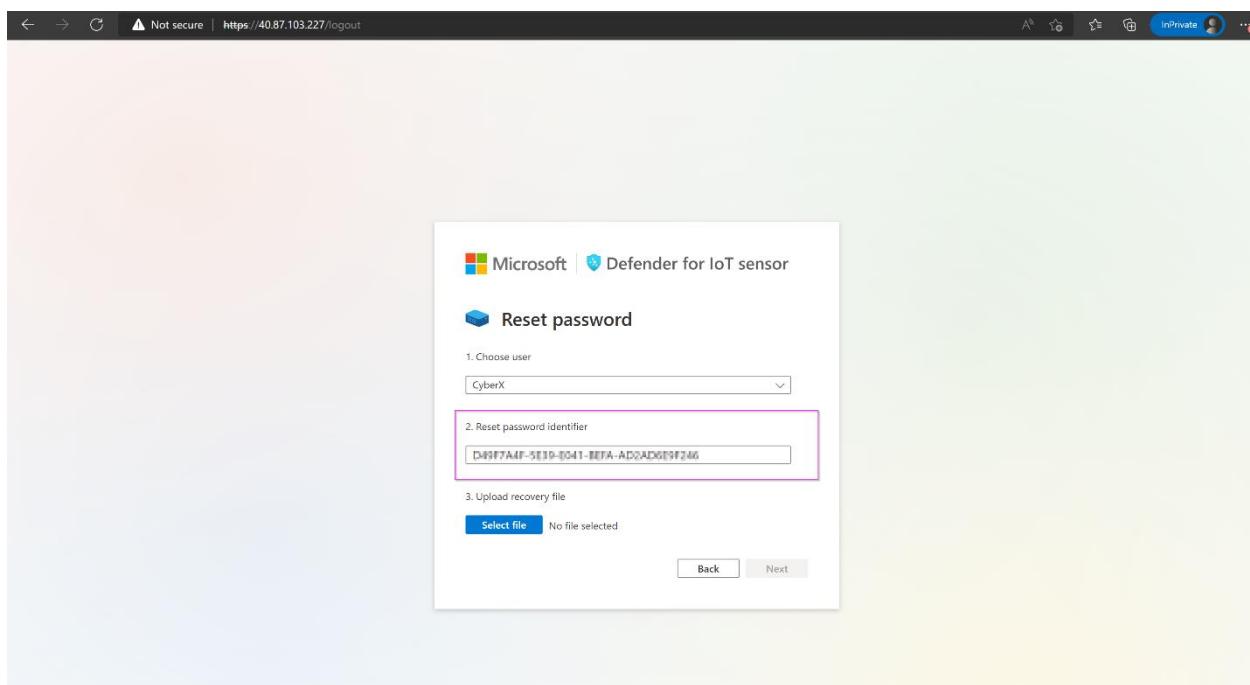
Sub0001-777-0e57-88h12

Recover Cancel

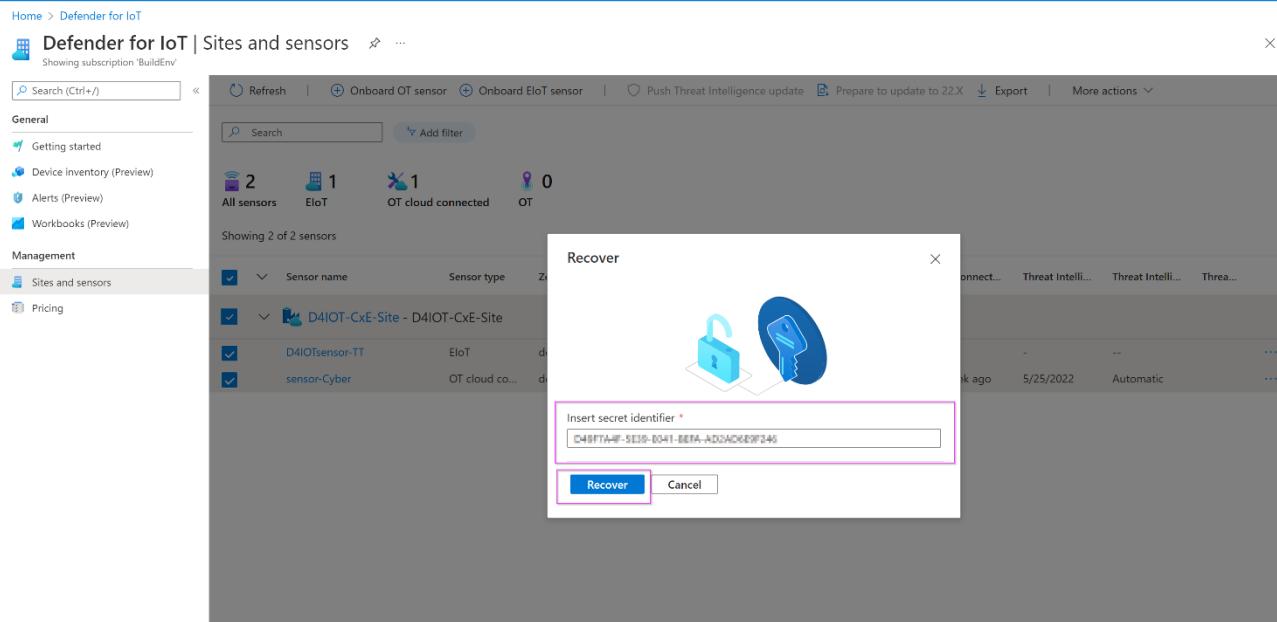
7. Return to the sensor console and type in the username followed by "Reset" as shown.



