

Summary

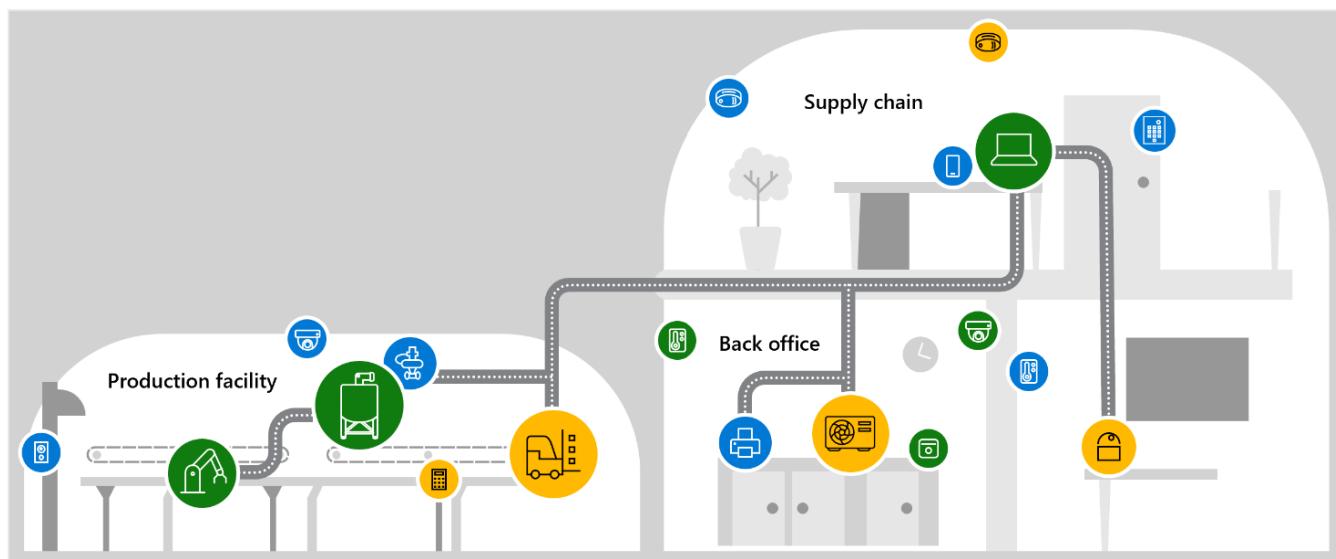
This Hands-on-Lab (HOL) will focus on securing your facilities. We will be simulating traffic by playing some Packet captures, visualizing and analyzing the data on the sensor console. Integrate our sensor with Microsoft Sentinel, to explore alert handling, and to write queries to help with alert investigation.

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 to write queries to help with alert investigation. This Hands-on-Lab (HOL) will focus on securing your facilities. The scenario below is one of many you would apply these lessons to, other scenarios are Oil, Gas, Utility, and Energy companies.



What is Microsoft Defender for IoT?

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

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

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

To learn more, watch this video:

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

Contents

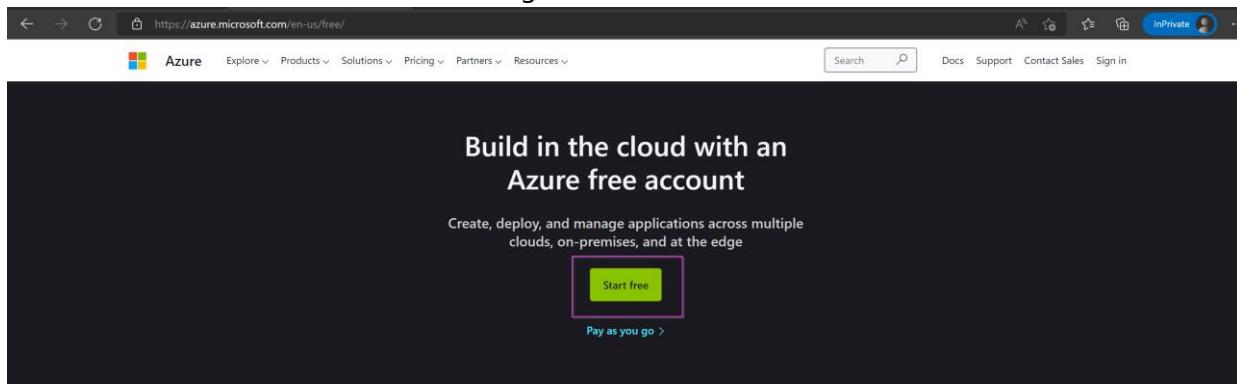
Summary.....	1
Architecture Diagram.....	1
What is Microsoft Defender for IoT?	1
Exercise 1: Enabling Defender	3
Task 1: Create an Azure Subscription	3
Task 2: Enabling Microsoft Defender for IoT on the Subscription.....	4
Exercise 2: Deploy the Sensor in Azure.....	6
Task 1: Create a Resource group to automatically deploy your sensor, storage account and network security group to	6
Task 2: Access your Virtual Machine.....	8
Task 3: Access your sensor via the console.....	14
Exercise 3: Perform an Upgrade	20
Task 1: Download the Upgrade ISO file	20
Task 2: Upgrade your sensor.....	20
Exercise 4: Simulate Data in your sensor.....	22
Task 1: Enabling the PCAP Player	22
Task 2: Play PCAP files.....	23
Exercise 5: Analyzing the Data	25
Task 1: Visualize on the Device Map	25
Task 2: View the associated Alerts	28
Task 3: Device Inventory	30
Task 4: View the Event Timeline	31
Task 5: Data Mining	31
Task 6: Generate a Risk Assessment report.....	33
Exercise 6: Cloud Connect your sensor.....	34
Task 1: Create the cloud connected sensor on the Cloud Management portal	34
Task 2: Upload the activation file to cloud connect your sensor.....	34
Task 3: Verify Cloud connection.....	35

Exercise 7: Manage your sensor via the Cloud Management Portal	36
Task 1: Manage your devices	36
Task 2: View your Alerts	38
Task 3: View your recommendations	40
Task 4: Visualize Data by utilizing Workbooks	40
Exercise 8: Integrate with Microsoft Sentinel	42
Task 1: Create a Log Analytics Workspace.....	42
Task 2: Install the Defender for IoT package.....	44
Task 3: Create Incidents.....	46
Task 4: Validate Defender for IoT logs are streamed correctly to Sentinel (KQLS on the data)	47
Task 5: Investigate Defender for IoT incidents	48
Task 6: Investigate further with IoT device entities	50
Task 7: Investigate the alert in Defender for IoT	51
Task 8: Acknowledge Alerts and Re-run PCAPs.....	52
Exercise 9: Automate response to Defender for IoT alerts.....	53
Exercise 10: Clean Up	53
Task 1: Delete resources.....	53
Exercise 11: Submit Feedback	53

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 search bar at the top has 'Subs' typed into it. Below the search bar, there are tabs for 'All', 'Services (12)', 'Resources (1)', 'Marketplace (20)', 'Resource Groups (0)', and 'Documentation (0)'. Under the 'Services' heading, '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). The 'Resources' section shows a single entry: 'Visual Studio Enterprise Subscription' under 'Subscription'. The 'Marketplace' section lists several 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). The 'Recent' sidebar on the left lists various Azure services and resources.

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

The screenshot shows the 'Subscriptions' blade in the Azure portal. At the top, there are buttons for '+ Add', 'Manage Policies', and 'View Requests'. Below that is a search bar and filter options: 'Subscriptions == global filter', 'My role == all', 'Status == all', and 'Add filter'. The main table displays one subscription row:

Subscription name	Subscription ID	My role	Current cost	Secure Score	Parent management group	Status	More
Visual Studio Enterprise Subscription	2131d18-92b6-4c00-b377-937eb90512a	Account admin	C\$11.29	41%		Active	...

Task 2: Enabling Microsoft Defender for IoT on the Subscription

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

Microsoft Defender for IoT

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

Marketplace (0)

Services

Microsoft Defender for IoT

IoT Hub
Microsoft Sentinel
Form recognizers
Power Platform

See all

Recent resources

Name

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

Documentation

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

Azure Active Directory

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

Group

Searching 1 of 34 subscriptions. Change Give feedback

Resource group 3 weeks ago

Resource group 3 weeks ago

Resource group 3 weeks ago

https://ms.portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/Overview

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.

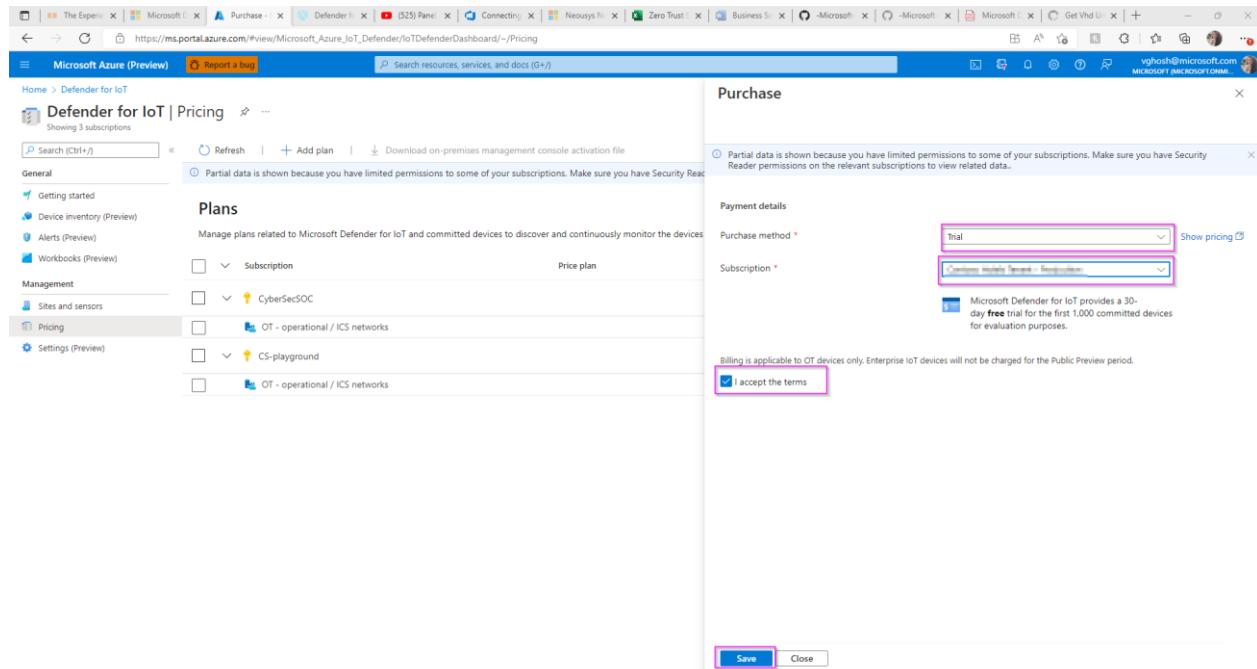
Onboard subscription

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”.



