

Summary

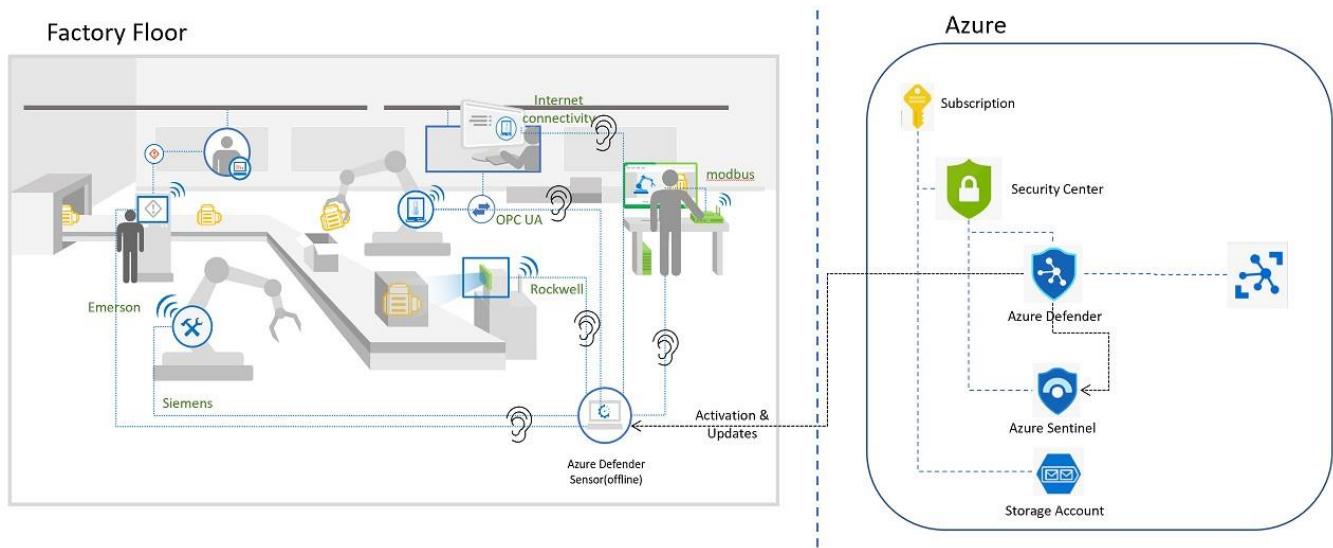
This Hands-on-Lab (HOL) will focus on securing your facilities. We will be simulating traffic by playing some Packet captures, visualizing and analyzing the data on the sensor console. Integrate our sensor with Microsoft Sentinel, to explore alert handling, and for writing queries to help with alert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

Internet of Things - Microsoft Defender for IoT HOL

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

Architecture Diagram

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



Contents

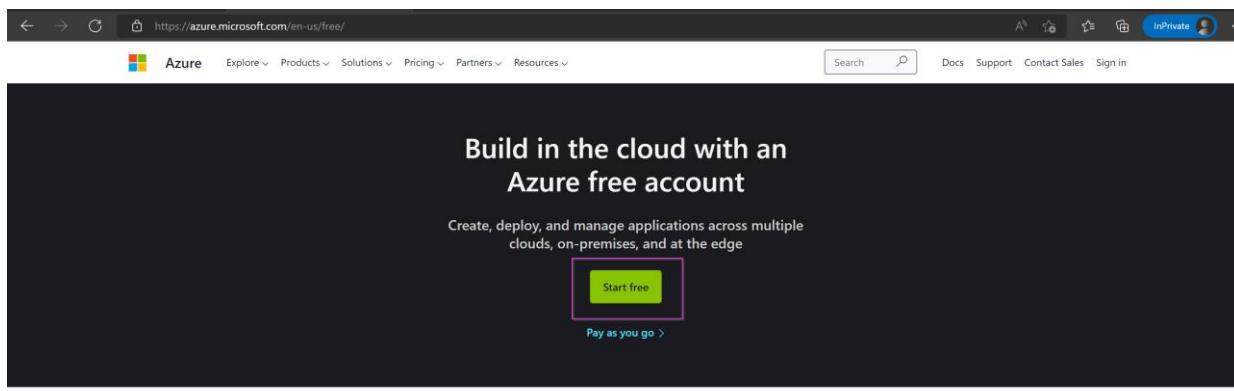
Summary.....	1
!! Since the PDF contains hyperlinks, please download the file before proceeding!!.....	1
Architecture Diagram.....	1
Exercise #1: Enabling Defender.....	2
Task 1: Create an Azure Subscription	2
Task 2: Enabling Microsoft Defender for IoT on the Subscription.....	3
Exercise #2: Deploy the Sensor in Azure	5
Task 1: Create a Resource group to automatically deploy your sensor, storage account and network security group to	5

Task 2: Access your Virtual Machine.....	7
Task 3: Access your sensor via the console.....	12
Exercise #3: Simulate Data in your sensor.....	18
Task 1: Enabling the PCAP Player.....	18
Task 2: Play PCAP files.....	20
Exercise 4: Analyzing the Data	21
Task 1: Visualize on the Device Map.....	21
Task 2: View the associated Alerts	24
Task 3: Device Inventory	26
Task 4: View the Event Timeline	27
Task 5: Data Mining	27
Task 6: Generate a Risk Assessment report.....	29
Exercise 5: Cloud Connect your sensor.....	30
Task 1: Create the cloud connected sensor on the Cloud Management portal	30
Task 2: Upload the activation file to cloud connect your sensor.....	30
Task 3: Verify Cloud connection.....	31
Exercise 6: Integrate with Microsoft Sentinel	32
Task 1: Connecting Data Connectors.....	32
Task 2: Acknowledge Alerts and Re-run PCAPs.....	37
Task 3: Sentinel interaction with IoT Incidents.....	38
Task 4: Kusto Query Language to Find Alert Details.....	40
Exercise 7: Perform an Upgrade	41
Task 1: Download the Upgrade ISO file	41
Task 2: Upgrade your sensor	41
Exercise 8: Clean Up	43
Task 1: Delete resources.....	43

Exercise #1: Enabling Defender

Task 1: Create an Azure Subscription

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



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

Subscriptions

Subscription	Type	Last updated
Visual Studio Enterprise Subscription	Subscription	8 months ago
cloud-shell-storage-eastus	Resource group	11 months ago

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

Subscription name	Subscription ID	My role	Current cost	Secure Score	Parent management group	Status
Visual Studio Enterprise Subscription	2121bd18-92b6-4c80-b379-937e1b90517a	Account admin	C\$518.29	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

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

Azure Active Directory

Microsoft Defender for IoT Micro agent Public Preview
microsoft-defender-for-iot@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 (highlighted with a red box)
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 (highlighted with a red box)
Settings (Preview)

No subscriptions onboarded

Define committed device coverage or work with the trial.