8. Copy the identifier.

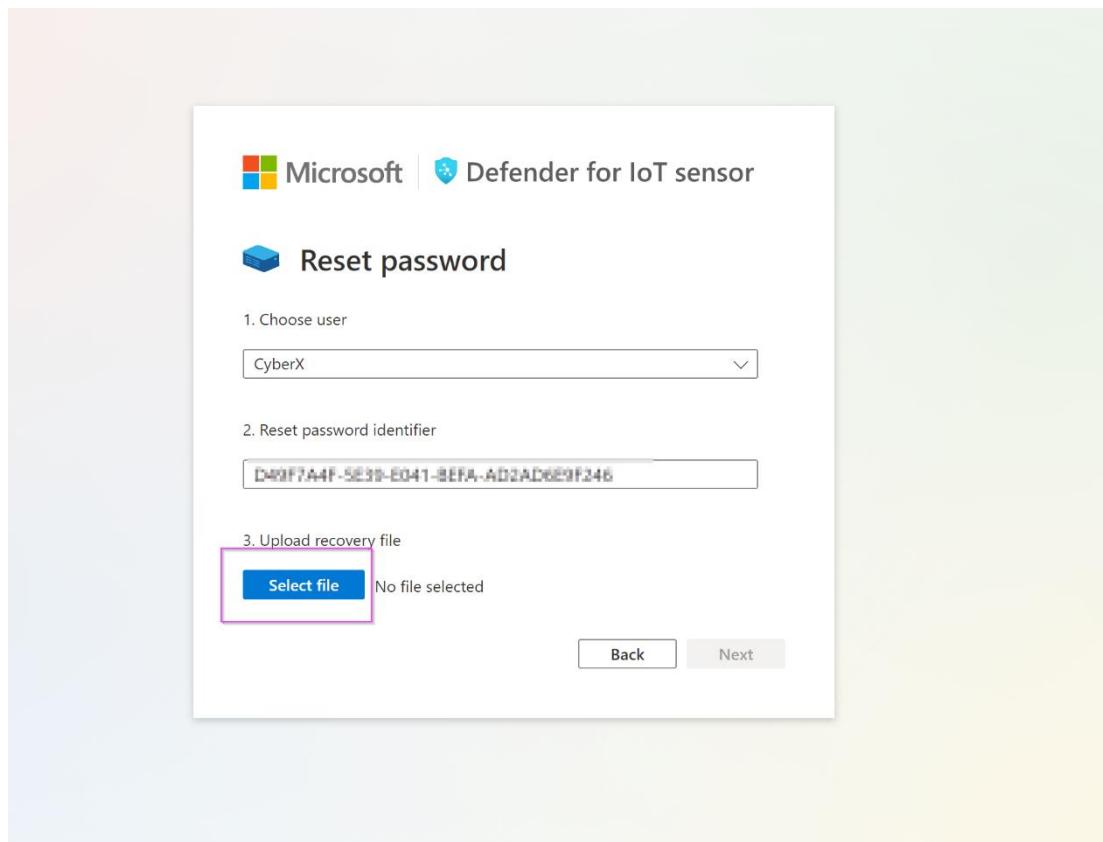


9. Paste in the box on the Defender for IoT Azure window. Click "**Recover**".



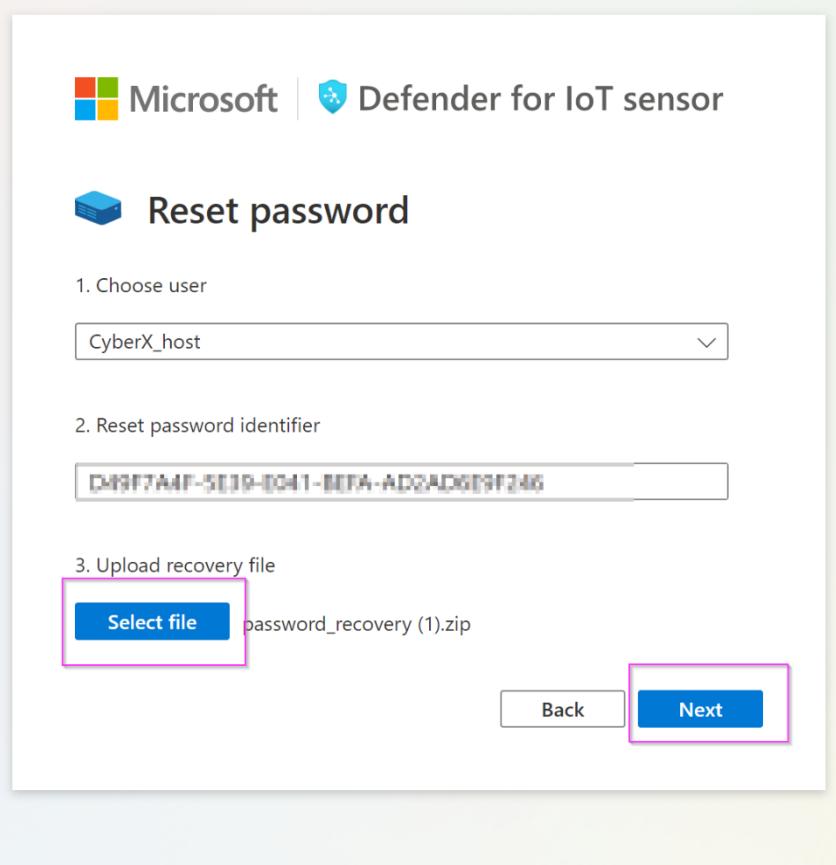
The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with 'General' and 'Management' sections. Under 'Management', 'Sites and sensors' is selected. The main area displays sensor statistics: 2 All sensors, 1 EIoT, 1 OT cloud connected, and 0 OT. Below 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 over the main content. It features a lock icon and a keyhole icon. Inside the modal, there's a text input field with the placeholder 'Insert secret identifier' containing the value 'D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246'. At the bottom of the modal are two buttons: 'Recover' (highlighted with a pink border) and 'Cancel'.

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 a 'Reset password' wizard window. It has three steps: 1. Choose user (dropdown menu set to 'CyberX'), 2. Reset password identifier (input field containing 'D49F7A4F-5E39-E041-BEFA-AD2AD6E9F246'), and 3. Upload recovery file (button labeled 'Select file' highlighted with a pink border, and text 'No file selected'). At the bottom are 'Back' and 'Next' buttons.