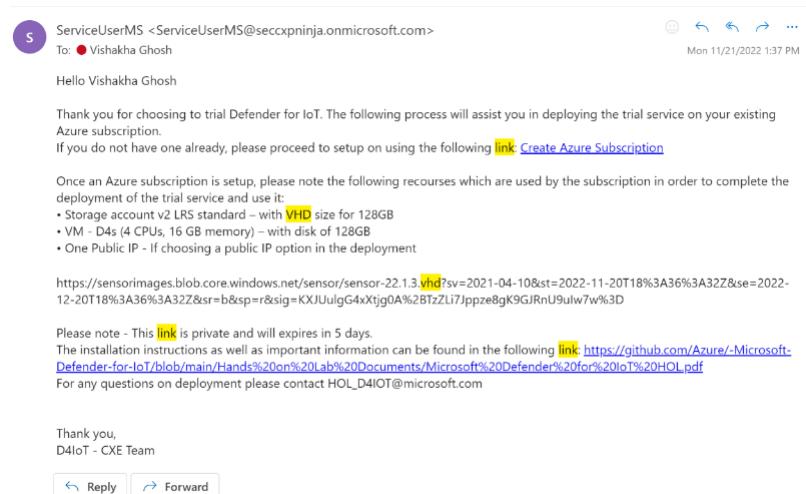
You now have a valid Microsoft Defender for IoT Trial with **1000 committed devices**. These devices represent all those equipment/sensors connected to your network in the facility you are analyzing. This configuration allows you a **30-day trial for free**.

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

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



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

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

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

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

The screenshot shows the 'Custom deployment' page in the Azure portal. At the top, there's a breadcrumb navigation 'Home >'. Below it, the title 'Custom deployment' with a subtitle 'Deploy from a custom template'. There are three tabs: 'Select a template' (disabled), 'Basics' (selected), and 'Review + create'. Under 'Template', there's a section for 'Customized template' which contains 4 resources. To the right are buttons for 'Edit template', 'Edit parameters', and 'Visualize'. The main area is titled 'Project details' with a note about selecting a subscription and resource group. It includes fields for 'Subscription' (BuildEnv) and 'Resource group' (Create new). Below this is the 'Instance details' section with fields for 'Region' (East US), 'Location' ([resourceGroup().location]), 'Deploy Public IP' (true), 'Put Password To Key Vault' (true), 'Source VHDURL' (empty), and 'Sensor Count' (1). Red numbers 1 through 7 are overlaid on the 'Subscription' and 'Resource group' fields.

- 1) Please select your **Subscription** linked to the trail service.
 - 2) Please create a new **Resource Group** (Use the hyperlink below the box). We recommend creating a new one to easily identify the relevant resources of the trail service.
 - 3) Please select the **Region** (Time zone) to which you are deploying the trail service to.
 - 4) Please leave the **Location** box with its default value, no need to change it.
 - 5) **[OPTIONAL]** Set the **Public IP** option to "true". However, doing this will open your sensor to the internet. If you have alternate ways to publish the sensor to end users, then just use the internal ip by setting "Deploy Public IP" to "false".
 - 6) Set this field to true if you want to store your secrets in keyvault.
 - 7) Please paste the link of the **VHD** copied from the email into the **Source VHDURL** field. **Please make sure there are no extra spaces after the link when you paste it.**
3. Once complete please click on the **Review + Create** button Upon validation completion, proceed to click on the **Create** button to initiate the process. The process runs for approx. 30 to 60 minutes.

Custom deployment

Deploy from a custom template

Validation Passed

Basics Review + create

Summary

Customized template 3 resources

Terms

Azure Marketplace Terms | Azure Marketplace

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

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

Create < Previous Next >

Task 2: Access your Virtual Machine.

Option #1: If you deployed with Keyvault

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

Microsoft.Template-20220713114358 | Overview

Your deployment is complete

Deployment name: Microsoft.Template-20220713114358
Subscription: Bullshin
Resource group: KeyVaultTest

Start time: 7/13/2022, 11:44:03 AM
Correlation ID: #0166659-4ef4-4268-b168-5c8887ada956

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
customx24k5p75npg2	Storage account	West US
SOC-Kv24k5p75npg2-Play	Key vault	West US
SOC-NSGx24k5p75npg2-Play	Network security group	West US
SOC-Identityx24k5p75npg2-Play	Managed identity	West US
SOC-vm24k5p75npg2-Play-image	Image	West US
SOC-vm24k5p75npg2-Play-nfd10	Regular Network Interface	West US
SOC-vm24k5p75npg2-Play-pg0	Public IP Address	West US
SOC-vm24k5p75npg2-Play-vfay	Virtual machine	West US
SOC-vm24k5p75npg2-Play-disk1_1load0x51e3de7491e16910774160h	Disk	West US
SOC-vmes24k5p75npg2-Play	Virtual network	West US

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

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

Key vault | Directory: Microsoft

Access policies

+ Create | Refresh | Delete | Edit

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

Showing 1 to 1 of 1 records.

Name ↑ Email ↑ Key Permissions

APPLICATION

SOC-vmsidentityuq63gjmwvo2do-Play

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

Key Management Operations
Cryptographic Operations
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign

Secret Management Operations
Get
List
Set
Delete
Recover
Backup
Restore

Certificate Management Operations
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 Secret Operations
Select all
Purge

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

- 5d62bf487e14fb8884e9582f29be8e1-977f-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-abf6aa26fcee90b34bd9-e88b-46f0-adf8-c7ce00a9954

Selected item

No item selected

Previous

Next

7. Click on "Create".

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

Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

Permissions Principal Application (optional)

Review + create

Key Permissions

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

Secret Permissions

Secret Management Operations	All selected
Privileged Secret Operations	None selected

Certificate Permissions

Certificate Management Operations	None selected
Privileged Certificate Operations	None selected

Principal

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

Application

Authorized application ⓘ	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

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

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

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

Resources Recommendations

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

Show 1 to 10 of 10 records. Show hidden types

	Type	Location	...
<input type="checkbox"/>	Storage account	West US	...
<input type="checkbox"/>	Key vault	West US	...
<input type="checkbox"/>	Network security group	West US	...
<input type="checkbox"/>	Managed identity	West US	...
<input type="checkbox"/>	Image	West US	...
<input type="checkbox"/>	Regular Network Interface	West US	...
<input type="checkbox"/>	Public IP address	West US	...
<input checked="" type="checkbox"/>	Virtual machine	West US	...
<input type="checkbox"/>	Disk	West US	...

9. Make a note of the Public IP address.

SOC Virtual machine

-Play

Essentials

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

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

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine

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

Networking

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

Option #2: If you deployed without Keyvault.

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

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.

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 of a deployment named 'Microsoft.Template-20220630145822'. The deployment status is 'Your deployment is complete'. It lists four resources: 'Reset-password', 'Post-Deploy0', 'VMdeployment', and 'copyvhdl', all in 'OK' status. Below the resources, there is a 'Next steps' section with 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'. The 'Resources' section displays a list of resources, including a virtual machine named 'SOC-vmficiwieu5atkwu-Play' which is highlighted with a red border.

Name	Type	Location
copyvhdl	Deployment Script	East US
customficiwieu5atkwu	Storage account	East US
SOC NSGficiwieu5atkwu-Play	Network security group	East US
SOC-vmficiwieu5atkwu-Play	Virtual machine	East US

5. Make a note of the Public IP address.

SOC Virtual machine

Essentials

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

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- default
DNS name	Not configured

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.

