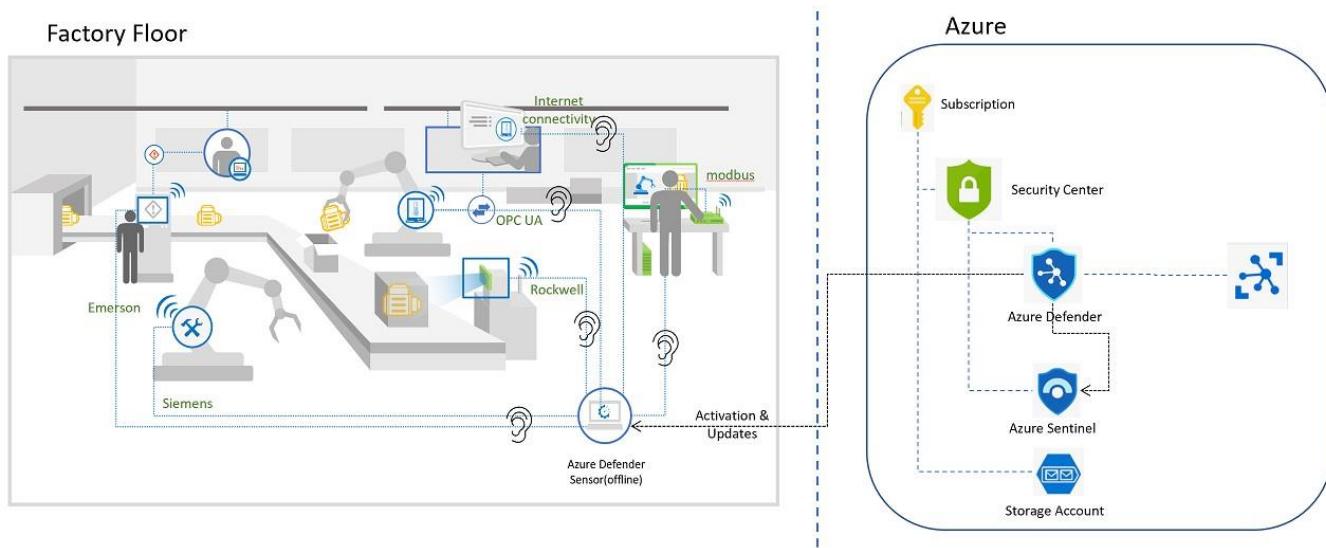


Internet of Things - Microsoft Defender for IoT HOL

Architecture Diagram

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



Contents

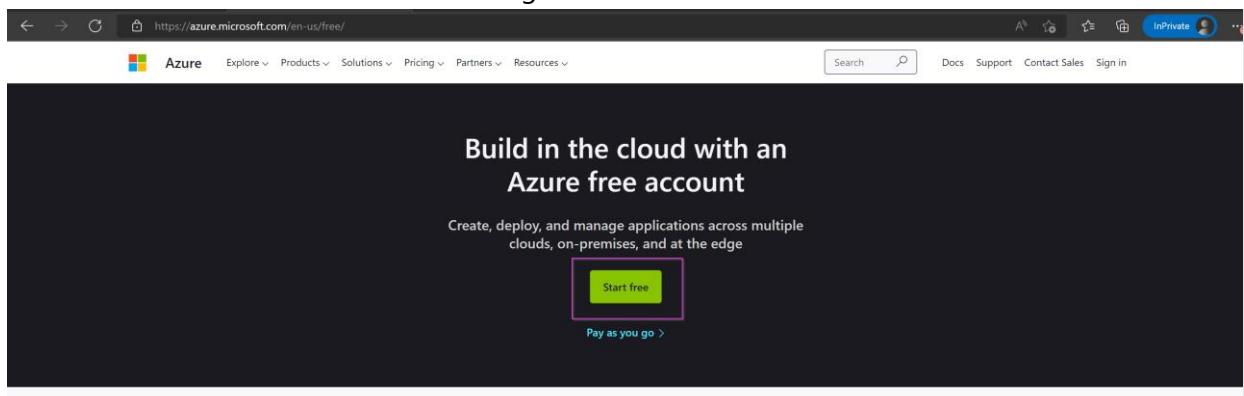
Architecture Diagram.....	1
Exercise #1: Enabling Defender	2
Task 1: Create an Azure Subscription	2
Task 2: Enabling Microsoft Defender for IoT on the Subscription.....	3
Exercise #2: Deploy the Sensor in Azure.....	5
Task 1: Create a Resource group to automatically deploy your sensor, storage account and network security group to.....	5
Task 2: Access your Virtual Machine.....	7
Task 3: Access your sensor via the console.....	11
Exercise #3: Simulate Data in your sensor.....	16
Task 1: Enabling the PCAP Player.....	16
Task 2: Play PCAP files.....	18
Exercise 4: Analyzing the Data	19
Task 1: Visualize on the Device Map.....	19
Task 2: View the associated Alerts.....	22
Task 3: Device Inventory	24

Task 4: View the Event Timeline.....	25
Task 5: Data Mining	25
Task 6: Generate a Risk Assessment report.....	27
Exercise 5: Cloud Connect your sensor.....	28
Task 1: Create the cloud connected sensor on the Cloud Management portal	28
Task 2: Upload the activation file to cloud connect your sensor.	28
Task 3: Verify Cloud connection	29
Exercise 6: Integrate with Microsoft Sentinel.....	30
Task 1: Connecting Data Connectors.....	30
Task 2: Acknowledge Alerts and Re-run PCAPs	35
Task 3: Sentinel interaction with IoT Incidents	36
Task 4: Kusto Query Language to Find Alert Details	38
Exercise 6: Clean Up.....	39
Task 1: Delete resources.....	39

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/](https://azure.microsoft.com/en-us/free/).
2. Click on “**Start Free**” as shown in the image



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

The screenshot shows the Microsoft Azure portal homepage. The left sidebar has 'Azure services' and 'Resource' sections. The main area is titled 'Subscriptions' with a sub-section for 'Azure Active Directory'. Below this, there's a list of subscriptions, including 'Visual Studio Enterprise Subscription' which is highlighted with a pink box. Other listed subscriptions include 'Event Hubs Clusters', 'Notification Hubs', 'Device Update for IoT Hubs', and 'Azure Synapse Analytics (private link hubs)'. There are also sections for 'Marketplace' and 'Recent' resources.

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

The screenshot shows the 'Subscriptions' blade in the Azure portal. It lists one subscription: 'Visual Studio Enterprise Subscription'. The blade includes filters at the top and a table with columns for Subscription name, Subscription ID, My role, Current cost, Secure Score, Parent management group, and Status. The 'Status' column shows 'Active' for the listed subscription.

Subscription name	Subscription ID	My role	Current cost	Secure Score	Parent management group	Status
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

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
Group
microsoft-defender-for-iot@service.microsoft.com

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

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

General

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

Management

Sites and sensors
Pricing (highlighted with a purple box)
Settings (Preview)

No subscriptions onboarded

Define committed device coverage or work with the trial.