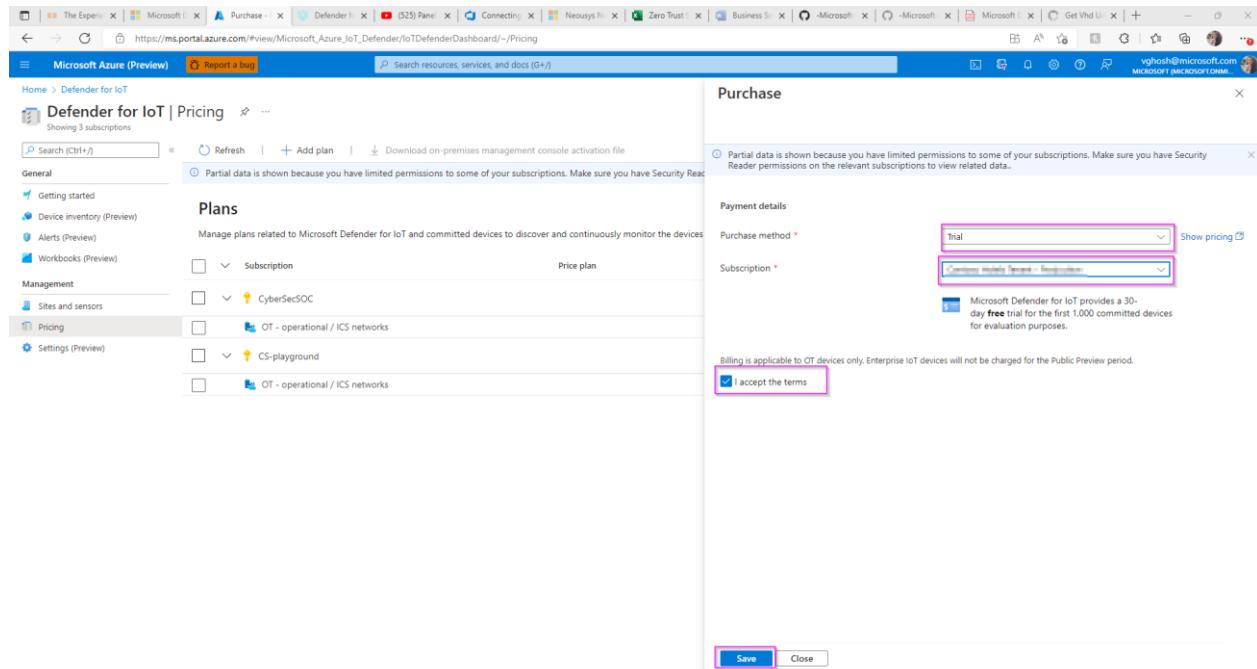
Onboard subscription

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

4. In the popup screen, select:

- a. **Purchase Method: Trail**

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



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

Exercise #2: Deploy the Sensor in Azure

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

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

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

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

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

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

Project details

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

Subscription * ① BuildEnv

Resource group * ② Create new

Instance details

Region * ③ East US

Location ④ [resourceGroup().location]

Deploy Public IP ⑤ true

Put Password To Key Vault ⑥ true

Source VHDURL * ⑦

Sensor Count 1

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

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

Validation Passed

Basics Review + create

Summary

Customized template 3 resources

Terms

Azure Marketplace Terms | Azure Marketplace

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

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

Create < Previous Next

Task 2: Access your Virtual Machine.

Option #1: If you deployed with Keyvault

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

Deployment details (Download)

Resource	Type	Status	Operation details
Reset-password0	Microsoft.Resources/deployments	OK	Operation details
Post-Deployment0	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.

Resources

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

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

Access policies

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

APPLICATION

Name	Email	Key Permissions
SOC-vmsidentityuq63gjmwvo2do-Play		

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

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

Create an access policy ...

SOC-KVuq63gjmwo2do-Play

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

Configure from a template
Key & Secret Management

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

Previous **Next**

5. Under "Principle" select a principle

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

Create an access policy ...

SOC-KVuq63gjmwo2do-Play

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

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Search by object ID, name, or email address

	John Doe
	Jane Smith
	Bob Johnson
	Mike Williams
	Sarah Davis
	David Lee

Selected item
No item selected

6. You can skip over "Application".

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

Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

Permissions Principal Application (optional)

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

Search by object ID, name, or email address

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

Selected item

No item selected

Previous

Next

7. Click on "Create".

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

Create an access policy ...

SOC-KVuq63gjmwvo2do-Play

Permissions Principal Application (optional)

Review + create

Key Permissions

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

Secret Permissions

Secret Management Operations	All selected
Privileged Secret Operations	None selected

Certificate Permissions

Certificate Management Operations	None selected
Privileged Certificate Operations	None selected

Principal

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

Application

Authorized application	None selected
Object ID	None selected

Previous

Create

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

The screenshot shows the Azure portal interface for the 'KeyVaultTest' resource group. The 'Resources' section displays a list of 10 items, with one item, '-Play', highlighted in pink. The highlighted item is a 'Virtual machine' located in 'West US'. Other resources listed include Storage account, Key vault, Network security group, Managed identity, Image, Regular Network Interface, Public IP address, Virtual machine, and Disk.

9. Make a note of the Public IP address.

The screenshot shows the Azure portal details for the virtual machine '-Play'. Under the 'Networking' tab, the 'Virtual machine' section shows the computer name as 'Sensor' and the operating system as 'Linux (ubuntu 18.04)'. The 'Networking' section highlights the 'Public IP address' (20.124.23.178) and the 'Private IP address' (10.10.10.1).

Option #2: If you deployed without Keyvault.

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

The screenshot shows the Azure portal deployment details for 'Microsoft.Template-20220630145822'. The 'Deployment' tab is selected, showing the status of four resources: 'Reset-password0', 'Post-Deploy0', 'VMdeployment', and 'copyvhd'. All resources are marked as 'OK'. The 'Deployment details' table provides a breakdown of the deployment status for each resource.