Not secure | https://xxx.xxx.xxx.xxx /login

Microsoft | Defender for IoT sensor

Sensor Sign in

User name

Password

Forgot password? (for admin users only)
[Reset](#)

Login

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

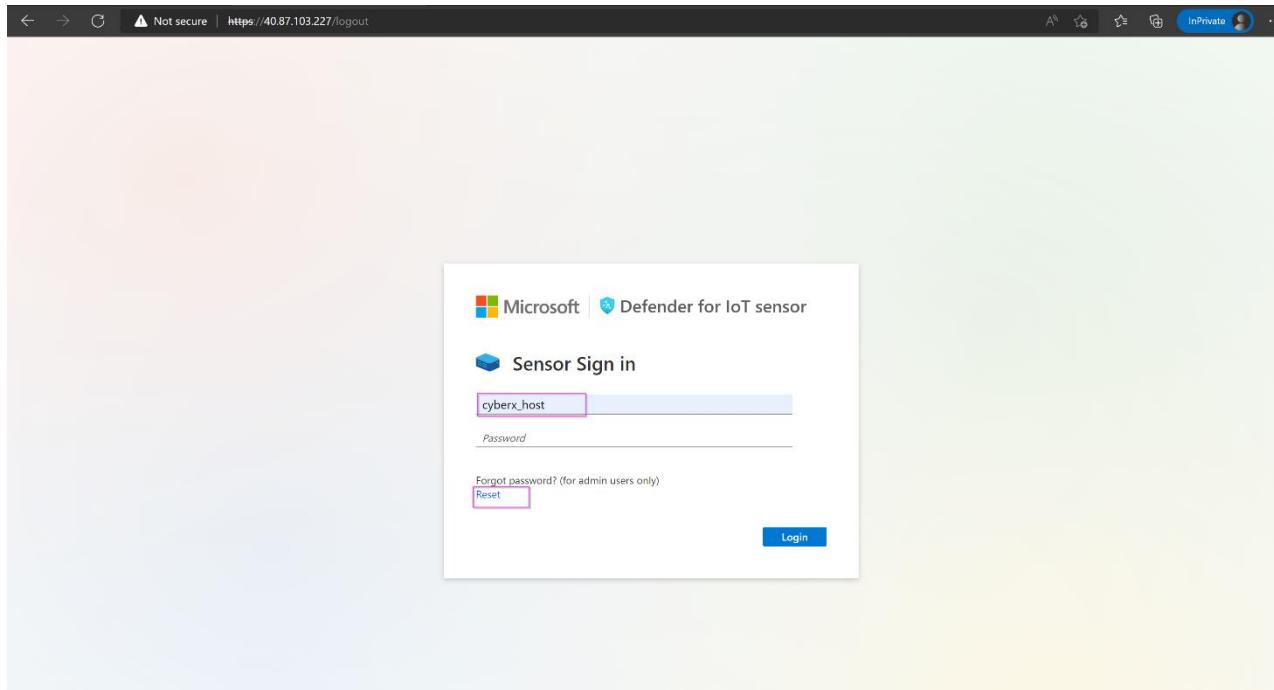
Recover

Insert secret identifier *

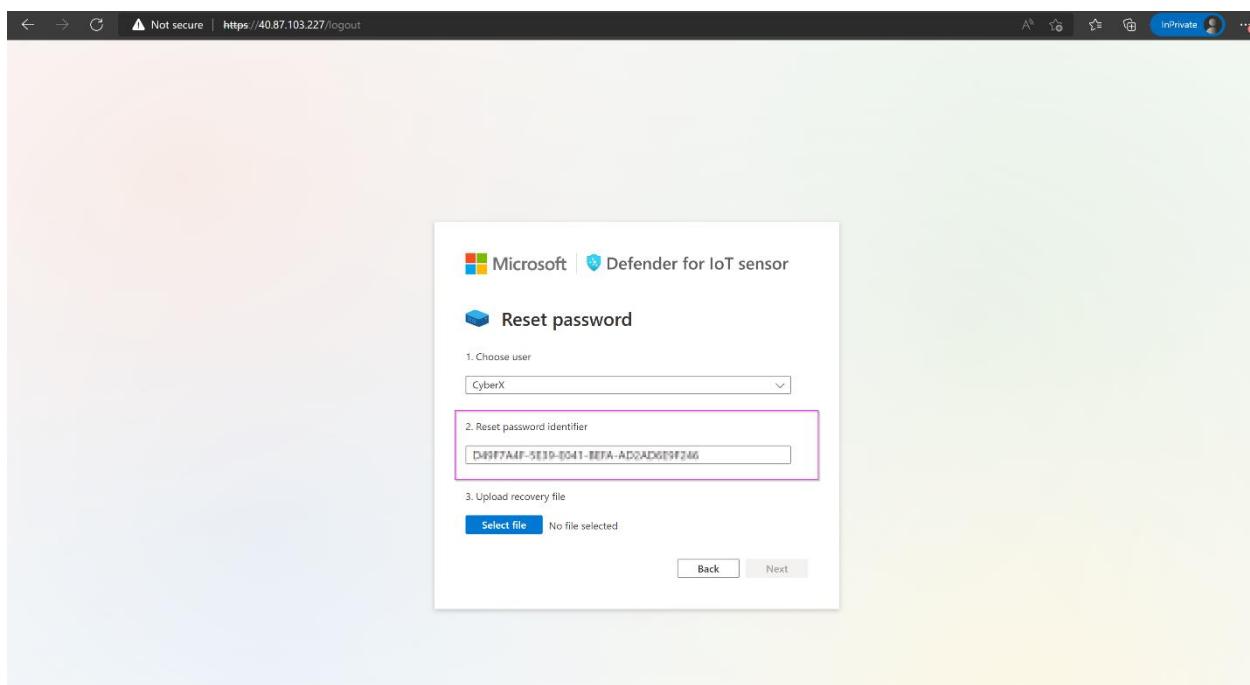
Sub0001-777-0e57-88h12

Recover Cancel

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



8. Copy the identifier.



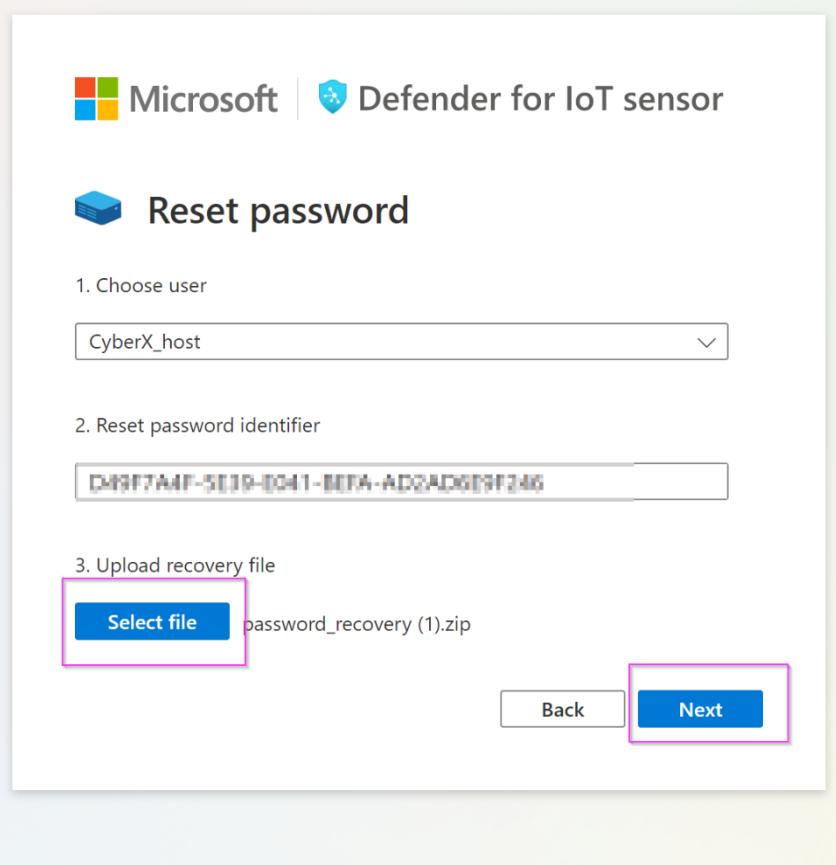
9. Paste in the box on the Defender for IoT Azure window. Click "**Recover**".

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'. 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, it says '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