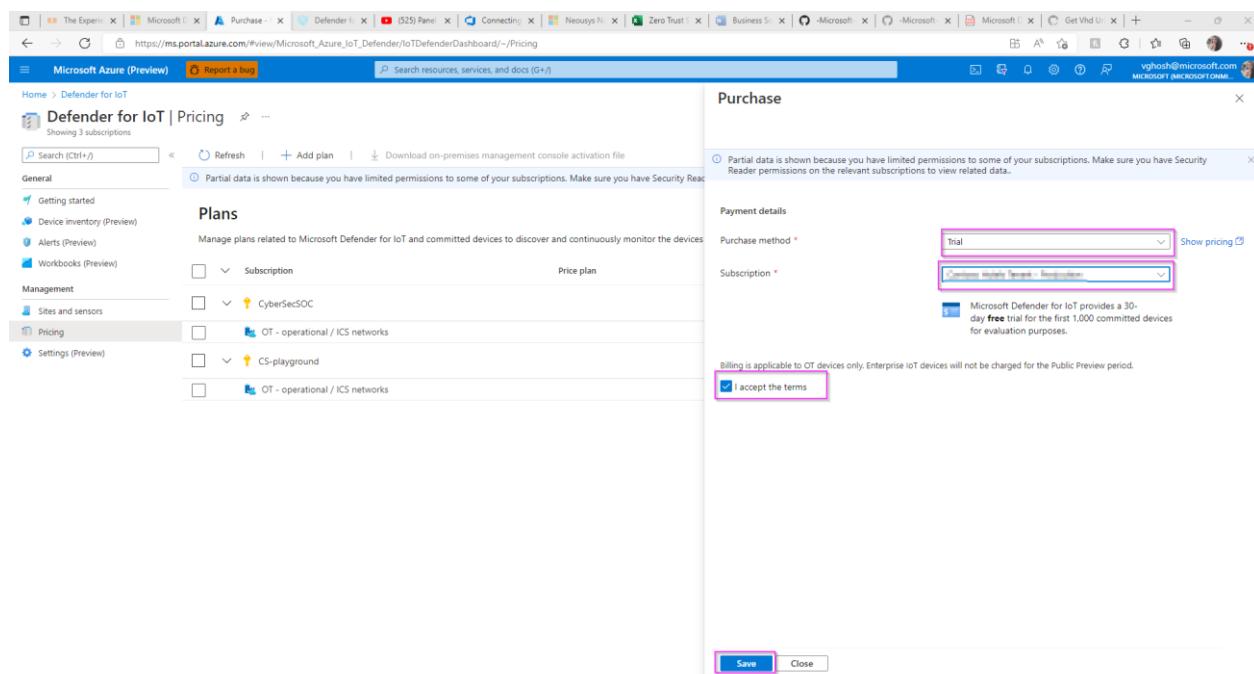
Onboard subscription

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**. The link for the IoT sensor installation is in the email you have received.

Please note - This link is private and will expire in 3 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 ⑧ 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.

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 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-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.

Resources

Name	Type	Location
customxx24k5pt75ngp2	Storage account	West US
SOC-KVx24k5pt75ngp2-Play	Key vault	West US
SOC-NSGx24k5pt75ngp2-Play	Network security group	West US
SOC-Identityx24k5pt75ngp2-Play	Managed identity	West US
SOC-vmsx24k5pt75ngp2-Play-image	Image	West US
SOC-vmsx24k5pt75ngp2-Play-pip0	Regular Network Interface	West US
SOC-vmsx24k5pt75ngp2-Play-pip0	Public IP address	West US
SOC-vmsx24k5pt75ngp2-Play	Virtual machine	West US
SOC-vmsx24k5pt75ngp2-Play-disk1	Disk	West US
SOC-vmsx24k5pt75ngp2-Play	Virtual network	West US

- Click on "Access Policies" -> "Add Access Policies".

Access policies

Current Access Policies

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions	Action
SOC-Identityx24...		0 selected	3 selected	0 selected	Delete

- On "Configure from template" select "Key & Secret Management", on "Select Principle" select "None selected" and type in your email.

The screenshot shows the 'Add access policy' dialog in the Microsoft Azure portal. The 'Principal' dropdown is open, displaying a list of Azure Active Directory users and service principals. One item, 'SOC-vmx24k5pt75ngp2-Play', is highlighted with a pink box.

5. Go to "Secrets" and select the item on the list.

The screenshot shows the 'Secrets' blade in the Microsoft Azure portal for the 'SOC-KVx24k5pt75ngp2-Play' vault. The 'Secrets' tab is selected, and the list shows one item: 'SOC-vmx24k5pt75ngp2-Play'. This item is highlighted with a pink box.

6. Click on the current version.

The screenshot shows the 'Versions' blade in the Microsoft Azure portal for the 'SOC-vmx24k5pt75ngp2-Play' secret. The 'CURRENT VERSION' row is selected and highlighted with a pink box.

7. Copy the secret value to your clipboard.

The screenshot shows the 'Secret Version' details in the Microsoft Azure portal for the 'cf3a7655cda64584ae6faa0514ee47e9' version. The 'Show Secret Value' button is highlighted with a pink box, and a tooltip indicates the value has been copied.

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

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

Deployments : 2 Failed 10 Succeeded
Location : West US

9. Make a note of the Public IP address.

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

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

Properties Monitoring Capabilities (7) Recommendations Tutorials

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

Option #2: If you deployed without Keyvault.

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

Deployment name: Microsoft.Template-20220630145822
Subscription: BuildEnv
Resource group: Vghosh_IoTSensor

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

Deployment details (Download)

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

Next steps
Go to resource group

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

Home > Microsoft.Template-20220630145822 > Reset-password0

Reset-password0 | Outputs

Deployment

Search (Ctrl+ /) vmObject

Outputs (Copied)

Overview Inputs Outputs Template

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

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

Home >

Microsoft.Template-20220630145822 | Overview

Deployment

Search (Ctrl+ /) Delete Cancel Redeploy Refresh

We'd love your feedback! →

Your deployment is complete

Deployment name: Microsoft.Template-20220630145822
Subscription: BuildEnv
Resource group: Vghosh_IoTSensor

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

Deployment details (Download)

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

Next steps

Go to resource group

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

Microsoft Azure (Preview) Search resources, services, and docs (G+)

Home > Microsoft.Template 20220503175515

XXX | resource group

Search (Ctrl+ /) Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete ...

View Cost JSON View

Overview

Subscription (move) : Deployments : 13 Succeeded

Subscription ID : Location : East US

Tags (edit) : Click here to add tags

Resources Recommendations

Filter for any field... Type == all × Location == all × Add filter

Showing 1 to 9 of 9 records. Show hidden types No grouping List view

Name	Type	Location
copyvhd	Deployment Script	East US
customficiw5uSatkwu	Storage account	East US
SOC NSGficiw5uSatkwu-Play	Network security group	East US
SOC-vmficiw5uSatkwu-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
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.

Microsoft | Defender for IoT sensor

Sensor Sign in

User name

Password

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

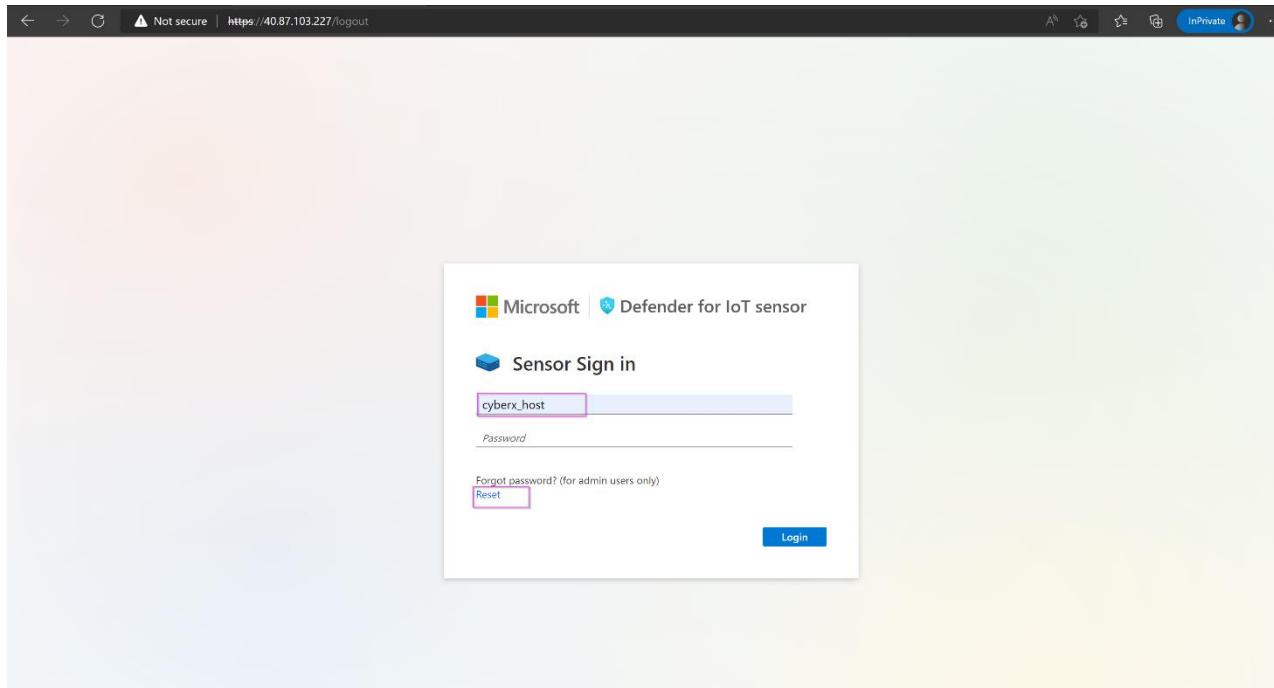
Login

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**.