11. Click on “**Next**”.



Microsoft | Defender for IoT sensor

Reset password

1. Choose user

CyberX_host

2. Reset password identifier

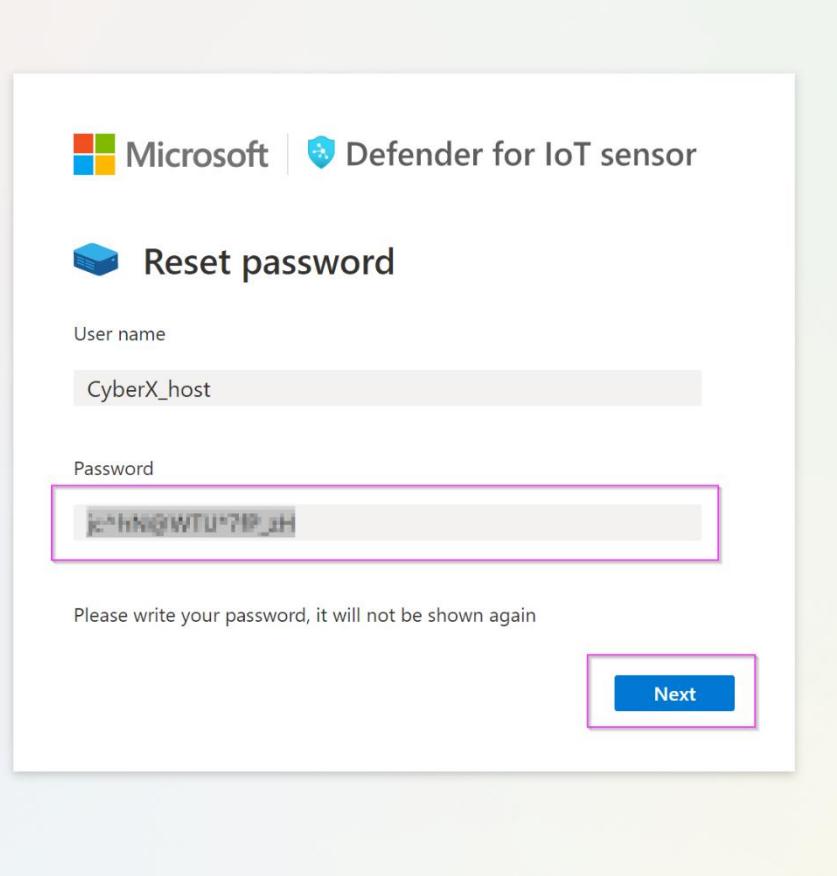
D9F7A4F-5E19-0411-BFA-AD2AD619F246

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.



Microsoft | Defender for IoT sensor

Reset password

User name

CyberX_host

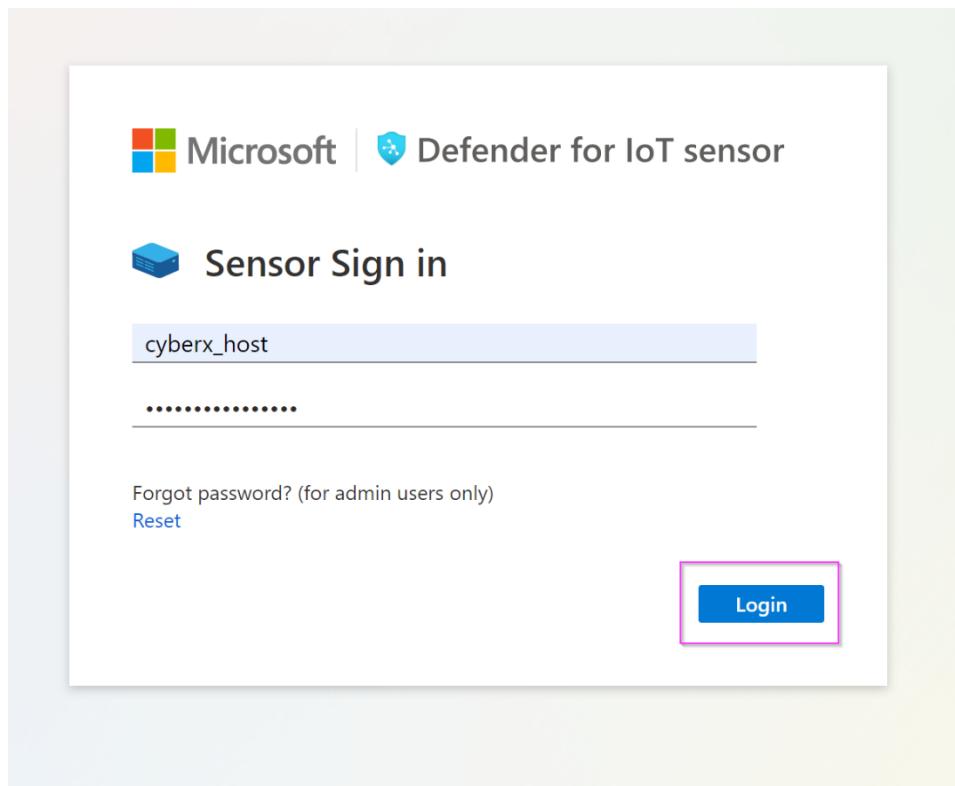
Password

j^<hn@WTU*7IP_jH

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".

The screenshot shows the Microsoft Defender for IoT dashboard. On the left, there's a navigation sidebar with sections like Discover, Analyze, and Manage. Under Manage, the 'System settings' option is selected and highlighted with a pink box. In the main content area, under 'Updates', there are two options: 'Software Update' and 'Threat Intelligence'. Both are shown in boxes with a pink border. Below them, under 'Security', is a box for 'Subscription & Activation Mode'. Under 'Health and troubleshooting', there are three boxes: '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' section selected. The 'Software Update' option under 'Updates' is highlighted with a pink box. The rest of the interface, including other update options and security features, remains the same.

3. Verify the version on the dashboard.

The screenshot shows the Microsoft Defender for IoT dashboard with the 'Overview' section selected. At the top, it displays 'Microsoft | vishalvadher - 22.2.8'. Below this, there are summary metrics: 0 PPS, 124 Devices, and 32 Alerts. Under 'General Settings', it shows the 'Version:' field containing '22.2.8.20-r-3bd7f37', which is also highlighted with a pink box. The left sidebar has the 'Overview' option selected.

Exercise 4: Simulate Data in your sensor.