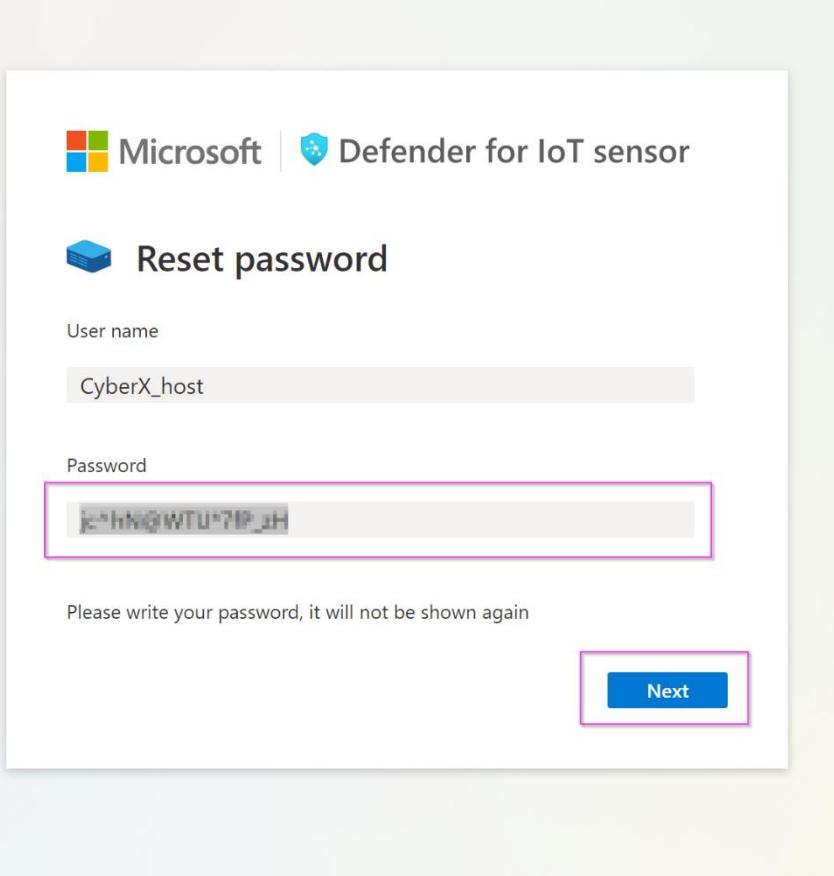
D9F7A4F-5E19-0411-BFA-AD2AD619F246

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

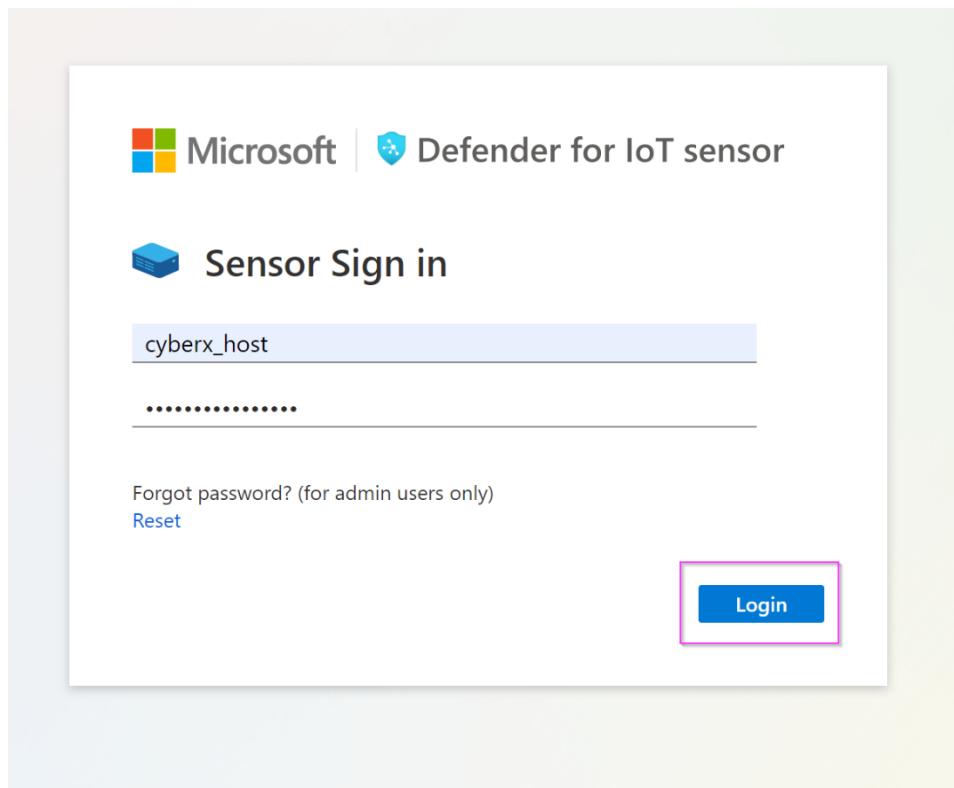
Password

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 the 'Updates' section, there are two options: 'Software Update' and 'Threat Intelligence'. The 'Software Update' option is also highlighted with a pink box. Other sections visible 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' section selected. The 'Software Update' option under the 'Updates' section is highlighted with a pink box.

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 that, there are summary metrics: 0 PPS, 124 Devices, and 32 Alerts. In the 'General Settings' section, there's a 'Version:' field containing '22.2.8.20-r-3bd7f37', which is highlighted with a pink box.

Exercise 4: Simulate Data in your sensor.

Task 1: Enabling the PCAP Player

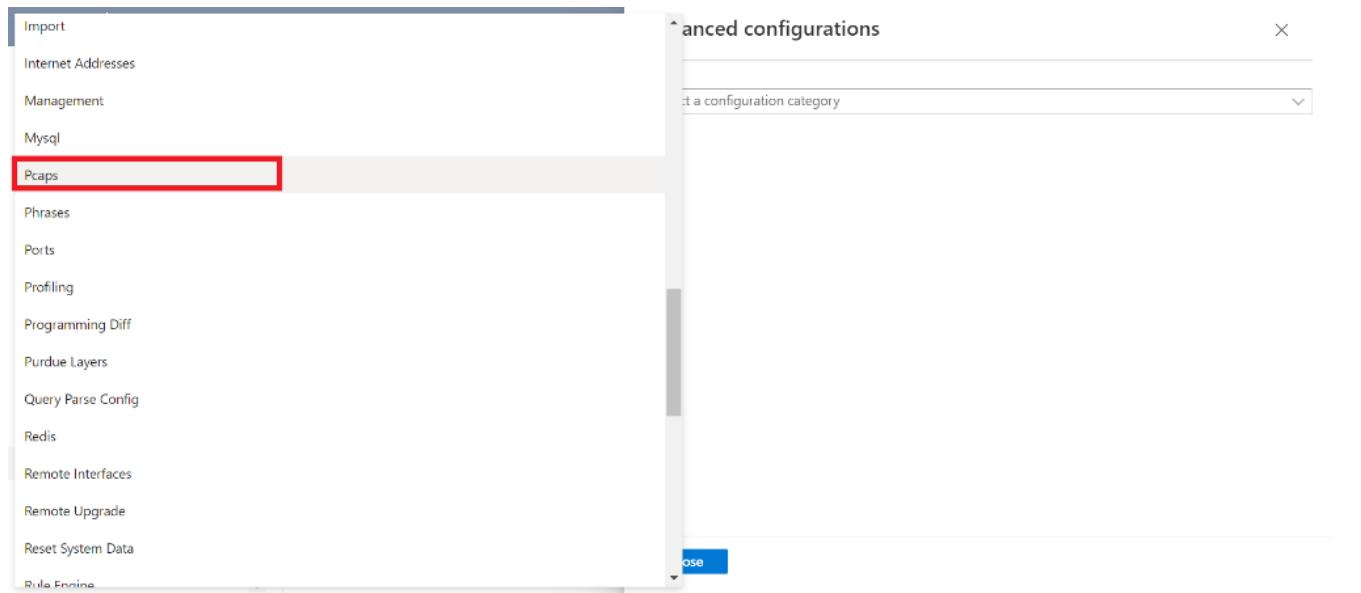
1. The PCAP player needs to be enabled to be visibly available for use in the UI. To do so, please select the "**System settings**" option from the scrolled down left side menu.

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

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

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

3. From "Select a Configuration Category", select Pcaps.



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

This screenshot shows the Microsoft Defender for IoT interface with the 'System settings' page selected. In the center, there's a 'SNMP MIB Monitoring' section. To its right, an 'Advanced configurations' dialog is open for the 'Pcaps' category. The 'enabled' variable is highlighted with a red box. At the bottom of the dialog, the 'Save' button is also highlighted with a red box.

Task 2: Play PCAP files

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

Microsoft | Microsoft Defender for IoT - 22.1.3

Home > System settings

Defender for IoT | System settings

Analyze

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

Manage

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

SSL/TLS Certificate

Manage SSL/TLS certificates installed on this sensor

Play PCAP

Upload and play PCAP files

Sensor management (highlighted)