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

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

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

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

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

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

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

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

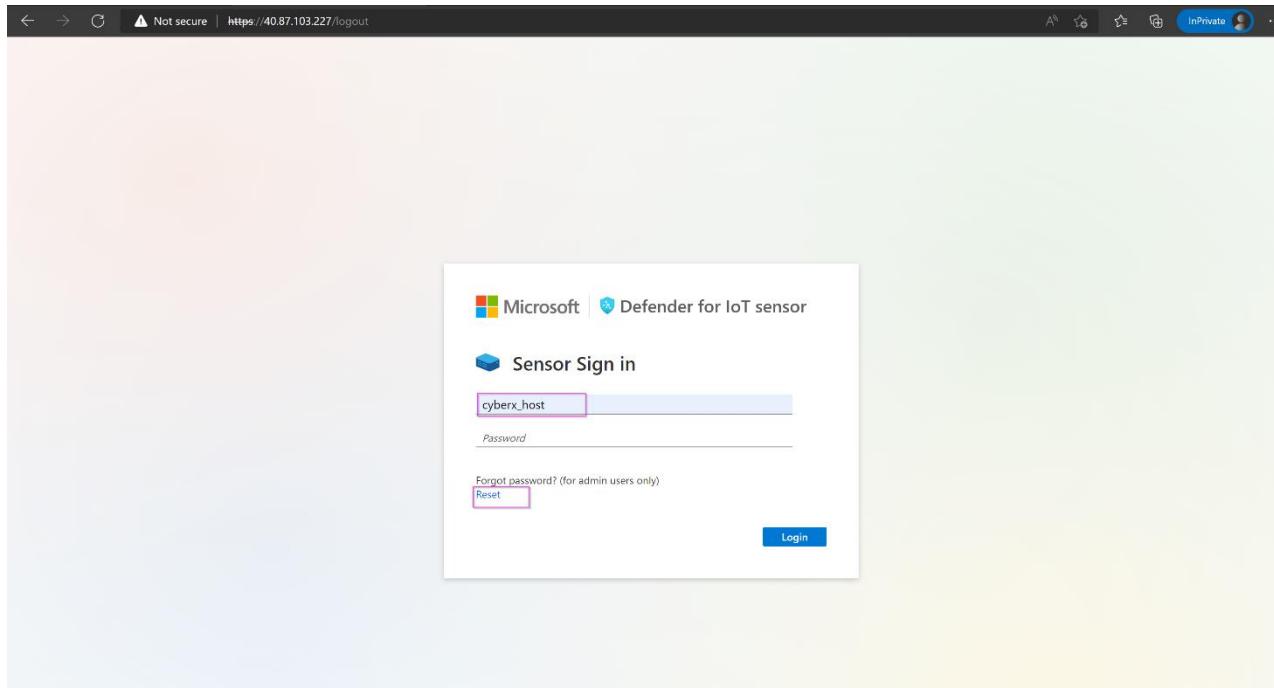
Recover

Insert secret identifier *

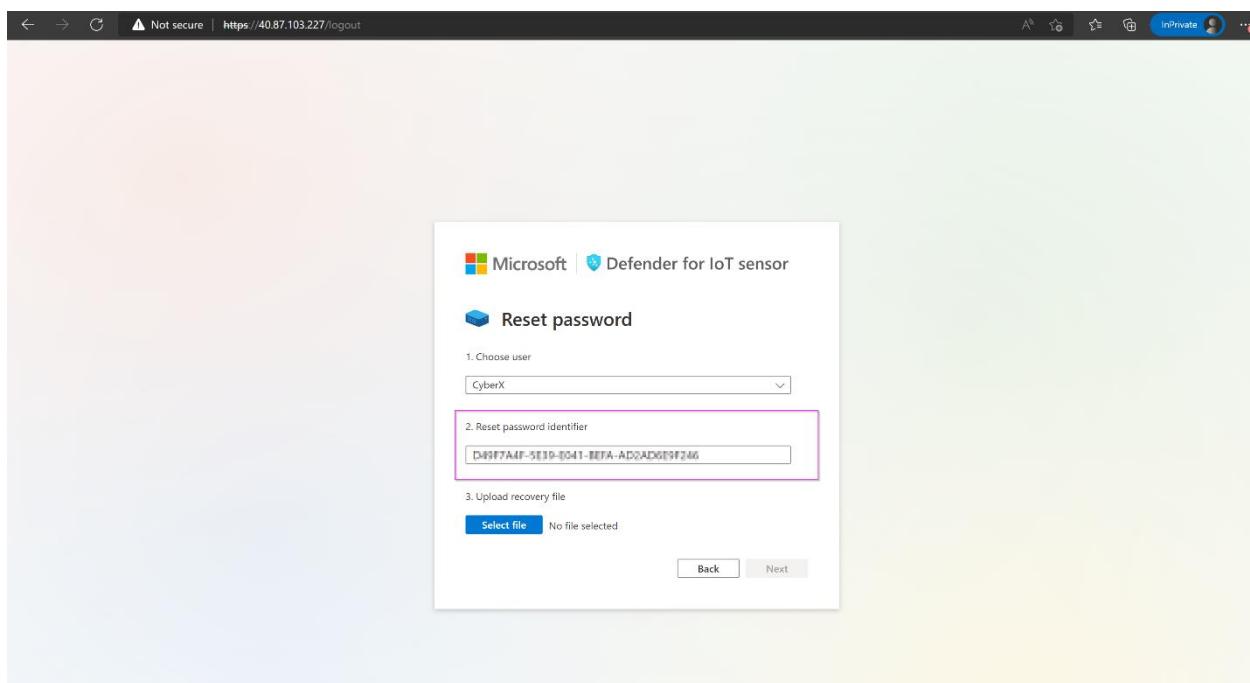
Sub0001-777-0e57-88h12

Recover Cancel

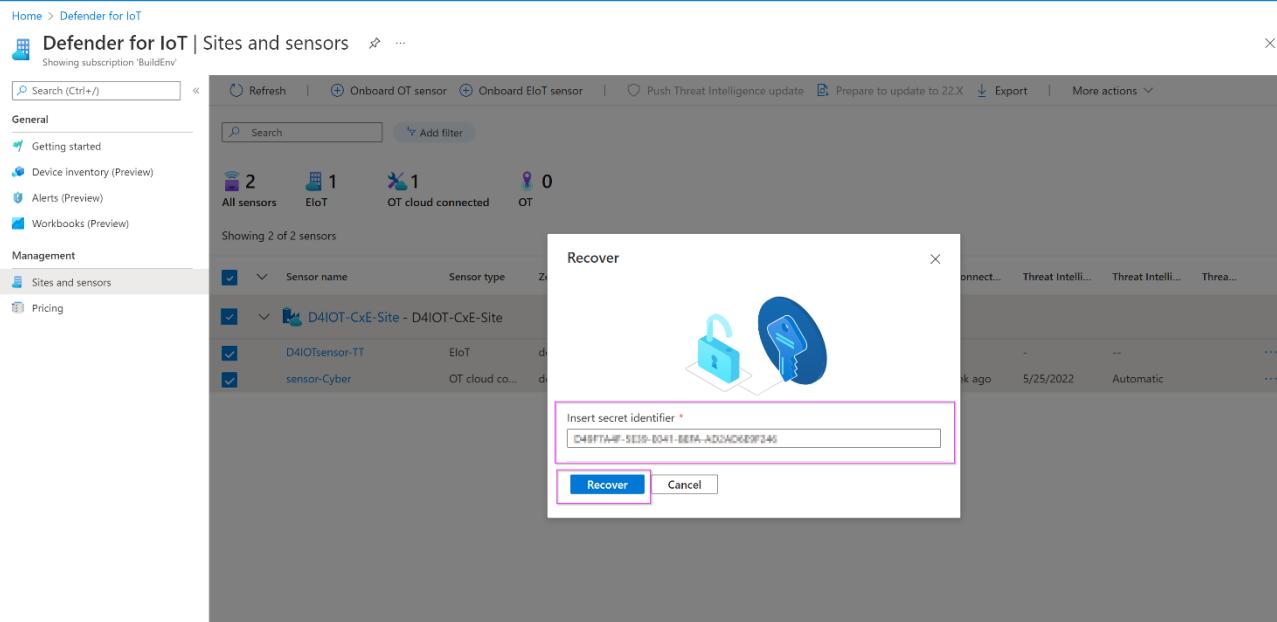
7. Return to the sensor console and type in the username followed by "Reset" as shown.



8. Copy the identifier.

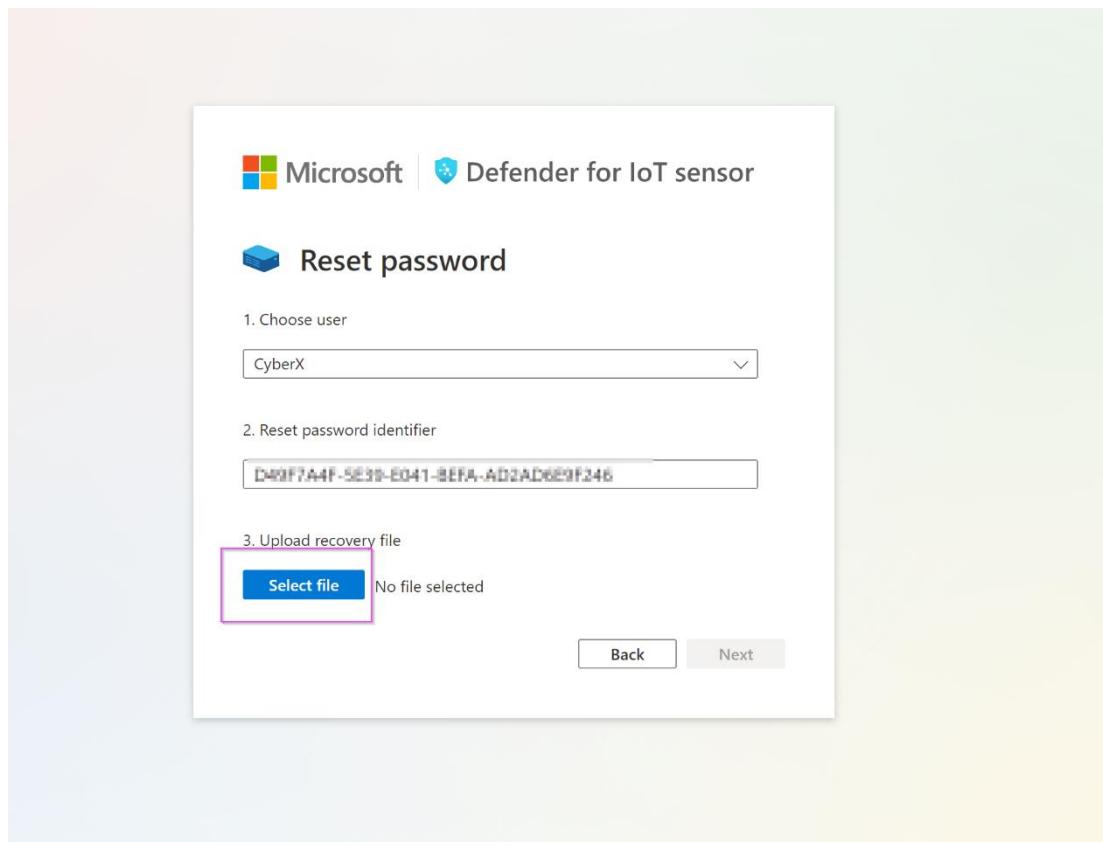


9. Paste in the box on the Defender for IoT Azure window. Click "**Recover**".



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, 'No file selected' is displayed. At the bottom are 'Back' and 'Next' buttons.

11. Click on “**Next**”.

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

Microsoft | Defender for IoT sensor

Reset password

1. Choose user
CyberX_host
2. Reset password identifier
D9F7A4F-5E19-0411-BFA-AD2AD619F246
3. Upload recovery file
Select file password_recovery (1).zip

Back Next

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

The screenshot shows the 'Reset password' process in Microsoft Defender for IoT sensor. Step 4 displays the temporary password 'j^>h@WTU*7IP_3H' in a highlighted input field. The 'Next' button is also highlighted with a pink box.