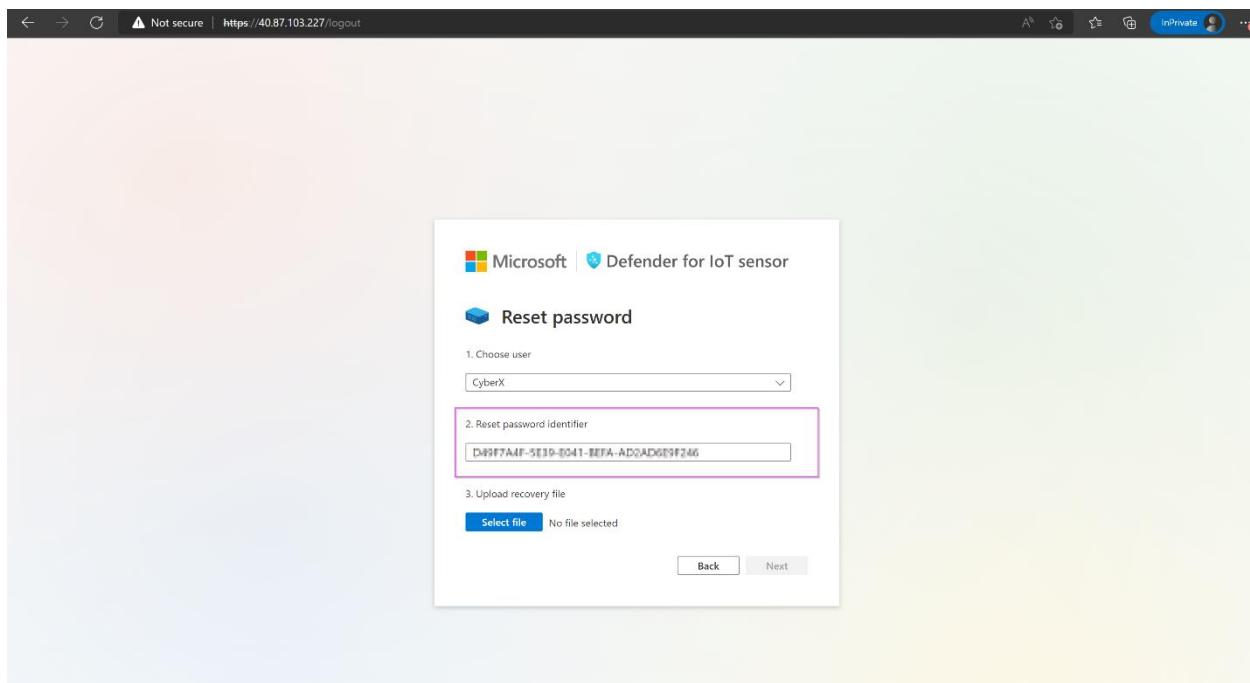
- After signing out, please return to the Azure portal and navigate to “**Defender for IoT**”. Select “**Sites and sensors**”, select your sensor from the list, and click on “**Recover my password**”.

- You will see this prompt asking for the “secret identifier”.

- Return to the sensor console and type in the username followed by “Reset” as shown.



6. Copy the identifier.



7. 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 IoT, 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.

8. 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 and 'No file selected' message. At the bottom are 'Back' and 'Next' buttons.

9. 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

10. 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

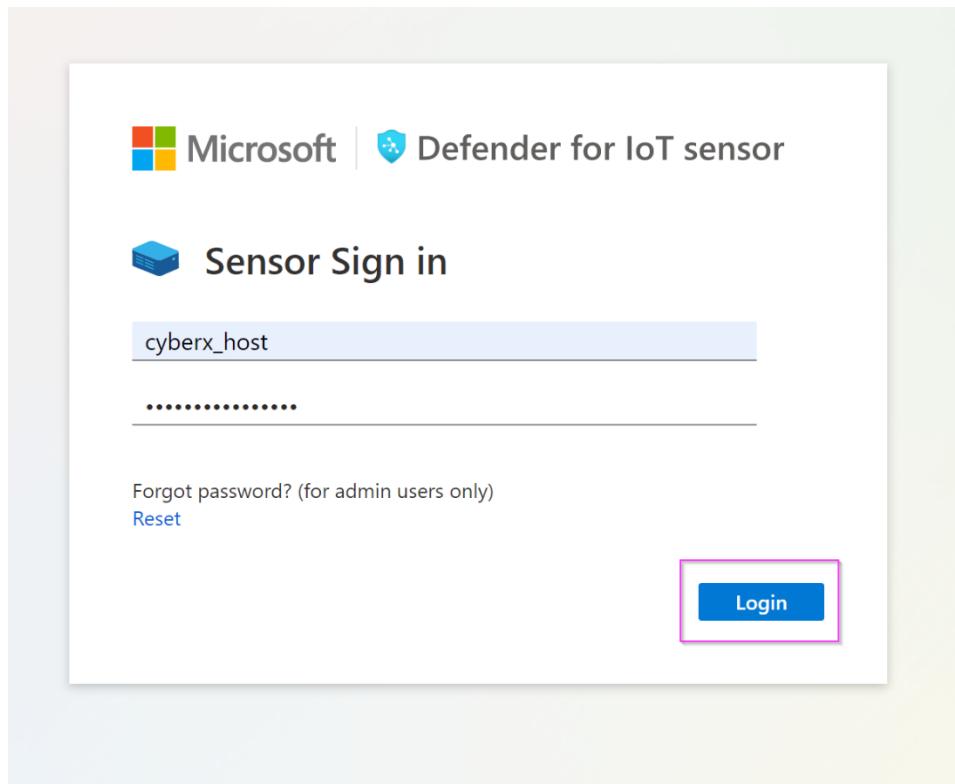
Password

j^>lh@WTU*7IP_3H

Please write your password, it will not be shown again

Next

11. Log in with the new password.



12. 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 web interface. The top navigation bar includes the Microsoft logo, the title "Microsoft Defender for IoT - 22.1.3", and a user profile icon. The left sidebar has a tree view with nodes like "Alerts", "Analyze" (with sub-options: Event timeline, Data mining, Risk assessment, Trends & statistics, Attack vector), "Manage" (with sub-options: System settings, Custom alert rules, Users, Forwarding), and "System settings". The "System settings" node is highlighted with a red box. The main content area is titled "Defender for IoT | System settings" and contains four cards under the heading "Basic": "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 status bar at the bottom right shows the host name "cyberx_host" and a circular icon.

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 is a sidebar with various configuration categories: Import, Internet Addresses, Management, Mysql, Pcaps (which is selected and 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.