Network monitoring

Integrations

Import settings

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

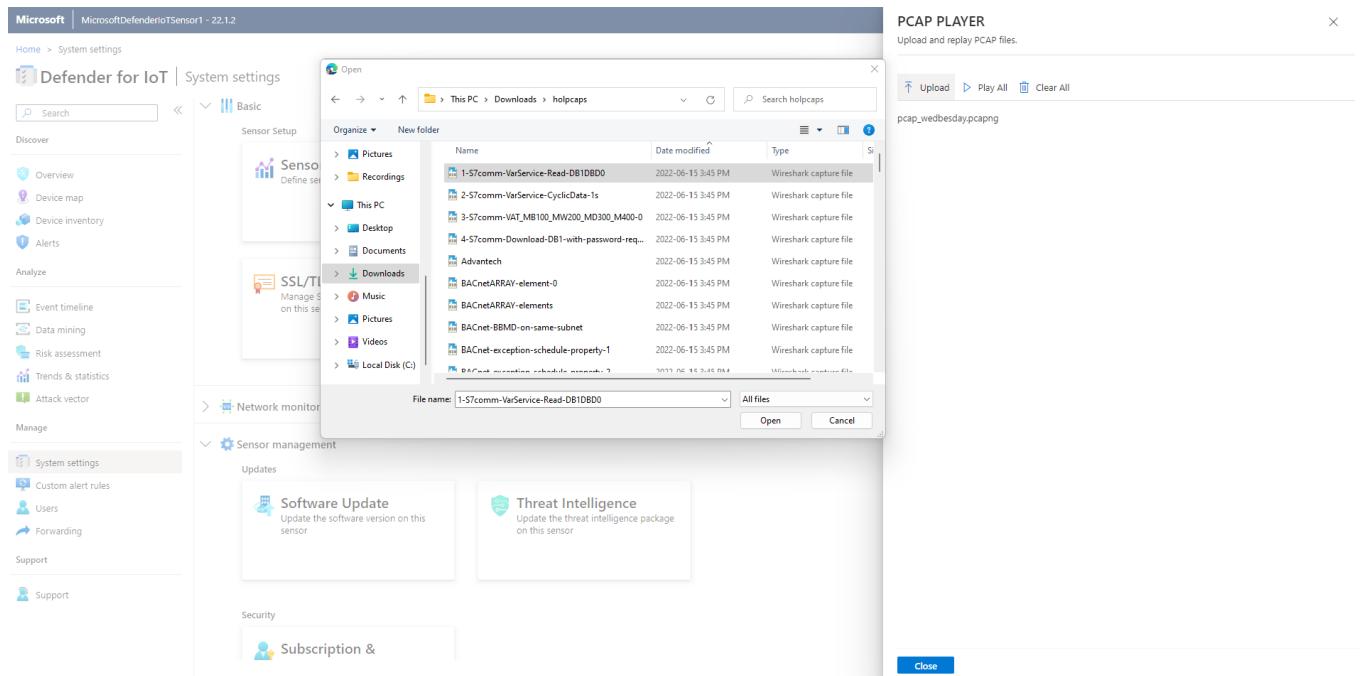
Advanced configurations

Pcaps

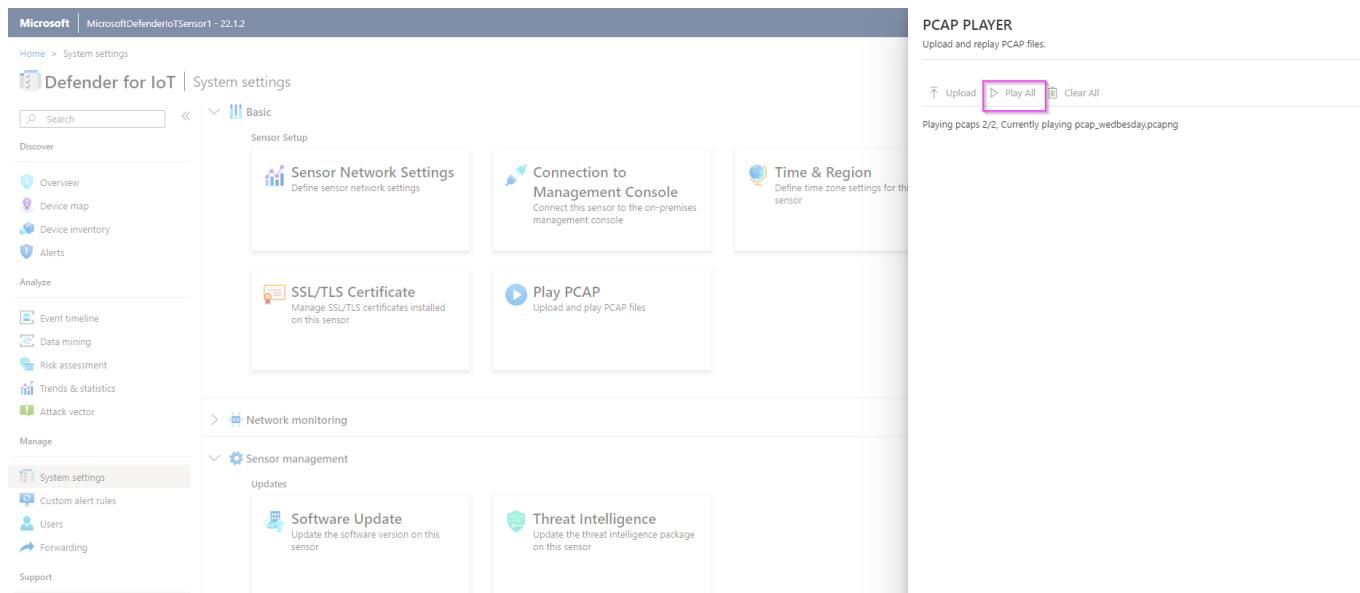
```
size.megabytes.max=44032
archive.size.megabytes.max=
size.megabytes.min=17408
archive.size.megabytes.min=
cache.should.save.pcap=1
archive.cache.dir=
filtered.cache.dir.size.megabytes.max=7168
filtered.cache.dir.size.megabytes.min=3072
filtered.archive.dir.size.megabytes.max=
filtered.archive.dir.size.megabytes.min=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

Save

Close



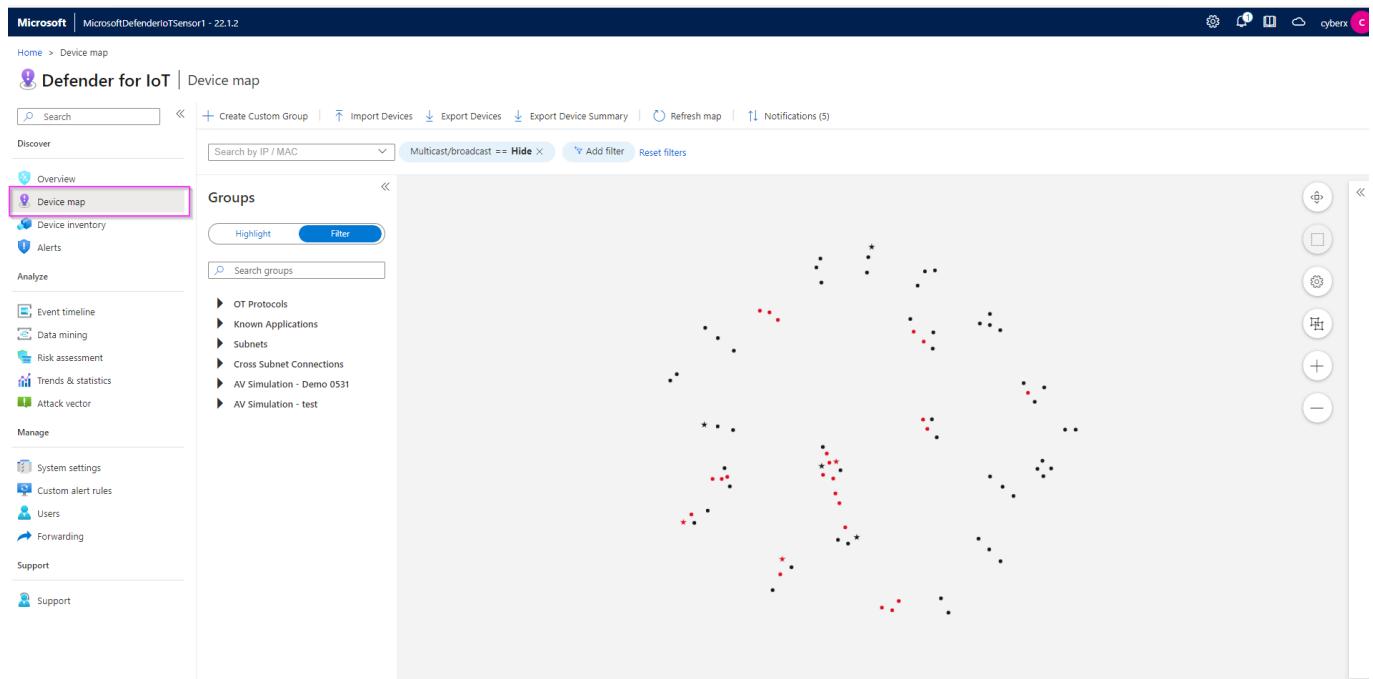
5. Click "Play All" to play the Pcaps.



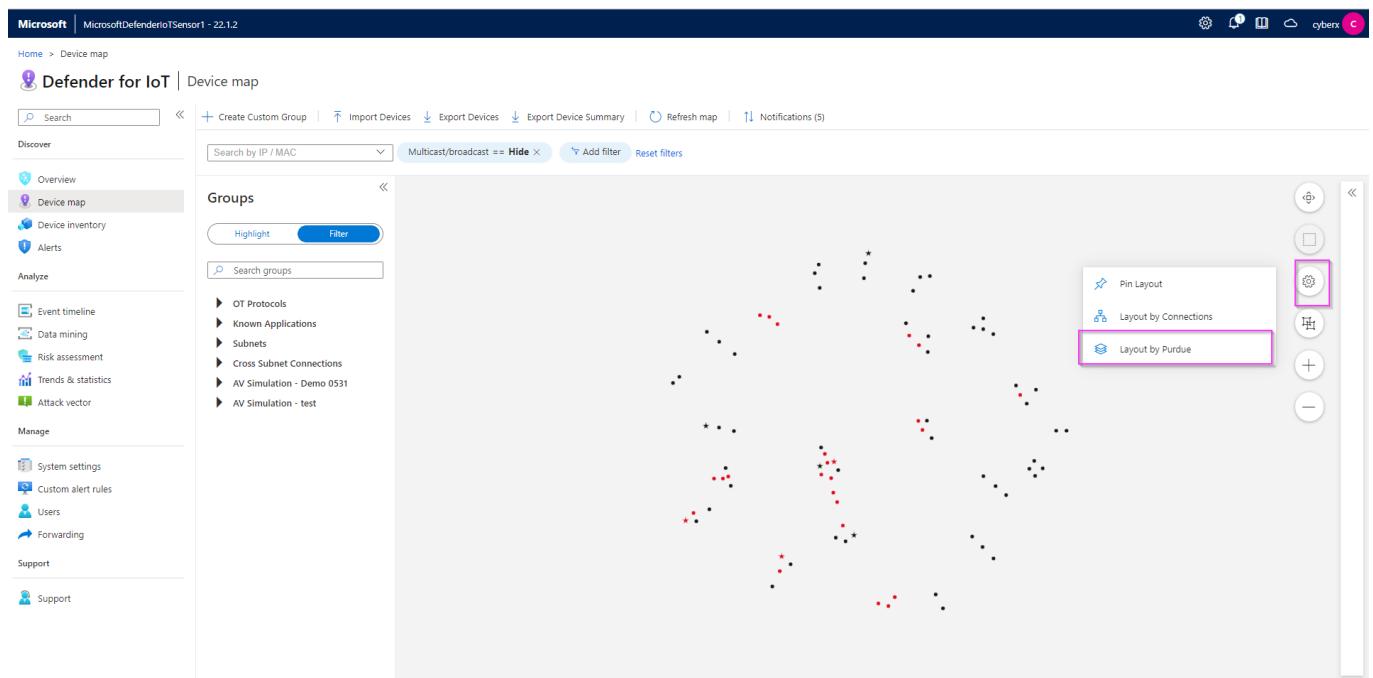
Exercise 5: Analyzing the Data

Task 1: Visualize on the Device Map

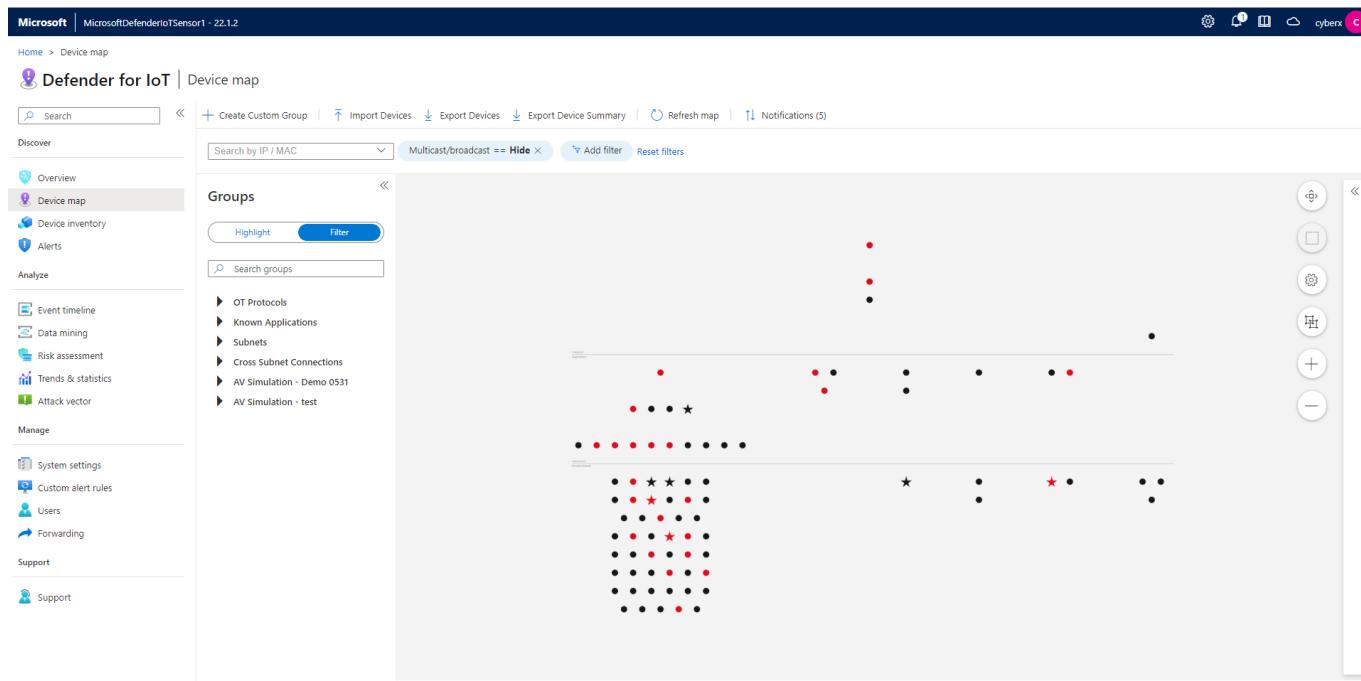
1. Click on “Device Map” from the menu on the left side.



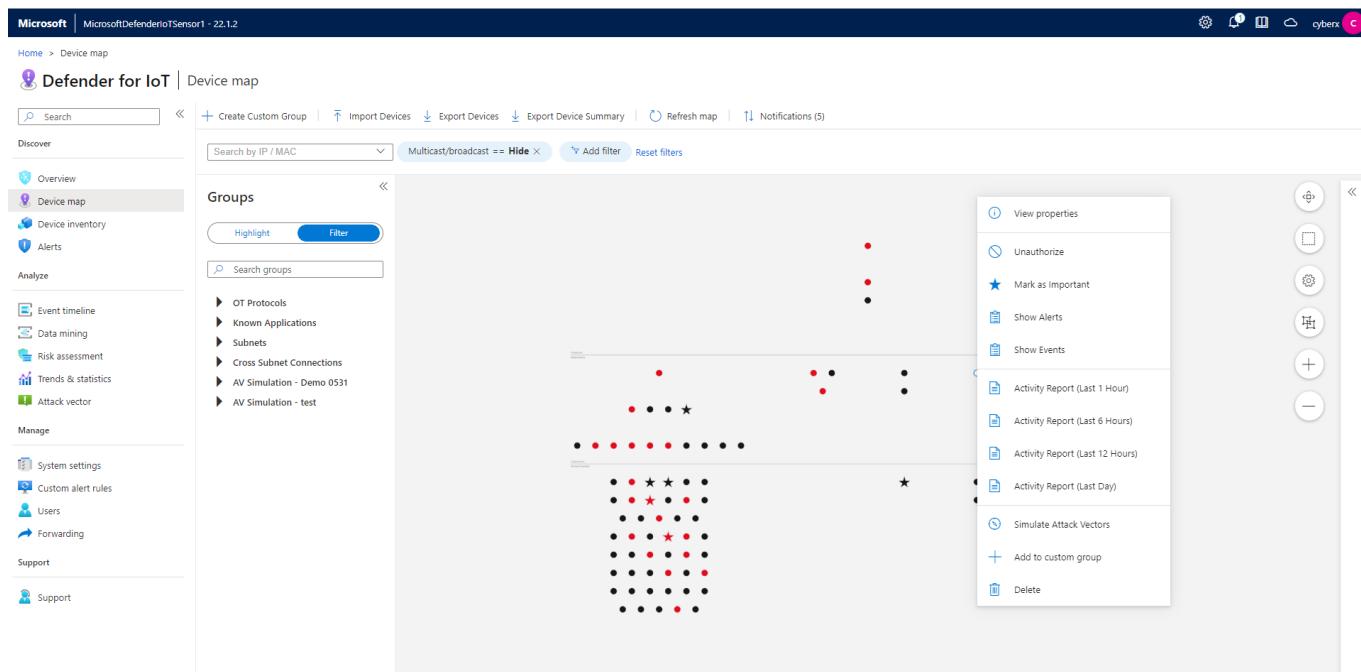
2. Click on the "Settings" option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.



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



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



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

The screenshot shows the Microsoft Defender for IoT Device map interface. On the left, a sidebar 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 with a similar layout to the previous one. It features a sidebar with various monitoring and management options. In the center, a network diagram displays four devices: 192.168.110.2, 192.168.110.1, 192.168.110.4, and 192.168.110.10. The device 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'. The interface maintains its dark blue theme.

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, showing details for 'Device | 192.168.110.21'. It includes sections for 'Authorized Status', 'Last Seen', and 'Alerts'. The 'Alerts' section is highlighted with a pink border and shows 2 alerts. Below it, 'Network Interfaces' and 'Protocols' (SSH, EtherNet/IP, TDS, FTP, CIP) are listed. A large table on the right displays 22 alerts, with columns for Severity, Name, Engine, Detection time, Status, and Source Device. Two specific alerts are highlighted with pink boxes: 'Unauthorized Internet Connectivity Detected' (Critical, Policy Violation, 2 weeks ago, New, 192.168.110.21) and 'EtherNet/IP Encapsulation Protocol Command Failed' (Major, Operational, 2 months ago, New, 192.168.110.2). A 'Group by' dropdown menu is visible at the top right.

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 'Alerts' selected. The main area displays a table of 22 alerts, with one alert highlighted by a pink box: 'Unauthorized Internet Connectivity Detected' (Critical, Policy Violation, 2 weeks ago, New, 192.168.110.21). To the right of this alert, a detailed view is shown. It includes a summary box with the alert ID (53), status (New), and detection time (2 weeks ago). Below this is a 'Description' section stating: 'A device defined in your internal network is communicating with addresses on the internet. These addresses have not been learned as valid addresses.' It also notes that 'Device 192.168.110.21 communicated with addresses shown in External Addresses. Verify that this device is properly configured.' At the bottom of the alert view are two buttons: 'View full details' and 'Take action'.

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

Showing 22 of 22 alerts

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

Task 3: Device Inventory

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

Showing 100 of 291 items

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

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

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Device inventory

Defender for IoT | Device inventory

Search | Save Filter | Refresh | Edit Columns | Export

Discover

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

Showing 100 of 291 items

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

Load More...

Task 4: View the Event Timeline

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

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Event timeline

Defender for IoT | Event timeline

Search | Create event | Refresh | Export

User Operations == Hide | Add filter | Reset filters

Discover

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

Event type

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

Load More...

Task 5: Data Mining

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

Create new report

Name * Report name

Description

Send to CM

Choose Category * Category

Order by Activity

Filter by Results within the last 3 minutes

IP address

MAC address

Port

Device group

Save Cancel

2. 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 * PLC Firmware Version

Description Report showing the firmware version of the different PLCs.

Send to CM

Choose Category * Modules and Firmware Versions

Order by Activity

Filter by Results within the last 3 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”.

The screenshot shows the Microsoft Defender for IoT interface under the 'Data mining' section. On the left, a sidebar lists various navigation options like Overview, Device map, Device inventory, Alerts, Event timeline, Data mining (which is selected and highlighted in grey), Risk assessment, Trends & statistics, and Attack vector. The main content area is titled 'Defender for IoT | Data mining'. It features a 'Recommended' section with six cards: Programming Commands, Internet Activity, Excluded CVEs, Active Devices (Last 24 Hours), Remote Access, and CVEs. Below this is a 'My reports' section with a table. The first row in the table, 'PLC Firmware Version', has a description 'Report showing the firmware version of the different PLCs.' and was last modified '2 minutes ago'. This row is also highlighted with a pink box. Other rows in the table include 'ALL' (last modified 4 days ago) and 'test' (last modified 3 months ago). At the top of the page, there's a search bar, a 'Create report' button, and several global navigation icons.

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

This screenshot shows the 'PLC Firmware Version' report page. At the top, there's a toolbar with Refresh, Expand all, Collapse all, Export to CSV (highlighted with a pink box), Export to PDF, Snapshots, Manage report, and Edit mode. The main content area displays the report title 'PLC Firmware Version' and a brief description: 'Report showing the firmware version of the different PLCs.'. Below this is a table with four columns: #, Name, Date Created, and Size. The table contains four rows, each representing a report file: 'risk-assessment-report-4.pdf' (just now, 2 MB), 'risk-assessment-report-3.pdf' (4 days ago, 2 MB), 'risk-assessment-report-2.pdf' (A month ago, 1 MB), and 'risk-assessment-report-1.pdf' (3 months ago, 1 MB). The entire report table is highlighted with a pink box.