Microsoft | Defender for IoT sensor

Reset password

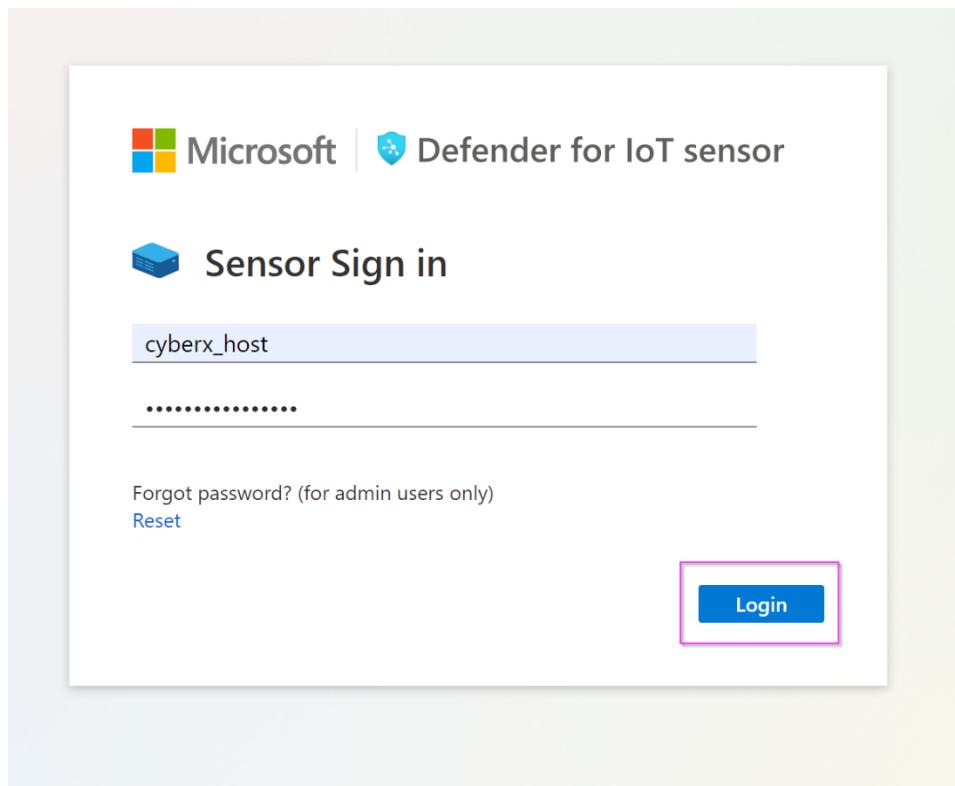
User name
CyberX_host

Password
j^>h@WTU*7IP_3H

Please write your password, it will not be shown again

Next

13. Log in with the new password.



14. Repeat this step for all the usernames.

Exercise #3: Simulate Data in your sensor

Task 1: Enabling the PCAP Player

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

The screenshot shows the Microsoft Defender for IoT - 22.1.3 interface. The left sidebar has a tree view with 'Alerts' expanded, showing 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', and 'Attack vector'. Under 'Manage', 'System settings' is highlighted with a red box. Other options include 'Custom alert rules', 'Users', and 'Forwarding'. The main content area is titled 'System settings' under 'Defender for IoT'. It contains four cards: 'Sensor Network Settings' (Define sensor network settings), 'Connection to Management Console' (Connect this sensor to the on-premises management console), 'Time & Region' (Define time zone settings for this sensor), and 'Subnets' (Define which networks should be monitored by this sensor). The top right corner shows user information for 'cyberx_host'.

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

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with sections like Alerts, Analyze, and Manage. Under Manage, 'System settings' is selected. The main area is titled 'Health and troubleshooting' and contains four cards: 'Backup & Restore', 'System Health Check', 'SNMP MIB Monitoring', and 'Advanced Configurations'. The 'Advanced Configurations' card is highlighted with a red box.

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

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

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

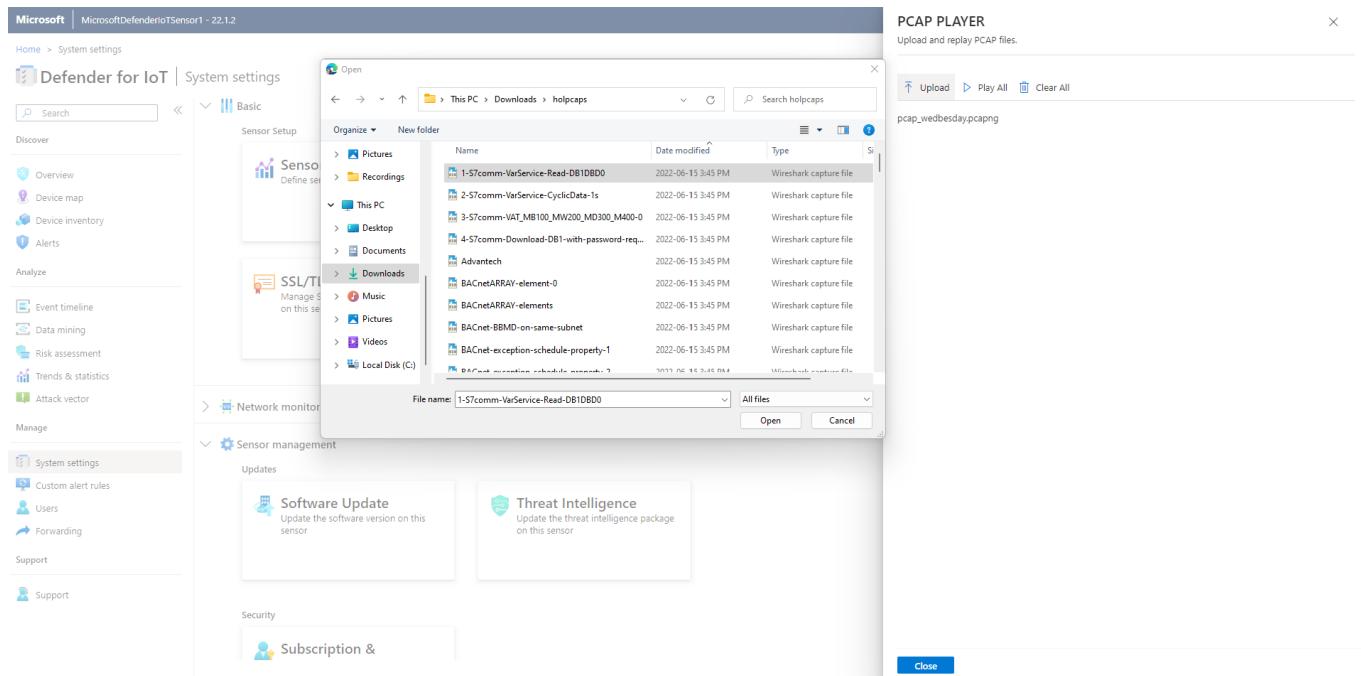
The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a sidebar with options like 'Analyze', 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', and 'Attack vector'. Under 'Manage', 'System settings' is selected. The main area shows 'Defender for IoT | System settings'. There are sections for 'Backup data and restore the latest backup' and 'SNMP MIB Monitoring'. On the right, a 'Advanced configurations' pane is open, specifically the 'Pcaps' tab. It contains several configuration parameters. A red box highlights the 'Save' button at the bottom of this pane.