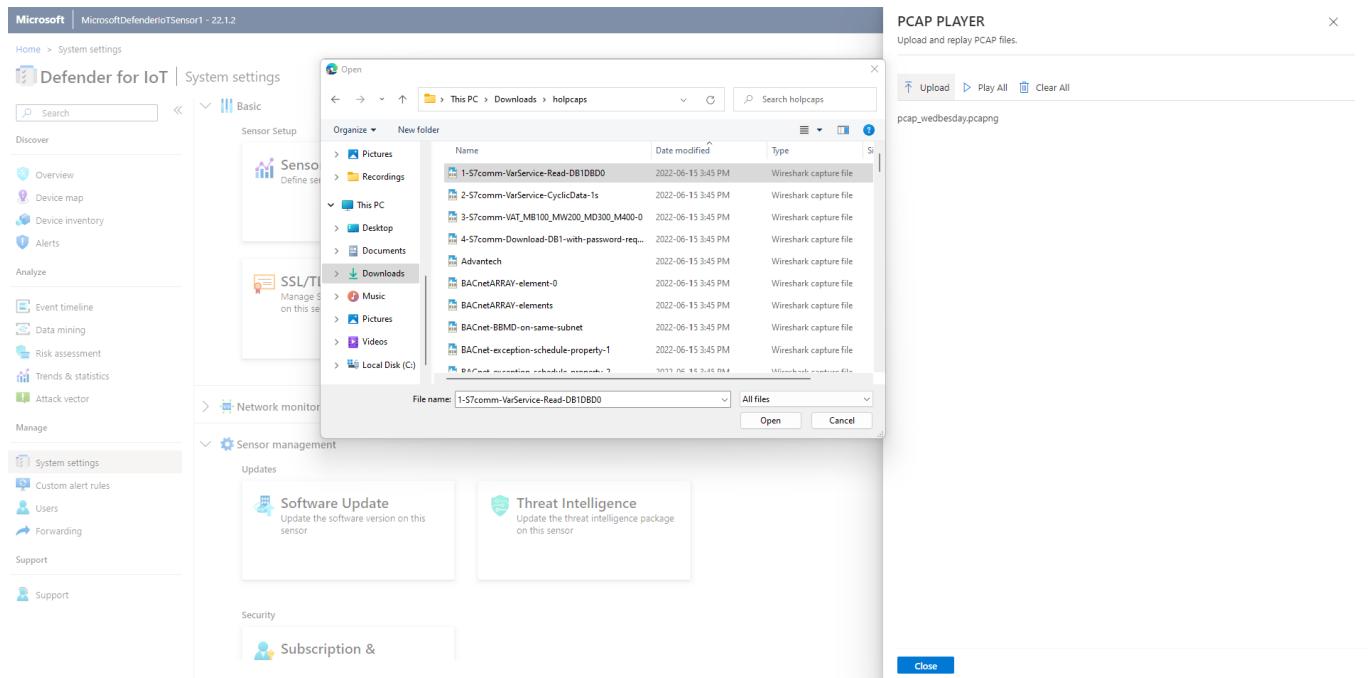
The screenshot shows the Microsoft Defender for IoT interface. On the left, there's a sidebar with options like 'Analyze', 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', and 'Attack vector'. Under 'Manage', 'System settings' is selected. In the main area, there are sections for 'Backup data and restore the latest backup' and 'SNMP MIB Monitoring'. A large red box highlights the 'Save' button at the bottom right of a floating 'Advanced configurations' window. The window also contains configuration parameters such as 'cache.should.save.pcap=1', 'archive.cache.dir=', '# 7 GB', 'filtered.cache.dir.size.megabytes.max=7168', 'filtered.cache.dir.size.megabytes.min=3072', 'player.max_size=1000', 'player.max_amount=20', 'player.params=enabled_0', and 'virtual.lan.hierarchy.depth.support=1'.

Task 2: Play PCAP files

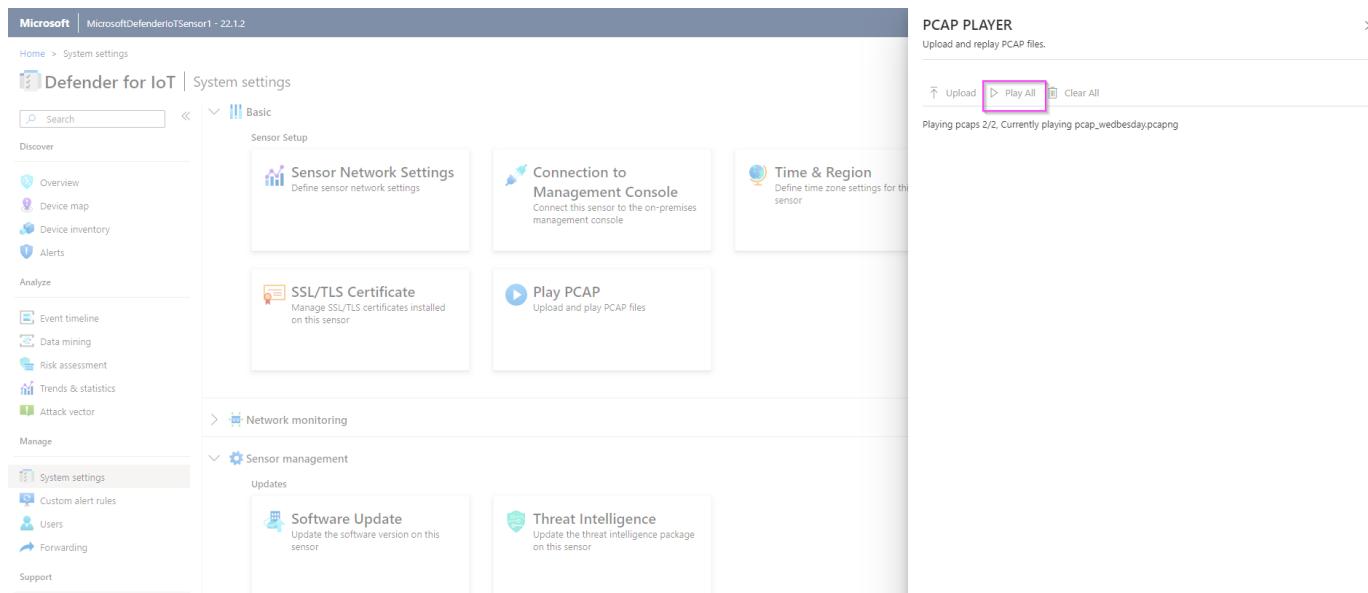
1. Use [this](#) link to download the holcaps.zip folder.
2. Unzip the folder.
3. Scroll all the way down to the bottom to locate if the PCAP Player is enabled (Shown in the image below in the red top square) or not. If the PCAP player is not shown, proceed to click on the arrow next to the **Sensor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

The screenshot shows the Microsoft Defender for IoT interface. The left sidebar includes 'Analyze', 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', 'Attack vector', 'Manage' (with 'System settings' selected), and 'Integrations'. A red box highlights the 'Sensor management' button under 'Manage'. In the main content area, there are sections for 'SSL/TLS Certificate' and 'Play PCAP'. The 'Play PCAP' section has a sub-instruction 'Upload and play PCAP files'. A red box highlights this section. Below it, the navigation menu continues with 'Network monitoring', 'Sensor management' (which is also highlighted by a red box), 'Integrations', and 'Import settings'.

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



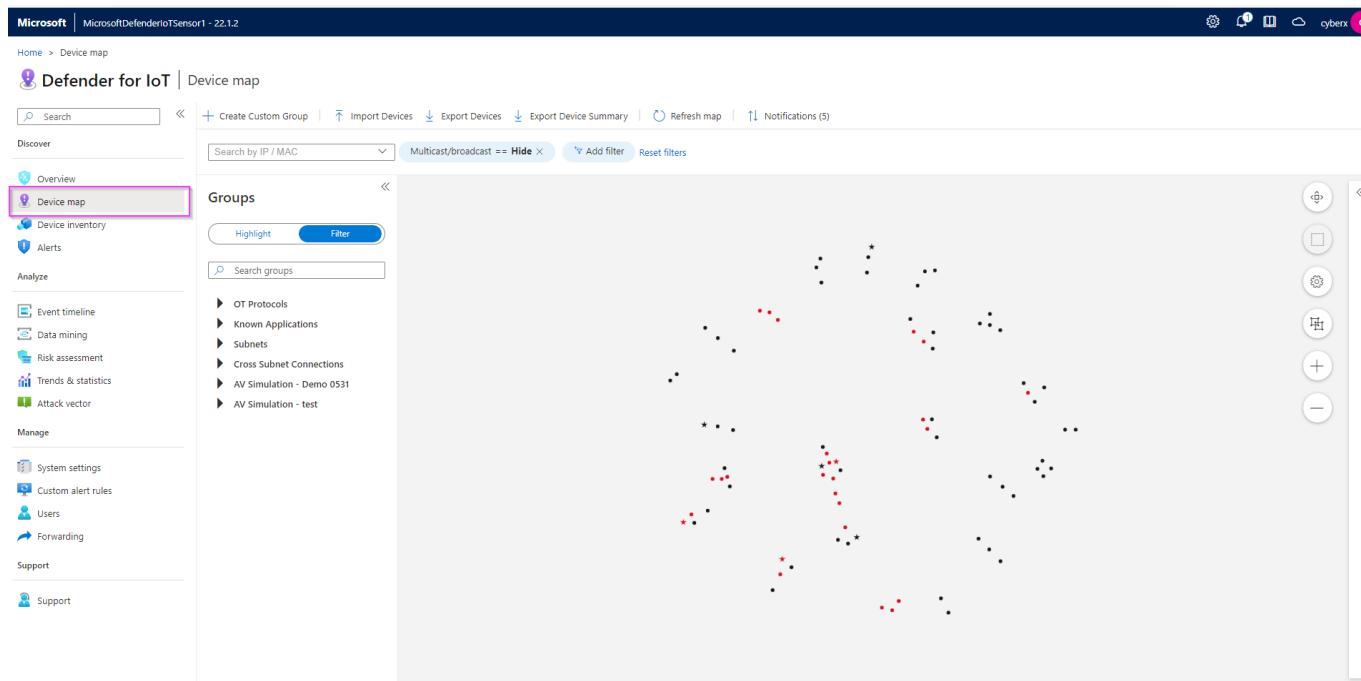
5. Click "Play All" to play the Pcaps.