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 Microsoft Defender for IoT Risk assessment page. The left sidebar includes 'Discover', 'Overview', 'Device map', 'Device inventory', 'Alerts', 'Event timeline', 'Data mining', 'Risk assessment' (selected and highlighted in grey), 'Trends & statistics', and 'Attack vector'. The main content area is titled 'Defender for IoT | Risk assessment'. A 'Generate report' button is located in the top right corner of the header. Below it is a 'Reports list' table with columns: #, Name, Date Created, and Size. The table contains four rows, each representing a risk assessment report: 'risk-assessment-report-4.pdf' (just now, 2 MB), 'risk-assessment-report-3.pdf' (4 days ago, 2 MB), 'risk-assessment-report-2.pdf' (A month ago, 1 MB), and 'risk-assessment-report-1.pdf' (3 months ago, 1 MB). The entire 'Generate report' button and the 'risk-assessment-report' table are highlighted with a pink box.

Exercise 6: Cloud Connect your sensor.

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

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

The screenshot shows the Microsoft Azure Cloud Management portal. In the top navigation bar, there's a search bar and several icons. Below it, the 'Defender for IoT | Sites and sensors' page is displayed. A pink box highlights the '+ Onboard OT sensor' button in the top right corner of the main content area. The page displays various metrics: 4 All sensors, 1 IoT, 2 OT cloud connected, and 1 OT. Under the 'Management' section, 'Sites and sensors' is selected, and it shows 4 of 4 sensors. The first sensor listed is 'D4IOT-CxE-Site - D4IOT-CxE-Site'. The entire interface has a light blue background with white and grey elements.

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 a registration form for a sensor. At the top, it says "Step 3: Register this sensor with Microsoft Defender for IoT". The form includes fields for "Sensor name" (with a pink box around the input field), "Subscription" (a dropdown menu with a pink box around it, showing "Please select a subscription" and "Onboard subscription"), and "Cloud connected" (a checkbox which is checked and highlighted with a pink box). There are also fields for "Automatic Threat Intelligence updates", "Sensor version" (set to "22.X and above"), "Site", "Resource name", "Display name", "Tags", and "Zone". At the bottom left is a "Register" button, which is also highlighted with a pink box.

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 sidebar with categories: Discover (Overview, Device map, Device inventory, Alerts), 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 and highlighted with a pink box. In the main area, under 'Sensor management', there are several sections: 'Updates' (Software Update, Threat Intelligence), 'Security' (Subscription & Activation Mode, highlighted with a pink box), and 'Health and troubleshooting' (Backup & Restore, System Health Check, SNMP MIB Monitoring).

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

The screenshot shows the Microsoft Defender for IoT Sensor management interface with the 'Subscription & Activation Mode' dialog box open. The dialog box contains fields for Activation Mode (Cloud Connected), Activation Status (Active), Tenant ID (5f1060f2-d9a4-4f59-bf0c-1dd8f3604a4b), Subscription ID (1c61ccbf-70a3-45a3-a1fb-848ce465d71a5), and a file upload input labeled 'Upload activation file:' with a 'Select file' button. The rest of the interface is visible in the background.

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 7: Manage your sensor via the Cloud Management Portal

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

Task 1: Manage your devices

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

Device inventory

447 Total devices

78 New devices

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

Showing 447 of 447 devices

Group by (Preview) No grouping

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

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

10.140.32.30 Unclassified

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

Network interfaces:

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

Protocols:

- SNMP

Tags:

- 10.140.32.0/24, 10.9.14.0/24, 10.140.32.0/24

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

10.140.32.30

Attributes

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

General information:

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

Network interfaces:

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

Protocols:

- SNMP

Tags:

- 10.140.32.0/24, 10.9.14.0/24, 10.140.32.0/24

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

Device inventory

Total devices 447 **New devices** 76

Devices by class

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

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

Showing 52 groups by vendor

Group by (Preview) Vendor

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

Task 2: View your Alerts

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

Getting started

Alerts

Device inventory

Incidents (Preview)

Recommendations (Preview)

Workbooks

Firmware inventory (Preview)

Management

Sites and sensors

Plans and pricing

Settings (Preview)

Troubleshooting + Support

Diagnose and solve problems

New support request (Preview)

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

Open alerts by severity

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

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

Showing 278 of 278 alerts

Group by No grouping

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

2. Click on any alert to see the details.

Showing 278 of 278 alerts

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

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

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

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

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

MITRE ATT&CK®

[View full details](#)

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

Alerts | Unauthorized Internet Connectivity Detected ...

Refresh | Download PCAP

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

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

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

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

MITRE ATT&CK®

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

Techniques: Internet accessible device: T0883

Alert details

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