Task 2: Play PCAP files

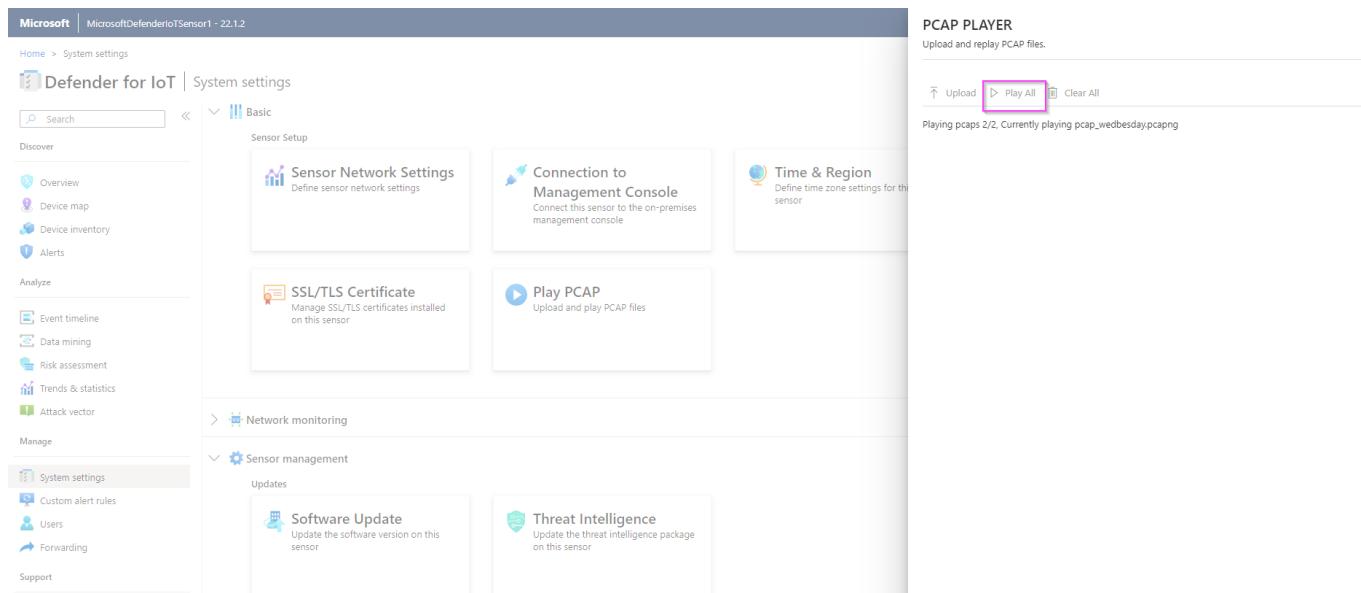
1. Use [this](#) link to download the holcaps.zip folder.
2. Unzip the folder.
3. Scroll all the way down to the bottom to locate if the PCAP Player is enabled (Shown in the image below in the red top square) or not. If the PCAP player is not shown, proceed to click on the arrow next to the **Sensor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

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar includes 'Analyze', 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', and 'Attack vector'. Under 'Manage', 'System settings' is selected. The main area shows 'Defender for IoT | System settings'. It features sections for 'SSL/TLS Certificate' and 'Play PCAP'. A red box highlights the 'Sensor management' button under 'Manage'. Another red box highlights the 'Play PCAP' section, which includes a 'Upload and play PCAP files' button.

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



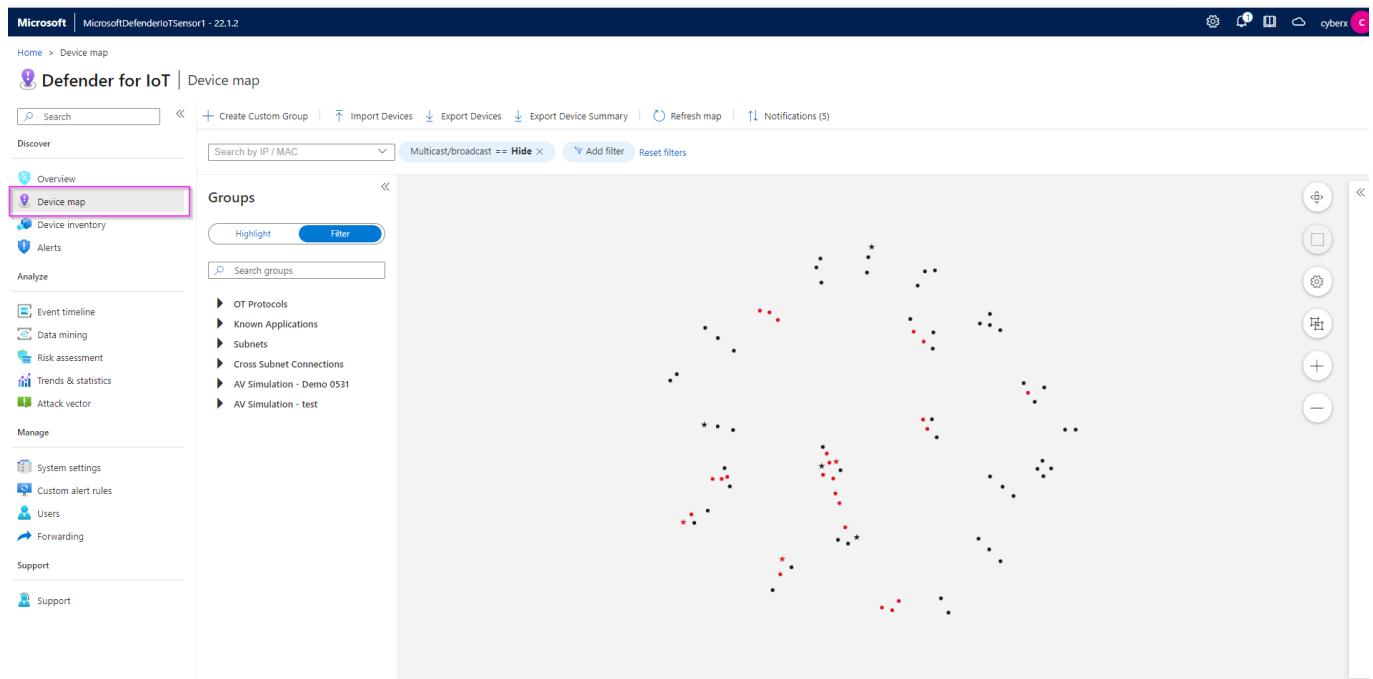
5. Click "Play All" to play the Pcaps.