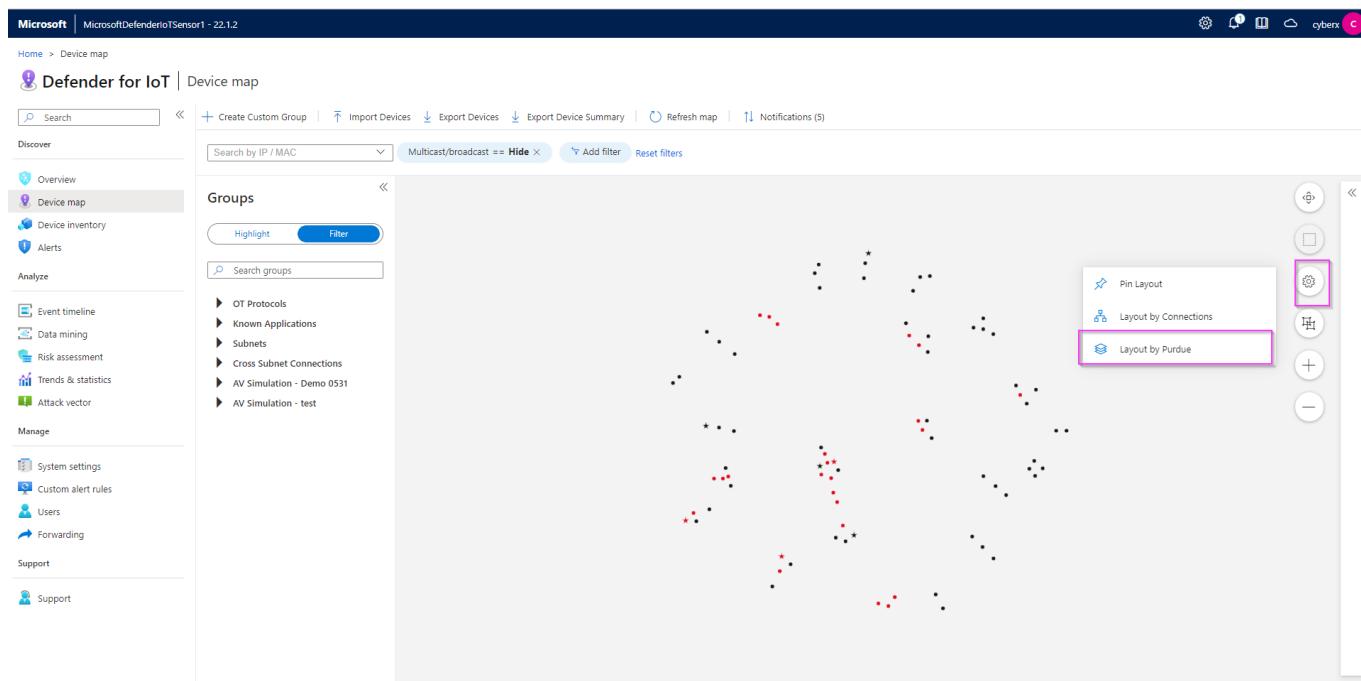
Exercise 4: Analyzing the Data

Task 1: Visualize on the Device Map

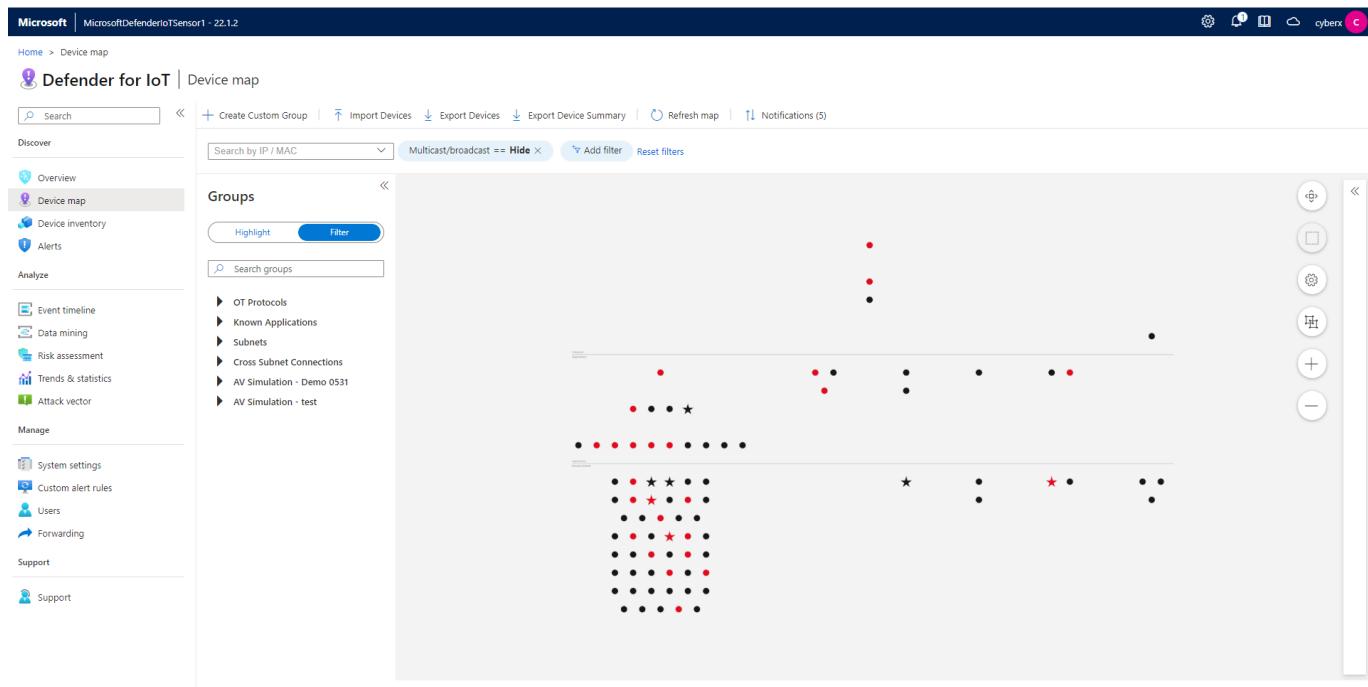
1. Click on “Device Map” from the menu on the left side.



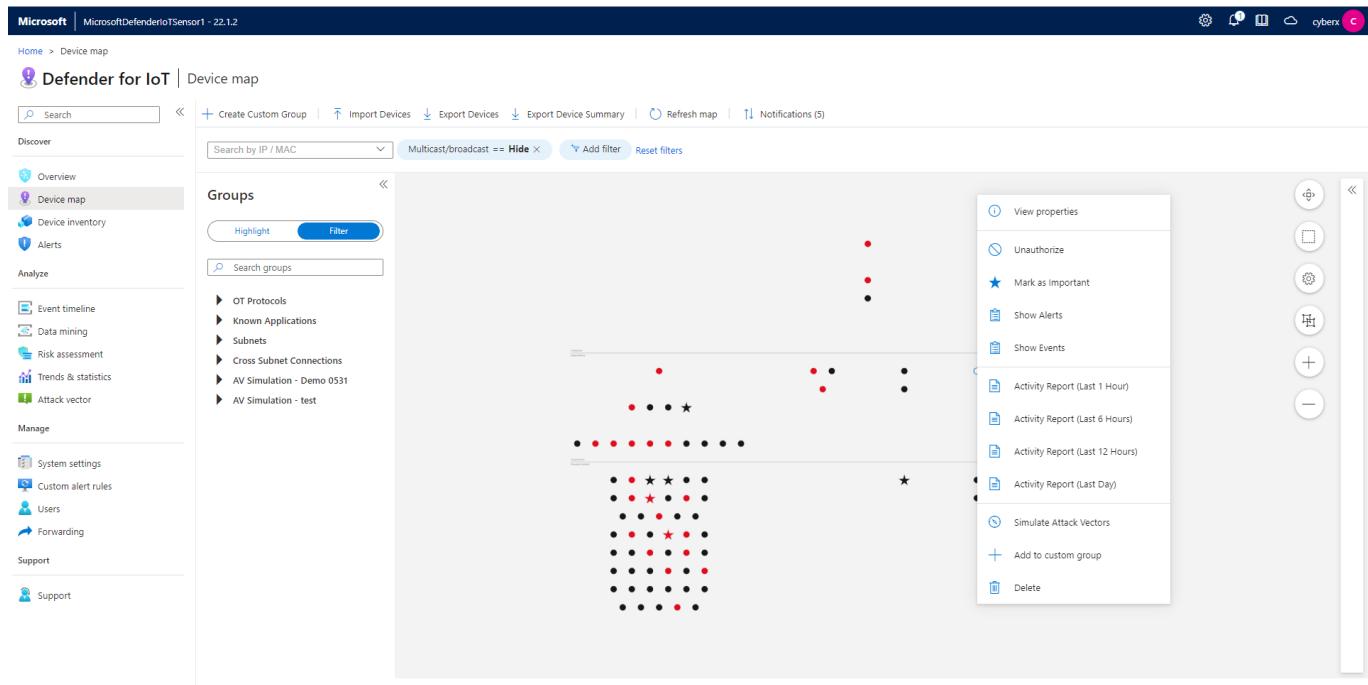
2. Click on the "Settings" option and select **Layout by Purdue** which will allow you to see the different layers between Corporate IT and site operations.