Task 1: Enabling the PCAP Player

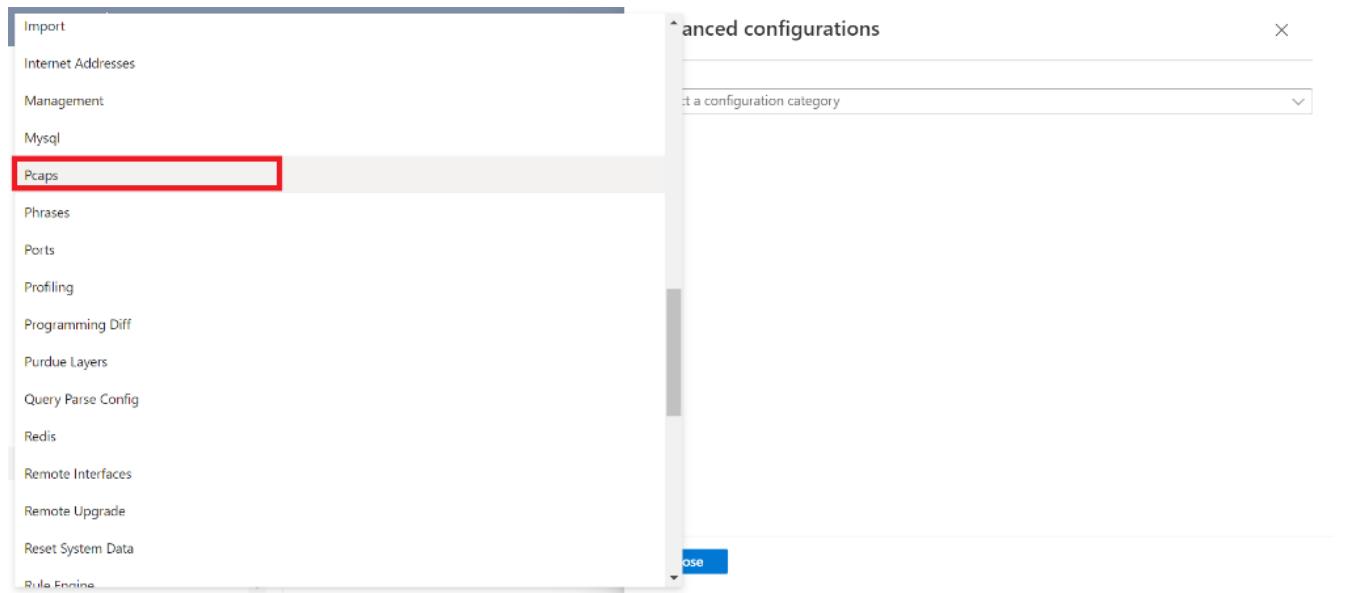
1. The PCAP player needs to be enabled to be visibly available for use in the UI. To do so, please select the "**System settings**" option from the scrolled down left side menu.

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 'Basic' under 'Sensor Setup' and contains four cards: '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 'Health and troubleshooting' and contains four cards: 'Backup & Restore', 'System Health Check', 'SNMP MIB Monitoring', and 'Advanced Configurations', which 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 shows 'Home > System settings'. Under 'System settings', 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', and 'Attack vector' are listed. 'System settings' is selected. In the center, there are sections for 'Backup data and restore the latest backup' and 'SNMP MIB Monitoring'. To the right, a modal window titled 'Advanced configurations' for 'Pcaps' is open, showing configuration settings. A red box highlights the 'enabled' variable, which is currently set to 0. Below it, the 'Save' button is also highlighted with a red box. At the bottom of the modal, there are 'Save' and 'Close' 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 System settings interface. On the left, there's a navigation sidebar with sections like Analyze (Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector) and Manage (System settings, Custom alert rules, Users, Forwarding). The 'System settings' option is selected. In the main content area, there are several cards: 'SSL/TLS Certificate' (Manage SSL/TLS certificates), 'Play PCAP' (Upload and play PCAP files, highlighted with a red box), 'Network monitoring', 'Sensor management' (highlighted with a red box), 'Integrations', and 'Import settings'. A vertical scrollbar is visible on the right side of the main content area.

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

The screenshot shows the Microsoft Defender for IoT System settings interface again. The 'System settings' section is selected in the sidebar. A file upload dialog box is open in the center, showing a list of pcap files in a folder named 'holpcaps'. The files listed are: 1-S7comm-VarService-Read-DB1DBD0, 2-S7comm-VarService-CyclicData-1s, 3-S7comm-VAT_MB100_MW200_MD300_M400-0, 4-S7comm-Download-DB1-with-password-req..., Advantech, BACnetARRAY-element-0, BACnetARRAY-elements, BACnet-BBMD-on-same-subnet, BACnet-exception-schedule-property-1, and BACnet-movement-schedule-property-1. The 'File name:' dropdown shows '1-S7comm-VarService-Read-DB1DBD0'. Below the dialog, there are cards for 'Software Update' and 'Threat Intelligence'. A 'Close' button is at the bottom right of the dialog.

5. Click “Play All” to play the Pcaps.

The screenshot shows the Microsoft Defender for IoT web interface. The left sidebar is titled 'Defender for IoT' and includes sections for Discover, Analyze, Manage, and Support. Under 'Discover', 'Device map' is highlighted with a pink box. The main content area shows several cards under 'Sensor Setup': 'Sensor Network Settings', 'Connection to Management Console', 'Time & Region', 'SSL/TLS Certificate', 'Play PCAP', and 'Network monitoring'. Below this, under 'Sensor management', there are 'Software Update' and 'Threat Intelligence' cards. On the right side, there is a 'PCAP PLAYER' section with a 'Play All' button highlighted with a pink box.

Exercise 5: Analyzing the Data

Task 1: Visualize on the Device Map

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

The screenshot shows the 'Device map' page. The left sidebar has 'Device map' selected. The main area features a network visualization with nodes represented by icons like servers, databases, and clouds, connected by lines indicating their relationships. There are also some red dots scattered across the map. On the right side, there are several control buttons for zooming and filtering the map view.

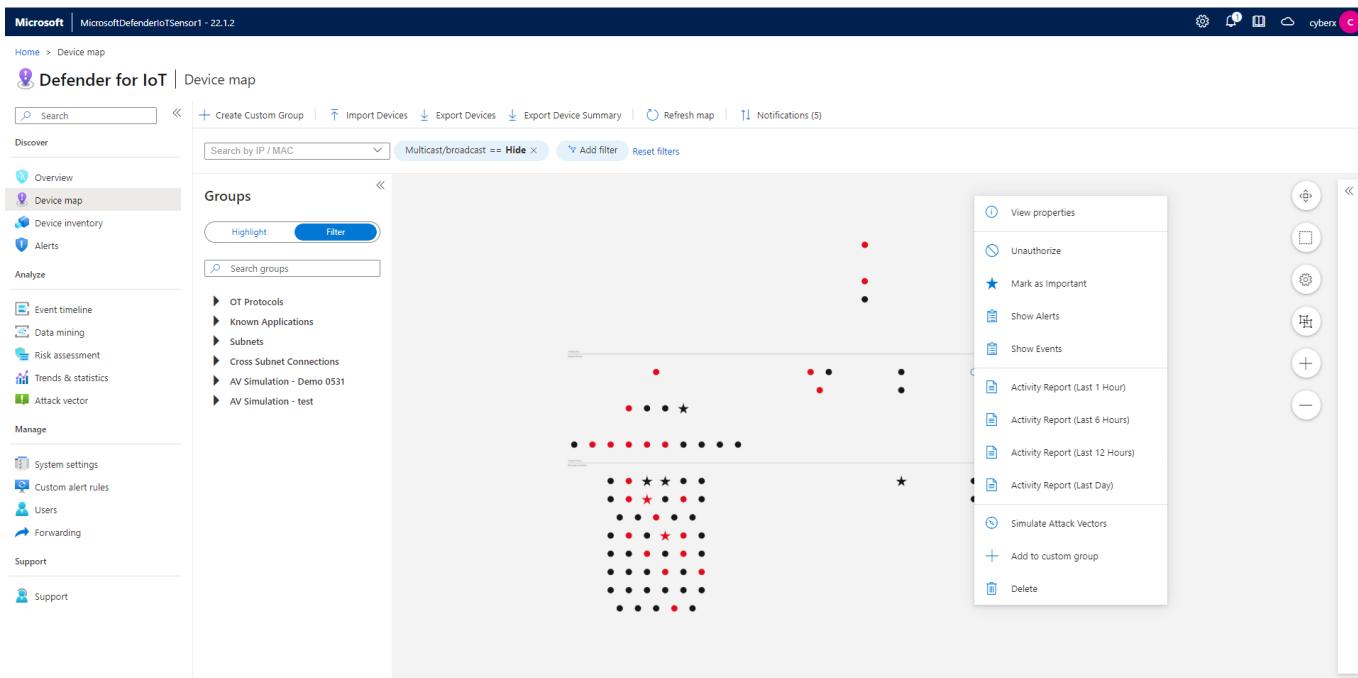
2. Click on the “Settings” option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.