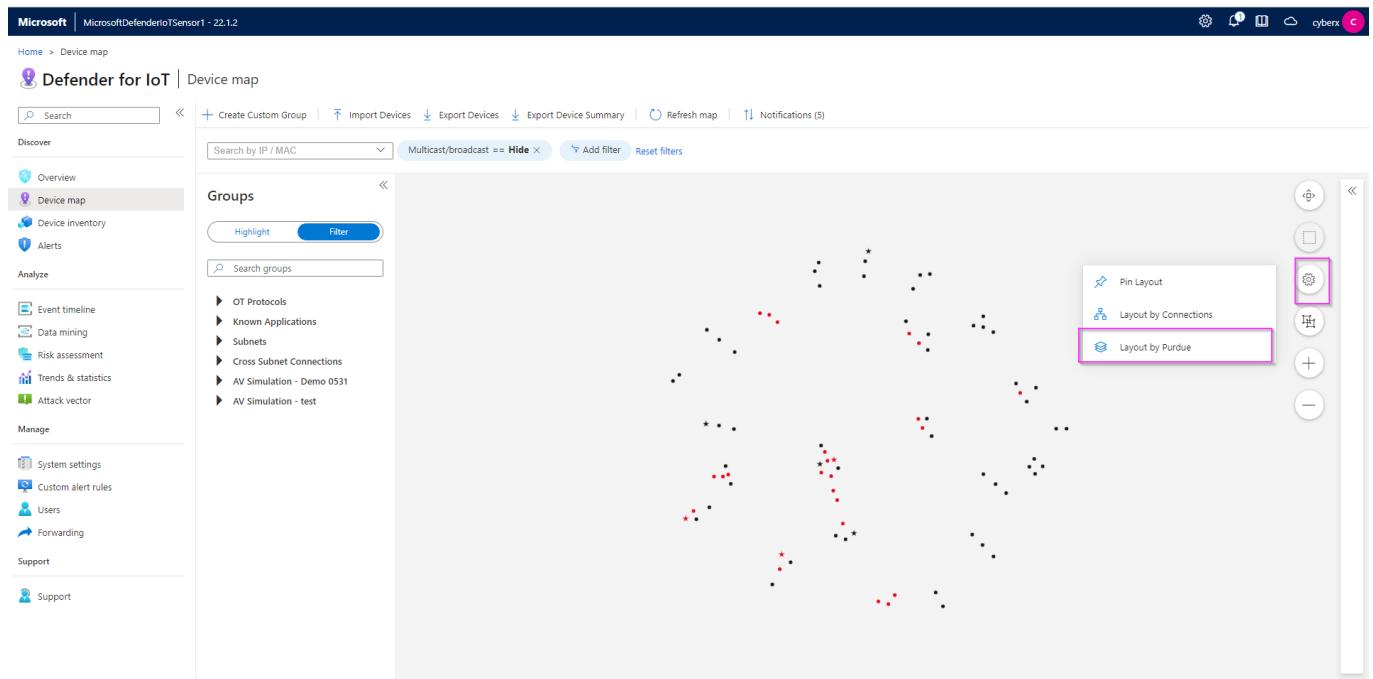
Exercise 4: Analyzing the Data

Task 1: Visualize on the Device Map

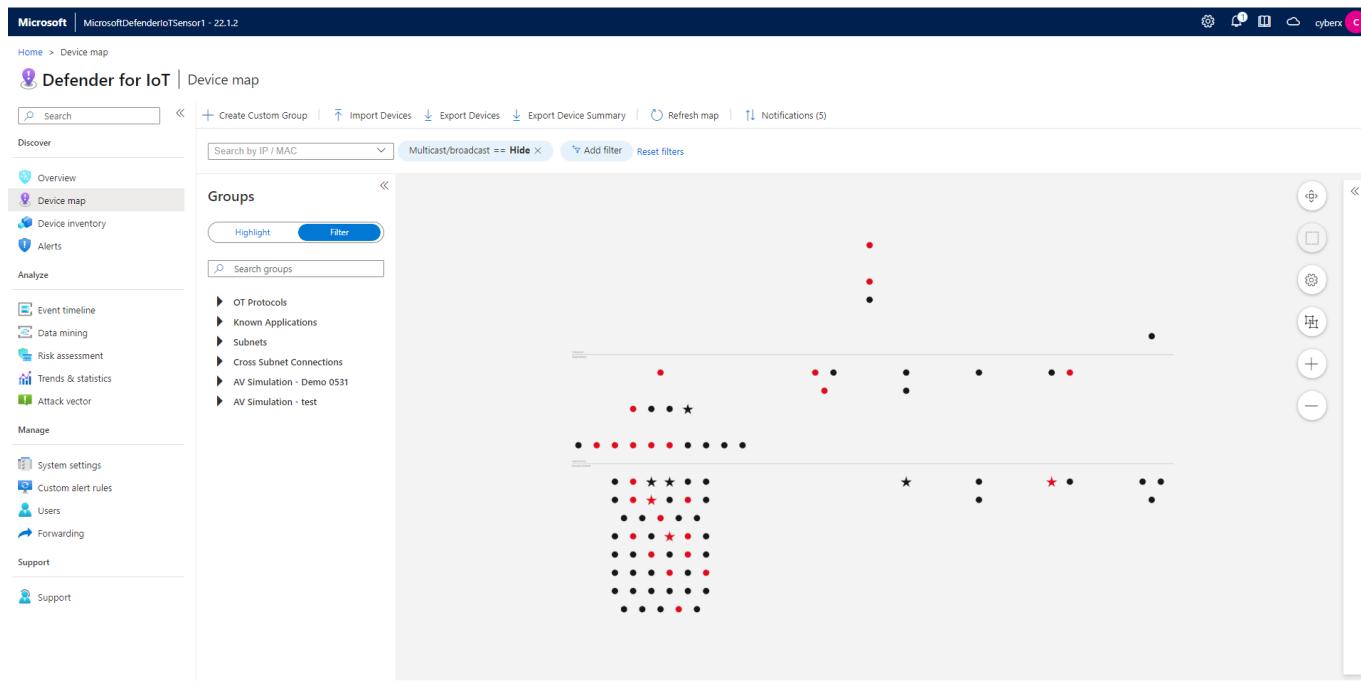
1. Click on “Device Map” from the menu on the left side.



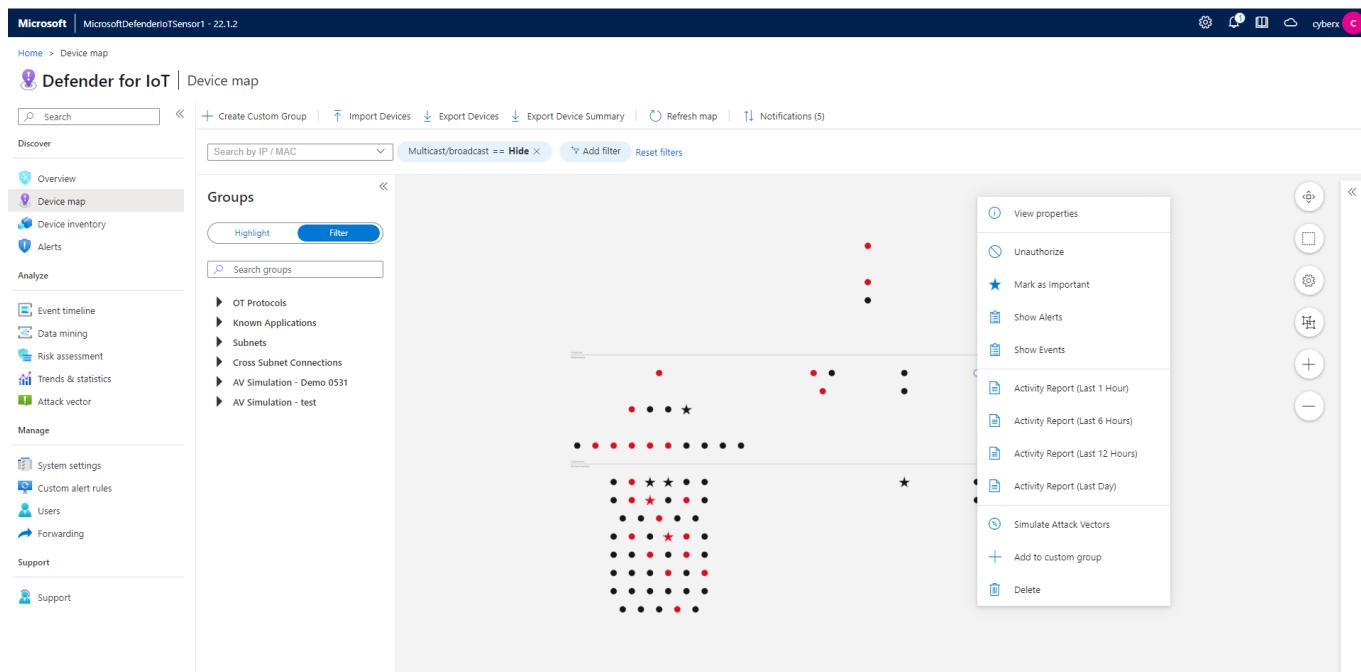
2. Click on the “Settings” option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.



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



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



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

The screenshot shows the Microsoft Defender for IoT Device map interface. On the left, a sidebar lists various categories: Discover, Overview, Device map (which is selected and highlighted in blue), Device inventory, Alerts, Analyze, Manage, and Support. Under the 'Analyze' section, there are links for Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector, System settings, Custom alert rules, Users, Forwarding, and Support. The main area displays a network diagram with three nodes: 192.168.109.1, 192.168.109.21, and 192.168.109.2. Each node has an alert icon. To the right of the nodes is a vertical toolbar with icons for zoom, refresh, and other navigation functions. On the far right, there is a vertical sidebar with icons for search, filter, and other settings.

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, similar to the previous one but with a different network topology. It features four nodes: 192.168.110.2, 192.168.110.1, 192.168.110.4, and 192.168.110.10. The node 192.168.110.10 has an alert icon. A context menu is open over this device, listing options such as 'View properties', 'Unauthorized', 'Mark as Important', 'Show Alerts' (which is highlighted with a pink box), 'Show Events', 'Activity Report (Last 1 Hour)', 'Activity Report (Last 6 Hours)', 'Activity Report (Last 12 Hours)', 'Activity Report (Last Day)', 'Simulate Attack Vectors', 'Add to custom group', and 'Delete'. The sidebar on the left and the vertical toolbar on the right are also visible.

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 search bar at the top is also highlighted with a pink box.

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

This screenshot shows the Microsoft Defender for IoT Alerts page. The 'Alerts' option in the left sidebar is selected and highlighted with a pink border. The main area displays a table of alerts with one row selected and highlighted with a pink border. This selected row corresponds to the 'Unauthorized Internet Connectivity Detected' alert from the previous screenshot. The right side of the screen shows a detailed view of this alert, including its ID (Alert ID: 53), status (New), and detection time (2 weeks ago). It also includes a 'Description' section with a note about a device communicating with external addresses and a 'Related Devices' section showing a connection between 'Source device' (192.168.110.21, Engineering Station) and 'Destination device' (Internet (37.142.39.186), Internet). At the bottom, there 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:f9:74:d8:21	INTEL CORPORA...					
192.168.100.1	192.168.100.1	50 minutes ago	Server	DNS							
192.168.1.11	192.168.1.11	50 minutes ago	PLC	Siemens S7	00:fb:54:db:ef:9	NETGEAR					
192.168.1.180	192.168.1.180	50 minutes ago	HMI	Siemens S7							
192.168.117.23	192.168.117.23	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:92:c6	SCHWEITZER EN...					
192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	00:23:ea:49:5a:c2	CISCO SYSTEMS ...					
192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	00:30:a7:08:97:0	SCHWEITZER EN...					
192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	00:cc:c1:02:09:da	EATON CORPOR...					
192.168.117.7	192.168.117.7	22 hours ago	PLC	Siemens SICAM	00:e0:a8:01:90:be	SAT GMBH & CO.	15.01	CPC65 (6065)			
192.168.117.239	192.168.117.239	22 hours ago	Unknown	Siemens SICAM	00:0c:29:28:28:38	VMWARE INC.					
192.168.117.8	192.168.117.8	22 hours ago	PLC	Siemens SICAM	00:e0:a8:01:90:bb	SAT GMBH & CO.	15.01	CPC65 (6065)			
192.168.107.10	FC50507	22 hours ago	DCS Controller	Yokogawa VNet/IP	00:00:64:9d:5d:10	YOKOGAWA DIG...					
192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9d:73:d4	YOKOGAWA DIG...					
192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	00:00:64:9e:84:e5	YOKOGAWA DIG...					
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-6EH14...	0	4	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-9EH14...	1	2	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	00:01:e3:11:22:33	SIEMENS AG	3.2.6	6E57 315-8EH14...	1	2	

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

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Device inventory

Defender for IoT | Device inventory

Search | Save Filter | Refresh | Edit Columns | Export

Discover

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

Showing 100 of 291 items

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

Load More...