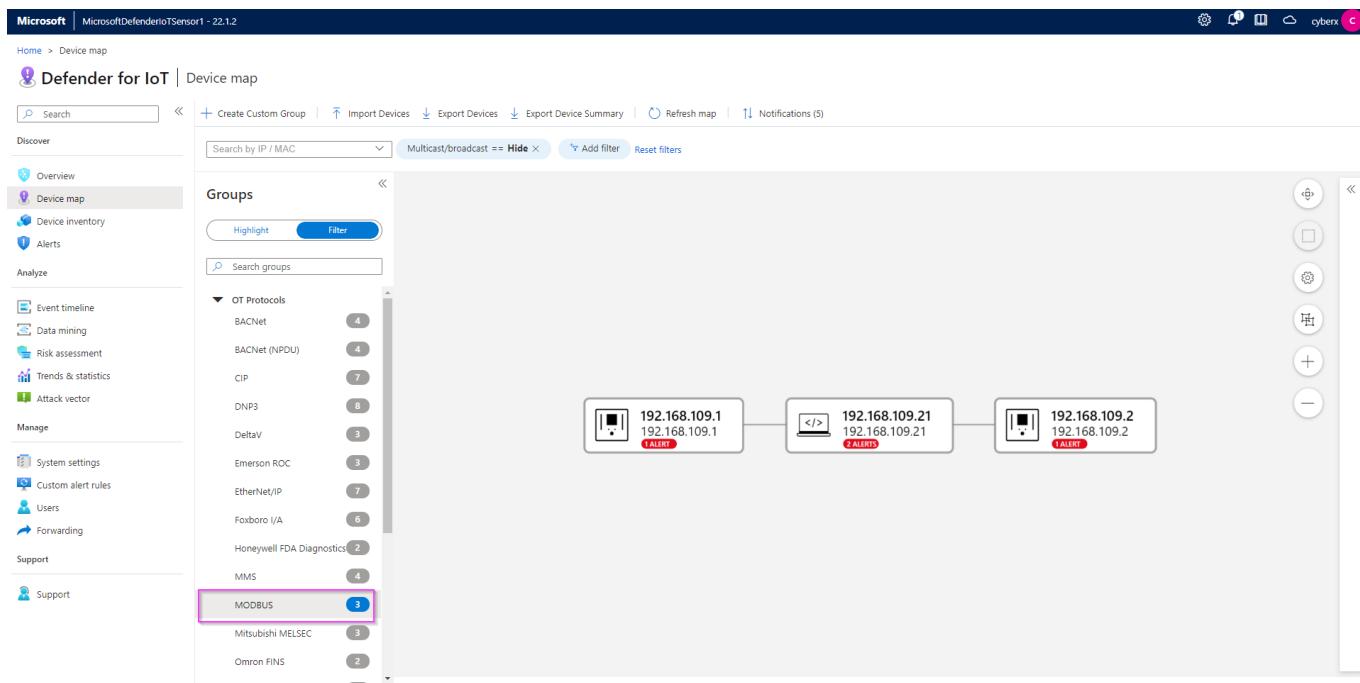
3. Once you confirm the changes, you will see the devices laid out as shown in the image below.



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

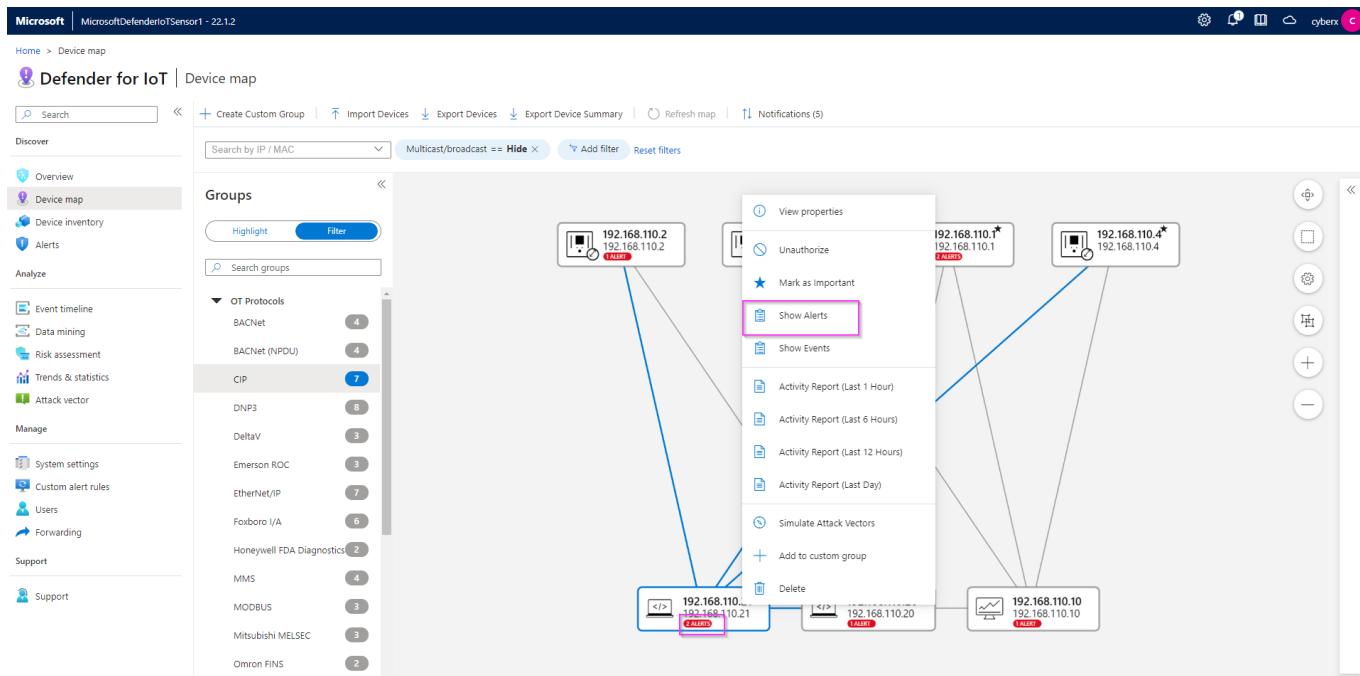


5. To filter by OT Protocols, expand the arrow, and pick the protocol you want to filter by. The console will display the devices that match the filter.



Task 2: View the associated Alerts

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



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

This screenshot shows the Microsoft Defender for IoT Device map interface. On the left, a sidebar displays device information for 'Device | 192.168.110.21', including its type (Engineering Station), vendor (INTEL CORPORATE), location (Automatic), and protocols (SSH, EtherNet/IP, TDS, FTP, CIP). The main pane shows a list of 22 alerts, with two specific ones highlighted:

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

A search bar at the top allows filtering by status and source/destination device.

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

This screenshot shows the Microsoft Defender for IoT Alerts page. The 'Alerts' option is selected in the sidebar. A single alert is selected, highlighted with a pink box, showing its details on the right side:

Unauthorized Internet Connectivity Detected
 Alert ID: 53
 See in Event timeline | See in Device map

Critical Severity | **New** Status | **2 weeks ago** Detection time

Description:
 A device defined in your internal network is communicating with addresses on the Internet. These addresses have not been learned as valid addresses.
 Device 192.168.110.21 communicated with addresses shown in External Addresses. Verify that this device is properly configured.