The screenshot shows the Microsoft Defender for IoT Device map interface. On the left, there's a navigation sidebar with sections like Discover, Overview, Device map (which is selected), Device inventory, Alerts, Analyze, Manage, and Support. The main area displays a network graph where nodes represent devices and connections between them. A context menu is open in the top right corner, listing options: Pin Layout, Layout by Connections, and Layout by Purdue. The 'Layout by Purdue' option is highlighted with a pink box.

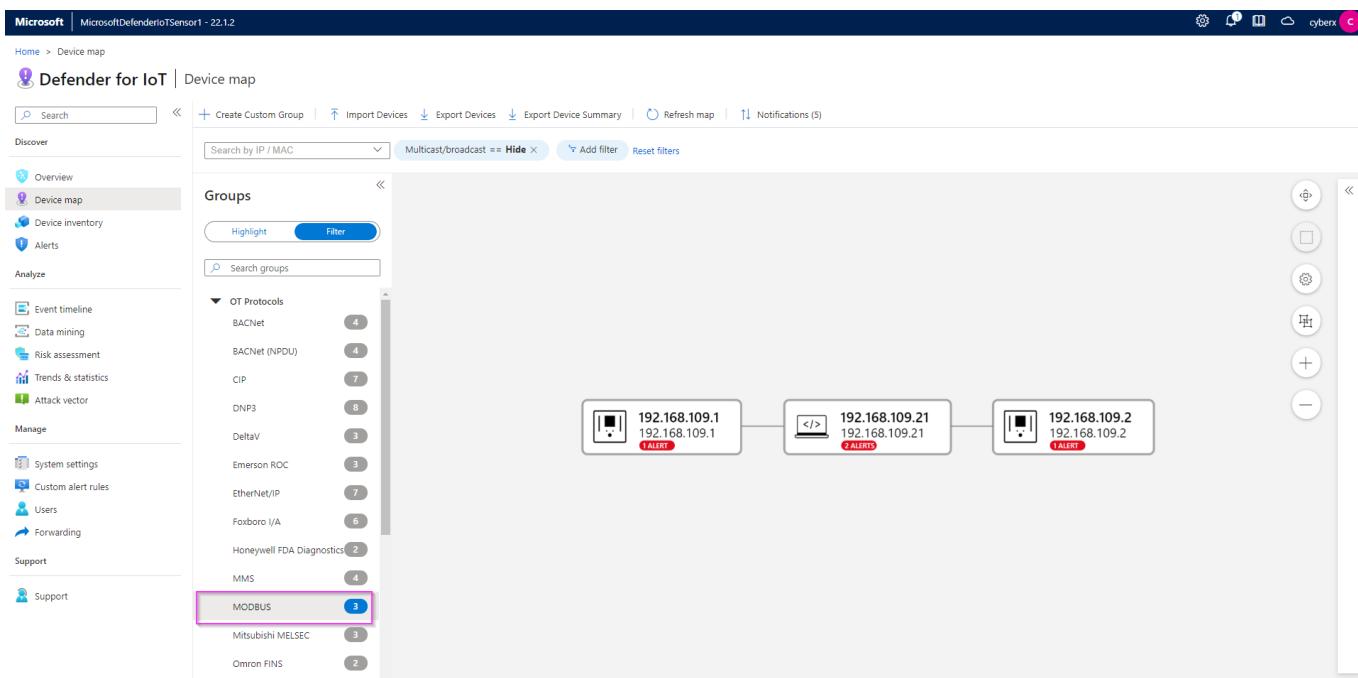
3. Once you confirm the changes, you will see the devices laid out as shown in the image below.

This screenshot shows the same Microsoft Defender for IoT Device map interface after applying the 'Layout by Purdue' option. The network graph now displays the devices in a more organized, grid-based layout, reflecting the structural changes made by the algorithm. The rest of the interface, including the sidebar and top navigation, remains the same as in the previous screenshot.