Task 4: View the Event Timeline

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

Microsoft | MicrosoftDefenderIoTSensor1 - 22.1.2

Home > Event timeline

Defender for IoT | Event timeline

Search | Create event | Refresh | Export

User Operations == Hide | Add filter | Reset filters

Discover

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

Event type

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

Load More...

Task 5: Data Mining

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

The screenshot shows the Microsoft Defender for IoT interface with the 'Data mining' tab selected. On the left, there's a sidebar with various navigation options like Overview, Device map, Device inventory, Alerts, Analyze, Manage, and Support. The main area displays a 'Recommended' section with cards for Programming Commands, Internet Activity, Excluded CVEs, Remote Access, CVEs, and Non Active Devices (Last 7 Days). Below this is a 'My reports' section showing a single entry named 'test'. To the right, a 'Create new report' dialog box is open, prompting for a 'Name' (Report name), 'Description', and 'Choose Category' (Category: PLC Firmware Version, Activity: Report showing the firmware version of the different PLCs). It also includes filters for Results within the last 3 Minutes, IP address, MAC address, Port, and Device group, along with a search bar. Buttons for 'Save' and 'Cancel' are at the bottom.

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

This screenshot is similar to the previous one but with several fields highlighted with pink boxes: 'Name' (Report name), 'Description', 'Choose Category' (Category: PLC Firmware Version, Activity: Report showing the firmware version of the different PLCs), 'Results within the last' (3 Minutes), 'IP address', 'MAC address', 'Port', 'Device group', and 'Firmware Version (GENERIC)' under 'Add filter type'. The 'Save' button is also highlighted with a pink box.

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

The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a navigation sidebar with sections like Discover, Analyze, Manage, and Support. Under Analyze, 'Data mining' is selected. In the main area, there's a 'Recommended' section with cards for Programming Commands, Internet Activity, Excluded CVEs, Active Devices (Last 24 Hours), Remote Access, CVEs, and Non Active Devices (Last 7 Days). Below that is a 'My reports' section with a table. One row in the table, 'PLC Firmware Version', has a pink box around it. The table columns are Name, Description, and Last modified.

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

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

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

Task 6: Generate a Risk Assessment report

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

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

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

Exercise 5: Cloud Connect your sensor

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

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

The screenshot shows the Microsoft Azure Cloud Management portal with the 'Defender for IoT | Sites and sensors' page selected. At the top, there's a search bar and several navigation icons. Below the header, there are sections for 'General' (Getting started, Device inventory (Preview), Alerts (Preview), Workbooks (Preview)) and 'Management' (Sites and sensors). The 'Sites and sensors' section is highlighted with a pink box. It displays statistics: All sensors (4), EIoT (1), OT cloud connected (2), and OT (1). Below this, it says 'Showing 4 of 4 sensors' and lists one entry: 'D4IOT-CxE-Site - D4IOT-CxE-Site'. The 'Onboard OT sensor' button at the top right of the main content area is also highlighted with a pink box.

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

The screenshot shows the 'Step 3: Register this sensor with Microsoft Defender for IoT' configuration page. It includes fields for 'Sensor name' (with a pink box around the input field), 'Subscription' (a dropdown menu with 'Please select a subscription' and 'Onboard subscription' options, both highlighted with a pink box), 'Cloud connected' (a checked checkbox highlighted with a pink box), 'Automatic Threat Intelligence updates' (an unchecked checkbox), 'Sensor version' (set to '22.X and above'), 'Site' (with 'Resource name' and 'Display name' fields, both with pink boxes around them), 'Tags' (a key-value pair field with a pink box around it), and 'Zone' (a dropdown menu with 'No subscription has been selected' and 'Create zone' options, both highlighted with a pink box). At the bottom left is a 'Register' button.

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

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

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

The screenshot shows the Microsoft Defender for IoT Sensor management interface. On the left, there's a 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 under 'Manage' is highlighted with a pink box. In the main area, there are sections for 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). The 'Subscription & Activation Mode' section contains a sub-instruction: 'Upload an activation file to reactivate this sensor'.

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

The screenshot shows the Microsoft Defender for IoT Sensor management interface with the 'Subscription & Activation Mode' dialog box open. The dialog box has a header 'Subscription & Activation Mode' and a sub-instruction 'Upload the activation file received from Microsoft Defender for IoT to reactivate this sensor.' It contains fields for Activation Mode (Cloud Connected), Activation Status (Active), Tenant ID (5f1060f2-d9a4-4f59-bf0c-1dd8f3604a4b), Subscription ID (1e61ccbf-70a3-45a3-a1fb-848ce45cd71a5), and an 'Upload activation file:' input field 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 6: Integrate with Microsoft Sentinel

Task 1: Connecting Data Connectors

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

2. Create a new workspace.

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

4. Click the Open Connector Page.

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

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

The screenshot shows the Microsoft Defender for IoT (Preview) configuration page. It has sections for 'Instructions' and 'Next steps'. Under 'Prerequisites', it lists 'Workspace' and 'Subscription' requirements. The 'Configuration' section starts with a 'Connect Microsoft Defender for IoT to Microsoft Sentinel' heading. It includes a note about selecting 'Connect' for desired subscriptions and links to 'Microsoft Defender for IoT pricing model' and 'Select the relevant Subscriptions to connect'. At the bottom, there's a table for connecting subscriptions. The 'Azure Pass - Sponsorship' row has a 'Connect' button (which is highlighted with a red box) and a 'Disconnect' button.

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

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

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

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

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

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

Task 2: Acknowledge Alerts and Re-run PCAPs

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

The screenshot shows the Microsoft Defender for IoT Sensor1 console. On the left, there's a navigation sidebar with sections like Discover, Overview, Device map, Device inventory, and Alerts. The 'Alerts' section is highlighted with a pink rectangle. In the main content area, the 'Alerts' blade is displayed, showing a list of 22 alerts. The alerts are grouped by severity: Critical, Major, and Warning. Each alert includes details such as Name, Engine, Detection time, Status, and Source Device. The 'Learn' button at the top right of the alert list is highlighted with a pink rectangle. The alert list table has columns for Severity, Name, Engine, Detection time, Status, and Source Device.

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

The screenshot shows the Microsoft Defender for IoT Sensor Settings page. On the left, there's a navigation sidebar with sections like Discover, Analyze, Manage, and Support. The main area shows basic sensor setup options: Sensor Network Settings, Connection to Management Console, Time & Region, SSL/TLS Certificate, and Play PCAP. A PCAP Player window is open on the right, showing a file named 'pcap_wednesday.pcapng' with a highlighted 'Play All' button.

Task 3: Sentinel interaction with IoT Incidents

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

The screenshot shows the Microsoft Sentinel Incidents page. The 'Incidents' tab is selected. A search bar at the top right has 'Product name : Microsoft Defender for IoT' and 'Owner : All' filters applied. The main table lists 16 incidents, including Unauthorized Internet Conne... and BACNet Operation Failed, with columns for Severity, Incident ID, Title, Alerts, Product names, Created time, Last update time, and Owner.