Related Devices:
 Source device: 192.168.110.21 Engineering Station → Destination device: Internet (37.142.39.186) Internet

At the bottom, there are 'View full details' and 'Take action' buttons.

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

Showing 22 of 22 alerts

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

Task 3: Device Inventory

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

Showing 100 of 291 items

IP Address	Name	Last Activity	Type	Protocols	MAC Address	Vendor	Firmware Version	Model	Operating System	Rack	Slot
192.168.100.8	192.168.100.8	50 minutes ago	Unknown	DNS, MDNS, Net...	54:14:f9:74:d8:21	INTEL CORPORA...					
192.168.100.1	192.168.100.1	50 minutes ago	Server	DNS							
192.168.1.11	192.168.1.11	50 minutes ago	PLC	Siemens S7	00:fb5:4dbef9	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
192.168.100.8	192.168.100.8	An hour ago	Unknown	DNS, MDNS, Net...	5:14:f3:74:d8:21	INTEL CORPORA...					
192.168.100.1	192.168.100.1	An hour ago	Server	DNS							
192.168.1.11	192.168.1.11	An hour ago	PLC	Siemens S7	0:0:fb:5:4:db:e1:3	NETGEAR					
192.168.1.180	192.168.1.180	An hour ago	HMI	Siemens S7							
192.168.117.23	192.168.117.23	22 hours ago	PLC	DNP3 (Identifier...)	0:30:a7:08:92:c6	SCHWEITZER EN...					
192.168.117.1	192.168.117.1	22 hours ago	Unknown	DNP3 (Identifier...)	0:23:e8:49:5:ec2	CISCO SYSTEMS ...					
192.168.117.22	192.168.117.22	22 hours ago	PLC	DNP3 (Identifier...)	0:30:a7:08:97:c0	SCHWEITZER EN...					
192.168.117.25	192.168.117.25	22 hours ago	PLC	DNP3 (Identifier...)	0:0:cc1:02:09:da	EATON CORPOR...					
192.168.117.7	192.168.117.7	22 hours ago	PLC	Siemens SICAM	0:0: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	0:0:c2:9:2:8:38	VMWWARE INC.					
192.168.117.8	192.168.117.8	22 hours ago	PLC	Siemens SICAM	0:0:e8:a0:01:90:bb	SAT GMBH & CO.	15.01	CPC65 (6065)			
192.168.107.10	FC50507	22 hours ago	DCS Controller	Yokogawa VNet/IP	0:0:0:64:9d:5:d10	YOKOGAWA DIG...					
192.168.107.1	192.168.107.1	22 hours ago	Unknown	Yokogawa VNet/IP	0:0:0:64:9d:7:3:d1	YOKOGAWA DIG...					
192.168.107.2	192.168.107.2	22 hours ago	Unknown	Yokogawa VNet/IP	0:0:0:64:9e:84:e5	YOKOGAWA DIG...					
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	0:0:1:e8:11:22:33	SIEMENS AG	3.2.6	6E57 315-6EH14...	0	4	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	0:0:1:e8:11:22:33	SIEMENS AG	3.2.6	6E57 315-9EH14...	1	2	
192.168.118.3	192.168.118.3	22 hours ago	PLC	Siemens S7	0:0:1:e8:11:22:33	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
Event timeline
Device inventory
Alerts
Analyze

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' section selected. A 'Create report' dialog box is open, overlaid on the main dashboard. The dialog box has several input fields and filters. The 'Choose Category' dropdown is set to 'Modules and Firmware Versions'. Other visible fields include 'Name' (with a placeholder 'Report name'), 'Description', 'Send to CM' (unchecked), 'Order by' (set to 'Category'), and various filtering options for IP address, MAC address, Port, and Device group. At the bottom of the dialog box are 'Save' and 'Cancel' buttons.

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

This screenshot shows the same 'Create new report' dialog box as the previous one, but with specific fields highlighted with pink boxes. The 'Name' field contains 'PLC Firmware Version', and the 'Description' field contains 'Report showing the firmware version of the different PLCs.'. The 'Choose Category' dropdown is set to 'Modules and Firmware Versions'. Under the 'Filter by' section, the 'Firmware Version (GENERIC)' option is selected. At the bottom right of the dialog box, the 'Save' button is highlighted with a pink box.

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

The screenshot shows the Microsoft Defender for IoT Data mining interface. On the left, there's a navigation sidebar with options like Overview, Device map, Device inventory, Alerts, Event timeline, Data mining (which is selected and highlighted in pink), Risk assessment, Trends & statistics, Attack vector, System settings, Custom alert rules, Users, Forwarding, and Support. The main area is titled 'Defender for IoT | Data mining' and has a 'Discover' section with 'Recommended' cards for Programming Commands, Internet Activity, Excluded CVEs, Active Devices (Last 24 Hours), Remote Access, CVEs, and Non Active Devices (Last 7 Days). Below this is a 'My reports' section with a table:

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 the 'PLC Firmware Version' report page. At the top, there are buttons for Refresh, Expand all, Collapse all, Export to CSV (highlighted in pink), Export to PDF, Snapshots, Manage report, and Edit mode. The report content itself is titled 'PLC Firmware Version' and describes 'Report showing the firmware version of the different PLCs.' Below the title, there's a table with data rows.

Task 6: Generate a Risk Assessment report

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

The screenshot shows the Microsoft Defender for IoT Risk assessment interface. The left sidebar includes options for Overview, Device map, Device inventory, Alerts, Event timeline, Data mining, Risk assessment (selected and highlighted in pink), Trends & statistics, Attack vector, System settings, Custom alert rules, Users, Forwarding, and Support. The main area features a 'Generate report' button highlighted in pink. Below it is a 'Reports list' table:

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

Exercise 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' (Pricing, Sensor name, Sensor type, Zone, Subscription ..., Sensor version, Sensor status, Last connect..., Threat Intelli..., Threat Intelli...). A message box says 'Trial subscription "BuildEnv" expired. Please contact Microsoft sales.' In the center, there are four categories: All sensors (4), IoT (1), OT cloud connected (2), and OT (1). Below these, it says 'Showing 4 of 4 sensors'. A table lists the sensor details: D4IOT-CxE-Site - D4IOT-CxE-Site, Locally managed. The 'Onboard OT sensor' button at the top right is 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' form. 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 table with a 'Key' column and a 'Value' column, with a pink box around the table), and 'Zone' (with a 'No subscription has been selected' dropdown and a 'Create zone' button). At the bottom is a 'Register' button 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 'Discover', 'Analyze', and 'Manage' sections. Under 'Manage', 'System settings' is selected and highlighted with a pink box. In the main area, under 'Sensor management', there are several cards: 'Software Update', 'Threat Intelligence', 'Subscription & Activation Mode' (which is highlighted with a pink box), 'Backup & Restore', 'System Health Check', and 'SNMP MIB Monitoring'. Each card has a brief description below it.

- 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 (set to 'Cloud Connected'), Activation Status (set to 'Active'), Tenant ID (a GUID), Subscription ID (another GUID), and a file upload input field labeled 'Upload activation file:' which is currently empty and highlighted with a pink box. The background shows the same interface as the first screenshot, with the 'System settings' section still highlighted.

Task 3: Verify Cloud connection

- 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	22.1.3.4162	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 shows it's connected, last log received was 6 days ago, and data received is shown in a line chart from June 19 to June 23. A button labeled 'Open connector page' is at the bottom.

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, Prerequisites, Configuration, and Select the relevant Subscriptions to connect. Under Configuration, there's a note about connecting to Microsoft Sentinel and a table where a row for 'Azure Pass - Sponsorship' has its 'Connect' button highlighted with a red box. The 'Disconnect' button and the status 'Disconnected' are also visible.

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 tabs for 'Instructions' (selected) and 'Next steps'. The main content starts with a 'Prerequisites' section, which lists requirements for workspace and subscription permissions. Below this is a 'Configuration' section with a 'Configuration' icon. It explains how to connect Microsoft Defender for IoT to Microsoft Sentinel by selecting 'Connect' next to each subscription whose IoT Hub's alerts you want to stream. A 'Search' input field is provided. A table lists a single subscription: 'Azure Pass - Sponsorship'. The 'Status' column for this subscription is highlighted with a red box and shows 'Connected' with a green checkmark icon. There are also 'Connect' and 'Disconnect' buttons for this row.