Take action

Entities

- Devices (1)**

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

Address
137.220.100.146

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

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

Open alerts by severity:

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

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

Showing 278 of 278 alerts

Group by: Severity

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

Troubleshooting + Support

Diagnose and solve problems New support request (Preview)

Task 3: View your recommendations

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

The screenshot shows the Microsoft Defender for IoT portal interface. On the left, there's a sidebar with various tabs like 'General', 'Device inventory', 'Alerts', and 'Recommendations (Preview)', which is highlighted with a pink box. The main area is titled 'Active recommendations' and shows 'Showing 2 of 2 recommendations'. There are two rows in a table:

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

- Click on any recommendation to view full details.

The screenshot shows the details of the 'Review PLC operating mode' recommendation. It includes a summary bar with 'Medium Severity', '16 Unhealthy devices', and 'Last update 3/20/2023'. Below this, there's a table of 16 unhealthy devices with columns for Name, IP, Site, and Last update time. A pink box highlights the 'Remediation steps' section, which contains three numbered steps:

- Check whether each PLC must be in unsecure state, such as Program or Remote.
- If the PLC can be configured to the secure Run mode, check that the PLC has a physical key switch.
- Do one of the following: If the PLC has a physical key switch, change the switch position to Run. If the PLC does not have a physical key switch, change the PLC operating mode to Run using the Engineering Station software.

Task 4: Visualize Data by utilizing Workbooks

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

The screenshot shows the Microsoft Defender for IoT Workbooks Gallery. On the left, there's a sidebar with categories: General (Getting started, Device inventory, Alerts, Recommendations (Preview), Workbooks), Management (Sites and sensors, Plans and pricing, Settings (Preview)), and Troubleshooting + Support (Diagnose and solve problems). The 'Workbooks' category is highlighted with a pink box. The main area displays a grid of workbooks. Under 'Quick start', there's an 'Empty' workbook. Under 'Recently modified workbooks (8)', there are eight items: 'Alerts Specific', 'Sensors Data', 'Detected MAC', 'Devices by Protocols', 'ByOS type', 'Workbook 3', 'DeviceInvestigation', and 'Workbook 2'. Under 'Defender for IoT (4)', there are four items: 'Sensor health', 'Alerts', 'Devices', and 'Vulnerabilities'.

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

Sensors

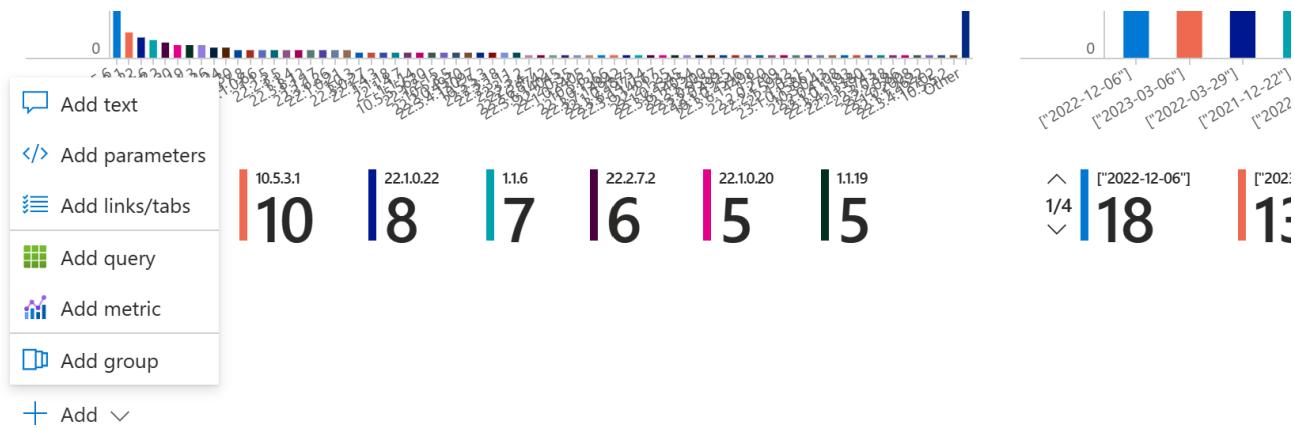
This report consolidates data regarding your sensors' health.

The screenshot shows the 'Sensor health - Overview' page. It includes a donut chart with the following data: Unavailable (842), Disconnected (313), and Ok (18). Below the chart are two line charts: 'Sensor version' and 'TI version'. The 'Sensor version' chart shows a high count of sensors (~150) with a small number of others. The 'TI version' chart shows a distribution of TI versions across different sensor IDs.

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

The screenshot shows the top ribbon of the application. The 'Edit' button is highlighted with a pink box. Other buttons include 'Workbooks', 'Help', and 'Auto refresh: Off'.

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



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

Exercise 8: Integrate with Microsoft Sentinel

Task 1: Create a Log Analytics Workspace

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

The screenshot shows the Azure portal search results for 'Microsoft Sentinel'. The search bar at the top contains the query 'Microsoft Sentinel'. The results page has a sidebar on the left with sections for 'Azure services', 'Resources', 'Tools', and 'Documentation'. The main area lists several resources under 'Services': 'Microsoft Sentinel' (selected), 'Microsoft Defender EASM', 'Microsoft Purview accounts', and 'Microsoft Defender for Cloud'. Under 'Marketplace', there are items like 'SOC 24x7 Monitoring with Microsoft Sentinel' and 'Advanced KQL for Microsoft Sentinel'. Under 'Documentation', there are links to 'What is Microsoft Sentinel?' and 'Microsoft Sentinel documentation'.

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

- Pick your subscription, Resource Group, Name and Region

Create Log Analytics workspace

Basics Tags Review + Create

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

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

Project details

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

Subscription *	CS-playground
Resource group *	CS-playground
	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 a heading "A cloud-native SIEM to h".

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

The screenshot shows the Microsoft Sentinel Content Hub. On the left is a sidebar with sections like General, Threat management, Content management, and Configuration. The main area shows a search bar with "Defender for IoT" typed in. Below the search bar are counts for Solutions (282), Standalone contents (269), Installed (0), and Updates (0). A grid of content items is shown, with one item highlighted: "Microsoft Defender for IoT" by Microsoft Sentinel, Microsoft Corporation. To the right, a detailed view of the "Microsoft Defender for IoT" solution is displayed, including its provider (Microsoft), support (Microsoft Support), version (2.0.2), and a description: "Defender for IoT on assessing your Internet of Things (IoT)/Operational Technology (OT) infrastructure". It lists "Underlying Microsoft Technologies used": a. Codeless Connector Platform/Native Sentinel Polling, Data Connectors: 1, Workbooks: 1, Analytic Rules: 15, Playbooks: 8. There are also links to learn more about Microsoft Sentinel and Solutions. At the bottom right of this panel is a large "Install" button.

3.Click on “Create”.

The screenshot shows the Microsoft Defender for IoT solution creation page. It has a header with the solution name and a "Create" button. Below the header is a plan dropdown set to "Microsoft Defender for IoT" and a "Create" button. A note at the bottom states: "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".

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

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

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

Project details