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

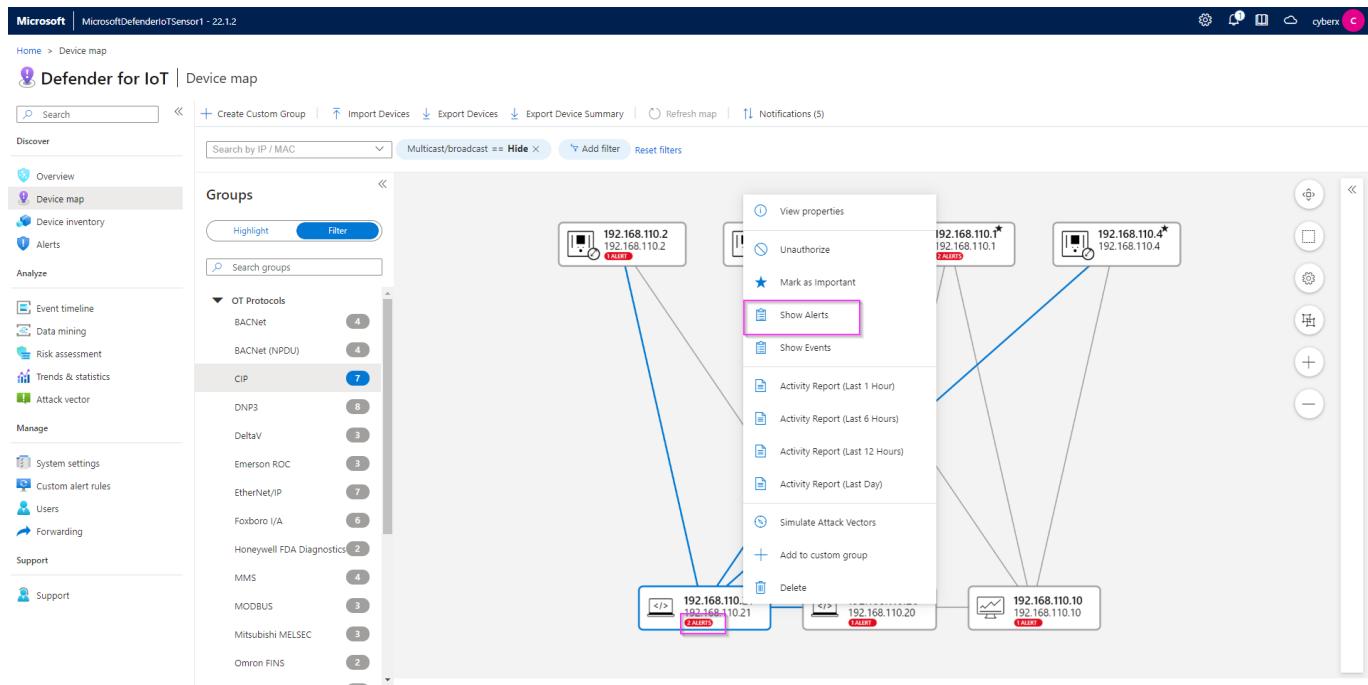


5.To filter by OT Protocols, expand the arrow, and pick the protocol you want to filter by. The console will display the devices that match the filter.



Task 2: View the associated Alerts

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



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

The screenshot shows the Device details page for device 192.168.110.21. The 'Alerts' tab is selected, displaying a list of alerts:

Severity	Name	Engine	Detection time	Status	Source Device
Critical	Unauthorized Internet Connectivity Detected	Policy Violation	2 weeks ago	New	192.168.110.21
Major	EtherNet/IP Encapsulation Protocol Command Failed	Operational	2 months ago	New	192.168.110.2

The 'Protocols' section is highlighted with a pink box.

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”.

The screenshot shows the Microsoft Defender for IoT interface. On the left, a sidebar menu has the 'Alerts' option highlighted with a red box. The main area displays a table of alerts. The first alert is for 'Unauthorized Internet Connectivity Detected' with a severity of 'Critical'. The second alert is also for 'Unauthorized Internet Connectivity Detected' with a severity of 'Critical'. Both alerts were detected 2 weeks ago and are marked as 'New'. A detailed view of the first alert is shown on the right, including its description, related devices, and 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.

This screenshot shows the same Microsoft Defender for IoT interface, but the 'Group by' dropdown in the top right corner is set to 'Source Device'. The table now lists alerts grouped by their source device IP address. There are 22 alerts in total, mostly categorized as 'New' or 'Closed'. The 'Alerts' option in the sidebar is again highlighted with a red box.

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
<input type="checkbox"/>	192.168.100.8	192.168.100.8	50 minutes ago	Unknown	DNS, MDNS, Net...	54:14:f3:74:d8:21	INTEL CORPORA...					
<input type="checkbox"/>	192.168.100.1	192.168.100.1	50 minutes ago	Server	DNS							
<input type="checkbox"/>	192.168.1.11	192.168.1.11	50 minutes ago	PLC	Siemens S7	00:0fb5:4d1bef:3	NETGEAR					
<input type="checkbox"/>	192.168.1.180	192.168.1.180	50 minutes ago	HMI	Siemens S7							
<input type="checkbox"/>	192.168.117.23	192.168.117.23	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:92:c6	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	00:23:ea:49:8ac2	CISCO SYSTEMS ...					
<input type="checkbox"/>	192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:97:c0	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	00:0cc1:02:09:da	EATON CORPOR...					
<input type="checkbox"/>	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)			
<input type="checkbox"/>	192.168.117.239	192.168.117.239	22 hours ago	Unknown	Siemens SICAM	00:0c:29:28:28:38	VMWARE INC.					
<input type="checkbox"/>	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)			
<input type="checkbox"/>	192.168.107.10	FCS0507	22 hours ago	DCS Controller	Yokogawa VNet/IP	00:00:64:9d:5d:10	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9d:73:d4	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9e:84:e5	YOKOGAWA DIG...					
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	

Load More...

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

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...	54:14:f3:74:d8:21	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	00:0fb5:4d1bef:3	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...)	00:30:a7:08:92:c6	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	00:23:ea:49:8ac2	CISCO SYSTEMS ...					
<input type="checkbox"/>	192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:97:c0	SCHWEITZER EN...					
<input type="checkbox"/>	192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	00:0cc1:02:09:da	EATON CORPOR...					
<input type="checkbox"/>	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)			
<input type="checkbox"/>	192.168.117.239	192.168.117.239	22 hours ago	Unknown	Siemens SICAM	00:0c:29:28:28:38	VMWARE INC.					
<input type="checkbox"/>	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)			
<input type="checkbox"/>	192.168.107.10	FCS0507	22 hours ago	DCS Controller	Yokogawa VNet/IP	00:00:64:9d:5d:10	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9d:73:d4	YOKOGAWA DIG...					
<input type="checkbox"/>	192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9e:84:e5	YOKOGAWA DIG...					
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	
<input type="checkbox"/>	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	

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".

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with various sections like Overview, Device map, Device inventory, Alerts, Analyze, Manage, Support, and Help. The 'Event timeline' section is currently selected. The main area displays a table of events with columns for Event type, Time, and Description. Some events include icons such as a device, a gear, or a lock.

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

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' section selected. On the left, there's a navigation sidebar. The main area shows a 'Create new report' wizard with fields for Name, Description, and Category. It also includes filters for IP address, MAC address, Port, and Device group. Below this, there's a 'Recommended' section with cards for Programming Commands, Internet Activity, Excluded CVEs, Remote Access, CVEs, and Non Active Devices (Last 7 Days). A 'My reports' section lists existing reports with names like 'ALL' and 'test'.

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

Create new report

Name *

Description

PLC Firmware Version Report showing the firmware version of the different PLCs.

Choose Category

Order by

Filter by

Results within the last Minutes +

IP address

MAC address

Port

Device group

Firmware Version (GENERIC)

+ Add filter type

Save Cancel

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

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.