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

The screenshot shows the Microsoft Defender for IoT (Preview) dashboard. The 'Next steps' tab is highlighted with a red box. Below it, there's a section for 'Recommended workbooks' with a single item: 'Azure Defender for IoT Alerts' by Microsoft. Under 'Query samples (2)', there are two examples of log queries. In the 'Relevant analytics templates (1)' section, there is one template listed: 'Create incidents based on Azure Defender f...' with a 'Severity' of 'High'. A 'CREATE RULE' button is visible, also highlighted with a red box. A 'Run' button is present next to each query example.

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.

The screenshot shows the 'Analytics rule wizard - Create new rule from template' page. The 'Review and create' tab is selected. At the top, a green banner indicates 'Validation passed.' Below the tabs, there are sections for 'Analytics rule details' and 'Analytics rule logic'. In the 'Analytics rule details' section, the 'Name' is set to 'MyNewRule', 'Description' is 'Create incidents based on all alerts generated in Azure Defender for IOT', and 'Status' is 'Enabled'. In the 'Analytics rule logic' section, 'Microsoft security service' is 'Microsoft Defender for IoT', 'Filter by severity' is 'Any', 'Include by alert name(s)' is 'Any', and 'Exclude by alert name(s)' is 'Any'. Under 'Automated response', 'Incident trigger (preview)' is 'Not configured'. At the bottom, there are 'Previous' and 'Create' buttons, with the 'Create' button highlighted with a red box.

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' link is highlighted with a pink box. 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 also highlighted with a pink box. 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, with the first row being 'High (154)'.

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 - 22.1.2 interface. On the left, there's a navigation sidebar with sections like Discover, Analyze, Manage, and Support. The 'Alerts' section is selected. The main content area shows a table of alerts with columns for Severity, Name, Engine, Detection time, Status, and Source Device. There are 22 alerts listed. A pink box highlights the 'Learn' button in the top right corner of the alert list table. The table shows various types of alerts such as Policy Violation, Anomaly, and Operational.

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

The screenshot shows two windows side-by-side. On the left is the 'System settings' page for a sensor named 'MicrosoftDefenderIoTSensor1 - 22.1.2'. The 'Discover' section is expanded, showing 'Overview', 'Device map', 'Device inventory', and 'Alerts'. The 'Analyze' section includes 'Event timeline', 'Data mining', 'Risk assessment', 'Trends & statistics', and 'Attack vector'. The 'Manage' section has 'System settings' selected, along with 'Custom alert rules', 'Users', 'Forwarding', and 'Support'. On the right is the 'PCAP PLAYER' window, which allows uploading and replaying PCAP files. A file named 'pcap_wednesday.pcapng' is listed, and the 'Play All' button is highlighted with a red box.

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 left sidebar lists sections like General, Threat management (with 'Incidents' selected), Content management, Configuration, and Support. The main area displays incident statistics: 16 Open incidents, 16 New incidents, and 0 Active incidents. Below this is a chart showing open incidents by severity: High (4), Medium (10), Low (2), and Informational (0). A search bar at the top is set to 'Search resources, services, and docs (G+)'. The main table lists incidents with columns for Severity, Incident ID, Title, Alerts, Product names, Created time, Last update time, and Owner. A filter bar at the top of the table specifies 'Product name : Microsoft Defender for IoT' and 'Owner : All'. The 'Severity' column is sorted by High. The first few rows show incidents such as 'Unauthorized Internet Conne...', 'Outstation Restarted', 'BACNet Operation Failed', and 'Firmware Change Detected'.

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: N/A

Bookmarks: 0

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

Tactics (1): Initial Access

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

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

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

View full details >

Incident workbook

Incident Overview

Analytics rule: MyNewRule

Tags

View full details

Actions

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

Microsoft Azure

Home > Microsoft Sentinel >

Incident

Incident ID: 16

Refresh

Unauthorized Internet Connectivity Detected

Incident ID: 16

Investigate in Microsoft Defender for IoT

Owner: Unassigned

Status: New

Severity: High

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

Evidence

Events: N/A

Alerts: 1

Bookmarks: 0

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

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/IAlert...

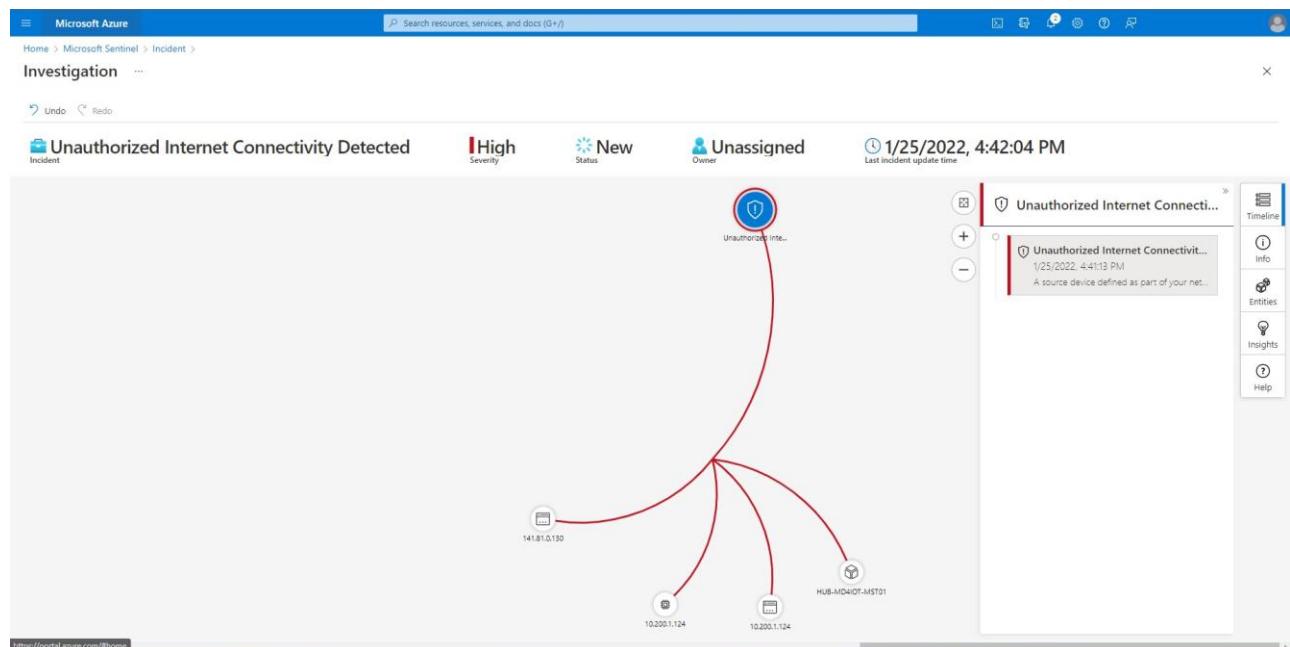
Remediation steps

Tags

Investigate

Actions

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



Task 4: Kusto Query Language to Find Alert Details

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

The screenshot shows the Microsoft Azure Microsoft Sentinel interface in the 'Logs' tab. The left sidebar includes 'Overview', 'Logs' (which is selected and highlighted with a red box), 'News & guides', 'Threat management', 'Incidents', 'Workbooks', 'Hunting', 'Notebooks', 'Entity behavior', 'Threat intelligence', 'Content management', 'Repository hub (Preview)', 'Repositories (Preview)', 'Community', 'Configuration', 'Data connectors', 'Analytics', 'Watchlist', 'Automation', and 'Settings'. The main area shows a query editor with the following Kusto query:

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

The 'Run' button is highlighted with a red box. The results table shows 51 records from the last 24 hours. The columns include TimeGenerated (UTC), DisplayName, AlertName, AlertSeverity, and Description. Some entries are collapsed, showing details like 'Unknown Object Sent to Outstation', 'Outstation Restarts Frequently', 'Firmware Change Detected', 'Port Scan Detected', 'Unauthorized Internet Connectivity Dete...', 'BACNet Operation Failed', 'Outstation Restarted', 'BACNet Operation Failed', 'Controller Stop', and 'BACNet Operation Failed'.

```
SecurityAlert | where CompromisedEntity == "hub-md4iot-mst01"
```

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 return...
10/1/2021, 4:00:07.358 PM	Controller Stop	Controller Stop	Low	The source devi...
10/1/2021, 4:00:07.445 PM	Port Scan Detected	Port Scan Detected	High	A source devi...

Exercise 6: Clean Up

Task 1: Delete resources

The Azure Passes will allow you to run the services for 90 days for training purposes. Although it is a 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.