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

Subscription * ⓘ

C3-playground

Resource group * ⓘ

C3-playground

Create new

Instance details

Workspace * ⓘ

HandsOnLab

Review + create

< Previous

Next : Data Connectors >

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

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

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

Solutions (1) Content sources . All

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

Standalone (2)

Workbook (2)

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

Content type i 15 Data connector 7 Playbook 1 Workbook

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

Manage Actions View details

24 Installed content items

Microsoft Defender for IoT

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

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

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

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

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

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

Content type i 15 Data connector 7 Playbook 1 Workbook

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

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	Last data received --	Content source ⓘ IoTOTThreatMonitoringwithDefenderforIoT	
	Microsoft Defender for Office 365 (Preview) Microsoft	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 search and filter controls: 'Search by ID, title, tags, owner or product', 'Severity: All', 'Status: 2 selected', and an 'Auto-refresh incidents' toggle. A prominent red box highlights the 'Product name' filter dropdown. This dropdown lists several products with checkboxes: Azure Information Protection, Microsoft Defender for Endpoint, Microsoft Defender for IoT (which is checked), 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, there's a chart titled 'Open incidents by severity' showing counts for High (121), Medium (458), Low (338), and Informational (0). Further right is a circular icon with three boxes and a plus sign, with the text 'No incidents selected' and 'Select an incident to view more details'. At the bottom of the main pane, there are buttons for '< Previous', '1 - 50', and 'Next >'.

3. Select a specific incident to begin your investigation.

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

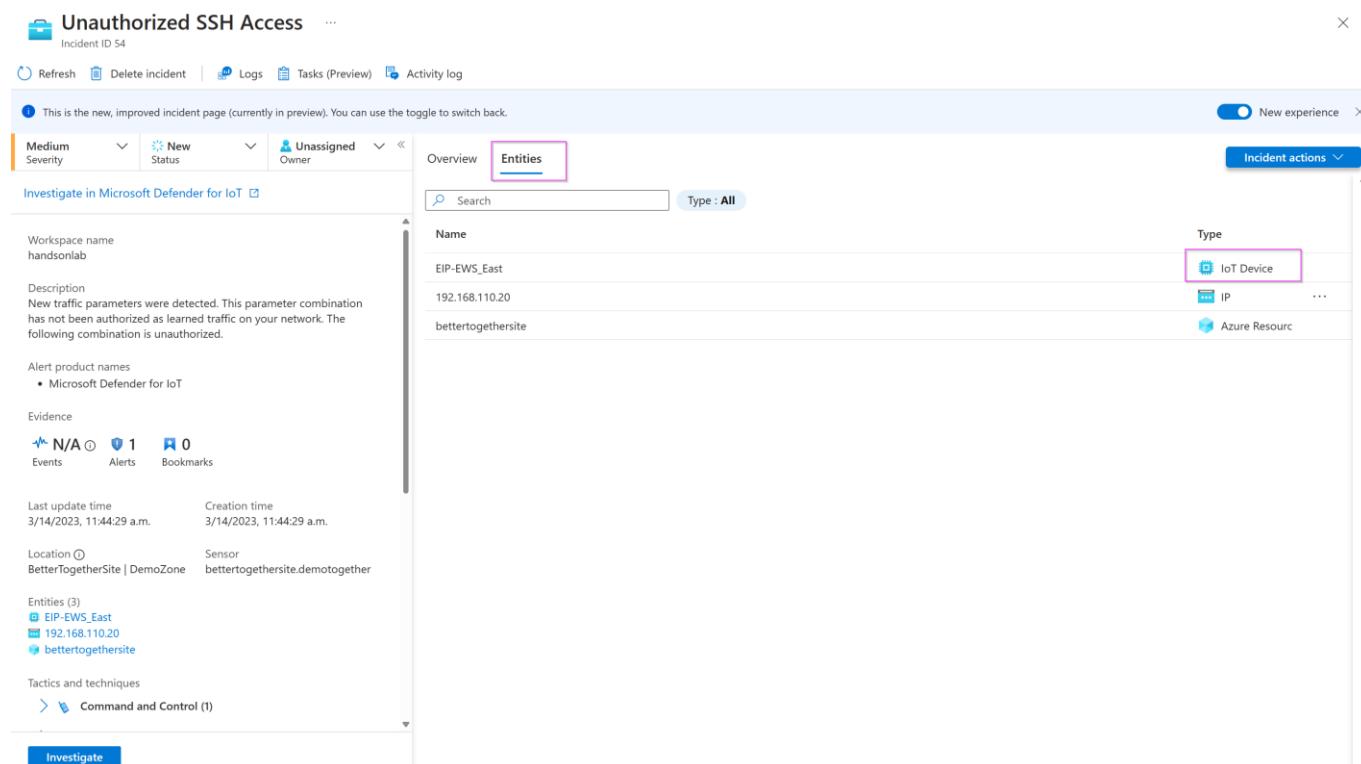
The screenshot shows the Microsoft Sentinel Incidents page with the 'Incidents' section selected in the sidebar. The main area displays 676 Open incidents, 676 New incidents, and 0 Active incidents. The 'Product name' filter is set to 'Microsoft Defender for IoT' and the 'Owner' filter is set to 'All'. The incident grid shows a list of incidents with columns for Severity, Incident ID, Title, Alerts, Product names, Created time, and Last update time. One specific incident is highlighted with a red box: 'Malicious Domain Name Request' (Incident ID: 107793). The right side of the screen shows the detailed view for this incident. It includes a summary table with columns for Unassigned Owner, New Status, and High Severity. The 'Description' section notes suspicious network activity. The 'Alert product names' section lists 'Microsoft Defender for IoT'. The 'Evidence' section shows 1 event and 0 alerts. The 'Last update time' is 09/22/22, 10:36 AM and the 'Creation time' is 09/22/22, 03:05 AM. The 'Entities' section lists an IP address: 192.168.42.29. The 'Tactics and techniques' section shows 'Command and Control (1)' and 'Initial Access (0)'. At the bottom, there are buttons for 'View full details' and 'Actions'.

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 "Entities" tab is selected. A table lists three entities:

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

The "IoT Device" row is highlighted with a pink box. Other tabs include Overview, Logs, Tasks (Preview), Activity log, and Incident actions. The page also displays incident details like workspace name, description, alert product names, evidence count (Events: N/A, Alerts: 1, Bookmarks: 0), last update time, creation time, location, and a list of entities.

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. The entry details:

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

Timeline content: All | **Severity:** All | **Tactics:** All

Description: The source device is not defined as a programming device but performed a read/write operation on a destination controller. Programming changes should only be performed by programming devices. A programming application may have been installed on this device.

Alert product names: Microsoft Defender for IoT

Evidence: N/A (Events: 1), Alerts: 0, Bookmarks: 0

Last update time: 11/29/22, 03:31 PM | **Creation time:** 11/29/22, 01:05 PM

Entities (4): 192.178.1.1, 192.178.2.2, contoso-site1, 192.178.1.1

Severity: High | **Status:** New | **Product name:** Microsoft Defender for IoT

Task 8: Acknowledge Alerts and Re-run PCAPs

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

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Alerts

Defender for IoT | Alerts

Search Refresh Edit Columns Export to CSV Change Status Learn

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

Showing 22 of 22 alerts Group by No grouping

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

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

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > System settings

Defender for IoT | System settings

Search Basic Sensor Setup

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

PCAP PLAYER Upload and replay PCAP files.

Upload Play All Clear All

1-S7comm-VaService-Read-D61DBD0.pcap
pcap_wednesdaypcapng

Sensor Network Settings Define sensor network settings

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

Time & Region Define time zone settings for this sensor

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

Play PCAP Upload and play PCAP files

Network monitoring Sensor management Integrations Import settings

Close

Exercise 9: Automate response to Defender for IoT alerts.

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

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

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

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

Exercise 10: Clean Up

Task 1: Delete resources

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

Search for the Resource Group created for this training.

Select Delete resource group on the top right side.

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

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

Exercise 11: Submit Feedback

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