Defender for IoT | Data mining

Refresh Expand all Collapse all Export to CSV Export to PDF Snapshots Manage report Edit mode

PLC Firmware Version

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.

The screenshot shows the Microsoft Defender for IoT Risk assessment interface. On the left, there's a navigation sidebar with sections like Discover, Analyze, and Manage. Under Analyze, the 'Risk assessment' option is selected and highlighted with a pink box. In the main content area, there's a 'Reports list' table with four entries. The first entry, 'risk-assessment-report-4.pdf', is also highlighted with a pink box. A 'Generate report' button is located above the table.

#	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 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 Defender for IoT Sites and sensors page. The left sidebar has sections like General, Management, and Pricing, with 'Sites and sensors' selected and highlighted with a pink box. The main area displays a summary of sensor counts: All sensors (4), EIoT (1), OT cloud connected (2), and OT (1). Below this, a table lists four sensors, both locally managed and cloud connected.

Sensor name	Sensor type	Zone	Subscription ...	Sensor version	Sensor status	Last connect...	Threat Intelli...	Threat Intelli...
D4IOT-CxE-Site - D4IOT-CxE-Site	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".

Step 3: Register this sensor with Microsoft Defender for IoT

Sensor name *

Subscription * Please select a subscription
Onboard subscription

Cloud connected ⓘ

Automatic Threat Intelligence updates

Sensor version * 22.X and above

Site *

- Resource name *** No subscription has been selected
Create site
- Display name ***
- Tags** Key : Value

Zone * No subscription has been selected
Create zone

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

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

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

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

Sensor management

Updates

- Software Update** Update the software version on this sensor
- Threat Intelligence** Update the threat intelligence package on this sensor

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

Security

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.

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

The screenshot shows the Microsoft Defender for IoT Sensor Management interface. On the left, there's a sidebar with categories like Discover, Analyze, and Manage. The main area has sections for Updates (Software Update, Threat Intelligence), Security (Subscription & Activation Mode), Health and troubleshooting (Backup & Restore, System Health Check). A right-hand panel titled 'Subscription & Activation Mode' displays activation status: Activation Mode is 'Cloud Connected', Activation Status is 'Active', Tenant ID is '5f1d60f2-d8a4-4f50-bf0c-1dd1813604a4b', and Subscription ID is '1cb61ccdf1-70d3-4fa3-a7fb-848ca65cd0a6'. There's a button to 'Upload activation file'.

Task 3: Verify Cloud connection

1. On the sensor console.

The screenshot shows the Microsoft Defender for IoT Overview page. It features a summary section with metrics: 0 PPS, 64 Devices, and 21 Alerts. Below this are four cards: General Settings (Version 22.1.3.4162, Threat Intelligence Version 2022.07.12, Connectivity type Cloud connected, Activation Valid, Certificate Valid), Traffic Monitoring (No chart to show), Top 5 OT Protocols, and Traffic By Port. The left sidebar mirrors the one from the previous screenshot.

2. On the Cloud management console.

Defender for IoT | Sites and sensors

Showing subscription 'BuildEnv'

General

Management

Sites and sensors

Pricing

Search (Ctrl+ /) Refresh Onboard OT sensor Onboard IoT sensor Push Threat Intelligence update Prepare to update to 22.X Export More actions

trial subscription "BuildEnv" expired. Please contact Microsoft sales.

4 1 2 1

All sensors IoT OT cloud connected OT

Showing 4 of 4 sensors

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

Exercise 7: Integrate with Microsoft Sentinel

Task 1: Create a Log Analytics Workspace

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

Microsoft Azure (Preview) Report a bug

Microsoft Sentinel

All Services Resources Marketplace Documentation Azure Active Directory (31)

Resource Groups (0)

Services

- Microsoft Sentinel** Resource type: microsoft.security/microsoftsentinel
- Microsoft Defender EASM
- Microsoft Purview accounts
- Microsoft Defender for Cloud

Resources

- Microsoft Sentinel Deployment and Migration
- Demo Microsoft Sentinel
- Advanced KQL for Microsoft Sentinel
- Advanced KQL for Microsoft Sentinel
- Marketplace
- SOC 24x7 Monitoring with Microsoft Sentinel
- Sentinel360 MDR & Managed Microsoft Sentinel
- NC Protect Data Connector for Microsoft Sentinel
- Microsoft Sentinel for SQL PaaS [Preview]
- Documentation
- What is Microsoft Sentinel? | Microsoft Docs
- Microsoft Sentinel documentation | Microsoft Docs
- Plan costs for Microsoft Sentinel | Microsoft Docs
- Commonly used Microsoft Sentinel workbooks | Microsoft Docs
- Continue searching in Azure Active Directory

Tools

Microsoft Learn Azure Monitor Microsoft Defender for Cloud Cost Management

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

3. 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
	Create new

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, there's 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. To the right, a detailed view of the "Microsoft Defender for IoT" solution is shown, 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. Below the form, there's a note about operational technology (OT) infrastructure and a section for "Underlying Microsoft Technologies used".

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 navigation sidebar with sections like Threat management, Content management, and Configuration. The Configuration section has a pink box around the 'Data connectors' link. In the main content area, there's a summary bar with icons for Logs (126), News & guides, and Search. Below it, the 'Data connectors' section shows 1 Connected item: Microsoft Defender for IoT by Microsoft. There are filters for Status (All), Providers (All), Data Types (All), and Status (Connected). A search bar at the top of the main area allows searching by name or provider.

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

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			

Description
Gain insights into your IoT security by connecting Microsoft Defender for IoT alerts to Microsoft Sentinel. You can get out-of-the-box alert metrics and data, including alert trends, top alerts, and alert breakdown by severity. You can also get information about the recommendations provided for your IoT hubs including top recommendations and recommendations by severity.

Last data received
--

Content source ⓘ IoT Threat Monitoring with Defender for IoT

Version 1.0.0 Author Microsoft

Supported by Microsoft Corporation | Email

[Open connector page](#)

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 displays three counts: 917 Open incidents, 917 New incidents, and 0 Active incidents. Below these are filters for Severity (All), Status (2 selected), and a search bar. A prominent red box highlights the 'Product name' filter dropdown. The dropdown shows several options, with 'Microsoft Defender for IoT' checked. Other options 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 dropdown are 'OK' and 'Cancel' buttons. To the right of the dropdown, a message says 'No incidents selected' and 'Select an incident to view more details'. The overall interface is clean with a light blue and white color scheme.

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.