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

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

Microsoft Sentinel | Incidents

Selected workspace: mylogoworkspace-msiot2

General

Threat management

Content management

Configuration

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

Content hub (Preview)

Repositories (Preview)

Community

Data connectors

Analytics

Watchlist

Automation

Settings

Open incidents: 16

New incidents: 16

Active incidents: 0

Open incidents by severity:

- High (4)
- Medium (10)
- Low (2)
- Informational (0)

Search by ID, title, tags, owner or product

Severity: All

Status: 2 selected

Product name: Microsoft Defender for IoT

Owner: All

Description: Unauthorized Internet Connectivity Detected

Incident ID: 16

Investigate in Microsoft Defender for IoT

Owner: Unassigned

Status: New

Severity: High

Alerts: 1

Events: 0

Bookmarks: 0

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

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

Entities (4): 141.81.0.139, 10.200.1.124, HUB-MD4IOT-MST..., 10.200.1.124

Tactics (1): Initial Access

View full details >

Tags

View full details

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

Microsoft Azure

Home > Microsoft Sentinel >

Incident

Incident ID: 16

Refresh

Unauthorized Internet Connectivity Detected

Incident ID: 16

Investigate in Microsoft Defender for IoT

Owner: Unassigned

Status: New

Severity: High

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

Evidence

Events: N/A (0)

Alerts: 1

Bookmarks: 0

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

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

Entities (4): 141.81.0.139, 10.200.1.124, HUB-MD4IOT-MST..., 10.200.1.124

Tactics (1): Initial Access

View full details >

Timeline

Alerts

Bookmarks

Entities

Comments

Search

Timeline content: All

Severity: All

Tactics: All

Jan 25 4:41 PM Unauthorized Internet Connectivity Detected

High | Detected by Microsoft Defender for IoT | Tactics: Initial Access

View playbooks

Unauthorized Internet Connectivity Detected

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

Severity: High

Status: New

Events: N/A

Product name: Microsoft Defender for IoT

Entities (4): 141.81.0.139, 10.200.1.124, HUB-MD4IOT-MST..., 10.200.1.124

Tactics (1): Initial Access

System alert ID: 741e1606-64de-5f93-8336--

Last update time: 01/25/22, 04:41 PM

Updates: 0 (0)

Start time: 01/25/22, 04:41 PM

End time: 01/25/22, 04:41 PM

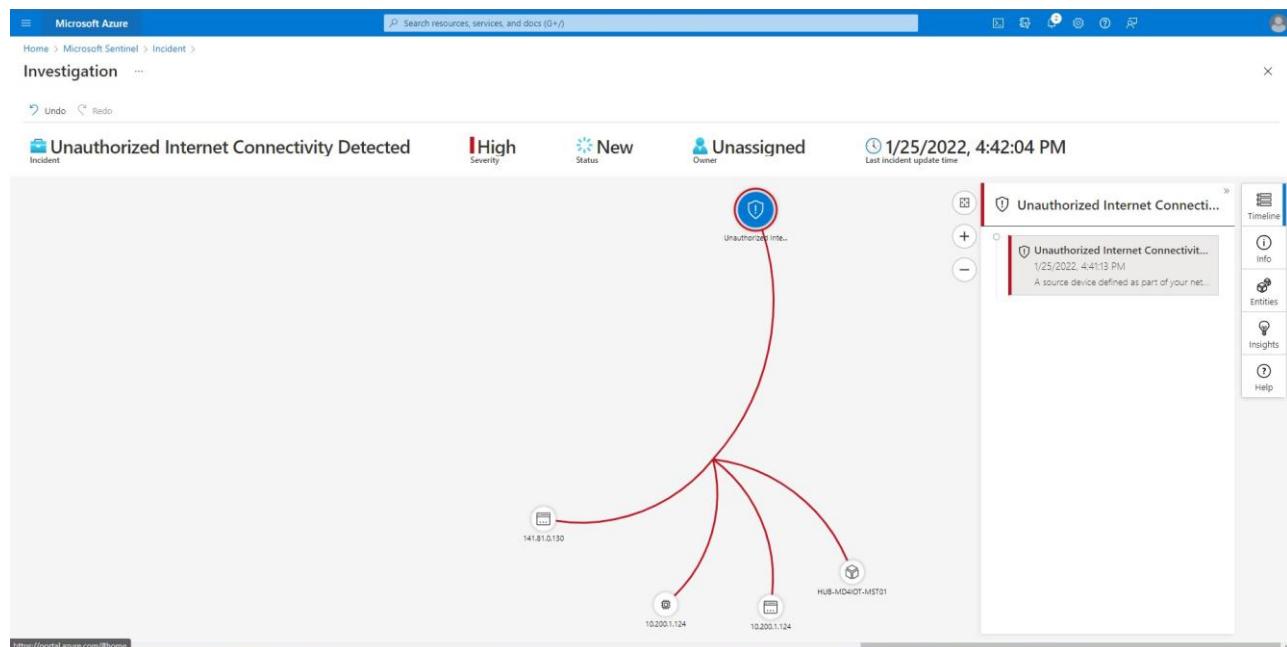
Alert link: https://portal.azure.com/#blade/Microsoft_Azure_IoT_Defender/Alert...

Remediation steps

Investigate

Actions

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



Task 4: Kusto Query Language to Find Alert Details

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

SecurityAlert | where ProviderName contains "IoTSecurity"

TimeGenerated (UTC)	DisplayName	AlertName	AlertSeverity	Description
1/25/2022, 3:41:27.651 PM	Unknown Object Sent to Outstation	Unknown Object Sent to Outstation	Medium	The destination device received an invalid request.
1/25/2022, 3:42:27.511 PM	Outstation Restarts Frequently	Outstation Restarts Frequently	Low	An excessive number of cold restarts were detected on a source device.
1/25/2022, 3:41:27.464 PM	Firmware Change Detected	Firmware Change Detected	Medium	Firmware was updated on a source device. This may be authentic or malicious.
1/25/2022, 3:42:27.361 PM	Port Scan Detected	Port Scan Detected	High	A source device was detected scanning network devices. This may be authentic or malicious.
1/25/2022, 3:44:27.356 PM	Port Scan Detected	Port Scan Detected	High	A source device was detected scanning network devices. This may be authentic or malicious.
1/25/2022, 3:43:27.373 PM	Unauthorized Internet Connectivity Dete...	Unauthorized Internet Connectivity Dete...	High	A source device defined as part of your network is communicating with an external network.
1/25/2022, 3:40:27.499 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.
1/25/2022, 3:42:27.473 PM	Outstation Restarted	Outstation Restarted	Low	A cold restart was detected on a source device. This means the device has been powered off and back on.
1/25/2022, 3:41:27.324 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.
1/25/2022, 3:41:27.443 PM	EtherNet/IP CIP Service Request Failed	EtherNet/IP CIP Service Request Failed	Medium	A server returned an error code. This indicates a server error.
1/25/2022, 3:41:27.407 PM	Controller Stop	Controller Stop	Low	The source device sent a stop command to a destination component.
1/25/2022, 3:41:27.384 PM	BACNet Operation Failed	BACNet Operation Failed	Medium	A server returned an error code. This indicates a server error.

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

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

Exercise 7: Perform an Upgrade

Task 1: Download the Upgrade ISO file

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

The screenshot shows the Azure Defender for IoT Getting started page for Sensors. The left sidebar includes links for General (Getting started, Device inventory (Preview), Alerts (Preview), Recommendations (Preview), Workbooks), Management (Sites and sensors, Plans and pricing, Settings (Preview)), and Troubleshooting + Support (Diagnose and solve problems). The main content area is titled "Sensor" and shows two options: "Buy preconfigured appliance" and "Purchase an appliance and install software". The "Purchase an appliance and install software" section includes a note about version 22.2.9 supporting a new cloud connectivity model. It also shows a dropdown menu for "Select version" set to "22.2.9 (Latest) - recommended" and a "Download" button. A pink box highlights the "Getting started" link in the sidebar and the "Select version" dropdown.

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 'Discover', there's a 'Network monitoring' section. Within this, a 'Sensor management' dropdown is open, showing options like 'Software Update' and 'Threat Intelligence'. The 'Software Update' box 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' section is again highlighted with a pink box, indicating where to click to upload the ISO file.

3. Verify the version on the dashboard.

The screenshot shows the Microsoft Defender for IoT dashboard with the 'Overview' section selected. At the top, it displays 'Microsoft | vishalvadher - 22.2.8'. Below this, there's a summary card with metrics: 0 PPS, 124 Devices, and 32 Alerts. Further down, under 'General Settings', it shows the 'Version:' field which contains the value '22.2.8.20-r-3bd7f37', which is also highlighted with a pink box.

Exercise 8: 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.