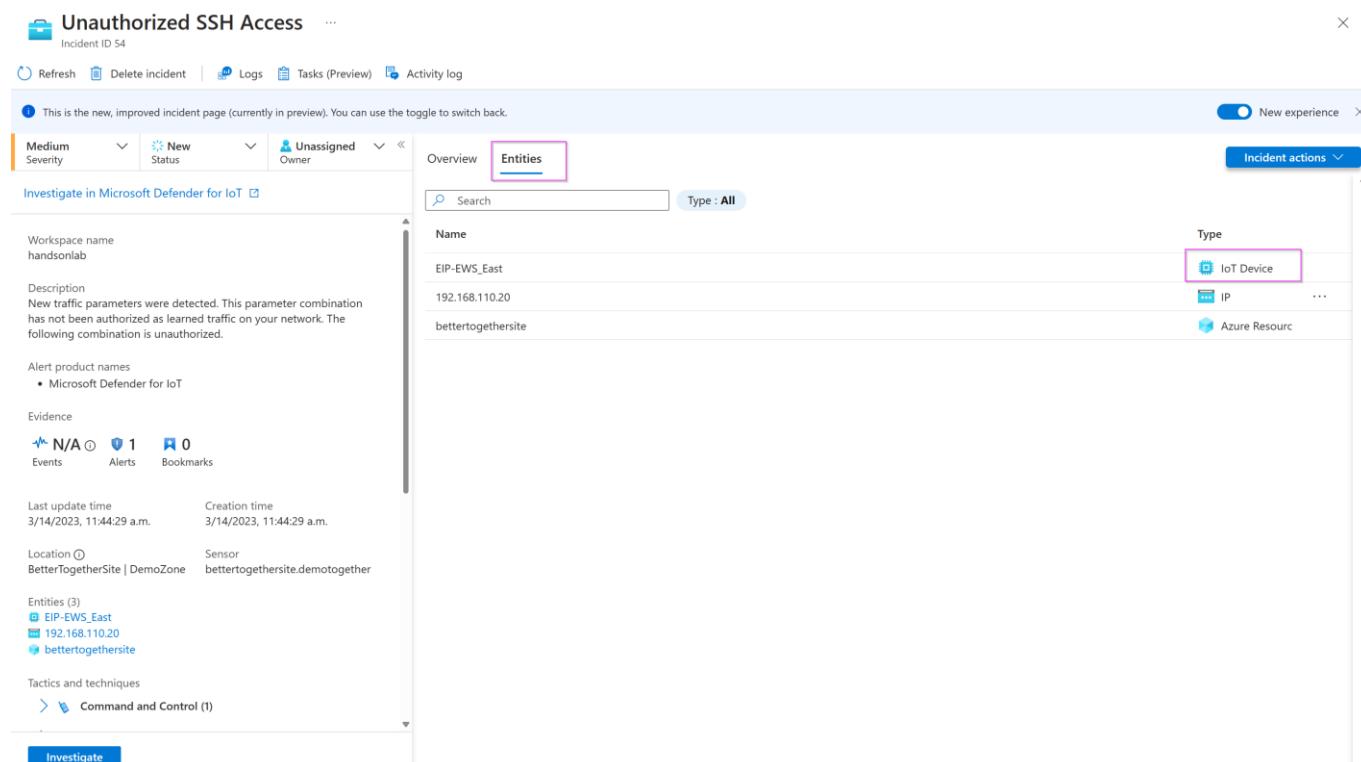
This screenshot shows the Microsoft Sentinel Incidents page with the 'Incidents' section selected from the sidebar. The main grid shows 676 Open incidents, 676 New incidents, and 0 Active incidents. The 'Product name' filter is set to 'Microsoft Defender for IoT'. The incident details pane on the right is open for an incident with ID 107793, titled 'Malicious Domain Name Request'. The pane includes sections for Description, Alert product names, Evidence, Last update time, Entities, Tactics and techniques, Incident workbook, and Incident Overview. It also features 'View full details' and 'Actions' buttons at the bottom. The entire incident details pane is highlighted with a large red box.

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 incident titled "Unauthorized SSH Access" (Incident ID 54). The page has tabs for Overview and Entities, with Entities selected. A search bar and a Type filter set to All are visible. The main content area displays a table of entities with columns for Name, Type, and additional actions. The first entity, "EIP-EWS_East", is highlighted with a pink box. Other entities listed include "192.168.110.20" and "bettertogethersite". The page also includes sections for Evidence (Events: N/A, Alerts: 1, Bookmarks: 0), Last update time (3/14/2023, 11:44:29 a.m.), Creation time (3/14/2023, 11:44:29 a.m.), Location (BetterTogetherSite | DemoZone, Sensor: bettertogethersite.demotogether), and Entities (3) with links to EIP-EWS_East, 192.168.110.20, and bettertogethersite. A Tactics and techniques section is also present.

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 navigation sidebar includes sections for General, Threat management, Content management, and Configuration. The 'Entity behavior' section is highlighted with a red box. The main area displays several cards with alert statistics:

- Accounts by # of alerts:** No data to display.
- Hosts by # of alerts:** 192.168.112.30 (1 alert).
- IPs by # of alerts (Preview):**

IP Address	Alert Count
192.168.1.1	162
192.168.2.2	160
10.0.100.104	22
10.35.1.237	22
10.240.43.147	19
- IoT devices by # of alerts (Preview):**

Device	Alert Count
192.168.1.1	96
192.168.2.2	96
10.0.100.104	10
10.240.5.95	9
10.240.43.147	8
- Azure resources by # of alerts (Preview):**

Resource	Alert Count
guy-site	96
alert-enricher-22-6-193	49
alert-enricher-22-6-188	37
default	15
TEST-KATY	6

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 Defender for IoT Incident details page for Incident ID 319410. The 'Timeline' tab is selected. The timeline entry for 'Unauthorized PLC Programming' is highlighted with a red box:

Unauthorized PLC Programming
Incident ID: 319410
Investigate in Microsoft Defender for IoT

The timeline entry details:

- Timestamp:** Nov 29 1:03 PM
- Description:** Unauthorized PLC Programming | High | Detected by Microsoft Defender for IoT | Tactics: 🛡️ 🚧 🛡️
- Severity:** High
- Owner:** Unassigned
- Status:** New
- Product name:** Microsoft Defender for IoT
- Entities:** 4 (192.178.1.1, 192.178.2.2, contoso-site1, 192.178.1.1)

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	192.168.122.1
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 8: Automate response to Defender for IoT alerts.

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

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

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

For a full list of DIoT Playbooks, refer to [this](#) document.

Exercise 9: Clean Up

Task 1: Delete resources

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

Search for the Resource Group created for this training.

Select Delete resource group on the top right side.

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

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